CERTIFICADO DE ANÁLISIS

Compilatio informa de las tasas de similitudes recuperadas. No son tasas de plagio. La puntuación por sí sola no permite interpretar si las similitudes encontradas son plagiadas o no. Consulte el informe de análisis detallado para interpretar el resultado.

Similitudes del documento :

4%

Similitudes de las partes 1 :

6%

ANALIZADO EN LA CUENTA

Apellido :	De Ingeniería y Gestión
Nombre :	Facultad
E-mail :	fig@untels.edu.pe
Carpeta :	V PROGRAMA TSP ELECTRONICA

INFORMACIÓN SOBRE EL DOCUMENTO

Autor(es) :	No disponible
Título :	07 - tsp final_ayllon basurto.pdf
Descripción :	No disponible
Analizado el :	13/01/2022 22:31
ID Documento :	phi8t9jm
Nombre del archivo :	07 - TSP Final_AYLLON BASURTO.pdf
Tipo de archivo :	pdf
Número de palabras :	5 972
Número de carácteres :	43 662
Tamaño original del archivo (kB) :	1 005.01
Tipo de carga :	Entrega manual de los trabajos
Cargado el :	13/01/2022 21:59

FUENTES ENCONTRADAS

Fuentes muy probables :	10 fuentes
Fuentes poco probables :	44 fuentes
Fuentes accidentales :	28 fuentes
Fuentes descartadas :	0 fuente

SIMILITUDES ENCONTRADAS EN ESTE DOCUMENTO/ESTA PARTE

Similitudes idénticas :	4%
Similitudes supuestas :	2%
Similitudes accidentales :	<1%

TOP DE FUENTES PROBABLES - ENTRE LAS FUENTES PROBABLES

Fuentes	Similitud
1. Documento: jvizo3xn - Documento confidencial de otro usuario	2%
2. **kevin-linares.blogspot.com**/.../exploracion-de-la-...dad-de-la-red.html	<1%
3. **dspace.unl.edu.ec**/.../1/Quezada Lozano, Henry Daniel.pdf	<1%
4. Fuente Compilatio.net oxl6vanw	<1%
5. **alicia.concytec.gob.pe**/.../UNTL_eee6bc66be054...6fe01276fc67dff267	<1%

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“PROPUESTA DE IMPLEMENTACIÓN Y VALIDACIÓN DE CONEXIONES SEGURAS PARA USUARIOS REMOTOS DE LA RED CORPORATIVA MALL PLAZA MEDIANTE VPN SSL CON MULTIFACTOR DE AUTENTICACIÓN”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

AYLLON BASURTO, CARMEN FLOR
ORCID: 0000-0001-8186-8749

ASESOR

CASTRO PULCHA, BERNARDO ELÍAS
ORCID: 0000-0001-8578-5940

Villa El Salvador
2021

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

V Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional
Facultad de Ingeniería y Gestión

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Siendo las **16:15 horas** del día jueves **16 de diciembre del 2021**, y debido a la emergencia sanitaria y aislamiento social por el COVID-19, se reunieron vía google meet (https://meet.google.com/cye-qitg-knd), los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: DR. LA ROSA LONGOBARDI, Carlos Jacinto	CIP N° **055254**
Secretario	: MG. CAMPOS AGUADO, Fredy	CIP N° **173769**
Vocal	: MG. LOPEZ CORDOVA, Jorge Luis	CIP N° **183016**

Designados con RESOLUCIÓN DE FACULTAD DE INGENIERÍA Y GESTIÓN Nº 432-2021-UNTELS-CO-V.ACAD-FIG, de fecha 09 de Diciembre del 2021.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de Ingeniero Electrónico y Telecomunicaciones, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional. (Resolución de Comisión Organizadora Nº 126-2021-UNTELS de fecha 06 de agosto del 2021, en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del V Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur", siendo que el Art. 4º del precitado Reglamento establece que: **"**La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo de Suficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otras modalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar 02 años de experiencia laboral, de acuerdo a lo establecido en la Resolución Nº 174-2019-SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)**...",** en el cual;

El Bachiller: **AYLLÓN BASURTO, CARMEN FLOR**

Sustentó su Trabajo de Suficiencia Profesional: **"PROPUESTA DE IMPLEMENTACIÓN Y VALIDACIÓN DE CONEXIONES SEGURAS PARA USUARIOS REMOTOS DE LA RED CORPORATIVA MALL PLAZA MEDIANTE VPN SSL CON MULTIFACTOR DE AUTENTICACIÓN"**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición **Aprobado por Unanimidad**, Equivalencia **Bueno**, de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS, vigente.

Siendo las **17:00 horas** del día jueves 16 de diciembre del 2021, se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado Evaluador.

Dr. Carlos Jacinto La Rosa Longobardi
CIP N°055254
PRESIDENTE

Mg. Fredy Campos Aguado
CIP N°173769
SECRETARIO

Mg. Jorge Luis López Córdova
CIP N°183016
VOCAL

PARTICIPANTE
Bachiller: CARMEN FLOR AYLLON BASURTO

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público y conservando las medidas de distanciamiento social y de emergencia sanitaria. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del Presidente del Jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del Jurado, la sustentación será reprogramada durante los cinco (05) días siguientes.

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

V Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional
Facultad de Ingeniería y Gestión

ACTA FINAL DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Siendo las **16:15 horas** del día jueves **16 de diciembre del 2021**, y debido a la emergencia sanitaria y aislamiento social por el COVID-19, se reunieron vía google meet (https://meet.google.com/cye-qitg-knd), los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: DR. LA ROSA LONGOBARDI, Carlos Jacinto	CIP N° **055254**
Secretario	: MG. CAMPOS AGUADO, Fredy	CIP N° **173769**
Vocal	: MG. LOPEZ CORDOVA, Jorge Luis	CIP N° **183016**

Designados con RESOLUCIÓN DE FACULTAD DE INGENIERÍA Y GESTIÓN Nº 432-2021-UNTELS-CO-V.ACAD-FIG, de fecha 09 de Diciembre del 2021.

Concluida la Sustentación del Trabajo de Actualidad, se procede a registrar la nota obtenida en la Sustentación del Trabajo de Suficiencia Profesional.

BACHILLER EVALUADO (A): **AYLLON BASURTO, CARMEN FLOR**

Nota de sustentación del Trabajo de Suficiencia Profesional	Condición	Equivalente
14	Aprobado por Unanimidad	Bueno

Dr. Carlos Jacinto La Rosa Longobardi
CIP N°055254
PRESIDENTE

Mg. Fredy Campos Aguado
CIP N°173769
SECRETARIO

Mg. Jorge Luis López Córdova
CIP N°183016
VOCAL

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público y conservando las medidas de distanciamiento social y de emergencia sanitaria. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del Presidente del Jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del Jurado, la sustentación será reprogramada durante los cinco (05) días siguientes.

DEDICATORIA

A mi madre, padre y hermana por el amor incondicional que me tienen, me brindaron cada palabra de aliento en los momentos que más los necesité, gracias a ellos logré culminar mi profesión.

AGRADECIMIENTO

Agradezco a Dios por haberme dado una madre que supo guiarme por el camino correcto. A mi asesor, Bernardo Pulcha, por su profesionalismo como guía de apoyo, ya que me brinda sus recomendaciones y observaciones, siendo claves en todo el proceso.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

La empresa Connect cuenta con más de 12 años brindando servicios a nivel de proyectos e implementación de soluciones de seguridad de redes, además, brinda soporte y gestión de Seguridad Perimetral, actualmente es socio estratégico del proveedor de servicios Claro.

Uno de los clientes al que se brinda soporte es la cadena de supermercados Mall Plaza, esta contaba con conexiones remotas por escritorio remoto solo para algunos usuarios, los cuales carecían de alguna tecnología que brinde la seguridad, confidencialidad y la autenticación al acceso para proteger la data almacenada en su red. Fuente: Fuente propia.

Frente a la pandemia, mediante el Decreto de Urgencia N.º 026-2020, el Estado Peruano estableció el trabajo remoto para las entidades públicas y privadas como medida laboral. Bajo este escenario la empresa Mall Plaza tuvo que implementar el trabajo remoto de gran parte de sus empleados, para lo cual requería inversión económica para obtener un pool de IPs públicas que abastezca a todas las publicaciones, así como para personal calificado que realice las constantes configuraciones necesarias.

Por la problemática expuesta, Mall Plaza utilizó lo servicios de nuestra empresa, Connect, para implementar una tecnología que permita a sus usuarios remotos acceder a su red de forma segura, confidencial, sin costos, escalable y que además brinde seguridad en la autenticación.

La tecnología implementada en Mall Plaza fue la red privada virtual de capa de conexión segura (VPN SSL) con Multi-factor de autenticación (MFA), las cuales se configuraron en el equipo firewall, de la marca Fortinet, bajo nuestra gestión. Nuestra metodología se divide en cuatro partes:

La primera parte es a partir de la recepción de la solicitud de implementación de la VPN SSL por parte del soporte de Connect.

Como segunda parte se analiza la topología para asignar el segmento de red que se brindará a los usuarios remotos, los destinos y datos de los usuarios.

La tercera parte consiste en la configuración del Firewall y del software Forticlient en los hosts finales.

Como última parte se realiza las validaciones de las conexiones remotas.

Como resultado de nuestra implementación de conexión VPN SSL, se garantiza la seguridad de la conexión de los usuarios remotos a los recursos locales de la empresa a través de una conexión cifrada sobre internet, evitando con esto alguna intromisión maliciosa, motivo de mi trabajo profesión.

INTRODUCCIÓN

Antes de que el mundo y el país experimentara la actual coyuntura de pandemia, en las empresas, universidades y entidades, era mínima la utilización de la conexión remota; sin embargo, bajo la obligación de confinamiento con el fin de evitar el contagio y asegurar la salud de cada habitante, varios rubros empresariales u organizaciones se vieron forzados a realizar sus procesos y tareas de forma remota.

Bajo este nuevo escenario se tuvieron que implementar servicios y recursos con el fin de brindar las herramientas necesarias a cada personal o estudiante.

Fue propósito de mi trabajo profesional la implementación de conexiones para usuarios remotos de la red corporativa Mall Plaza mediante VPN SSL con multi-factor de autenticación, la cual brinda acceso a recursos perimetrales específicos de la cadena MALL PLAZA a 47 trabajadores de esta empresa que requieren esta conexión para fines laborales de distintas áreas como RR.HH., soporte, gerencia, contabilidad, etc. con medidas óptimas, eficiente, escalable y segura, ya que el avance de la tecnología permite mejorar la seguridad a través de túneles de datos, especificaciones al acceso de las redes internas mediante políticas y sistemas de autentificación MFA de los usuarios a través de una VPN SSL mediante el equipo Fortinet, que protege la confidencialidad e integridad de la información.

Cada usuario puede conectarse desde internet a la LAN de Mall Plaza mediante el software FortiClient, previamente configurado, para la conexión segura a los datos sensibles que brinda la organización, a la vez se evita intromisiones no deseadas a la empresa

CAPÍTULO I

ASPECTOS GENERALES

La cadena Mall Plaza contaba con conexiones remotas para pocos usuarios, dichas conexiones se realizaban por medio de publicaciones de sus servicios internos (base de datos, Directorio Activo, etc.) a través de internet, que carecían de alguna tecnología que brinde la seguridad adecuada, así como también un método de autenticación que evite la suplantación de identidad. Considerando que, como entidad privada, Mall Plaza es responsable de los datos sensibles de sus clientes, empleados y de la propia empresa, su deber es garantizar la seguridad, confidencialidad y la autenticación al acceso, para proteger la data almacenada en su red, ya que sería un gran riesgo sufrir el robo de dichos datos por vulneración de las conexiones establecidas. Se tuvo que incorporar el trabajo remoto para todos los empleados de la empresa por el Covid-19; de lo expuesto la solución es la red privada virtual de capa de conexión segura (VPN SSL) ya que brinda seguridad y óptima conexión para los usuarios de la red corporativa.

1.1. Contexto

La empresa Connect, actúa como marca comercial del GRUPO DALISA SAC con inicio de operación en 2007. Es una empresa dedicada a brindar distribución, integración y servicios profesionales de soluciones de seguridad, comunicaciones unificadas, redes y optimización.

Cuenta con amplia experiencia, aportando valor en implementación y puesta en operación en las soluciones que ofrece, teniendo como principal objetivo que la tecnología sea un medio para que los clientes logren cumplir los objetivos propios del negocio, para lo cual cuenta con un catálogo de soluciones y servicios de ingeniería que comprende:

- Seguridad administrada
- Seguridad Administrada virtual
- Gestión de aplicaciones
- Optimización Virtual

- Protección contra ataques DDoS
- Hosted IP PBX
- PBX gestionada
- LAN gestionada
- Wifi gestionado
- Balanceo de enlaces

Para cumplir con el ciclo del servicio posventa cuenta con un área de soporte, donde laboro, que realiza las configuraciones e implementaciones a demanda del cliente, mediante soporte remoto y local en caso de interrupción de servicio a su infraestructura de red en un horario 24x7x365 con la finalidad de asegurar la disponibilidad de su servicio.

La implementación presentada en este documento la elaboré en el área de Soporte Connect a uno de los clientes más importantes, como lo es Mall Plaza.

1.2. Delimitación del Proyecto

1.2.1. Temporal

Este proyecto tuvo una duración aproximada de 2 meses, a partir del 7 de agosto del 2020 al 28 de setiembre del 2020, actualmente operativo y a satisfacción del cliente.

1.2.2. Espacial

La implementación en el Firewall de la cadena Mall Plaza se realizó de forma remota, por su parte el despliegue del software para la conexión VPN (Forticlient) lo ejecutaron los usuarios finales mediante un manual de configuración para el Forticlient, desarrollado previamente. Este equipo Firewall se encuentra físicamente en el distrito de Villa el Salvador.

1.3. Objetivos

1.3.1. Objetivo General

Realizar la implementación de una conexión segura para los usuarios remotos de la cadena Mall Plaza para accesos a los servicios internos de su gestión empresarial.

1.3.2. Objetivo Específicos

- Definición del segmento de red que se configurará en la VPN, ya que el usuario remoto tomará una IP perteneciente a este segmento de red para su conexión VPN.
- Configuración de la VPN SSL y la autenticación de los usuarios al momento de la conexión.
- Validación de la conexión del usuario remoto donde se valide la calidad del servicio VPN.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes Nacionales

Se revisó diferentes trabajos de suficiencia profesional de la UNTELS respecto al tema de la Red Privada Virtual (VPN), las cuales se mencionan a continuación:

Abraham Casanova, (2020) *Diseño de una red privada virtual orientada al teletrabajo de organizaciones con escasos recursos económicos por la coyuntura del covid-19*, UNTELS. Presenta un diseño de una VPN con el protocolo Túneles Punto a Punto (PPTP), en equipos de la marca Mikrotik con la opción de usar un dominio de un servidor nube en lugar de una IP publica estática, esto permite interconectar a los colaboradores externos en localidades remotas optimizando el rendimiento de la infraestructura de redes, tanto física y lógica. Además, redujo costos de inversión, para asegurar la continuidad laboral mediante el teletrabajo en las organizaciones de bajos recursos. Este trabajo me permitió precisar la función de la VPN punto a punto haciendo uso de diferentes parámetros de seguridad y haciendo uso de un dominio en lugar de IP.

Omar Zapata, (2017), *Diseño de una red convergente utilizando VPN IPsec entre la central de una farmacia localizada en lima metropolitana y su sucursal ubicada en Jauja-Junín*, UNTELS. Presenta un diseño de la VPN de Seguridad del protocolo de Internet (Ipsec) mediante equipos routers Cisco 386 donde garantiza funciones de encriptación de alto rendimiento como el cifrado 3DES (Triple Data Encryption Standard) a su vez cuenta con una calidad de servicio (QoS) avanzada lo cual puede poner en cola y priorizar el tráfico de voz sobre el tráfico de datos para asegurar una conexión de voz sobre IP (VoIP) esto asegura una alta calidad desde la red. Este diseño tiene las mismas características que una red MPLS con VoIP; sin embargo, este sistema es mucho más económico. Este trabajo me reforzó la importancia de

la VPN para las comunicaciones remotas punto a punto con conexiones mediante IPs públicas y realiza el uso del cifrado 3DES el cual es usado por el protocolo SSL en mi presente trabajo de suficiencia profesional.

De La Cruz Bernilla Segundo Magdaleno, Vera Cruz Jean Ronald Steven (2019), *Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo*, Universidad Nacional Pedro Ruiz Gallo. En este trabajo se realiza una implementación de una VPN en la Universidad Nacional Pedro Ruiz Gallo con el objetivo de brindar una solución económica y que brinde una comunicación segura que facilite la obtención de recursos de la universidad. Respecto al presente trabajo el beneficio que se obtiene al contar con una VPN en la red es tener un eficiente acceso a los recursos que se desea acceder, brindando seguridad y confidencialidad al acceso de los datos, además de ser una solución económicamente accesible. Por otro lado, demuestra por el test realizada a la VPN ya implementada que se logra una encriptación e integridad de los datos deseados. Para mi trabajo me ayuda a tener la garantía de las características deseadas respecto a la seguridad de la VPN.

Se concluye respecto a la tesis y trabajos revisados que la implementación de una VPN varía según el tamaño de la red corporativa y a las funciones que se desee para la conexión, las cuales usan encriptación y protocolos de seguridad, estos pueden estar basados en software o hardware, siendo esta última la más efectiva ya que soporta las configuraciones de los parámetros de seguridad, en mi trabajo se realiza la configuración tanto en el hardware y software cumpliendo la encriptación y protocolos de seguridad

2.1.2. Antecedentes Internacionales

A nivel internacional se revisó la siguiente tesis respecto al tema de la Red Privada Virtual (VPN) las cuales son las siguientes:

Henry Quezada, (2016), *Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja*, en la Universidad Nacional de Loja de Ecuador. En este trabajo se realiza el uso de la

herramienta VPN Open Source para el diseño de redes privadas virtuales, esto es una solución abierta basada en software libre que provee un acceso seguro usando los estándares SSL/TLS que cifra las comunicaciones. Configuró y validó en un VirtualBox 30 máquinas virtuales con el sistema operativo Linux Mint las conexiones al Servidor de Acceso que tiene configurado el OpenVPN en cual se evidencia una óptima conexión y segura. Este trabajo me ayuda a entender las conexiones múltiples por usuario mediante un software libre con el cifrado del protocolo TLS lo cual es como guía para mi presente trabajo ya que mi trabajo usa el protocolo SSL/TLS y las conexiones múltiples.

Mukatshung Claude Nawej, (2016), *Evaluation of Virtual Private Network Impact on Network Performance*, en la University of South África. En esta tesis se desarrolla un análisis del impacto que tiene una red al implementarse una VPN, para ello se compara las métricas de los parámetros de rendimiento y retraso a través de una simulación de una red sin VPN y otra con la VPN implementada, las aplicaciones usadas para las mediciones son HTTP, FTP, CBR y el simulador utilizado fue el NS2. Los resultados del análisis del trabajo fueron que la VPN no tiene un mayor impacto en el tráfico UDP, pero si un impacto en TCP, por lo cual para la aplicación CBR no hubo mayores cambios con una red utilizando VPN. En los casos de HTTP y FTP si hubo impacto que dependieron del tamaño del paquete. En base a ello la conclusión del trabajo es que, si bien hay un impacto en el rendimiento y retraso para las aplicaciones HTTP y FTP analizadas, estas puedes ser reducidas eligiendo un adecuado hardware, tamaño de paquete y algoritmo de encriptación para la VPN.

Se concluye respecto a este trabajo que el impacto en tráfico TCP es mayor a la UDP debido a que la TCP es un protocolo orientado a la conexión, además que el impacto que pueda tener la red con VPN implementado se debe al procesamiento que los paquetes sufren por la encriptación y desencriptación que se realiza. Sin embargo, también se concluye que el impacto es reducido eligiendo adecuadamente un hardware que brinde las garantías para la implementación de la VPN, así como la configuración que

mejor adecue los parámetros de tamaño de paquete y algoritmo de encriptación.

2.2. Bases Teóricas

2.2.1. Seguridad Perimetral

Según la revista Fortinet. (2021). Perimeter Firewall. La red perimetral hace referencia a la infraestructura que esta entre la red de la organización y la Internet, se crea en ella filtros seguros para los datos que transitan entre ellas. Una seguridad perimetral debe contar con recursos capaces de monitorear y filtrar tráfico malicioso, así como el de gestionar el tráfico en general.

2.2.1.1. Tipos de Seguridad Perimetral

- Zonas desmilitarizadas (DMZ): Una Demilitarized Zone (DMZ) es una red perimetral que brinda protección a una red interna o local de una red no confiable. Es una subred que esta entre la red pública y la red privada como se puede ver en la Figura 1. Pone al alcance los servicios de una red a redes potencialmente maliciosas, por lo cual añade una capa de seguridad a través de filtros que protejan los datos de la red interna, generalmente se hace uso de firewalls para aplicar dichos filtros.

  Las organizaciones almacenan en la DMZ servidores para el sistema de nombres de dominio o Domain Name System (DNS), el File Transfer Protocol (FTP), el correo, el proxy, el protocolo de Voice over IP (VoIP) y los servidores web. Estos servicios están al alcance desde el exterior, pero limitan el acceso desde la LAN con el fin de que sea más difícil para un pirata informático obtener acceso directo a los datos internos a través de Internet.

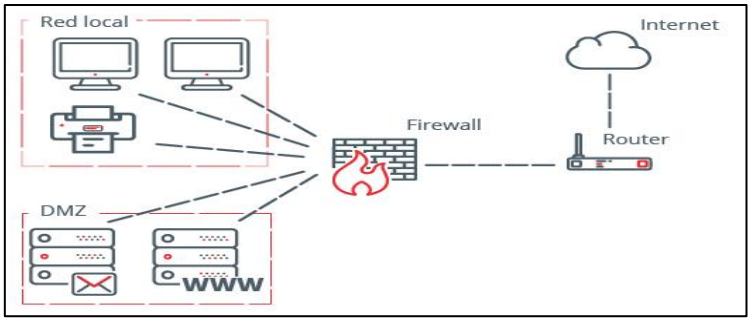


Figura 1. Red local con DMZ

Fuente: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

- Sistemas de prevención y detección de intrusiones: Un sistema de prevención de intrusiones o Intrusion Prevention System (IPS) identifica tráfico malicioso y bloquea automáticamente el acceso a la red interna de dicho tráfico. Un sistema de detección de intrusiones o Intrusion Detection System (IDS) monitorea el tráfico y busca amenazas conocidas y actividades sospechosas. El IDS alerta a los equipos de seguridad cuando detecta algún riesgo o amenaza. La integración de IDS e IPS en un solo producto permite el monitoreo, detección y prevención de amenazas de manera más fluida.

- Sistemas de cortafuegos: También llamado firewall, es una aplicación de seguridad que protege el límite entre una red privada y una red pública. Evita que ingresen a la red datos no deseados o sospechosos. Protege contra ataques cibernéticos y otros tráficos maliciosos al escanear cada paquete de datos que intenta ingresar a la red. Un firewall perimetral examina cada paquete de datos, así determina si contiene una amenaza basándose en la información del encabezado y la carga útil del paquete; también puede filtrar el tráfico tanto interno como externo. El tráfico interno es el tráfico que se origina en su red y viaja entre usuarios, redes internas y dispositivos. El tráfico externo es el tráfico que proviene de Internet desde fuera de la red, por lo que se tiene mayores riesgos ya que hay millones de amenazas en Internet. En la figura 2 se puede apreciar las 4 primeras marcas lideres como Palo Alto, Fortinet, Cisco y Check Point a nivel de Firewall.

Figura 2. Magic quadrant for network firewalls 2020

Fuente: https://www.hillstonenet.com/gartner-network-firewalls-2020/

2.2.2. Tipos Comunes de Redes

2.2.2.1. LAN Y WAN

Según Cisco. (2021). Introduction to Networks. Estas redes son las más comunes de infraestructuras de red:

- Área local (LAN): Es una infraestructura que proporciona acceso a usuarios y dispositivos finales en un área geográfica pequeña.
- Área amplia (WAN): Son redes que se extienden en área geográficas amplias, generalmente administrada por una corporación más grande o un proveedor de servicios de internet (ISP).

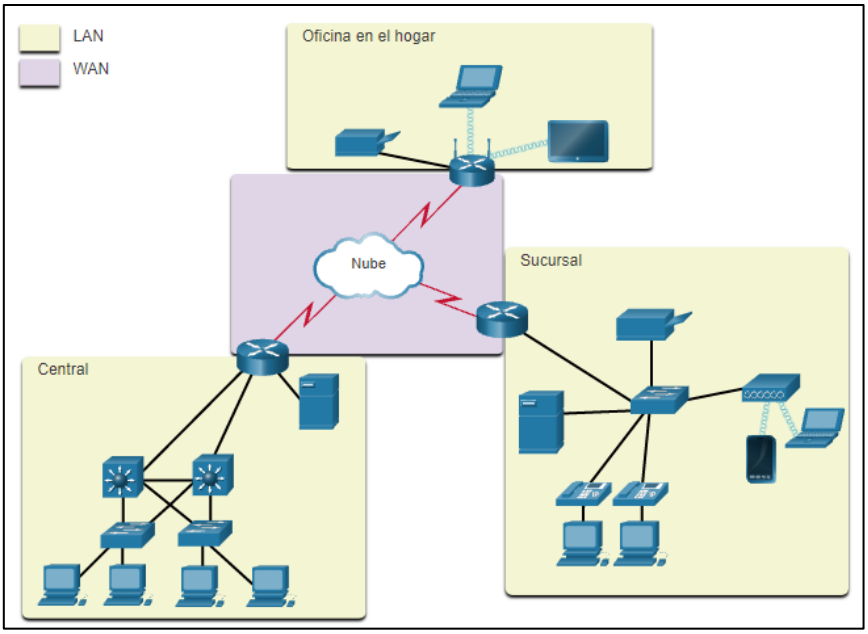


Figura 3. LAN conectadas a una WAN.

Fuente: https://contenthub.netacad.com/itn/1.4.2

2.2.2.2. Internet

Según Cisco. (2021). Introduction to Networks.Internet. Es una colección global de redes interconectadas de LAN Y WAN, este no pertenece a una persona o un grupo, a su vez garantiza una comunicación efectiva.

2.2.3. Seguridad de la Red

2.2.3.1. Amenazas de Seguridad.

Según la revista Fortinet. (2021). Network Security. La seguridad de la red es fundamental ya que en los últimos años se ha vuelto propenso a ataques con robos de información, está compuesta por una variedad de aplicaciones, configuraciones y herramientas implementadas para proteger la integridad de su red del uso no autorizado.

Las tecnologías de seguridad de red están diseñadas para mitigar amenazas individuales y prevenir interrupciones a la infraestructura de la red. Estas son las amenazas más comunes:

- Malware: Engloba una variedad de software malicioso que pueden afectar los sistemas informáticos, como troyanos, spyware, gusanos, adware y otros. Cada tipo de malware toma diferentes acciones que pueden afectar la red, desde el acceso a información personal confidencial hasta el robo de detalles financieros.
- Virus troyano - Está diseñado para parecer un programa útil, pero cuando se usa, abre una puerta para que un pirata informático acceda al sistema de una computadora.
- Gusanos: Los gusanos informáticos son un tipo de malware que puede operar por sí solo, sin un programa host, para ralentizar los procesos de su red. Estos gusanos consumen la potencia de procesamiento de su computadora y el ancho de banda de la red para hacer que la eficiencia de su red disminuya.
- Spyware y adware - El software espía o spyware actúa como un espía dentro de los datos de su red informática. Recopila información sobre un usuario, persona u organización específicos y potencialmente comparte esa información con un tercero sin el consentimiento del usuario. El adware trabaja para obtener información sobre usted como consumidor y redirigirá las solicitudes de búsqueda a sitios web publicitarios. Recopilará datos con fines de marketing y luego personalizará los anuncios en función de la información recopilada de su historial de compras y búsquedas.
- Botnets: Un botnet es un malware que consiste en potencialmente millones de bots que infectan varias computadoras, que luego se pueden controlar de forma remota. Esta red de robots se utiliza para realizar ataques a gran escala en numerosos dispositivos, realizando simultáneamente actualizaciones y cambios sin el consentimiento o conocimiento previo de los usuarios.
- Ataques de día cero – Estos se producen desde el primer día que se conoce una vulnerabilidad.
- Amenazas de Atacantes – Es cuando alguien realiza un ataque a un dispositivo de usuario o recursos de red.

- Ataques por denegación de servicio distribuido - Un ataque de denegación de servicio distribuido (DDoS) es un intento dirigido de interrumpir el flujo de tráfico normal a un servidor, red o servicio abrumando con tráfico inesperado en forma de solicitudes ilegítimas. A medida que el servidor intenta responder al aluvión de solicitudes, sus recursos se utilizan hasta que ya no puede manejar tráfico legítimo. Este ataque evita el tráfico normal a una red mediante el uso de sistemas informáticos comprometidos para impedir que el tráfico llegue a su destino.
- Intercepción y robo de datos - Esta captura información privada de la red de una empresa u organización.
- Robo de identidad - Este roba las credenciales desde que el usuario acceda con sus credenciales a datos privados.
- Amenazas internas - Esto se da en dispositivos perdidos o robados por parte del empleado, también la conexión de un USB con virus.

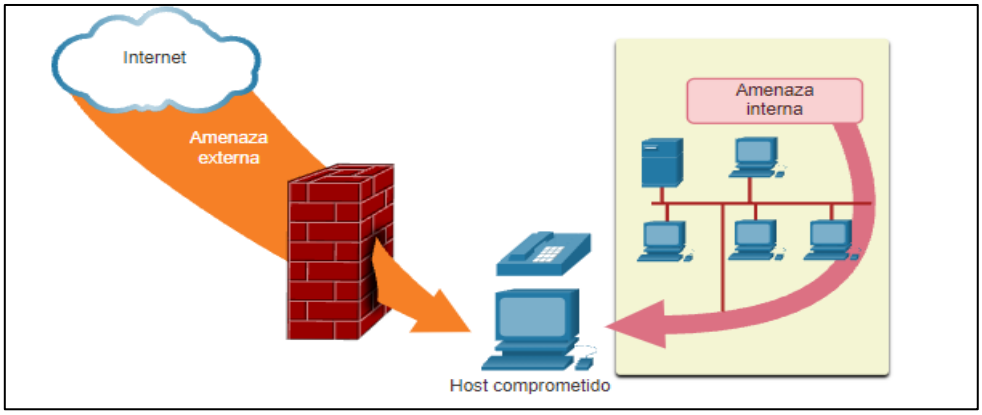


Figura 4. Amenazas internas y externas.
Fuente: https://contenthub.netacad.com/itn/1.8.1

2.2.3.2. Soluciones de Seguridad.

Según la Portal de Hacknoid. (2020). Soluciones de seguridad Informática. Estos son los componentes básicos de seguridad:

- Antivirus y antispyware: Estos protegen dispositivos finales para que no sean infectados con software malicioso.

- Filtrado de Firewall: Este bloquea el acceso no autorizado de la red dentro y fuera. También cuenta con perfiles y políticas de seguridad para impedir el acceso no autorizado, de las cuales se mencionará, Según Idgrup. (2020). Funciones de un Firewall.

- Políticas de Seguridad:

Es el conjunto de reglas y procedimientos que regulan la red interna, usa, protege y distribuye toda la información que directa o indirectamente le pertenece. Las políticas constan de estos datos: origen, destino, puerto, perfiles de seguridad, interfaz y Nat.

- Perfiles de Seguridad:

En esta parte se realizan perfiles de seguridad en el cual se aplica a las políticas tanto para la navegación como la comunicación interna, las cuales son las siguientes: antivirus, filtro web, filtro de DNS, control de aplicaciones y Intrusion Prevention.

Por otra parte, según Cisco. (2021). Introduction to Networks.Internet. La implementación de seguridad de la red en redes de las empresas normalmente consiste en la integración de numerosos componentes a la red para controlar y filtrar el tráfico. Las redes más grandes y las redes corporativas utilizan filtros antivirus, antispyware y firewall, pero también tienen otros requisitos de seguridad:

- Sistemas de firewall dedicados - Estos proporcionan capacidades de firewall más avanzadas que pueden filtrar grandes cantidades de tráfico con más granularidad.
- Listas de control de acceso – La Access Control List (ACL) filtran el acceso y el reenvío de tráfico mediante direcciones IP y aplicaciones.
- Sistemas de prevención de intrusiones (IPS) -Ataques de día cero son identificados gracias a este sistema.

- Redes Privadas Virtuales (VPN) – Proporcionan a una organización el acceso seguro para trabajadores remotos.

2.2.4. Red Privada Virtual (VPN)

Según Fortinet Document Library. (2020). VPN. La tecnología de Virtual Private Network (VPN) permite a los usuarios remotos conectarse a redes informáticas privadas para obtener acceso a sus recursos de forma segura. Esto es útil para los empleados que requieren acceder de forma segura a la red de su oficina a través de internet desde su hogar o mientras está viajando. A diferencia de usar una conexión sobre internet que es insegura, una VPN asegura que no haya intromisiones de usuarios que no estén autorizados. La VPN también es útil cuando se requiere conectar redes privadas de distintas oficinas. Los beneficios de una VPN son:

- Bajo costo de implementación.
- Privacidad de los datos.
- Acceso desde todas partes.
- Flexibilidad.
- Escalabilidad.

2.2.5. Tipos de VPN

2.2.5.1. VPN Site to Site

Según la página Fortinet Document Library. (2020). VPN. Una VPN de sitio a sitio se refiere a una conexión establecida entre varias redes. Esta podría ser una red corporativa donde se requiere que varias oficinas trabajen en conjunto. Las VPN de sitio a sitio son útiles cuando las empresas desean priorizar el tráfico privado y protegido, así como también las organizaciones cuentan con más de una oficina distribuida en grandes ubicaciones geográficas. Estas empresas generalmente desean acceder a recursos alojados en una red principal.

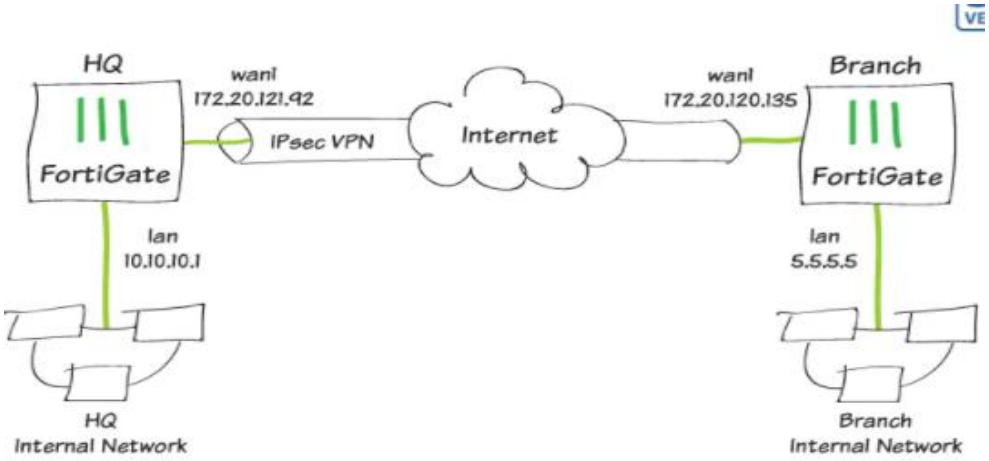


Figura 5. Topología de una VPN site to site

Fuente:

https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/962850/site-to-site-ipsec-vpn-with-two-fortigates

2.2.5.2. VPN de acceso remoto

Según la página Palo Alto networks. (2020) una VPN de acceso remoto se refiere a una conexión temporal establecida entre dos o más usuarios y una ubicación central. Una VPN de acceso remoto es una herramienta útil para empresas con trabajadores remotos, ya sea que están viajando o en sus hogares. Este tipo de VPN se puede utilizar para proporcionar a los trabajadores en diferentes ubicaciones una experiencia similar a la de aquellos en la oficina principal que pueden conectarse al servidor en sus escritorios mediante un cable Ethernet.

2.2.6. Protocolos de VPNs

Con una VPN, los datos atraviesan Internet a través de un protocolo de túnel seguro, donde están encriptados para evitar que terceros lean sus datos mientras viajan. Según la página Palo Alto networks. (2020). VPN. Los dos conjuntos de protocolos de red más populares para el cifrado son:

2.2.6.1. VPN de protocolo de Internet Seguro (VPN IPsec)

VPN Internet Protocol security (VPN IPsec) utiliza una combinación de hardware y software para imitar una conexión similar a la de tener una computadora conectada a la red de área local (LAN) de una organización, lo que permite el acceso a cualquier cosa que pueda tener una computadora interna. Esto se debe a que IPsec funciona en la capa de red y debe ser administrado físicamente por ingenieros de red en lugar de mediante software. La mayoría de las soluciones VPN IPsec requieren la instalación de hardware y software especiales para que el usuario obtenga acceso a la red. El principal beneficio de esta configuración son las capas adicionales de seguridad. Cuando la red está protegida no solo por software sino también por hardware, es más difícil para los ciberdelincuentes infiltrarse en la red y robar datos críticos.

2.2.6.2. VPN de capa de sockets seguros (VPN SSL)

Permite a los usuarios individuales acceder a la red de una organización, las aplicaciones cliente-servidor y las utilidades y directorios de la red interna sin la necesidad de software especializado. Las VPN SSL brindan una comunicación segura a través de una conexión encriptada para todo tipo de dispositivos. Todo el tráfico entre un navegador web y un dispositivo VPN SSL se cifra con el protocolo SSL o de seguridad de la capa de transporte (TLS). Los usuarios individuales de VPN SSL no tienen que decidir qué protocolo usar para que la VPN haga su trabajo. La VPN SSL utiliza automáticamente el protocolo criptográfico más nuevo y actualizado que se ha instalado en el navegador del usuario.

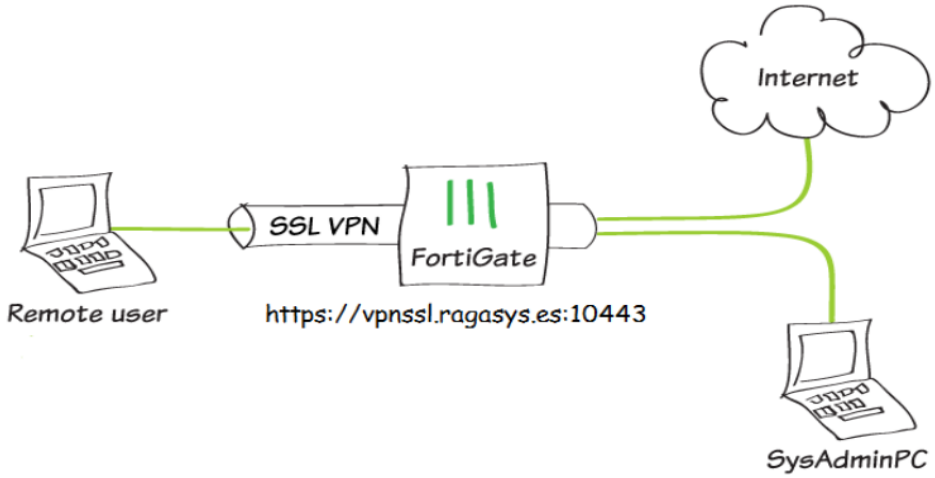


Figura 6. Topología de acceso de usuario remotos a través de la VPN SSL.
Fuente: https://blog.ragasys.es/configuracion-fortigate-vpn-ssl-acceso-remoto

Existen dos tipos principales de VPN SSL:

- VPN SSL PORTAL

  En la VPN SSL modo portal, el usuario final puede acceder a múltiples servicios de red de forma segura a través de una única conexión SSL a un sitio web. El sitio se llama portal porque solo tiene una puerta para múltiples recursos. El usuario remoto puede acceder a la puerta de enlace VPN utilizando cualquier navegador web moderno para la autenticación definida por la puerta de enlace.

- VPN SSL TUNEL

  Una VPN SSL de túnel permite que un navegador web acceda de forma segura a varios servicios de red, que no solo están basados en la web, a través de un túnel que está bajo SSL. Estos servicios pueden ser redes propietarias o software creado para uso corporativo únicamente, es decir que no se puede acceder directamente a través de Internet. Si una organización prefiere una VPN SSL de túnel, el administrador de red tendrá que explicar a

los empleados qué descargas o aplicaciones adicionales se necesitan para que el sistema funcione correctamente.

2.2.7. Algoritmo de Cifrado

Según Julio César Mendoza. (2008). Demostración de cifrado simétrico y asimétrico. El algoritmo de cifrado se divide en dos las cuales son:

2.2.7.1. Cifrado Simétrico

Utiliza claves secretas iguales para el cifrado y el descifrado. Los dos dispositivos de red deben conocer la clave para decodificar la información. Ejemplos: DES, 3DES y AES

2.2.7.2. Cifrado Asimétrico

Utiliza claves diferentes para el cifrado y el descifrado, una clave cifra el mensaje, mientras que una segunda clave descifra el mensaje Ejemplos: RSA

2.2.8. Protocolo de Seguridad

2.2.8.1. Secure Sockets Layer (SSL)

Según IBM, (2020). Este protocolo cifra mediante un algoritmo simétrico como DES o RC4. Un algoritmo de clave pública - generalmente RSA- se utiliza para el intercambio de las claves de cifrado y para las firmas digitales. El algoritmo utiliza la clave pública en el certificado digital del servidor. Con el certificado digital del servidor, el cliente también puede verificar la identidad del servidor. Las versiones 1 y 2 del protocolo SSL sólo proporcionan autenticación de servidor. La versión 3 agrega la autenticación del cliente, utilizando los certificados digitales de cliente y de servidor.

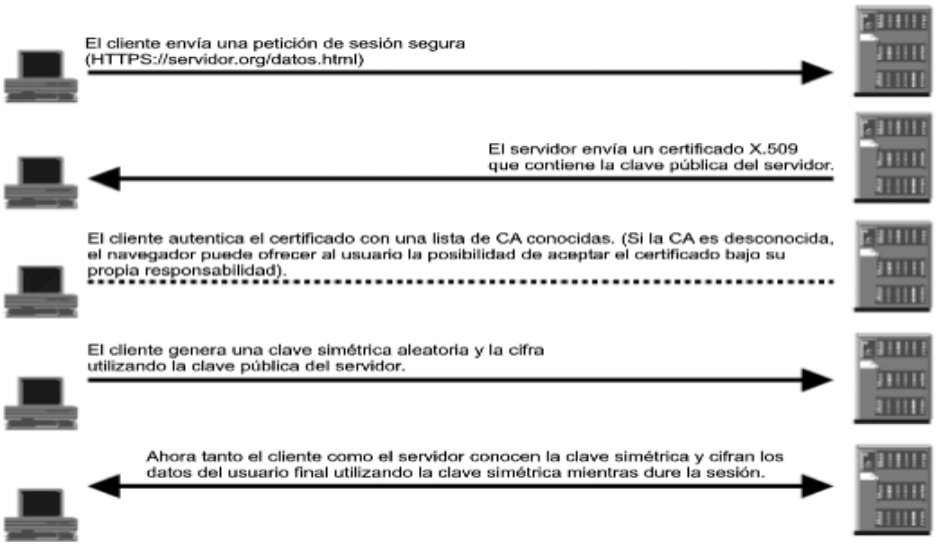


Figura 7. conexión SSL entre un navegador web y un servidor web.
Fuente: https://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user277.htm

2.2.8.2. Transport Layer Security (TLS)

Es una versión mejorada de SSL. Funciona de un modo muy parecido a SSL, utilizando cifrado que protege la transferencia de datos e información, El protocolo TLS ha evolucionado a partir del protocolo Netscape SSL 3.0, pero TLS y SSL no pueden interactuar.

2.2.9. Autenticación Multi-factor (MFA)

Según Fortinet. (2021). Multi-factor Autenticación. Es una tecnología de seguridad que requiere múltiples métodos de autenticación de categorías independientes de credenciales para verificar la identidad de un usuario para un inicio de sesión u otra transacción.

2.2.9.1. Ejemplos de Factores de Autenticación

El MFA utiliza tres métodos de autenticación comunes para verificar la identidad de un usuario, las cuales son:

- Conocimiento: este es el factor con el que los usuarios están más familiarizados. Se solicita al usuario que proporcione información que conozca, como una contraseña, un número de identificación

personal (PIN), una clave de seguridad o la respuesta a una pregunta de seguridad.

- Posesión: este factor verifica la identidad del usuario utilizando algo que posee. Por ejemplo, enviando un código a un teléfono móvil, correo electrónico y MAC
- Inherencia: este factor verifica a la persona mediante algún atributo personal único, como la autenticación biométrica o el reconocimiento de voz.

2.2.10. Método de Validación

Una vez que la VPN SSL sea implementada el siguiente paso es la validación de la solución, según el National Institute of Standards and Technology (NIST) en su publicación especial SP 800-113, los aspectos de la solución que deben ser evaluadas o validadas son:

- Conectividad:

  Se debe garantizar que el usuario pueda mantener la conexión VPN SSL para poder acceder a los recursos destinados a estar disponibles por la VPN SSL. Se debe verificar que la aplicación cliente de la VPN SSL pueda ser instalado y ejecutado sin problemas en el sistema operativo a ser utilizado, así como también por los navegadores que más probablemente use el usuario final.

- Autenticación:

  Debe verificarse la autenticación del usuario usando el método o múltiples métodos de autenticación implementados.

- Control de acceso:

  Se debe verificar que los recursos estén protegidos por las políticas de seguridad que se estableció, para esto se debe validar monitoreando el tráfico de red verificándose los registros de las conexiones VPN SSL.

- Interoperabilidad de aplicaciones y clientes.

  La VPN SSL no debe interrumpir ni tampoco interferir con las aplicaciones de software existentes. Esto es aún más importante para las aplicaciones que son accesibles mediante la VPN SSL.

- Gestión.

  Se debe poder gestionar la solución por los administradores de forma segura y eficaz, es decir se debe verificar que los administradores puedan realizar copias de seguridad, así como restauraciones.

- Inicio de sesión.

  Los registros y su gestión deben ser manejadas de acuerdo con las políticas y requerimientos de la organización.

- Rendimiento.

  La VPN SSL implementada debe brindar un rendimiento adecuado en momentos donde haya uso normal de la red, así como en momentos pico. Debido a que el tráfico cifrado consume más procesamiento que un tráfico no cifrado podría provocarse cuellos de botella. Además, el rendimiento podría verse afectado por la autenticación en servidores RADIUS, LDAP, AD, etc.

  Las pruebas o validaciones se deben realizar en una variedad de aplicaciones que se utilizarán a través de la VPN SSL, sobre todo las que tienen más probabilidades de ser afectadas por latencias o rendimiento de la red. También es posible limitar el número de usuarios simultáneos, limitar la cantidad de tráfico de aplicaciones cifradas, etc. Como medidas para mejorar el rendimiento.

- Diseño y maquetación de portales.

  El portal para el acceso a la VPN SSL debe ser intuitivo y sencillo de navegar. Así mismo debe contener las funciones requeridas por los usuarios y solo mostrar los recursos para los cuales el usuario está autorizado.

- Seguridad de la Implementación.

  Se debe asegurar que se habilite las funciones de seguridad que protejan de posibles vulnerabilidades el dispositivo que implemente la VPN SSL, estas funciones deben proteger contra secuencias de comandos entre sitios, inyección de lenguaje de consulta estructurado (SQL) y ataques de desbordamiento de búfer. Así mismo el dispositivo debe tener los últimos parches o versión instalada.

- Puesto final de Seguridad.

  Verificar que las máquinas cliente cumplen con requisitos de seguridad (por ejemplo, firewall, software antivirus) para tener acceso a la VPN SSL.

- Configuración por defecto.

  Las implementaciones de VPN SSL tienen muchas opciones de configuración predeterminadas. Se debe revisar los valores predeterminados para cada configuración de tal manera que la configuración sea necesario para respaldar los objetivos de la organización.

2.3. Definición de términos básicos

MFA: Método de control de acceso a computadoras en el que un usuario sólo tiene acceso después de presentar con éxito varias pruebas separadas a un mecanismo de autenticación.

VPN: Red privada segura construida empleando enlaces públicos. Cuenta con seguridad y cifra para asegurar que solo los usuarios autorizados puedan acceder a la red.

LAN: Red de dispositivos (ordenadores, concentradores, impresoras, ...) conectados entre sí en un área geográfica pequeña.

WAN: Conexión de ordenadores y/o redes a gran distancia, vía red telefónica o mediante un sistema de intercambio de paquetes. Habitualmente enlaza varias redes locales no contiguas.

SSL: Protocolo diseñado para permitir comunicaciones a través de Internet cifradas y autentificadas.

TLS: Protocolo criptográfico que permite que las aplicaciones se comuniquen a través de Internet de un modo que ayude a impedir escuchas, manipulación de mensajes y falsificaciones.

Active Directory (AD): Es un sistema centralizado que automatiza la gestión de los datos de usuarios, la seguridad, y los recursos distribuidos en la red.

SSH: Protocolo que permite la conexión segura con ordenadores remotos. Cifra clave pública para cifrar las comunicaciones y autentificar usuarios.

DNS: Esquema de traducción a direcciones numéricas de Internet de cadenas de palabras que identifican usuarios y localizaciones.

Ping: Nombre de la utilidad empleada en TCP/IP para comprobar la posibilidad de acceso a un ordenador. Durante una comprobación de ping, se envían paquetes de petición de eco ICMP a otro nodo con la dirección IP especificada, y se espera a que regresen los paquetes de respuesta de eco, "ping".

Backup: Es una copia de seguridad a mayor o menor escala. Puede ser una versión reciente de la información contenida en todos los equipos.

DES: Es un cifrado simétrico de bloque, que cifra bloques de texto de 64 bits. La clave es de 64 bits (56 + 8 de paridad). Hace uso de permutaciones, operaciones XOR y sustituciones. Debe su fortaleza al uso de Cajas S, que ofrecen trasformaciones no lineales.

RC4: Sistema de cifrado de flujo empleado en los protocolos TLS/SSL y WEP.

IP (Internet Protocol): Protocolo de comunicación de datos digitales que funciona en la capa de red del modelo OSI.

Forticlient: Software que permite la conectividad a una red interna

Firewall: Filtra el tráfico que se intercambia entre una red confiable y otras redes no confiables. Todo ello, en función de unas reglas establecidas previamente. autorizadas.

Servidor: Es un aparato informático que almacena, distribuye y suministra información.

Traceroute: Comando de diagnóstico de redes para mostrar las posibles rutas o caminos de los paquetes, mide las latencias de tránsito y los tiempos de ida y vuelta a través de redes de Protocolo de Internet.

CLI (command): Programa informático por medio de una línea de texto simple, los comandos varían debido a los diferentes fabricantes.

Topología física: Esquema que representa la conexión física de la red, donde se aprecia dispositivos de red, la ubicación y la conexión ya sea por cables o de forma inalámbrica.

Topología lógica: Esquema que representa la conexión lógica de la red, muestra el direccionamiento y el enrutamiento del intercambio de la información en la red.

Split Tunneling: Envía parte de su tráfico de Internet a través de una conexión VPN cifrada y permitir que el resto viaje a través de un túnel diferente en la Internet abierta.

Protocolo criptográfico: Está diseñado para permitir una comunicación segura bajo un conjunto dado de circunstancias.

CAPÍTULO III

DESARROLLO DEL TRABAJO PROFESIONAL

3.1. Determinación y Análisis del Problema

El cambio de la modalidad de trabajo de Mall Plaza de forma remota se dio por la coyuntura de la Pandemia, ya que el problema general era que las conexiones inseguras por escritorio remoto para algunos usuarios, estas carecían de alguna tecnología que brinde la seguridad adecuada, así como también un método de autenticación que evite la suplantación de identidad y escalabilidad para los usuarios, ya que el usuario al realizar sus labores en su hogar es voluble al robo de información como se puede apreciar en la figura 8 el usuario utilizó sus credenciales a una página en cual se puede validar mediante el wireshark la contraseña por lo que se valida que es una conexión insegura y vulnerable:

Figura 8. Conexión de un usuario sin VPN

Fuente: Propia

Considerando que, como entidad privada debe garantizar la seguridad, confidencialidad, escalabilidad y la autenticación al acceso, para proteger la data almacenada en su red y del usuario, Mall Plaza realizo la creación del ticket al área donde laboro ya que gestionamos su equipo Fortinet para la implementación de la VPN. Se realizó la configuración de la VPN SSL ya que este permite agregar más usuarios luego de la implementación, también brinda restricciones por políticas de acuerdo con el perfil del usuario y los destinos a los que pueda tener acceso. A su vez este equipo brinda validación respecto a la conexión de los usuarios y también información de las IPs que toman, los destinos y el tráfico que consumen, se puede obtener en un tiempo definido y tiempo real.

3.2. Modelo de Solución Propuesto

De la problemática expuesta mi trabajo fue implementar un servicio que permita a sus usuarios remotos acceder a su red de forma segura y autenticación. Este servicio, no tuvo costo y fue de fácil configuración por parte de los usuarios en sus dispositivos ya que el cliente cuenta con su equipo Fortinet 300E y fue a solicitud del cliente mediante un ticket. El servicio implementado en Mall Plaza es con Secure sockets Layer VPN (SSL VPN) es escalable ya que se pueden ir agregando usuarios después de la implementación y cuenta con seguridad para los datos e información que se transmiten en la virtual private network (VPN). A continuación, presento mi Estructura del Desglose del Trabajo (EDT) que desarrolle con los cuatros fases del modelo de solución propuesto.

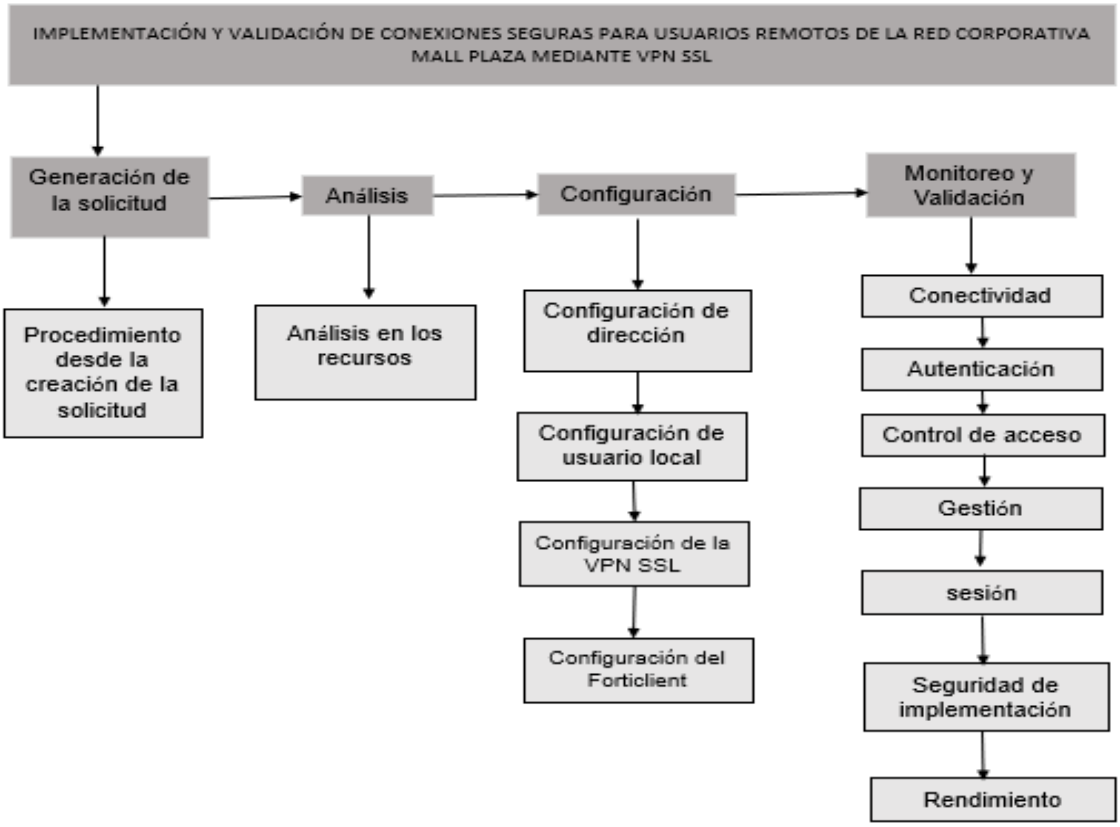


Figura 9. Estructura del Desglose del Trabajo

Fuente: Elaboración propia

Nuestra implementación y validación se estructuro en 4 Fases: Procesos de la solicitud del cliente, análisis, configuración y validación:

Tabla 1. Diagrama de GANTT

ACTIVIDADES	TIEMPO																																				
	AGOSTO																SETIEMBRE																					
	7	10	11	12	13	14	17	18	19	20	21	24	25	26	27	28	31	1	2	3	4	7	8	9	10	11	14	15	16	17	18	21	22	23	24	25	28
Generación de solicitud																																					
Fase de análisis																																					
Fase de configuración																																					
Fase de Monitoreo y validación																																					

Fuente: Elaboración propia

3.2.1. Generación de la Solicitud

La cadena Mall Plaza presentó su solicitud para la creación de la VPN SSL (Ver anexo 01). La cual fue derivada al área de soporte para la atención respectiva y finalmente a mi persona, se tiene un proceso de inicio a fin donde se detalla mediante correos el avance de la solicitud en cual se concluye con la validación del cliente (Ver anexo 02). En la Tabla 2 se puede apreciar la actividad del manejo de los correos desde la generación del ticket.

Tabla 2. Procedimiento de la recepción de correos para los clientes de Connect cuando generan un ticket.

RESPONSABLE	***N.º***	***DESCRIPCION DE ACTIVIDAD***
CLARO	1	El cliente genera ticket de implementación comunicándose al área de Claro: 080000911 opción 4. Soporte de Primer Nivel de Claro recibe la solicitud del cliente. Soporte de Primer Nivel de Claro envía correo a Connect (**soporte@connect.pe)** con el requerimiento
CONNECT	2	Inicio del procedimiento en Connect
	3	Recepción del ticket de Claro y generación del ticket interno en el sistema de tickets de Connect. El operador de Soporte Connect contesta el correo confirmando la recepción e indicando el ticket interno. Procede a la actualización de estatus.
	4	Soporte Connect se comunica con el cliente y se identifica como soporte gestionado de Claro. Se consulta al cliente mayor detalle del requerimiento solicitado.
	5	Se realiza lo solicitado
	6	Explicación y documentación del caso mediante correo a SSGF de Claro. Se documenta el ticket interno en el Sistema de Tickets de Connect Se espera la conformidad del cliente o SSGF mediante correo para el cierre del caso.
	7	Fin del procedimiento.

Fuente: Connect

3.2.2. Fase de Análisis

Efectué un análisis previo de la información antes de poder realizar las configuraciones utilizando el Firewall Fortinet:

- Topología

  Como se puede apreciar en la imagen la conexión de los usuarios es mediante internet por el aplicativo Forticlient para que establezcan una conexión VPN segura de acceso remoto hacia los segmentos de la LAN. Las cuáles serán protegidas mediante el protocolo SSL Y TLS.

Esta configuración no afecta físicamente a su topología, ya que las configuraciones se realizan en el firewall y el usuario final.

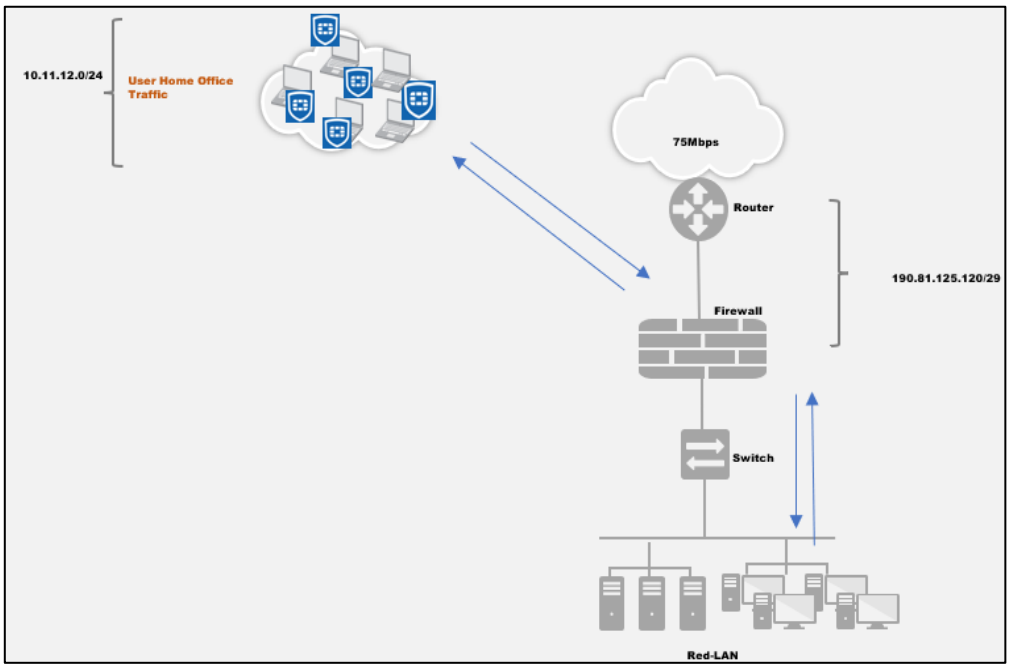


Figura 10. Topología de la conexión VPN SSL de los usuarios remotos
Fuente: Mall Plaza

Se puede apreciar en la Figura 10 que la empresa cuenta con una WAN (190.81.125.122) por lo cual esta IP será configurada tanto en la VPN SSL ver figura 17 y en el Forticlient de cada usuario ver figura 20. El puerto que se configura para esta conexión es el 10443 ya que no suele ser usada para publicaciones que pueda tener la empresa.

- Información de los usuarios

Con esta información se configuró el correo del usuario para la doble autenticación cuando se conecta al Forticlient, la información de correo debe ser única para los usuarios ya que no se pueden repetir ver Anexo 3, también con esta información se contabilizó y creó los usuarios remotos, se puede apreciar en el punto 3.2.3.2.

- Información de los segmentos configurados en el Firewall

Con esta información se configuraron las políticas y segmento de red para la conexión VPN SSL ya que este no se puede repetir con otros segmentos que este en uso en la LAN por que entraría en conflicto o no se podría levantar la VPN, se puede apreciar en el punto 3.2.3.3 el segmento de red (10.11.12.1 - 10.11.12.254) el segmento que tomará la VPN con el análisis realizado.

Tabla 3. Tabla resumen de direcciones configuradas en el Firewall

IP	***MASCARA***
318	/32
1	/30
1	/29
61	/24
20	/23
1	/19

Fuente: Propia

Analizando las direcciones configuradas en el Firewall ver anexo 4, se concluye que el segmento de red para la VPN SSL tendrá el rango de 10.11.12.1 - 10.11.12.254, de la cual no está siendo usada.

También se definirá los segmentos de redes las cuales los usuarios al conectarse a la VPN tendrán como destino, esta información brinda la empresa MALL PLAZA por nuestro parte se validará que estos segmentos estén configurados para poder nosotros agregarlos a las políticas como se aprecia en el punto C de la sección 3.2.3.3.

3.2.3. Fase de Configuración

3.2.3.1. Direcciones

Se realizaron la creación de las direcciones para que los equipos se conecten a través de la VPN y se configuren en las políticas como destino para el usuario. Esto se realizó desde la pestaña “Policy & Objects” >> “Objects” >> “Addresses; allí se agregó el nombre, subred y mascará como en la siguiente figura 9:

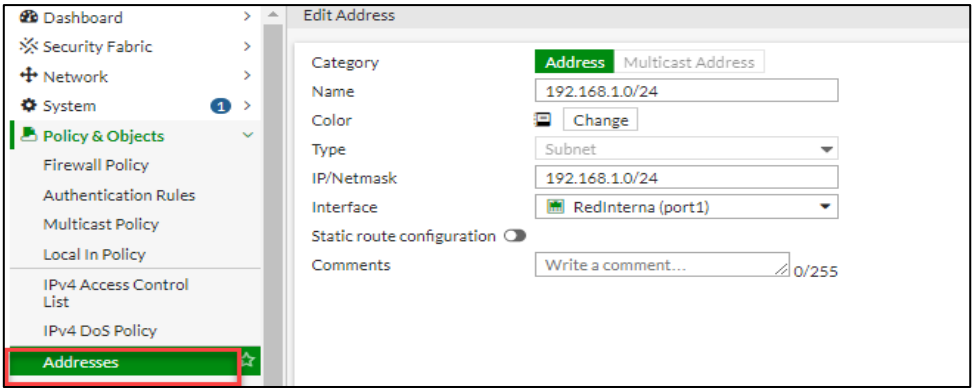


Figura 11. Configuración de direcciones

Fuente: Firewall de Mall Plaza

3.2.3.2. Usuario

Luego de haber creado todas las direcciones útiles, se deben crear los usuarios que accederán a la VPN, esto se realizó desde la pestaña “User & Device” >> “User”>> “User Definition”; allí en la parte superior se crea el nuevo usuario y se especifica el tipo de autenticación el cual se tomó usuario local, como en la siguiente figura 10:

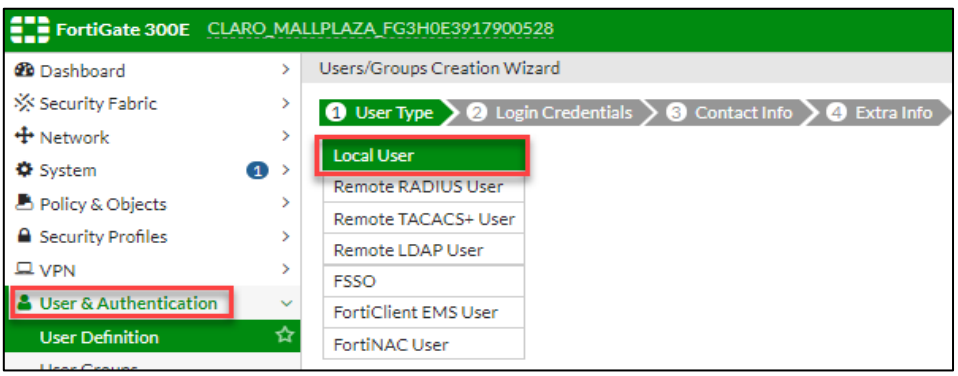


Figura 12. Configuración de usuario

Fuente: Firewall de Mall Plaza

Luego de este paso solicita el nombre del usuario y contraseña:

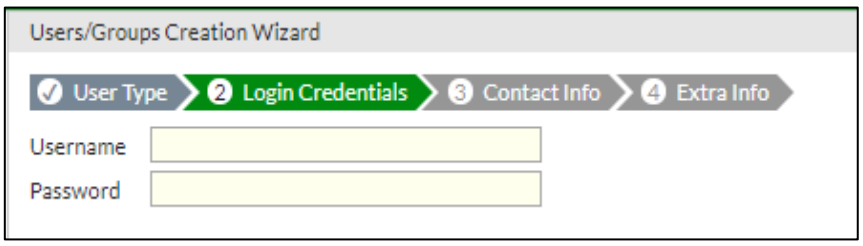


Figura 13. Configuración de los datos del usuario

Fuente: Firewall de Mall Plaza

Se realizó esta configuración por comando para activar el two-factor email para cada usuario con sus cuentas de correos, esto es para la autenticación, cuando el usuario se conecte por el Forticlient este reciba el token en su cuenta inscrita y coloque este al FortiClient para completar la conexión.

```
CLARO_MALLPLAZA_FG3H~528 # config user local

CLARO_MALLPLAZA_FG3H~528 (local) # edit lfontalvo

CLARO_MALLPLAZA_FG3H~528 (lfontalvo) # set two-factor email

CLARO_MALLPLAZA_FG3H~528 (lfontalvo) # set email-to "leidys.fontalvo@mallplaza.com"

CLARO_MALLPLAZA_FG3H~528 (lfontalvo) # end
```

Figura 14. Comando para activar la autenticación por email

Fuente: Firewall de Mall Plaza

Como siguiente paso después de crear los usuarios, se creará un grupo, para la facilidad de configuración al momento de crear la VPN, esto se realizó en la pestaña: “User & Device” >> “User” >> “User Groups”, allí se crea un nuevo grupo donde se solicita el nombre del grupo y el tipo del grupo.

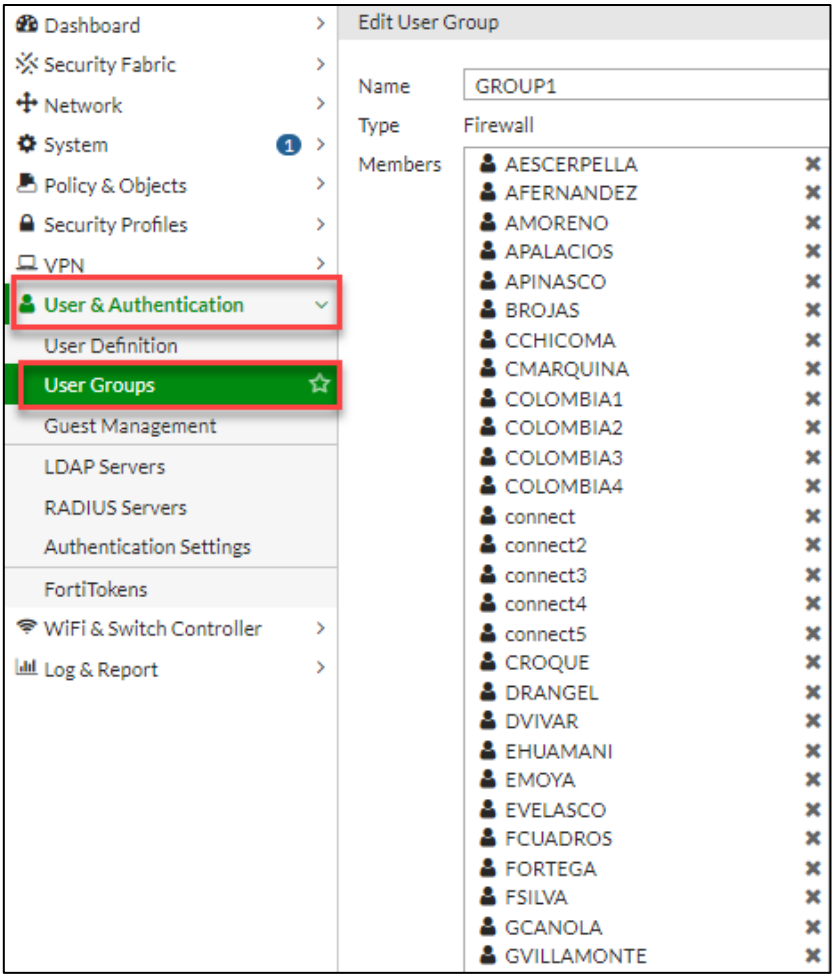


Figura 15. Configurar grupo

Fuente: Firewall de Mall Plaza

3.2.3.3. Configuración de la VPN SSL

Se tiene los siguientes pasos:

A. En primer lugar, se configuró el portal de acceso que tendrá la VPN, esto se configuró en la pestaña “VPN” >> “SSL” >> “Portal”, y se editó la opción “full access”, allí se habilitó la opción “Enable Tunnel Mode” para habilitar el “Split Tunneling” esto permite solo el tráfico interno que se enrutará a través del túnel VPN, se configura la interfaz web que tendrá la VPN, se limitó la conexión por usuario y se agregó el segmento de red “VPN_SSL(10.11.12.1 - 10.11.12.254)” que tomará una dirección de este segmento cuando un usuario se conecte por el FortiClient.

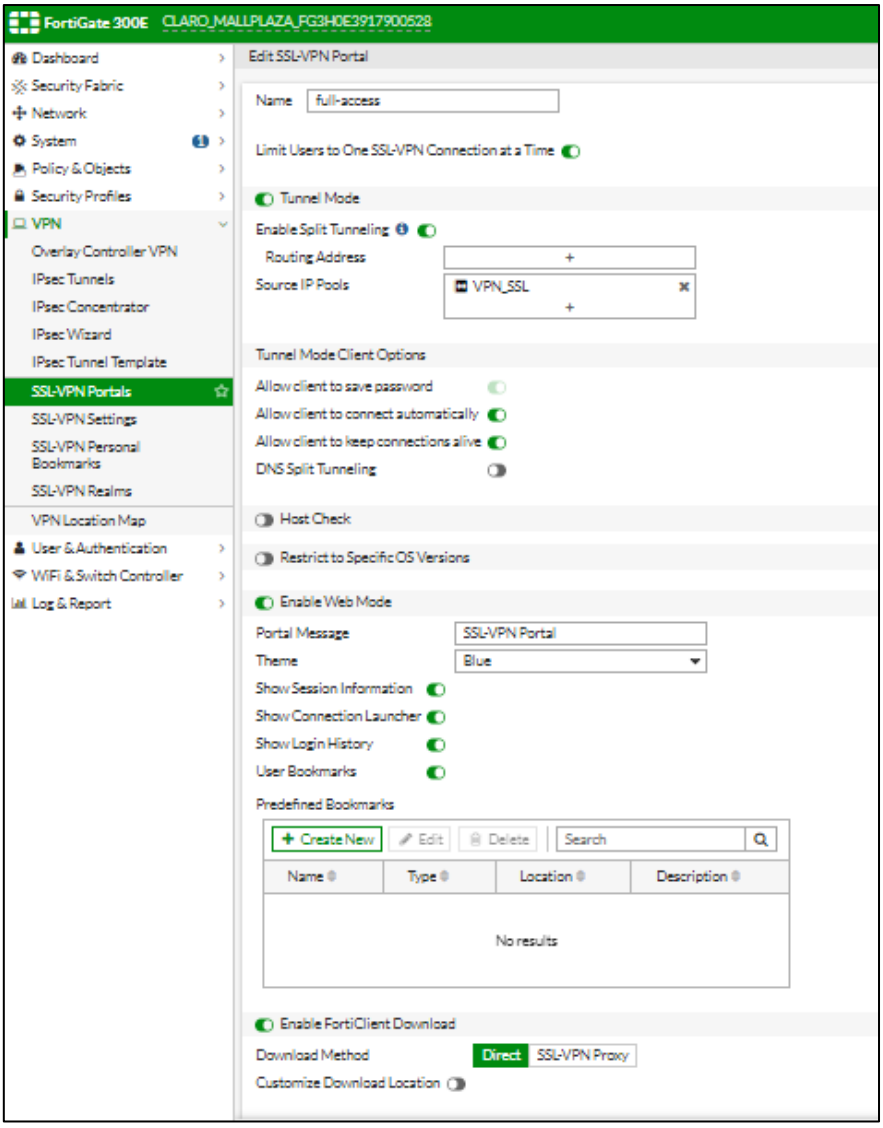


Figura 16. Configurar VPN SSL Portal

Fuente: Firewall de Mall Plaza

B. Luego se configuraron los parámetros de la VPN, esto se realizó en la pestaña “VPN” >> “SSL” >> “Settings”, allí se especificó el puerto del firewall que tiene conexión a internet, el puerto por el cual se realiza la conexión es el 10443, también se define el tiempo máximo de sesión inactiva, se asignó el rango de direcciones que serán asignados a los usuarios VPN marcando la opción “Specify custom IP ranges” y agregando allí el rango de IP, este se crea de la misma manera que se hizo en la sección 3.2.3.1.Luego de esto se agregó el grupo creado con su respectivo portal en “ Authentication/Portal Mapping”

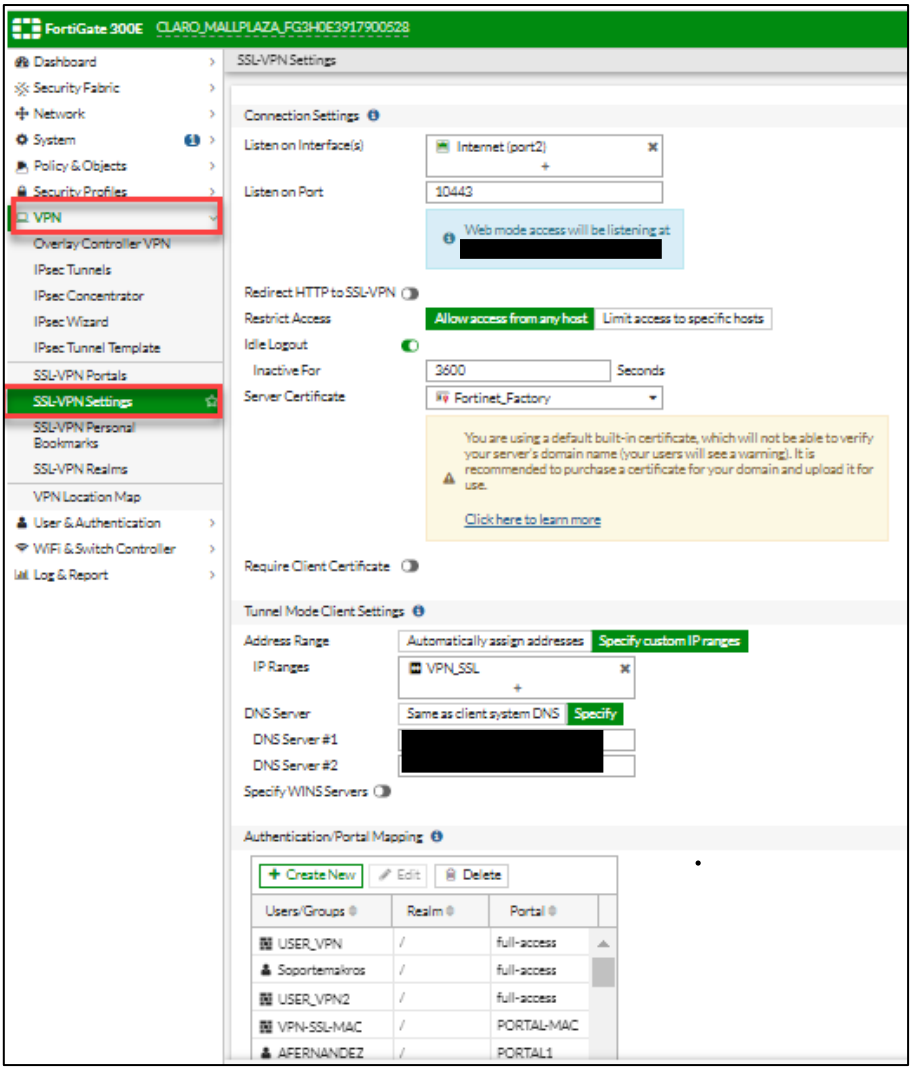


Figura 17. Configurar VPN Settings

Fuente: Firewall de Mall Plaza

C. Es necesario crear políticas para esta VPN para que los usuarios VPN puedan acceder a la red interna de la empresa, esto se realizó en la pestaña “Policy & Objects” >> “Policy” >> “IPv4”, allí se asignó como interfaz de origen el “ssl.root”, en direcciones orígenes, en dirección origen se colocó VPN_SSL y se especifica el grupo de usuarios creado anteriormente o los usuarios, la interfaz de destino será la red interna y dirección destino serán los segmentos permitidos que tendrán los usuarios. También deben estar activados los filtros de seguridad como el antivirus y certificate - inspection, estos se tomaron los defaults del equipo los cuales protegen la conexión.

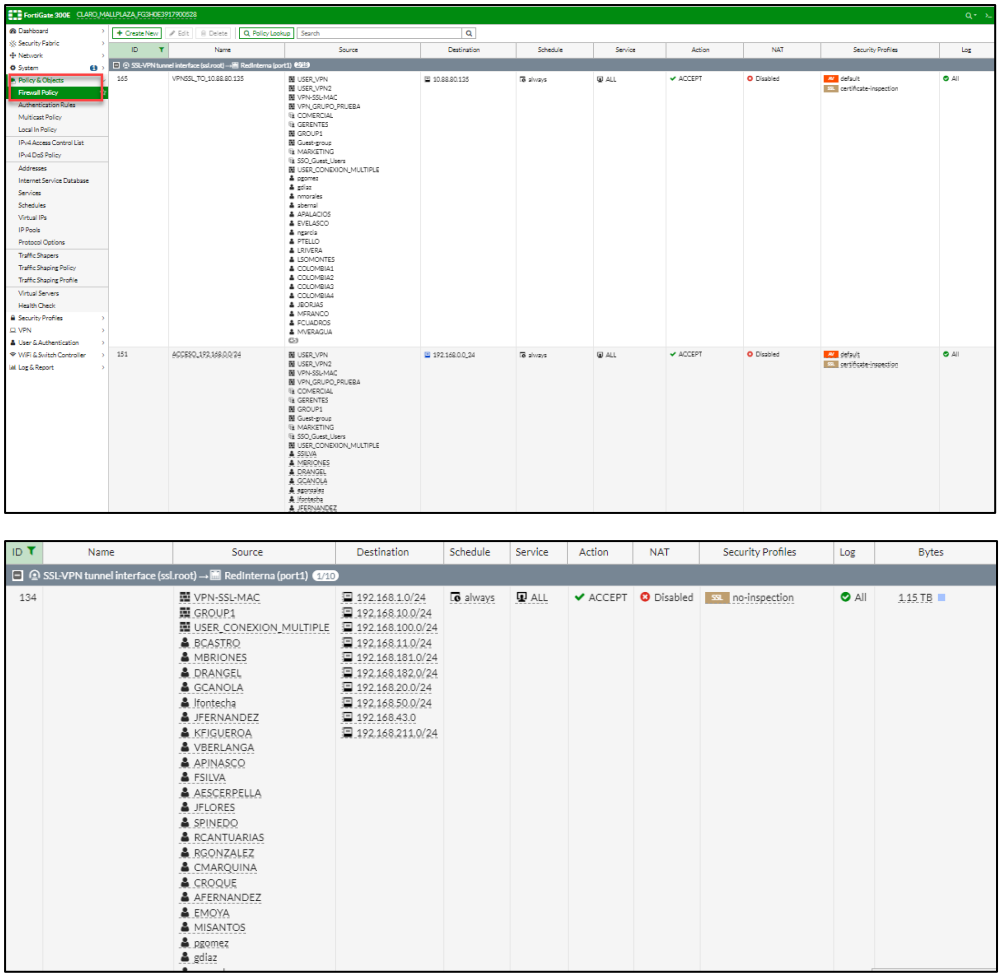


Figura 18. Configuración de las Políticas

Fuente: Firewall de Mall Plaza

3.2.3.4. Configuración del Forticlient

Culminando la configuración en el firewall se requiere ingresar al equipo del cliente para poder realizar la respectiva instalación del software para que este ingrese y se conecte a la VPN, para el caso de Firewall Fortinet se usa el FortiClient, el cual se descarga gratis desde la página de Fortinet en www.fortinet.com.

Como se visualiza en la figura 17, en el aplicativo de Forticlient se accede a la opción de las tres líneas “Adicionar una nueva conexión”, allí se podrá agregar la IP pública de conexión, el puerto y el usuario como en la figura 18:

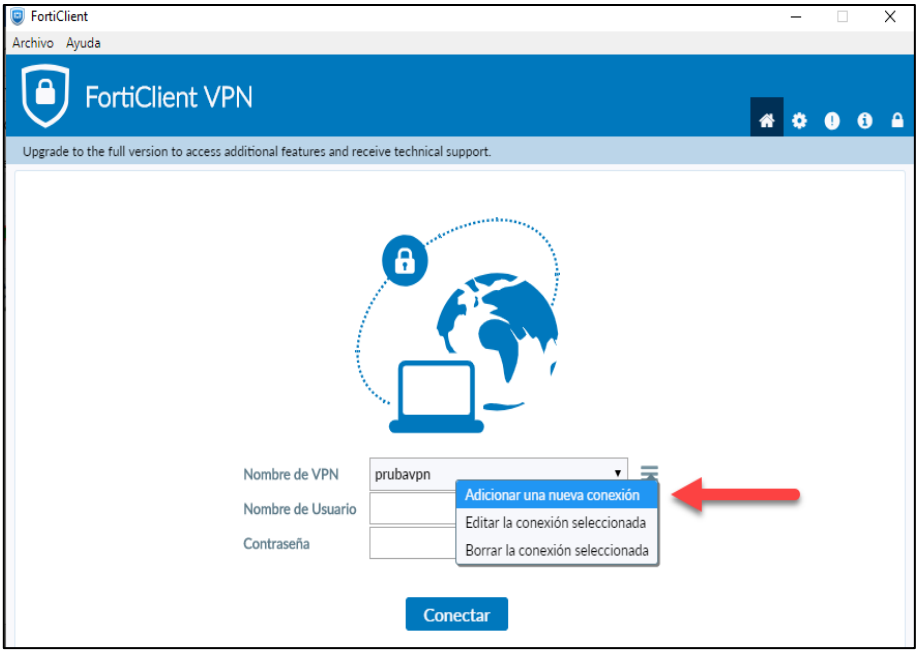


Figura 19. Configurar nueva conexión en el Forticlient

Fuente: Propia

Figura 20. Configuración del Forticlient.

Fuente: Propia

3.2.4. Fase de Monitoreo y Validación

3.2.4.1. Método de Conectividad

Se valida el acceso al destino configurado en la política 134 sección 3.2.3.3 (C), no se tiene perdida de paquetes ni tiempos elevados en la conexión.

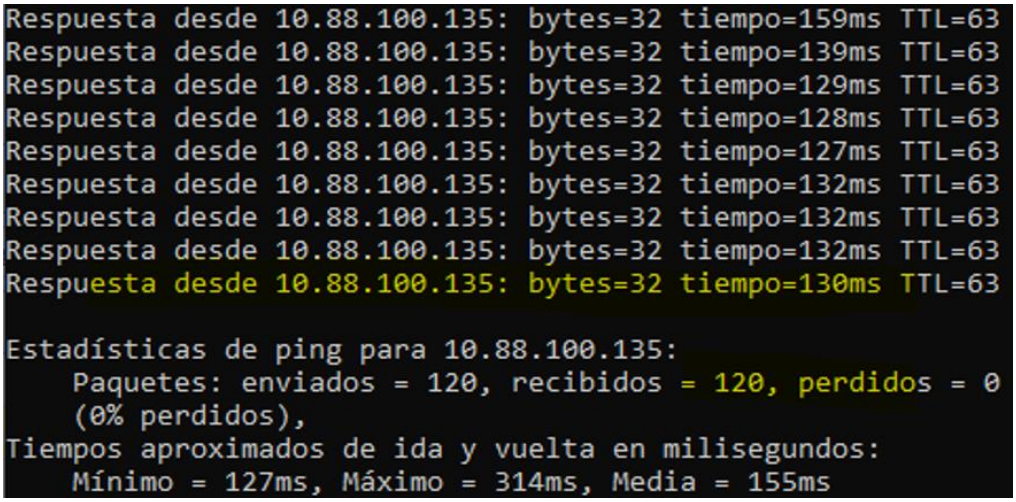


Figura 21. Conectividad por ping hacia el destino de la red interna

Fuente: Propia

3.2.4.2. Método de Autenticación

Cuando el usuario ingresa sus credenciales en el Forticlient automáticamente el token es enviado a la cuenta de correo configurado en el usuario como se observa en la figura 20, teniendo el token se procede a colocar en el aplicativo en la opción de token, luego esto se valida la conexión del usuario como se observa en la figura 21.

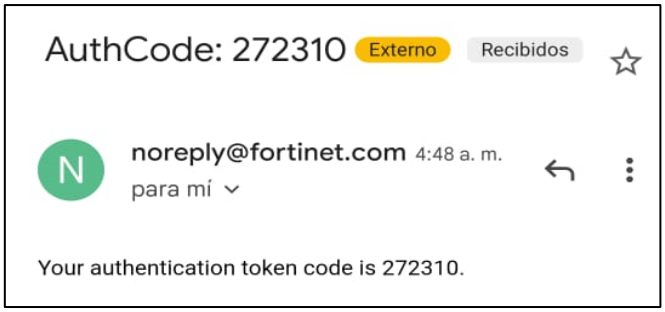


Figura 22. Token enviado a la cuenta asociada del usuario

Fuente: Propia

Se verifica conexión del usuario el cual tiene la IP 10.11.12.3 la cual pertenece al segmento de la red VPN_SSL configurado en la VPN SSL.

Figura 23. Conexión del usuario remoto en el Forticlient

Fuente: Propia

3.2.4.3. Método de Control de acceso

Se puede visualizar el usuario pruebatoken con IP 10.11.12.3 está pasando correctamente por su política 134 en la cual fue configurada.

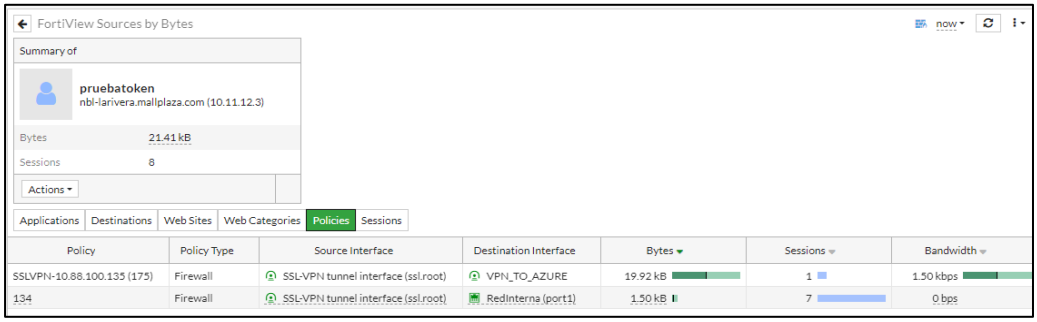


Figura 24. Validación del usuario a la política configurada

Fuente: Propia

3.2.4.4. Método de Gestión

En caso de una avería del equipo se tiene la opción de poder descargar Backup en el cual se puede recuperar la información de todo lo configurado en el equipo.

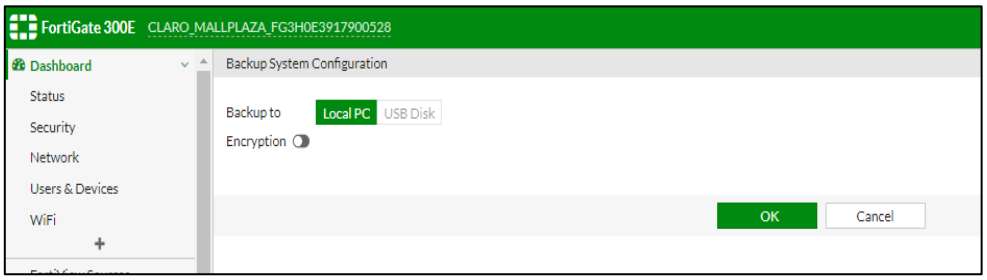


Figura 25. Pestaña donde se descargar el Backup

Fuente: Firewall Mall Plaza

3.2.4.5. Sesión

Se valida las conexiones de los usuarios con las IPs que toman respecto al segmento que se configuró para las conexiones VPN, el tiempo de conexión y el volumen de tráfico que usan.

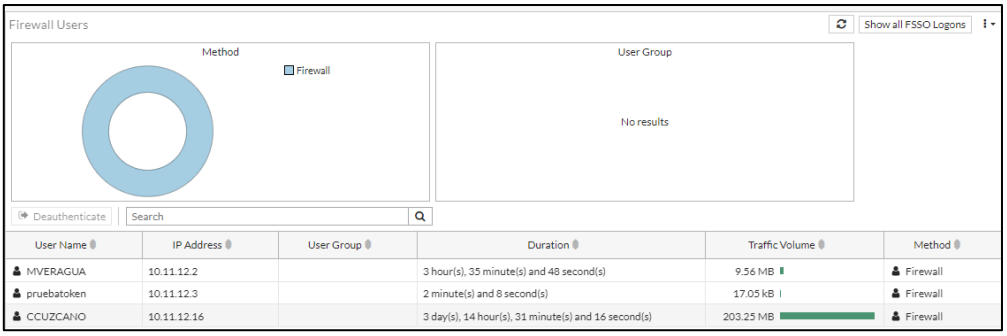


Figura 26. Información de los usuarios conectados

Fuente: Firewall Mall Plaza

3.2.4.6. Método de Rendimiento

Se valida que la conexión del usuario es única, ya que en caso un usuario intente acceder en otro PC con las mismas credenciales esta no se le va a permitir ya que lo retiraría de la otra sesión del FortiClient.

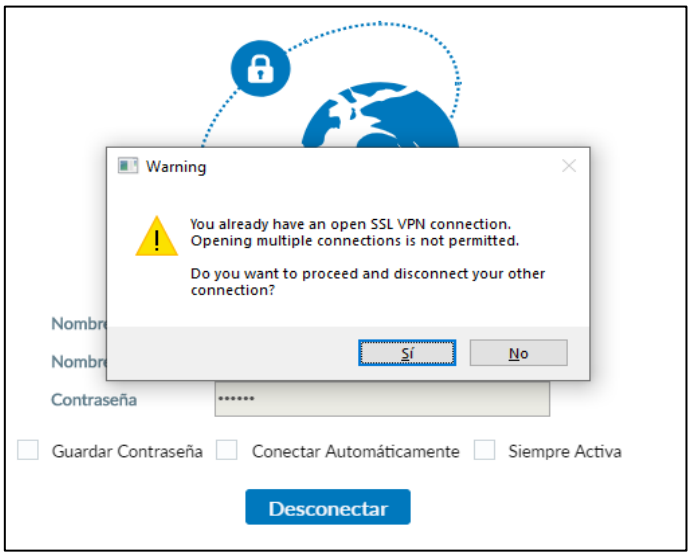


Figura 27. Alerta cuando un usuario se conecta a otra PC

Fuente: Propia

3.2.4.7. Método de Seguridad

Según el Portal de Fortinet (2021), se tiene vulnerabilidades que afectaron directamente la implementación de VPN SSL la cuales son:

- CVE-2018-13379: Esto permite que un atacante no autenticado descargue archivos a través de solicitudes de recursos HTTP que son diseñadas especialmente.

Tabla 4. Versiones afectadas por la vulnerabilidad CVE-2018-13379

FortiOS 6.0	*6.0.0 to 6.0.4*
FortiOS 5.6	5.6.3 to 5.6.7
FortiOS 5.4	5.4.6 to 5.4.12

- CVE-2018-13382 Esta vulnerabilidad de autorización permite que un atacante no autenticado cambie la contraseña de un usuario del portal web SSL VPN mediante solicitudes HTTP que son diseñadas especialmente.

Tabla 5. Versiones afectadas por la vulnerabilidad CVE-2018-13382

FortiOS 6.0.0	*6.0.0 to 6.0.4*
FortiOS 5.6.0	5.6.0 to 5.6.8
FortiOS 5.4.1	5.4.6 to 5.4.12

El equipo del cliente cuenta con la versión 6.4.1 el cual no le afecta las vulnerabilidades indicadas por Fortinet.

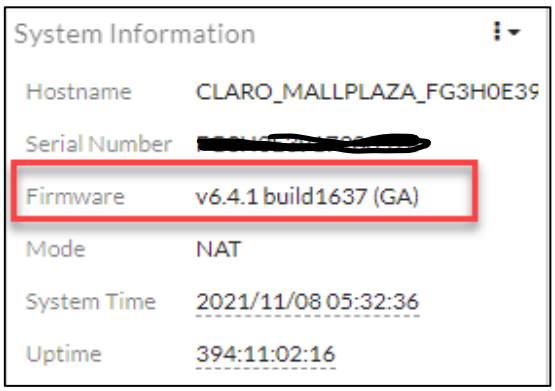


Figura 28. Versión del Sistema operativo del Firewall

Fuente: Firewall Mall Plaza

3.3. Resultados

- Se tiene el siguiente resultado para el método de conectividad:

  Método: Conectividad por Ping

  Desarrollo: El usuario remoto se conecta mediante el aplicativo FortiClient haciendo el uso del CMD, realiza ping a una IP privada 10.88.100.135 perteneciente al segmento de red LAN de Mall Plaza.

  Resultado: Exitoso, se tiene conexión al destino, no se tienen tiempos elevados ni perdida de paquetes.

- Se tiene el siguiente resultado para el método de autenticación:

  Método: Método de autenticación mediate token

  Desarrollo: El usuario se conecta al FortiClient con sus credenciales, luego de esto se envía un token al correo asociado del usuario, este token se digita en el aplicativo FortiClient como paso final para la conexión.

  Resultado: Se valida que el token es enviado únicamente a la cuenta asociada del usuario.

- Se tiene el siguiente resultado para el método Control de acceso:

  Método: Método de control de acceso

  Desarrollo: Cuando el usuario se conecta por el FortiClient se puede validar en el firewall las sesiones que toma el usuario en la pestaña de Fortiview como las políticas por las cuales está pasando el tráfico.

  Resultado: Exitoso, se valida el uso de las políticas creadas para los usuarios.

- Se tiene el siguiente resultado para el método de gestión:

  Método: Método de gestión

  Desarrollo: El firewall cuenta con la opción de descargar Backup, con esta información en caso de pérdida de servicio por avería del firewall se tiene un repuesto de información de lo configurado en el firewall.

  Resultado: Recuperación del servicio en caso de avería.

- Se tiene el siguiente resultado para el método de sesión:

  Método: Método de sesión

  Desarrollo: Cuando el usuario se conecta por el FortiClient este toma una IP respecto al segmento de la VPN configurado, lo cual se puede validar en el Firewall en la pestaña de Fortiview.

  Resultado: Exitoso, el usuario tiene asignado una IP que pertenece al segmento de red de la VPN configurada.

- Se tiene el siguiente resultado para el método de Rendimiento:

  Método: Método de sesión

  Desarrollo: Cuando el usuario se conecta por el FortiClient este usuario no puede volver a conectarse en otra PC mientras su usuario siga activo.

  Resultado: Exitoso, ya que cuando se conecta en otra PC cierra sesión en otra y así hace la conexión única para usuario.

- Se tiene el siguiente resultado para el método de Seguridad:

  Método: Método de seguridad mediante wireshark

  Desarrollo: Se puede apreciar la conexión del usuario sin VPN Y con VPN, en el cual la conexión sin VPN se puede captar el tráfico que realiza, mediante que la conexión con VPN este tráfico es encriptado.

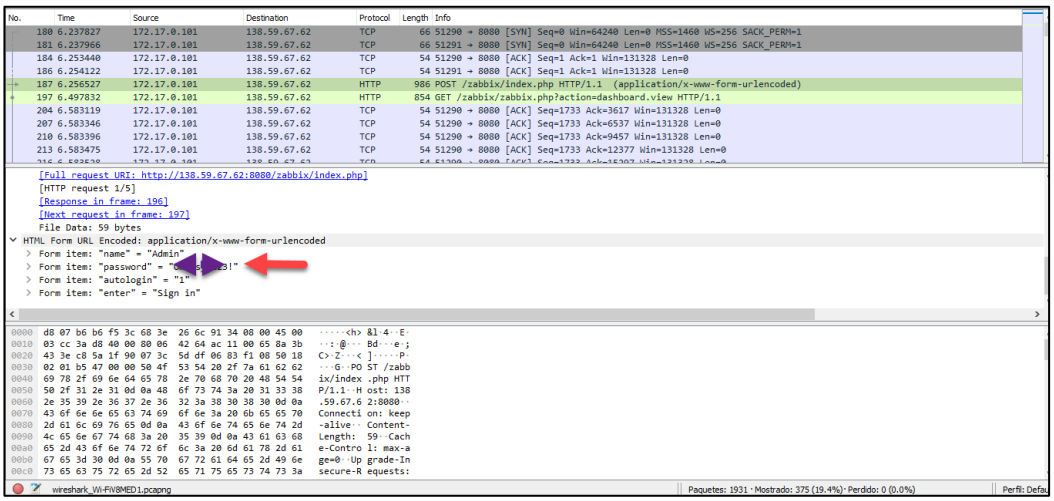


Figura 29. Análisis wireshark sin VPN

Fuente: Propia

Se realiza un Follow stream para seguir el flujo de la información.

Figura 30. Resultados del análisis wireshark sin VPN

Fuente: Propia

Como se puede visualizar a través del wireshark, la información de la máquina sin VPN es analizada mediante el protocolo que se utilizan para el envío de la información que es visible como los datos del usuario y contraseña, por lo cual podría ser extraída por maliciosas instituciones.

A continuación, se instalará la herramienta la PC para la evaluación de seguridad de la red y se realizará el intercambio de la información del usuario.

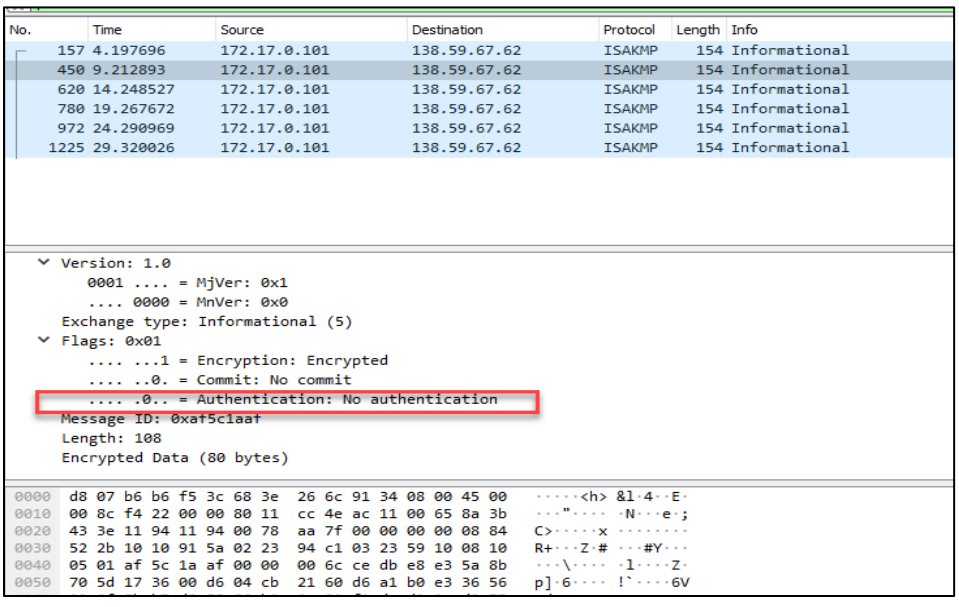


Figura 31. Análisis wireshark con VPN

Fuente: Propia

Se realiza un Follow stream para seguir el flujo de la información.

Figura 32. Resultados del análisis wireshark con VPN

Fuente: Propia

Resultado: Exitoso, la información del usuario de la PC conectada a la VPN es analizada mediante el protocolo que utilizan para el envío de información, esta información aparece encriptada.

CONCLUSIONES

- Para determinar el segmento correcto a usar en la VPN se debe revisar y analizar las redes en los equipos encargados de los enrutamientos, en las pruebas realizadas se verifica el asignamiento de la IP del usuario en la conexión del FortiClient respecto al segmento configurado en la VPN, por lo que la solución es viable y exitosa.
- Para realizar la configuración del servicio VPN SSL y autenticación fue necesario conocer los requerimientos de la empresa Mall Plaza como son los destinos, servicios, usuarios y cuentas, se concluye en las validaciones realizadas que la autenticación de los usuarios al conectarse a la VPN es exitosa y única, ya que el token es enviado al correo del usuario como paso final para la conexión en la VPN.
- Se concluye exitosamente la conexión de los usuarios VPN en las diferentes pruebas de validación donde se obtuvo conectividad, seguridad, autenticación y gestión.
- Esta implementación es una buena práctica respecto a las conexiones remotas ya que luego de la implementación se estuvieron incorporando más usuarios.
- De acuerdo con los resultados se concluye que la implantación de VPN SSL es segura respecto al sistema anterior de la conexión por escritorio remoto mediante internet.

RECOMENDACIONES

- Se recomienda habilitar lo registros de logs en las futuras políticas para los nuevos usuarios para así poder tener un historial de tráfico realizado por el usuario.
- Para el uso de los clientes, se recomienda el uso del aplicativo "Forticlient VPN", por su entorno gráfico, de fácil acceso y con un sistema de encriptación.
- Se recomienda generar Backup cada cierto tiempo respecto a las configuraciones que se tienen en el firewall, en caso de alguna avería del equipo.
- Se recomienda a futuro poder tener una alta disponibilidad de activo – pasivo en el firewall en caso de avería del equipo.

REFERENCIAS BIBLIOGRÁFICAS

Ealde, Business School D. (2020). Ciberseguridad y riesgos digitales. www.ealde.es/seguridad-perimetral-y-su-aplicacion/

Fortinet, Inc. All Rights Reserved (2021). SSL VPN. www.fortinet.com/resources/cyberglossary/ssl-vpn

Fortinet, Inc. All Rights Reserved (2021). Multifactor authetication . www.fortinet.com/resources/cyberglossary/multi-factor-authentication

Fortinet, Inc. All Rights Reserved(2021). remote access. www.fortinet.com/resources/cyberglossary/remote-access

CISCO, CCNA (2020). Modulo 1. https://www.ccna.es/ccna-1-v7-0-curricula-capitulo-1/

Omar Zapata, (2017*), Diseño de una red convergente utilizando VPN IPsec entre la central de una farmacia localizada en lima metropolitana y su sucursal ubicada en Jauja-Junin*, UNTELS. http://repositorio.untels.edu.pe/jspui/handle/123456789/405

Abraham Casanova, (2020*), Diseño de una red privada virtual orientada al teletrabajo de organizaciones con escasos recursos económicos por la coyunturadelcovid-19*, UNTELS. http://repositorio.untels.edu.pe/jspui/handle/123456789/586

De La Cruz Bernilla Segundo Magdaleno, Vera Cruz Jean Ronald Steven (2019), *Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo*, Universidad Pedro Ruiz de Gallo. https://repositorio.unprg.edu.pe/handle/20.500.12893/8266

Henry Quezada, (2016), *Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja, en la Universidad Nacional de Loja de Ecuador*. https://dspace.unl.edu.ec/jspui/bitstream/123456789/17159/1/Quezada%20Lozano%2C%20Henry%20Daniel.pdf

Mukatshung Claude Nawej, (2016), *Evaluation of Virtual Private Network Impact on Network Performance*, University of South África. https://uir.unisa.ac.za/handle/10500/22177

ANEXOS

Anexo 1. Solicitud del cliente para la creación de usuarios VPN.

MALL PLAZA PERÚ S.A. || CID.3709342 || SVA-CAMBIOS:20474141 || Crear usuarios VPN con MFA

FS Franco Llacua Santi <fllacua.sapia@claro.com.pe>
Vie 7/08/2020 11:02

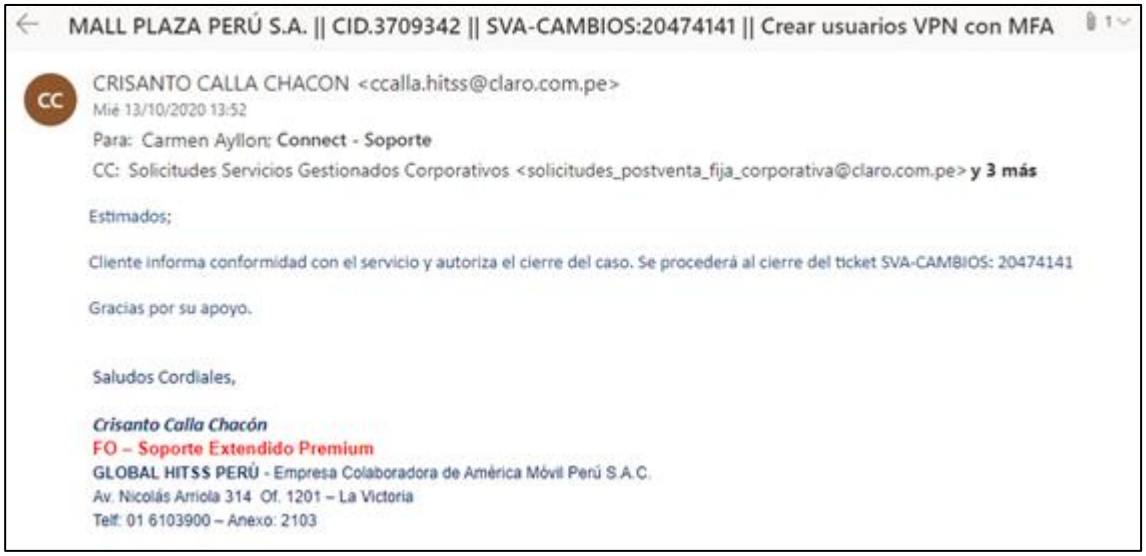
Para: **Connect - Soporte**
CC: Solicitudes Post-Venta Fija Corporativa <solicitudes_postventa_fija_corporativa@claro.com.pe> **y 1 usuarios más**

Estimados Connect,

Para informarles que se ha creado el siguiente ticket de atención.

Razón Social:	MALL PLAZA PERÚ S.A.
Nombre del Contacto:	Omar Escalante
Número(s) del Contacto:	982799694 / 956125352
Correo:	omar.escalante@mallplaza.com
CID:	3709342
Detalle de la Solicitud:	Cliente solicita la creación de los siguientes usuarios VPN con MFA: **(ver correo infra líneas abajo).**
Disponibilidad del cliente:	Inmediata.
Nro.INC SVA-CAMBIOS:	20474141

Anexo 2. Validación del cliente



MALL PLAZA PERÚ S.A. || CID.3709342 || SVA-CAMBIOS:20474141 || Crear usuarios VPN con MFA

CC CRISANTO CALLA CHACON <ccalla.hitss@claro.com.pe>
Mié 13/10/2020 13:52

Para: Carmen Ayllon; **Connect - Soporte**
CC: Solicitudes Servicios Gestionados Corporativos <solicitudes_postventa_fija_corporativa@claro.com.pe> **y 3 más**

Estimados;

Cliente informa conformidad con el servicio y autoriza el cierre del caso. Se procederá al cierre del ticket SVA-CAMBIOS: 20474141

Gracias por su apoyo.

Saludos Cordiales,

Crisanto Calla Chacón
FO – Soporte Extendido Premium
GLOBAL HITSS PERÚ - Empresa Colaboradora de América Móvil Perú S.A.C.
Av. Nicolás Arriola 314 Of. 1201 – La Victoria
Telf: 01 6103900 – Anexo: 2103

Anexo 3. Relación de los usuarios con sus respectivos correos para la configuración de autenticación.

Usuario Vpn	Cuenta de correo
yguecha	yarid.guecha@mallplaza.com
jrengifo	Juan.rengifo@mallplaza.com
esaavedra	estefania.saavedra@mallplaza.com
kquintero	Kristhian.quintero@mallplaza.com
jamortegui	John.amortegui@mallplaza.com
dquintero	diego.quintero@mallplaza.com
jruiz	juan.ruiz@mallplaza.com
cmancera	carolina.mancera@mallplaza.com
lcamargo	laura.camargo@mallplaza.com
mmelo	miguel.melo@mallplaza.com
aperez	anny.perez@mallplaza.com
mnova	maria.nova@mallplaza.com
agutierrez	alejandra.gutierrez@mallplaza.com
jacevedo	juan.acevedo@mallplaza.com
dcastro	daniela.castro@mallplaza.com
jgonzalez	juan.gonzalez@mallplaza.com
pbeltran	paula.beltran@mallplaza.com
scamargo	sandra.camargo@mallplaza.com
mdelgado	Maria.delgado@mallplaza.com
mdiaz	Monica.diaz@mallplaza.com
jramirez	john.ramirezb@mallplaza.com
dgonzalez	Daniela.gonzalez@mallplaza.com
hjaraba	harol.jaraba@mallplaza.com
ssuarez	sebastian.suarez@mallplaza.com
csilva	carolina.silva@mallplaza.com
rguzman	Rosnaira.Guzman@mallplaza.com
smontealegre	Sergio.Montealegre@mallplaza.com
vpedraza	Victor.pedraza@mallplaza.com
rcastro	Rosa.Castro@mallplaza.com
mflorez	Madeley.florez@mallplaza.com
fmunoz	Felipe.Munoz@mallplaza.com
myances	Mariaeugenia.Yances@mallplaza.com
lcabarcas	liliana.cabarcas@mallplaza.com
praigosa	paulina.raigosa@mallplaza.com
srodriguez	simon.rodriguez@mallplaza.com
lfontalvo	leidys.fontalvo@mallplaza.com
egonzalez	eduardo.gonzalez@mallplaza.com
asanchez	Alvaro.sanchez@mallplaza.com
mgil	misael.gil@mallplaza.com
ypalacios	yinna.palacios@mallplaza.com
mpinedo	miguel.pinedo@mallplaza.com
jvrgaz	johan.vargas@mallplaza.com
ddonado	daniela.donado@mallplaza.com
lrincon	Luis.rincon@mallplaza.com
ycardenas	yecenia.cardenas@mallplaza.com
jcorreal	juliana.correal@mallplaza.com
csoler	Cristina.soler@mallplaza.com

Anexo 4. Relación de direcciones configuradas en el Firewall.

IP	MASCARA
190.81.174.163	255.255.255.255
192.168.100.2	255.255.255.255
192.168.100.6	255.255.255.255
192.168.100.3	255.255.255.255
206.51.26.33	255.255.255.255
204.187.87.33	255.255.255.255
192.168.100.4	255.255.255.255
192.168.100.0	255.255.255.0
192.168.100.7	255.255.255.255
108.20.1.44	255.255.255.255
192.168.100.61	255.255.255.255
192.168.100.64	255.255.255.255
192.168.100.102	255.255.255.255
192.168.100.111	255.255.255.255
192.168.100.113	255.255.255.255
192.168.1.0	255.255.255.0
192.168.100.0	255.255.255.0
192.168.100.89	255.255.255.255
192.168.10.0	255.255.255.0
192.168.100.110	255.255.255.255
192.168.100.109	255.255.255.255
192.168.100.110	255.255.255.255
192.168.100.134	255.255.255.255
192.168.100.89	255.255.255.255
192.168.100.57	255.255.255.255
192.168.100.125	255.255.255.255
192.168.10.10	255.255.255.255
192.168.100.72	255.255.255.255
192.168.100.121	255.255.255.255
192.168.100.141	255.255.255.255
192.168.100.104	255.255.255.255
192.168.100.127	255.255.255.255
192.168.100.93	255.255.255.255
192.168.100.115	255.255.255.255
192.168.100.54	255.255.255.255
192.168.10.0	255.255.255.0
192.168.100.75	255.255.255.255
192.168.100.79	255.255.255.255
192.168.100.101	255.255.255.255
192.168.100.90	255.255.255.255
192.168.100.86	255.255.255.255

192.168.100.73	255.255.255.255
192.168.100.64	255.255.255.255
192.168.100.107	255.255.255.255
192.168.100.66	255.255.255.255
192.168.100.53	255.255.255.255
192.168.100.113	255.255.255.255
192.168.100.223	255.255.255.255
192.168.100.128	255.255.255.255
192.168.100.111	255.255.255.255
192.168.100.78	255.255.255.255
192.168.100.206	255.255.255.255
192.168.100.34	255.255.255.255
192.168.100.245	255.255.255.255
192.168.100.92	255.255.255.255
192.168.100.74	255.255.255.255
192.168.100.102	255.255.255.255
192.168.100.111	255.255.255.255
192.168.100.61	255.255.255.255
192.168.100.78	255.255.255.255
192.168.100.108	255.255.255.255
192.168.1.0	255.255.255.0
192.168.1.57	255.255.255.255
192.168.100.84	255.255.255.255
192.168.10.8	255.255.255.255
192.168.100.100	255.255.255.255
192.168.100.200	255.255.255.255
192.168.100.251	255.255.255.255
192.168.100.225	255.255.255.255
192.168.100.67	255.255.255.255
192.168.100.140	255.255.255.255
192.168.100.94	255.255.255.255
192.168.100.60	255.255.255.255
192.168.100.204	255.255.255.255
192.168.100.87	255.255.255.255
192.168.100.192	255.255.255.255
192.168.1.198	255.255.255.255
192.168.100.115	255.255.255.255
192.168.100.61	255.255.255.255
192.168.100.245	255.255.255.255
192.168.100.69	255.255.255.255
192.168.100.98	255.255.255.255
192.168.50.5	255.255.255.255
192.168.50.11	255.255.255.255
200.37.63.74	255.255.255.255

192.168.1.56	255.255.255.255
192.168.10.3	255.255.255.255
192.168.100.25	255.255.255.255
192.168.50.0	255.255.255.0
192.168.50.11	255.255.255.255
192.168.50.7	255.255.255.255
192.168.100.56	255.255.255.255
192.168.100.55	255.255.255.255
192.168.100.88	255.255.255.255
192.168.50.6	255.255.255.255
192.168.100.18	255.255.255.255
200.29.143.245	255.255.255.255
192.168.100.0	255.255.255.0
66.235.133.33	255.255.255.255
65.55.171.158	255.255.255.255
192.168.50.100	255.255.255.255
192.168.50.101	255.255.255.255
192.168.50.102	255.255.255.255
192.168.10.11	255.255.255.255
192.168.50.9	255.255.255.255
192.168.100.29	255.255.255.255
192.168.50.3	255.255.255.255
192.168.1.65	255.255.255.255
192.168.50.5	255.255.255.255
213.199.180.150	255.255.255.255
192.168.100.77	255.255.255.255
192.168.1.66	255.255.255.255
192.168.100.24	255.255.255.255
192.168.20.0	255.255.255.0
192.168.100.26	255.255.255.255
192.168.100.74	255.255.255.255
10.110.0.90	255.255.255.255
10.105.17.34	255.255.255.255
192.168.20.0	255.255.255.0
10.96.0.0	255.224.0.0
192.168.100.206	255.255.255.255
192.168.100.103	255.255.255.255
192.168.100.33	255.255.255.255
192.168.100.40	255.255.255.255
192.168.10.18	255.255.255.255
192.168.1.59	255.255.255.255
192.168.100.75	255.255.255.255
192.168.20.18	255.255.255.255
192.168.10.6	255.255.255.255

192.168.10.14	255.255.255.255
192.168.10.9	255.255.255.255
192.168.10.5	255.255.255.255
192.168.10.17	255.255.255.255
192.168.10.2	255.255.255.255
10.1.0.14	255.255.255.255
192.168.100.250	255.255.255.255
192.168.100.124	255.255.255.255
192.168.100.0	255.255.255.0
192.168.100.161	255.255.255.255
192.168.100.86	255.255.255.255
192.168.100.241	255.255.255.255
192.168.100.142	255.255.255.255
192.168.100.109	255.255.255.255
192.168.100.70	255.255.255.255
192.168.100.27	255.255.255.255
192.168.1.63	255.255.255.255
192.168.100.73	255.255.255.255
192.168.100.203	255.255.255.255
192.168.100.38	255.255.255.255
192.168.100.232	255.255.255.255
192.168.100.143	255.255.255.255
192.168.100.172	255.255.255.255
192.168.100.117	255.255.255.255
10.81.215.0	255.255.255.0
192.168.100.130	255.255.255.255
10.81.215.85	255.255.255.255
192.168.100.95	255.255.255.255
192.168.100.105	255.255.255.255
192.168.100.39	255.255.255.255
192.168.100.97	255.255.255.255
192.168.100.134	255.255.255.255
192.168.100.34	255.255.255.255
192.168.100.35	255.255.255.255
192.168.50.17	255.255.255.255
192.168.100.136	255.255.255.255
192.168.100.106	255.255.255.255
192.168.100.32	255.255.255.255
192.168.100.120	255.255.255.255
192.168.100.194	255.255.255.255
192.168.100.166	255.255.255.255
192.168.100.149	255.255.255.255
192.168.100.253	255.255.255.255
192.168.100.78	255.255.255.255

207.210.103.242	255.255.255.255
192.168.100.207	255.255.255.255
192.168.100.164	255.255.255.255
192.168.50.77	255.255.255.255
192.168.100.163	255.255.255.255
216.158.88.226	255.255.255.255
192.168.100.66	255.255.255.255
192.168.100.215	255.255.255.255
192.168.100.104	255.255.255.255
192.168.100.148	255.255.255.255
192.168.100.71	255.255.255.255
192.168.100.138	255.255.255.255
192.168.100.145	255.255.255.255
192.168.100.99	255.255.255.255
192.168.100.221	255.255.255.255
192.168.100.58	255.255.255.255
192.168.100.235	255.255.255.255
192.168.100.31	255.255.255.255
192.168.100.54	255.255.255.255
192.168.10.26	255.255.255.255
54.199.244.219	255.255.255.255
192.168.100.225	255.255.255.255
192.168.100.248	255.255.255.255
192.168.100.2	255.255.255.255
192.168.100.30	255.255.255.255
192.168.100.63	255.255.255.255
192.168.100.48	255.255.255.255
192.168.100.156	255.255.255.255
192.168.100.37	255.255.255.255
192.168.109.0	255.255.255.0
192.168.110.0	255.255.255.0
192.168.181.0	255.255.255.0
192.168.182.0	255.255.255.0
10.15.0.0	255.255.254.0
10.84.233.0	255.255.255.0
10.1.0.0	255.255.254.0
192.168.181.23	255.255.255.255
192.168.181.89	255.255.255.255
192.168.181.15	255.255.255.255
192.168.181.85	255.255.255.255
192.168.181.21	255.255.255.255
192.168.181.46	255.255.255.255
192.168.181.38	255.255.255.255
192.168.181.95	255.255.255.255

192.168.181.120	255.255.255.255
192.168.181.173	255.255.255.255
192.168.182.170	255.255.255.255
192.168.182.206	255.255.255.255
192.168.181.97	255.255.255.255
192.168.181.43	255.255.255.255
192.168.181.161	255.255.255.255
192.168.181.110	255.255.255.255
192.168.181.82	255.255.255.255
192.168.181.172	255.255.255.255
192.168.181.150	255.255.255.255
192.168.181.72	255.255.255.255
192.168.181.14	255.255.255.255
192.168.181.148	255.255.255.255
192.168.181.58	255.255.255.255
192.168.181.167	255.255.255.255
192.168.181.133	255.255.255.255
192.168.181.11	255.255.255.255
192.168.181.132	255.255.255.255
192.168.181.112	255.255.255.255
192.168.50.1	255.255.255.255
192.168.181.56	255.255.255.255
192.168.181.57	255.255.255.255
192.168.181.37	255.255.255.255
192.168.181.70	255.255.255.255
192.168.181.145	255.255.255.255
192.168.181.190	255.255.255.255
192.168.181.79	255.255.255.255
192.168.181.20	255.255.255.255
192.168.181.157	255.255.255.255
192.168.181.140	255.255.255.255
192.168.181.168	255.255.255.255
192.168.181.24	255.255.255.255
192.168.182.175	255.255.255.255
192.168.182.185	255.255.255.255
192.168.182.37	255.255.255.255
192.168.182.12	255.255.255.255
192.168.182.18	255.255.255.255
192.168.182.73	255.255.255.255
192.168.181.28	255.255.255.255
192.168.181.166	255.255.255.255
192.168.182.40	255.255.255.255
192.168.100.42	255.255.255.255
192.168.182.67	255.255.255.255

192.168.182.25	255.255.255.255
151.101.4.84	255.255.255.255
192.168.181.12	255.255.255.255
192.168.181.47	255.255.255.255
192.168.182.13	255.255.255.255
192.168.50.14	255.255.255.255
192.168.50.27	255.255.255.255
192.168.50.28	255.255.255.255
192.168.181.53	255.255.255.255
192.168.182.0	255.255.255.0
192.168.100.0	255.255.255.0
192.168.50.31	255.255.255.255
192.168.50.4	255.255.255.255
185.165.29.78	255.255.255.255
84.200.16.242	255.255.255.255
111.90.139.247	255.255.255.255
72.167.191.69	255.255.255.255
198.71.232.3	255.255.255.255
103.224.212.218	255.255.255.255
172.35.1.112	255.255.255.255
54.85.125.203	255.255.255.255
192.168.182.34	255.255.255.255
192.168.50.29	255.255.255.255
192.168.182.138	255.255.255.255
0.0.0.0	255.255.255.255
192.168.181.45	255.255.255.255
192.168.182.103	255.255.255.255
192.168.182.23	255.255.255.255
192.168.181.67	255.255.255.255
192.168.11.0	255.255.255.0
192.168.182.36	255.255.255.255
10.235.3.200	255.255.255.255
10.85.233.77	255.255.255.255
192.168.182.83	255.255.255.255
192.168.182.79	255.255.255.255
192.168.100.11	255.255.255.255
192.168.181.39	255.255.255.255
190.81.125.126	255.255.255.255
10.1.1.187	255.255.255.255
192.168.62.169	255.255.255.255
192.168.62.148	255.255.255.255
192.168.1.9	255.255.255.255
192.168.50.9	255.255.255.255
192.168.181.9	255.255.255.255

99.61.237.252	255.255.255.255
99.61.237.253	255.255.255.255
67.192.177.156	255.255.255.255
67.192.177.157	255.255.255.255
192.168.182.126	255.255.255.255
192.168.181.49	255.255.255.255
192.168.182.57	255.255.255.255
192.168.182.136	255.255.255.255
192.168.182.26	255.255.255.255
192.168.128.26	255.255.255.255
192.168.50.131	255.255.255.255
192.168.1.136	255.255.255.255
192.168.10.31	255.255.255.255
192.168.10.66	255.255.255.255
10.82.215.30	255.255.255.255
10.82.215.0	255.255.255.0
10.15.1.159	255.255.255.255
10.15.3.0	255.255.255.0
10.181.8.0	255.255.255.0
10.181.9.0	255.255.255.0
10.181.10.0	255.255.255.0
10.2.0.0	255.255.254.0
10.3.0.0	255.255.254.0
10.4.0.0	255.255.254.0
10.5.0.0	255.255.254.0
10.6.0.0	255.255.254.0
10.7.0.0	255.255.254.0
10.8.0.0	255.255.254.0
10.9.0.0	255.255.254.0
10.10.0.0	255.255.254.0
10.11.0.0	255.255.254.0
10.12.0.0	255.255.254.0
10.13.0.0	255.255.254.0
10.17.0.0	255.255.254.0
10.18.0.0	255.255.254.0
10.19.0.0	255.255.254.0
10.21.0.0	255.255.254.0
10.22.0.0	255.255.254.0
10.23.0.0	255.255.254.0
10.181.5.0	255.255.255.0
10.181.7.0	255.255.255.0
192.168.31.0	255.255.255.0
192.168.32.0	255.255.255.0
192.168.33.0	255.255.255.0

192.168.34.0	255.255.255.0
10.15.5.0	255.255.255.0
10.85.233.0	255.255.255.0
172.35.0.0	255.255.255.0
172.35.1.0	255.255.255.0
192.168.62.0	255.255.255.0
192.168.61.0	255.255.255.0
192.168.64.0	255.255.255.0
192.168.65.0	255.255.255.0
192.168.102.0	255.255.255.0
192.168.70.0	255.255.255.0
192.168.71.0	255.255.255.0
10.15.2.0	255.255.255.0
10.15.4.0	255.255.255.0
190.81.125.120	255.255.255.248
104.42.2.34	255.255.255.255
10.88.100.0	255.255.255.0
192.168.1.0	255.255.255.0
192.168.10.0	255.255.255.0
10.90.1.0	255.255.255.0
192.168.0.0	255.255.255.0
192.168.62.73	255.255.255.255
192.168.100.13	255.255.255.255
192.168.0.66	255.255.255.255
8.8.8.8	255.255.255.255
4.2.2.2	255.255.255.255
10.15.1.175	255.255.255.255
10.15.1.175	255.255.255.255
192.168.100.8	255.255.255.255
192.168.63.0	255.255.255.0
10.15.1.149	255.255.255.255
10.85.233.16	255.255.255.255
10.15.1.152	255.255.255.255
192.168.151.0	255.255.255.0
192.168.2.0	255.255.255.0
192.168.10.33	255.255.255.255
10.88.80.135	255.255.255.255
192.168.50.2	255.255.255.255
192.168.43.0	255.255.255.0
10.13.13.0	255.255.255.0
192.168.62.19	255.255.255.255
10.88.100.135	255.255.255.255
192.168.211.0	255.255.255.0
172.22.137.0	255.255.255.0

172.22.138.0	255.255.255.0
172.22.139.0	255.255.255.0
192.168.100.13	255.255.255.255
30.20.10.0	255.255.255.0
149.20.207.7	255.255.255.255
190.223.26.34	255.255.255.255
10.41.55.0	255.255.255.0
192.168.0.0	255.255.255.0
10.10.1.0	255.255.255.252