UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA DE INGENIERÍA ELÉCTRICA

ALTERNATIVAS DE SEGURIDAD DE DATOS EN LA RED LOCAL PARA MEDIANAS Y PEQUEÑAS EMPRESAS

PRESENTADO POR:

CRISTHIAN ALBERTO BUENDÍA ARDÓN

PARA OPTAR AL TÍTULO DE:

INGENIERO ELETRICISTA

CIUDAD UNIVERSITARIA, MAYO DE 2025

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSC. JUAN ROSA QUINTANILLA

SECRETARIO GENERAL:

LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO:

ING. LUIS SALVADOR BARRERA MANCÍA

SECRETARIO:

ARQ. RAÚL ALEXANDER FABIÁN ORELLANA

ESCUELA DE INGENIERÍA ELÉCTRICA

DIRECTOR INTERNO:

ING. WERNER DAVID MELÉNDEZ VALLE

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA DE INGENIERÍA ELÉCTRICA

Trabajo de Graduación previo a la opción al Grado de:

INGENIERO ELECTRICISTA

Título:

ALTERNATIVAS DE SEGURIDAD DE DATOS EN LA RED LOCAL PARA MEDIANAS Y PEQUEÑAS EMPRESAS

Presentado por:

CRISTHIAN ALBERTO BUENDÍA ARDÓN

Trabajo de Graduación Aprobada por:

Docente Asesor:

PhD. CARLOS OSMÍN POCASANGRE JIMÉNEZ

SAN SALVADOR, MAYO 2025

TRABAJO DE GRADUACION APROBADO POR:

Docente Asesor:

PhD. CARLOS OSMÍN POCASANGRE JIMÉNEZ

NOTA Y DEFENSA FINAL

En esta fecha, miércoles 9 de abril de 2025, en la Sala de Lectura de la Escuela de Ingeniería Eléctrica, a las 11:30 a.m. horas, en presencia de las siguientes autoridades de la Escuela de Ingeniería Eléctrica de la Universidad de El Salvador:

1. Ing. Werner David Meléndez Valle
   Director Interino
   Firma

2. MSc. José Wilber Calderón Urrutia
   Secretario
   Firma

Y, con el Honorable Jurado de Evaluación integrado por las personas siguientes:

- DR. CARLOS OSMIN POCASANGRE JIMÉNEZ
  (Docente Asesor)
  Firma
- ING. WERNER DAVID MELÉNDEZ VALLE
  Firma
- ING. LUIS ERNESTO ESCOBAR BRIZUELA
  Firma

Se efectuó la defensa final reglamentaria del Trabajo de Graduación:

ALTERNATIVAS DE SEGURIDAD DE DATOS EN LA RED LOCAL PARA MEDIANAS Y PEQUEÑAS EMPRESAS

A cargo del Bachiller:

- BUENDÍA ARDÓN CRISTHIAN ALBERTO

Habiendo obtenido en el presente Trabajo una nota promedio de la defensa final: 7.3
(Siete punto tres)

AGRADECIMIENTOS

Agradezco primera mente a Dios por brindarme la vida y la voluntad para poder salir adelante en cada una de mis decisiones por darme la fuerza y la visión de poder terminar todo este proceso de enseñanza y aprendizaje.

Agradezco de primeras instancias a mi amada madre, Gracias a ella es este gran logro sus valores, su enseñanza y cada uno de sus apoyos hacia mi persona puedo avanzar en esta siguiente etapa de mi vida.

Agradecido con cada uno de los Ingenieros docentes que me impartió clases en todo este tiempo, por sus enseñanzas, por sus normas por su granito de arena que en estas instancias me hacen un mejor profesional, A mi asesor de Tesis. Dr. Carlos Osmin pocasangre por guiarme en este proceso paso a paso con el fin de tener una experiencia inolvidable en este proceso de Proyecto de graduación, por sus concejos y su enseñanza.

Agradecido de manera enorme con la Sra. Reina Vides por ese apoyo que me ha dado en todos estos años con la documentación con el recordatorio de muchas cosas y hasta el final ayudándome con elevarme la moral siempre la recordare con mucho cariño, finalizando a todas mis amistades que estuvieron conmigo todos estos años estoy muy agradecido con ustedes,

Con el apoyo que me dieron en mi lugar de trabajo estoy muy agradecido por cada una de las lecciones de la vida cotidiana de lo duro que es iniciar desde abajo y por supuesto el valor que se la da a la posición en la que uno pueda llegar a visualizar agradecido con mis compañeros de trabajo.

¡¡MUCHAS GRACIAS POR TODO!!

CRISTHIAN ARDON

INDICE

INDICE DE FIGURAS

PRACTICA 4

PRACTICA 5

PRACTICA 6

INDICE DE TABLAS

SIGLAS Y ACRONIMOS

PYMES: Pequeñas y medianas empresas en el salvador.

LAN: Local Área Network (Redes Locales)

WIFI: Wireless Fidelity (fidelidad inalámbrica)

SGSI :Sistemas de Gestión de la Seguridad de la Información

SOC: Centros de Operaciones de Seguridad

VPN: Red Privada Virtual

WAN: Wide Área Network, o Red de Área Amplia

HFC: Hibrido de Fibra Óptica con Cable coaxial

GPON: Gigabit Passive Optical Network (Red Óptica Pasiva de Gigabit)

VLAN: (Virtual Local Area Network, o Red de Área Local Virtual)

USB: El USB (Universal Serial Bus)

LED: Light Emitting Diode (Diodo Emisor de Luz)

LCM: Liquid Crystal Module (Módulo de Cristal Líquido)

IoT: Internet of Things (Internet de las Cosas)

Proxy ARP: Address Resolution Protocol (Protocolo de resolución de direcciones)

Transición BSS: Basic Service Set Transition (Transición de conjunto de servicios básicos)

UAPSD: Unscheduled Automatic Power Save Delivery (Entrega automática no programada de ahorro de energía)

PMF: Protected Management Frames (Marco de administración protegido)

DHCP: Dynamic Host Configuration Protocol (Protocolod e configuración dinámica)

DNS: Domain Name System (Sistema de Nombres de Dominio)

ISP: Internet Service Provider (Proveedor de Servicios de Internet)

GB: Gibabyt

MB: Megabyt

IPS: Sistema de prevención de intrusos

CAPITULO 1. DESAFÍOS EN LA SEGURIDAD INTERNA DE PEQUEÑAS Y MEDIANAS EMPRESAS

1.1 INTRODUCCION

En la era digital actual, la protección de la información se ha convertido en un pilar fundamental para el éxito y la sostenibilidad de las empresas. Las medianas y pequeñas empresas (PYMES) en El Salvador, aunque son el motor de la economía nacional, enfrentan desafíos significativos en materia de seguridad de datos debido a la falta de recursos, conocimiento técnico y estrategias adecuadas para proteger sus redes locales. Este contexto ha generado un aumento en los riesgos asociados a ciberataques, pérdida de información confidencial y vulneración de la privacidad, lo que puede tener consecuencias devastadoras para estas organizaciones.

Esta tesis tiene como objetivo explorar y proponer alternativas de seguridad de datos viables y accesibles para las PYMES en El Salvador, enfocándose en la protección de sus redes locales. A través de un análisis de las amenazas cibernéticas más comunes, las vulnerabilidades presentes en estas empresas y las soluciones tecnológicas disponibles, se busca proporcionar un marco de referencia que permita a las PYMES implementar medidas de seguridad efectivas sin incurrir en costos excesivos. La relevancia de este estudio radica en su contribución al fortalecimiento de la resiliencia digital de las PYMES, un sector que, aunque vital para la economía, ha sido históricamente subestimado en cuanto a su preparación frente a riesgos tecnológicos. Además, este trabajo pretende servir como guía práctica para empresarios, técnicos y tomadores de decisiones, ofreciendo recomendaciones adaptadas al contexto salvadoreño y a las particularidades de las empresas de menor escala.

En las siguientes secciones, se abordarán los fundamentos teóricos de la seguridad de datos, se analizarán las amenazas más recurrentes en el ámbito local y se presentarán alternativas de seguridad que combinen eficacia, facilidad de implementación y accesibilidad económica. Con este enfoque, se espera contribuir a la creación de un entorno digital más seguro y confiable para las PYMES en El Salvador.

1.2 Objetivos

1.2.1 Objetivo General

Proponer una alternativa de seguridad de datos en la red local para mediana y pequeñas empresas basados en normas internacionales.

1.2.2 Objetivo Especifico

- Proponer una metodología básica para la implementación de la ISO/IEC 27001:2022.
- Seleccionar un equipo que cumpla con la normativa propuesta para poder proteger la información del usuario evitando ataques cibernéticos.
- Diseñar una guía de paso a paso asociada a la instalación y configuración del equipo suministrado en base a los requerimientos de la Norma ISO/IEC.
- Proponer recomendaciones de buenas prácticas de seguridad de la información.

1.3 Alcances

Este estudio se centrará exclusivamente en las medianas y pequeñas empresas (PYMES) de El Salvador, analizando sus necesidades específicas en materia de seguridad de datos y considerando una propuesta para cubrir las necesidades en algún equipo que brinda seguridad interna a la red, La investigación se enfocará en la seguridad de las redes locales (LAN) de las PYMES, abordando temas como la protección de datos internos, la prevención de accesos no autorizados y la mitigación de riesgos asociados a la conectividad interna.
Se identificarán y analizarán las amenazas cibernéticas más frecuentes que afectan a las PYMES en El Salvador, como malware, phishing, ransomware y ataques de ingeniería social, entre otros. El estudio propondrá alternativas de seguridad que sean económicamente viables y técnicamente factibles para las PYMES, priorizando soluciones de bajo costo y fácil implementación.
La investigación tendrá en cuenta el contexto tecnológico, legal y económico de El Salvador, incluyendo normativas locales relacionadas con la protección de datos y la ciberseguridad.
No incluye grandes empresas o entidades gubernamentales: Este trabajo no abordará la seguridad de datos en grandes corporaciones o instituciones gubernamentales, ya que sus necesidades y recursos difieren significativamente de las PYMES.
Aunque se mencionarán brevemente los riesgos asociados a las redes externas (como Internet), el enfoque principal estará en la seguridad de las redes internas (LAN). El estudio incluirá recomendaciones prácticas para la implementación de medidas de seguridad, pero no abarcará la ejecución técnica directa en empresas específicas.

1.4 Marco teórico

1.5 Antecedentes

En los últimos años, la digitalización de los procesos empresariales ha transformado la forma en que las organizaciones operan, almacenan y comparten información. Sin embargo, este avance tecnológico también ha traído consigo un aumento significativo de los riesgos cibernéticos. Según un informe de la Unión Internacional de Telecomunicaciones (UIT), El Salvador se encuentra entre los países de América Latina con mayor exposición a ciberataques, especialmente dirigidos a pequeñas y medianas empresas (PYMES), que representan más del 90% del tejido empresarial del país. Estudios previos, como el realizado por la Cámara de Comercio e Industria de El Salvador en 2022, revelaron que el 60% de las PYMES en el país han experimentado al menos un incidente de seguridad informática en los últimos tres años. Estos incidentes incluyen robos de información confidencial, ataques de ransomware y violaciones de la privacidad de clientes. A pesar de esto, solo el 20% de estas empresas cuenta con medidas de seguridad básicas, como firewalls o software antivirus actualizado, lo que evidencia una falta de conciencia y preparación frente a las amenazas digitales. A nivel internacional, organizaciones como el Foro Económico Mundial han destacado la importancia de la ciberseguridad para las PYMES, señalando que estas empresas son particularmente vulnerables debido a sus limitaciones financieras y técnicas. En América Latina, países como México y Colombia han implementado programas gubernamentales para fomentar la adopción de prácticas de seguridad informática en las PYMES. Sin embargo, en

El Salvador, las iniciativas en este ámbito son incipientes y no existen políticas públicas específicas que aborden las necesidades de seguridad digital de este sector. En el ámbito académico, investigaciones como la de García et al. (2021) han explorado soluciones de seguridad para PYMES en otros países de la región, proponiendo modelos de bajo costo basados en software libre y buenas prácticas de gestión de redes. No obstante, estas propuestas no han sido adaptadas al contexto salvadoreño, donde factores como la infraestructura tecnológica, el acceso a internet y la cultura empresarial presentan particularidades que requieren un enfoque específico. En este sentido, la presente investigación busca llenar un vacío en la literatura y en la práctica, ofreciendo alternativas de seguridad de datos adaptadas a las necesidades y realidades de las PYMES en El Salvador. Al hacerlo, se espera contribuir no solo a la protección de la información empresarial, sino también al fortalecimiento de la competitividad y la sostenibilidad de este sector clave para la economía nacional.

1.6 Planteamiento del problema

La ciberseguridad es la práctica de proteger sistemas, redes y datos del acceso no autorizado, el uso, la divulgación, la interrupción, la modificación o la destrucción. En pocas palabras, es la seguridad de todo lo que está conectado a internet. Nuestro país ha reconocido la importancia de la ciberseguridad y ha implementado diversas iniciativas para proteger la infraestructura crítica y los datos de sus ciudadanos. Algunas de estas iniciativas incluyen: Estrategia Nacional de Ciberseguridad, Centros de Operaciones de Seguridad (SOC), y programas de capacitación. Las pequeñas y medianas empresas en nuestro país se ven expuestas a este tipo de problemas y no tienen la capacidad o el acceso a estos recursos, por lo tanto, el presente trabajo tiene como finalidad proponer alternativas de bajo costo.
Se pretende en el documento proporcionar con las mejores las mejores propuestas en ciberseguridad, reflejando las mejores prácticas comunes disponibles públicamente, que se derivan de un consenso entre expertos internacionales con una amplia variedad de habilidades, conocimientos y experiencia en el tema. Se agregará también, orientación adicional para implementar los requisitos de la norma ISO/IEC 27001:2022 y NIST SP 800-53 que se define como Sistemas de Gestión de la Seguridad de la Información (SGSI). La adopción traerá beneficios a la empresa como: Resistencia a los ciberataques, Preparación ante nuevas amenazas, Integridad, confidencialidad y disponibilidad de la información, Seguridad en todos los soportes, Protección en toda la empresa, y Ahorro de costos. El equipo propuesto deberá se capaz de manejar velocidades de internet mayores a 50 Mbps, que se logre integrar a otros sistemas, para poder instalarlo y configurarlo mostrando su generalidad su funcionalidad y su descripción general. Se presente el uso del equipo de protección para la red de seguridad y explicación y concientización a su importancia dirigido hacia pequeñas y medianas empresas.

1.7 Justificación

En un mundo cada vez más digitalizado, la seguridad de los datos se ha convertido en un aspecto crítico para la operación y sostenibilidad de las empresas. Sin embargo, las medianas y pequeñas empresas (PYMES) en El Salvador enfrentan desafíos significativos en este ámbito debido a la falta de recursos económicos, conocimiento técnico y estrategias adecuadas para proteger su información. Esta situación las hace especialmente vulnerables a

ciberataques, que pueden resultar en pérdidas financieras, daños a la reputación y, en casos extremos, el cierre definitivo de los negocios.
La importancia de este estudio radica en su enfoque en un sector que, aunque representa más del 90% del tejido empresarial del país y es un motor clave para la economía nacional, ha sido históricamente descuidado en materia de ciberseguridad. Según datos de la Cámara de Comercio e Industria de El Salvador, el 60% de las PYMES han experimentado al menos un incidente de seguridad informática en los últimos años, y la mayoría carece de medidas básicas de protección. Este vacío no solo pone en riesgo a las empresas individuales, sino que también afecta la confianza de los consumidores y la competitividad del país en el mercado global.
Además, la investigación es relevante porque propone soluciones accesibles y adaptadas al contexto salvadoreño. Muchas de las alternativas de seguridad disponibles en el mercado están diseñadas para grandes corporaciones con presupuestos amplios y equipos técnicos especializados, lo que las hace inalcanzables para las PYMES. Este estudio busca cerrar esa brecha, ofreciendo recomendaciones prácticas, económicas y fáciles de implementar que permitan a estas empresas proteger sus redes locales sin incurrir en costos prohibitivos.
Desde una perspectiva social, el fortalecimiento de la seguridad de datos en las PYMES contribuye a la creación de un entorno empresarial más seguro y confiable, lo que a su vez fomenta la innovación, el empleo y el crecimiento económico. Asimismo, este trabajo puede servir como base para futuras investigaciones y políticas públicas que promuevan la ciberseguridad en el sector empresarial salvadoreño.

En resumen, esta tesis no solo aborda un problema urgente y desatendido, sino que también ofrece soluciones viables que pueden tener un impacto tangible en la protección de la información, la sostenibilidad de las PYMES y el desarrollo económico de El Salvador.

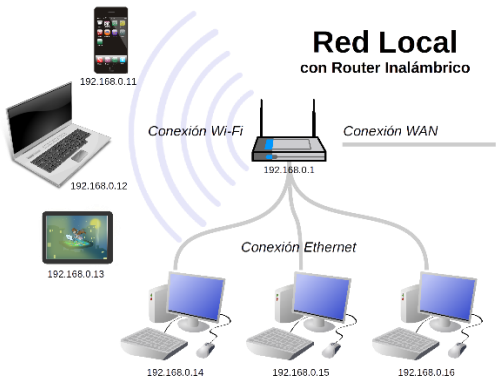
1.8 Conceptos básicos de seguridad en la red local

1.8.1 Red Local (LAN)

Una red de área local (LAN, por sus siglas en inglés) es un conjunto de dispositivos interconectados dentro de un área geográfica limitada, como una oficina, un edificio o un campus. Las LAN permiten compartir recursos, como impresoras, archivos y conexiones a internet, entre los dispositivos conectados.

FIGURA 1

Topología de una red local



Nota. Representación de una Red local convencional Fuente: (Kinetic, 2022)

1.8.2 Seguridad en la red Local

Se refiere a las medidas y prácticas diseñadas para proteger los datos, dispositivos y usuarios dentro de una LAN contra accesos no autorizados, ataques cibernéticos y otras amenazas. La seguridad de la red local es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información.

1.8.3 Amenazas en una red LAN

- Malware: Software malicioso, como virus, gusanos y ransomware, que puede infectar los dispositivos de la red.
- Ataques de phishing: Intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas.
- Accesos no autorizados: Intrusos que obtienen acceso a la red sin permiso, ya sea desde dentro o fuera de la organización.
- Ataques de denegación de servicio (DoS): Intentos de sobrecargar la red para que deje de funcionar.
- Interceptación de datos: Robo de información transmitida a través de la red.

1.8.4 Medidas de seguridad básicas

- Firewalls: Dispositivos o software que filtran el tráfico entrante y saliente, bloqueando accesos no autorizados.
- Contraseñas fuertes: Uso de contraseñas complejas y únicas para acceder a dispositivos y sistemas de la red.
- Actualizaciones de software: Mantener todos los sistemas y aplicaciones actualizados para corregir vulnerabilidades.

- Encriptación: Protección de datos mediante técnicas que los convierten en información ilegible para personas no autorizadas.
- Segmentación de la red: Dividir la red en subredes para limitar el acceso a áreas críticas.

1.8.5 Protocolos de seguridad

- WPA3 (Wi-Fi Protected Access 3): El estándar más reciente para proteger redes inalámbricas.
- VPN (Red Privada Virtual): Conexiones seguras que permiten a los usuarios acceder a la red de forma remota de manera cifrada.
- IEEE 802.1X: Protocolo de autenticación para controlar el acceso a la red.

1.8.6 Gestión de Usuarios y permisos

- Autenticación: Verificación de la identidad de los usuarios antes de permitirles el acceso a la red.
- Control de acceso: Asignación de permisos específicos a usuarios o grupos para limitar su acceso a ciertos recursos.
- Auditorías: Monitoreo y registro de actividades en la red para detectar comportamientos sospechosos.

1.8.7 Copia de seguridad (Back up)

Realizar copias periódicas de los datos críticos para garantizar su recuperación en caso de pérdida, robo o daño.

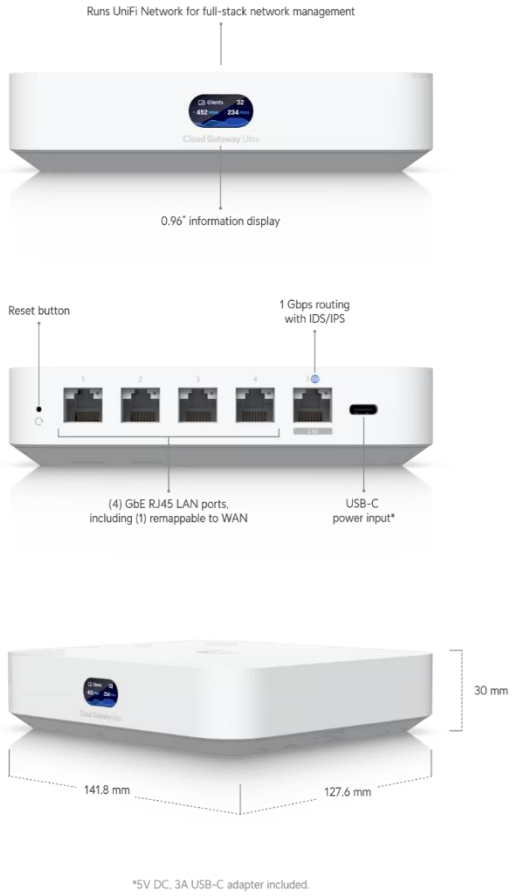
CAPITULO 2. ALTERNATIVA EN EQUIPO PARA LA SEGURIDAD DE LA RED EN PEQUEÑAS Y MEDIANAS EMPRESAS

2.1 Equipo Ubiquiti Cloud Gateway Ultra

El Ubiquiti Cloud Gateway Ultra es una solución todo en uno que combina rendimiento, seguridad y facilidad de gestión, diseñada específicamente para PYMES y profesionales que buscan una red confiable y escalable. Su integración con el ecosistema UniFi lo convierte en una opción atractiva para quienes necesitan una solución robusta pero sencilla de administrar.

FIGURA 2

Equipo UCG-ULTRA y sus características físicas



Nota. La figura muestra Equipo físico ubiquiti cloud Gateway ultra. Fuente: UniFi (2022)

2.2 Características del dispositivo Ubiquiti Cloud Gateway Ultra

UniFi Cloud Gateway Ultra es una pequeña pero potente puerta de enlace UniFi multi-WAN. La puerta de enlace viene con 4 puertos LAN incorporados, de los cuales uno se puede reasignar a un segundo puerto WAN. Su diseño pequeño y limpio le permite colocar

fácilmente este Cloud Gateway en un lugar más cercano o incluso colocarlo a la vista en un armario o estantería.

Como su nombre lo indica, Cloud Gateway Ultra es una puerta de enlace y una consola en la nube en uno. Esto significa que no necesita una UniFi Cloud Key u otra consola para administrarlo. Se ejecuta en el sistema operativo UniFi con solo la aplicación de red UniFi, por lo que solo necesita conectarse a Internet para ponerlo en funcionamiento.

A pesar de su pequeño factor de forma, el Cloud Gateway Ultra sigue siendo bastante potente. Puede enrutar el tráfico con velocidades de hasta 1 Gbit por segundo, con IDP e IPS activados. Y, por supuesto, también es compatible con VPN, VLAN y site-magic.

Tabla 1

Especificaciones técnicas en las características internas del Equipo UCG-Ultra

Especificaciones	
CPU	Quad-core ARM® Cortex®-A53 (IPQ5322) at 1.5 GHz
Memoria	3 GB
Almacenamiento	16 GB eMMC
Pantalla	0.9″ display
Máxima conexión IPS/IDS	1 Gbps
Puertos WAN	1x 2.5 GbE RJ45
Puertos LAN	4x Gigabit RJ45
Alimentación	USB C (5V / 3A)
Consumo	6.2 Watt
Dimensiones	142 x 127 x 30 mm
Supported Clients	300+
Supported UniFi Devices	30+
IDS and IPS Threat detection	Yes
Built-in Access Point	No (Necesita un AP externo)
Wireguard VPN / Site-Magic Throughput	500 Mbps
Routing Performance without IPS/IDS	1 Gbps

Routing Performance with IPS/IDS	1 Gbps

Nota. Especificaciones técnicas de equipo ubiquiti cloud Gateway ultra (2022)

Como puede ver en las especificaciones anteriores, admite conexiones de puerto WAN de hasta 2,5 Gbit por segundo. Sin embargo, los puertos LAN son solo de 1 Gbit, esto solo significa que no puede utilizar completamente la conexión WAN de 2.5 Gbit con un solo cliente.

Ahora, normalmente se puede utilizar, por ejemplo, la agregación de enlaces, en la que se combinan dos puertos LAN como uno solo, lo que permite duplicar el rendimiento. Pero eso no es posible en Cloud Gateway Ultra. E incluso si eso fuera posible, hay otro problema.

Todos los puertos LAN juntos también están limitados a 1 Gbps que van aguas arriba al puerto WAN (fuente). Esto significa que incluso dos clientes no podrán descargar un archivo con 1 Gbit por segundo simultáneamente.

En pocas palabras, solo puede usar una conexión WAN de hasta 1 Gbit por segundo.

2.2.1 Wireguard VPN y Site Magic

Las conexiones VPN son excelentes para la seguridad o incluso necesarias en entornos empresariales para obtener acceso a los recursos de la empresa. Pero siempre tienen un costo, y es la velocidad de conexión. Una conexión VPN simplemente requiere mucha potencia de procesamiento, lo que se traduce en un menor rendimiento.

Con UniFi Cloud Gateway Ultra, no podrás mantener la conexión WAN de 1 Gbit cuando utilices una VPN, pero debería ser capaz de alcanzar velocidades de hasta 500 Mbit por segundo cuando utilices Wireguard VPN o Site-Magic.

2.2.1 Pantalla

Al igual que el recientemente lanzado UniFi Express, viene el UCG-Ultra con una pequeña pantalla LCM de 0,96 pulgadas que solo se usa para mostrar el estado del dispositivo. No es una pantalla táctil, por lo que no podemos usarla para deslizar el dedo por la configuración o reiniciar el dispositivo.

2.2.3 Gestión Centralizada a Través de UniFi:

- El dispositivo se integra con el ecosistema UniFi de Ubiquiti, permitiendo una gestión centralizada y remota de la red a través de la interfaz UniFi Network Application.
- Ideal para administrar múltiples dispositivos y redes desde una sola plataforma.

2.2.4 Alto Rendimiento:

- procesador de cuatro núcleos y memoria RAM suficiente para manejar redes con alto tráfico.
- Soporta velocidades de internet de hasta 1 Gbps (dependiendo de la configuración y el proveedor de servicio**s).**

2.2.5 Conectividad segura:

- Incluye funciones avanzadas de seguridad, como firewall integrado, VPN (Site-to-Site y Client VPN), y soporte para VLANs.
- Protección contra amenazas en tiempo real con Intrusion Detection System (IDS) y Intrusion Prevention System (IPS).

2.2.6 Diseño Compacto y Eficiente:

- Diseño pequeño y silencioso, ideal para entornos de oficina o pequeños centros de datos.
- Bajo consumo de energía, lo que lo hace eficiente y económico para operar.

2.2.7 Conectividad y Puertos:

- Puertos Ethernet: Varios puertos Gigabit Ethernet para conectar dispositivos locales, como switches, puntos de acceso y servidores.
- Puerto WAN: Para la conexión a internet.
- USB-C: Para alimentación y futuras expansiones.

2.2.8 Escalabilidad:

- Compatible con otros dispositivos UniFi, como puntos de acceso inalámbricos, switches y cámaras de seguridad, lo que permite escalar la red según las necesidades del negocio.

2.2.9 Actualizaciones Automáticas:

- Recibe actualizaciones de firmware automáticamente para mantener la seguridad y el rendimiento al día.

2.3 Ventajas para pequeñas y grandes empresas

2.3.1 Fácil Implementación:

La configuración inicial es sencilla gracias a la interfaz intuitiva de UniFi y las guías paso a paso.

2.3.2 Ahorro de Costos:

Al integrar múltiples funciones (gateway, firewall, VPN) en un solo dispositivo, se reduce la necesidad de hardware adicional.

2.3.3 Seguridad Profesional:

Las funciones de IDS/IPS y VPN ofrecen un nivel de seguridad comparable al de soluciones empresariales más costosas.

2.3.4 Monitoreo y Análisis:

La plataforma UniFi proporciona herramientas avanzadas para monitorear el tráfico, identificar cuellos de botella y optimizar el rendimiento de la red.

CAPITULO 3. MANUAL DE USO Y CONFIGURACIÓN PARA EQUIPO UBIQUITI CLOUD GATEWAY ULTRA

3.1 GUIA #1 INSTALACION DE EQUIPO UNIFI UBIQUITI CLOUD GATEWAY

INTRODUCCION

En la presente practica se explicará los primeros pasos para conectar a un equipo UBIQUITI CLOUD GATEWAY sus partes externas y funcionalidades internas. Se pretende en esta guía de laboratorio instruirlo para que pueda instalarlo de forma fácil segura y correcta.

OBJETIVO GENERAL

- Detallar el proceso en el cual el usuario será capaz de instalar de manera correcta el equipo UNIFI llamado "UBIQUITI CLOUD GATEWAY" dejándolo conectado y listo para su uso.

OBJETIVOS ESPECIFICO

- Instruir al usuario para la instalación física del equipo UNIFI
- Crear Usuario en Unifi OS utilizando dirección IP
- Instalar aplicación móvil adecuada al sistema operativo

DESARROLLO DE LA PRACTICA

El Equipo UNIFI UBIQUITI CLOUD GATEWAY es un dispositivo compacto de seguridad de red es de la serie de UNIFI, es diseñado específicamente para albergar una cantidad considerable de usuarios dedicado a pequeñas y medianas empresas.

- Dimensiones:
    - Ancho: 141.8 mm (5.6")
    - Profundidad: 127.5mm (5")
    - Altura:30mm (1.2")
- Puertos WAN predeterminados
    - 1 RJ45 de 2.5GbE
- Puertos LAN

    - 4 GbE RJ 45
- Alimentación
    - Entrada de Alimentación 120-240 VAC
    - Consumo Máximo 6.2W
- Pantalla
    - Pantalla LCM de estado 0.96”
    - Administrable vía blouthout
- Software en Aplicación Móvil
    - UniFi iOS™: versión 10.12.0 y posteriores
    - UniFi Android™: Versión 10.11.2 y posteriores

El equipo UCG-ULTRA es conocido por su pequeño tamaño y gran eficiencia ideal para implementar seguridad avanzada en redes de oficinas con espacios y equipos limitados.

Figura 1_1

Equipo UCG-Ultra

Nota. La figura muestra el detalle de puertos UCG-ULTRA. Fuente: UniFi (2022)

Paso 1. Como primer paso sacaremos el equipo de su caja y podremos observar los componentes que trae directamente, Su fuente de poder 120Vac un cordón UTP y una base para pegar en superficies verticales

Figura 1_2

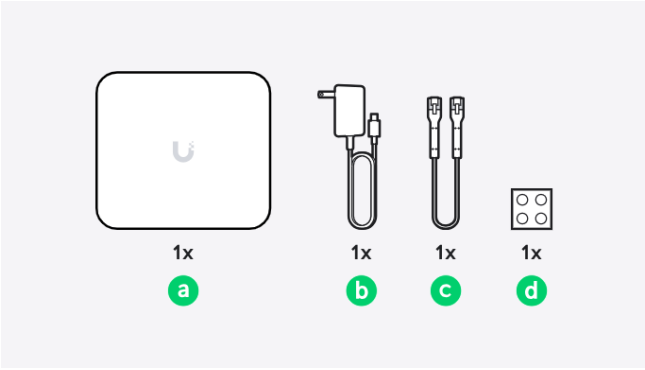
Accesorios dentro de la caja en el equipo UCG-Ultra

Nota. La figura muestra el Equipo UNIFI con sus accesorios. Fuente: UniFi (2022)

1.2 Preparado el equipo procederemos a su conexión de la siguiente manera:

Figura 1_3

Representación en los accesorios en orden dentro de Caja



Nota. La figura muestra los Accesorios asignados por orden. Fuente UniFi (2022)

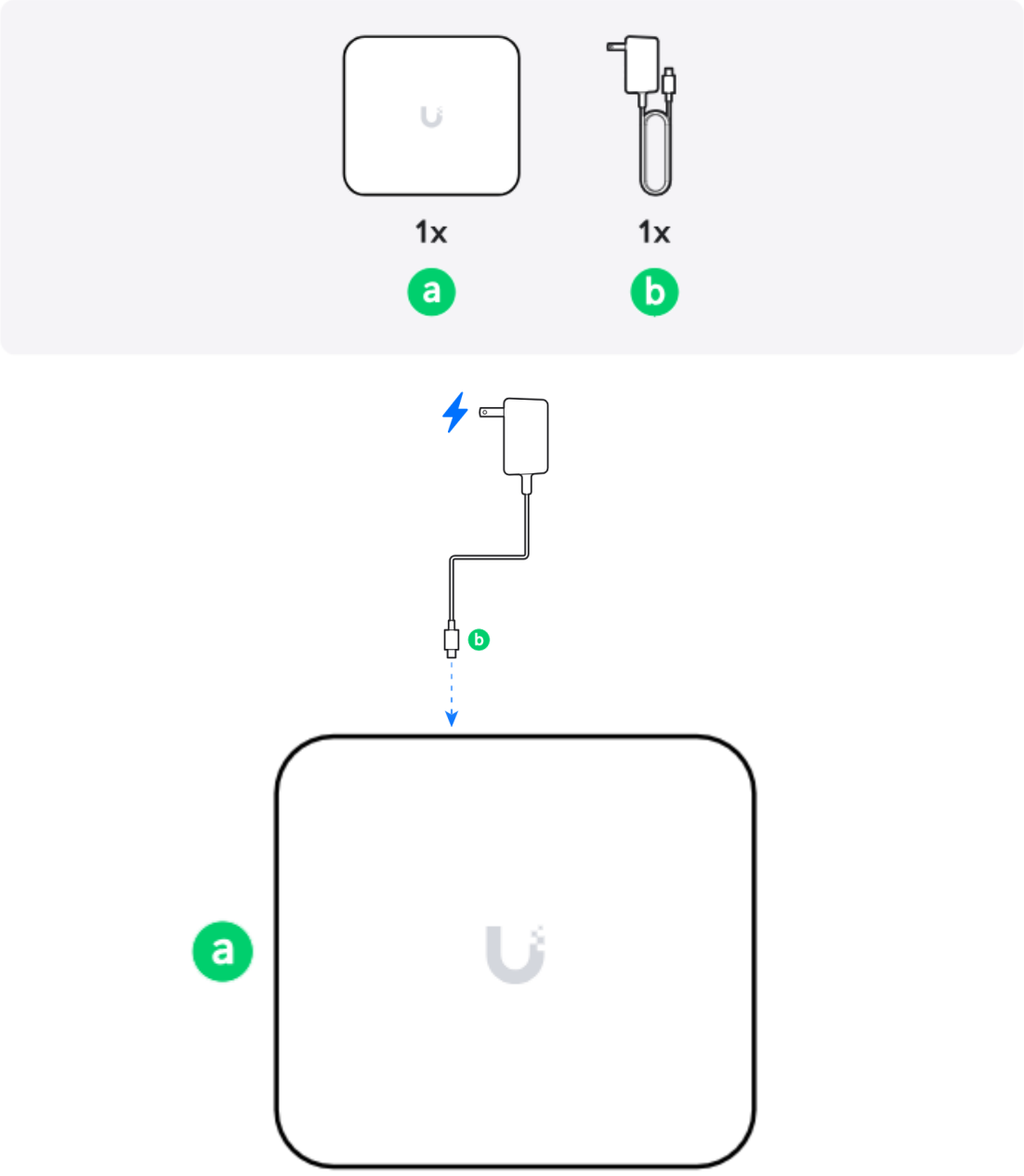
a. Equipo Unifi
b. Fuente de poder 120Vac
c. Cable UTP

d. Base para superficies verticales

PASO 2. Conectaremos El equipo UNIFI a su fuente de poder al mismo tiempo conectando punto de red al equipo

Figura 1_4

Conexión Física de equipo UCG-Ultra con accesorios.

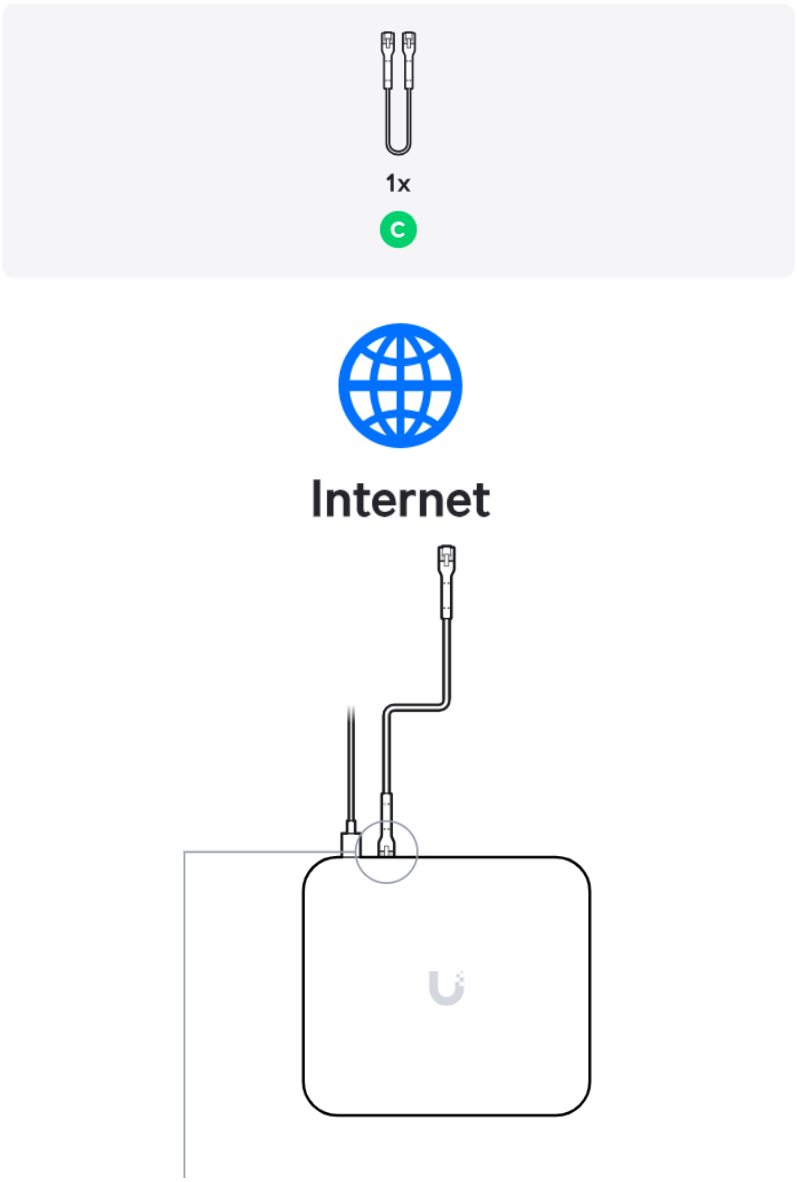


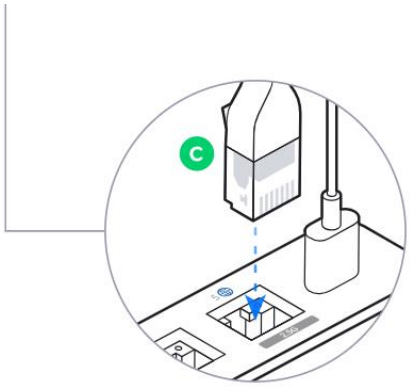
Nota. La figura muestra la Conexión de equipo con su respectiva fuente. Fuente UniFi (2022).

PASO 3. Conectaremos el equipo a la red, podríamos utilizar el cable UTP que viene en la caja del equipo, o se podría utilizar un UTP CAT 6 creado por uno mismo adecuando la cantidad de metros entre la conexión del equipo y el Router.

FIGURA 1_5

Conexión a internet Local





Nota. La figura muestra la Conexión a red de internet al equipo UCG-Ultra. Fuente: UniFi (2022)

Paso 4. Como siguiente punto el equipo ya está instalado e inicializando ahora descargaremos la aplicación en el celular del usuario para tener control adicional del equipo UNIFI.

Figura 1_6

Descarga de aplicación bajada de IOS o Playstore según sistema operativo

Nota. La figura muestra la Aplicación de UNIFI. Fuente: UniFi(2022)

Paso 5. Luego se entrelazarán con la aplicación UNIFI en su celular para estar conectados y monitorear equipo y se inicializara en la PC para su configuración. Cabe destacar que la conexión inicial será vía bluetooth con el nombre UNIFI.

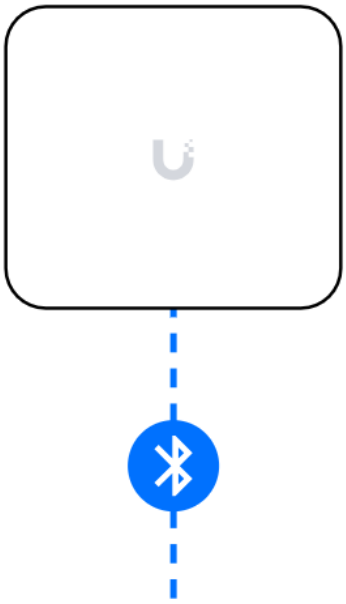
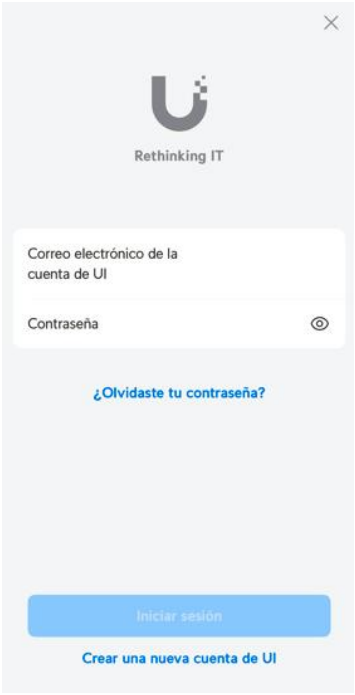


Figura 1_7. Conexión vía bluetooth de equipo UNIFI

Paso 6. Para el siguiente paso crearemos la cuenta ya sea en el dispositivo móvil o en la PC ambas se hacen de la misma manera con validación de correo, cabe destacar que ser parte de usuario UNIFI es gratuito y tendrá acceso también

FIGURA 1_7

Inicio de sesión para ingreso a equipo



Nota. La figura muestra el Crear Usuario en la plataforma UniFi. Fuente: UniFi(2022)

Paso 7. Para el siguiente paso se va a validar en el correo correspondiente para validar cuenta con los dos pasos y terminar instalando el equipo UCG-ULTRA.

CONCLUCION

- La administración del UCG-ULTRA se puede configurar mediante conexión móvil o mediante PC conectado por cable ethernet.
- Se tiene que crear cuenta en la página Unifi para poder ser usurario directo y poder iniciar sesión de manera gratuita.
- De manera sencilla se puede instalar el equipo físico sin tener muchas complicaciones.

3.2 GUIA # 2 DESCRIPCION DE EQUIPO UNIFI UBIQUITI CLOUD GATEWAY INTRODUCCION

En la siguiente guía se pretende enseñar al usuario a crear una cuenta en la plataforma debido a que para el equipo UCG-ULTRA se debe ingresar con usuario. Entender cada una de las características iniciales de la pantalla principal del equipo UCG-ULTRA.

OBJETIVO GENERAL

Aprender a identificar cada uno de los iconos en el panel de control y sus funciones, cada una de sus partes y sus características principales.

OBJETIVO ESPECIFICO

- Crear usuario para inicializar la configuración en el equipo UCG-ULTRA
- Enseñar paso a paso la configuración inicial del quipo UCG-ULTRA
- Mostrar de manera clara la pantalla principal y explicar cada uno de sus menús y para que funcionan

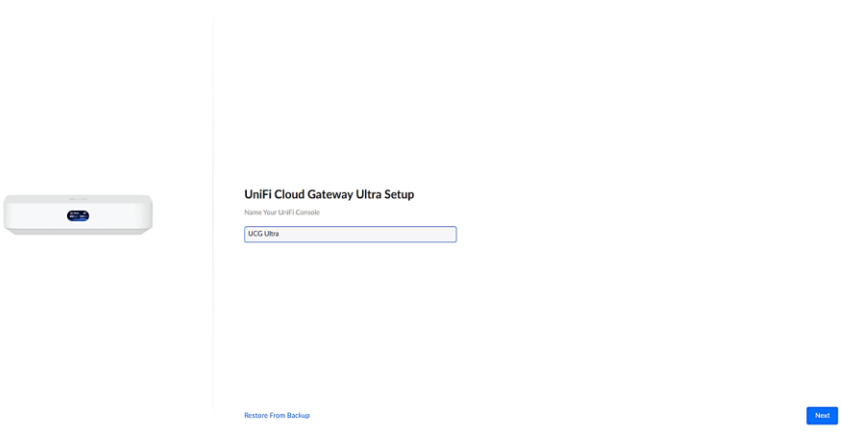
DESARROLLO

En esta práctica se pretende iniciar con la configuración general de equipo UCG-ULTRA, ya que el equipo está instalado de manera física y encendido y conectado específicamente en el puerto 5, ahora se pretende verlo internamente. En esta guía se explicará cómo configurar el dispositivo desde la computadora para fines prácticos.

Paso 1. Como primer paso. Se conecte uno de los puertos del equipo UCG-ULTRA a una PC se abrirá automáticamente o si no se puede ingresar con la dirección IP a la cual está conectada directamente por ser servidor de CLARO se ingresa 192.168.1.110 para el inicio de la configuración del equipo iniciando con el nombre que se le requiere poner al equipo UCG- ULTRA,

Figura 2_1

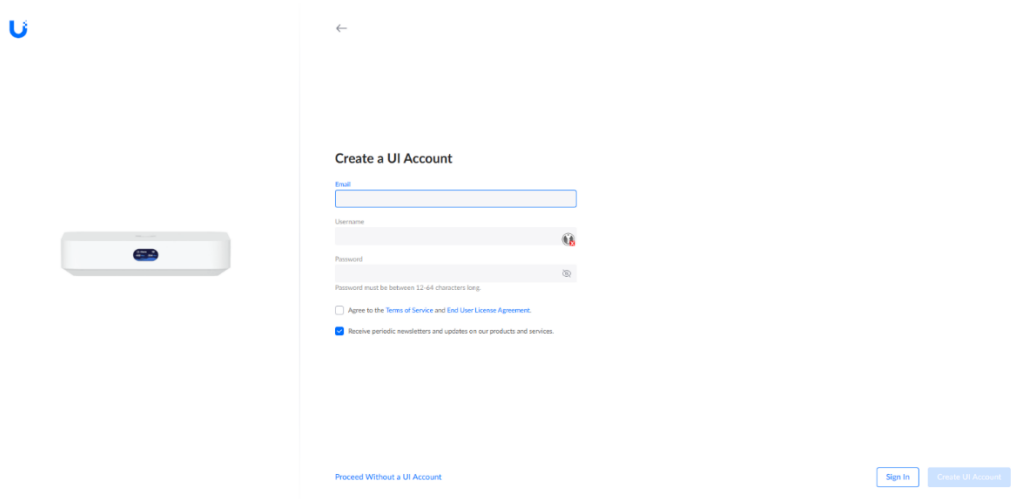
Inicio en Configuración externa de equipo UCG-Ultra



Nota. La figura muestra el Nombre asignado a equipo. Fuente: UCG-Ultra (2024)

Figura 2_2

Creación de usuario para ingresar a equipo

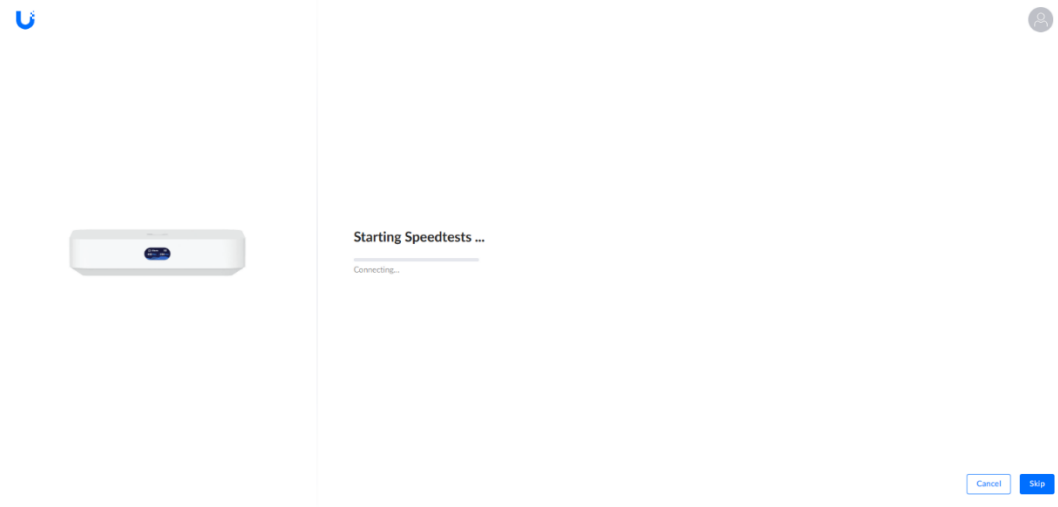


Nota. La figura muestra el Ingreso de credenciales a equipo UNIFI. Fuente: UCG-Ultra (2024)

Paso 2. Ahora que ya se validó correo ingresaremos directamente a nuestro equipo UCG-ULTRA véase la figura 2_3, A continuación, la pestaña principal que se abrirá será un Speed test automático para verificar como está la conexión a internet, como se muestra en la figura 2_4.

Figura 2_3

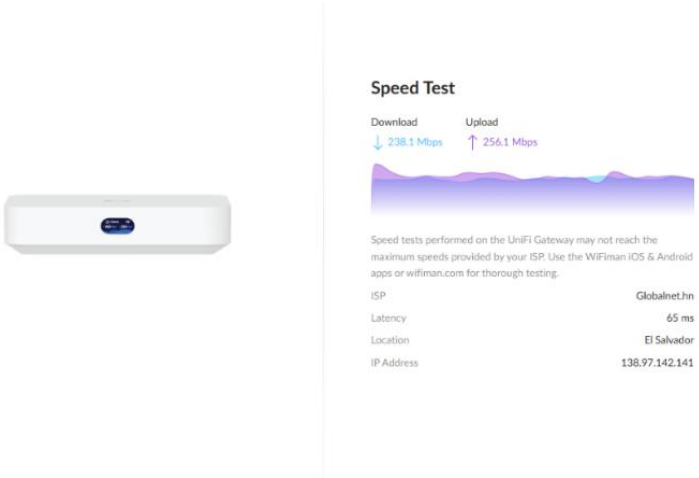
Iniciando sistema en UCG-Ultra



Nota. La figura muestra el proceso luego de ingresar credenciales. Fuente: UCG-Ultra(2022)

Figura 2_4

Se realiza test de velocidad automatica al ingresar al equipo

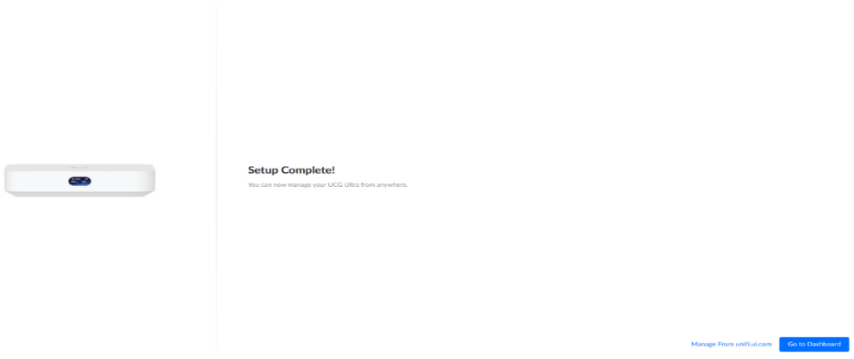


Nota. La figura muestra los Valores de velocidad de subida y de bajada registrados en equipo Fuente: UCG-Ultra (2022)

Paso 3. Una vez ya se termine es test de velocidad la configuración inicial estará completa y se nos abrirá un panel de control como se muestra en la figura 2_6

FIGURA 2_5

La configuración se completo y se procede al inicio del funcionamiento del equipo.



Nota. La figura muestra la Configuración en red completada. Fuente: UCG-Ultra (2024)

Paso 4. Ahora podemos observar el panel de control y podremos ver la medida de datos usados en determinados periodos de tiempo y algunos sitios y protocolos que se utilizan en la red, tanto en la red cableada cono en la red inalámbrica mostrados en la Figura 2_6

FIGURA 2_6

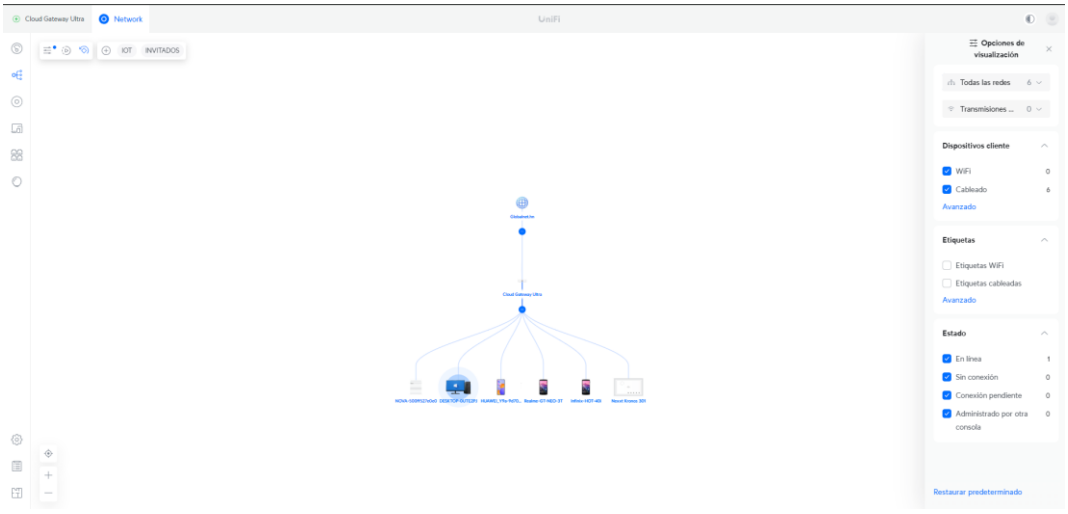
Panel de control mostrando actividad en consumo de ancho de banda

Nota. En la figura se puede observar el Panel de control de equipo. Fuente: UCG-Ultra (2024)

Paso 5. En la parte izquierda podremos observar un grupo de iconos los cuales son para visualizar de distintas formas las conexiones del equipo UNIFI, actualmente nos encontramos en el Panel del control, en el siguiente apartado veremos la topología de red aquí podremos ver los dispositivos conectados a la red y si tenemos dispositivos de ubiquiti podremos ver una jerarquía, por ejemplo, Aps, switch, extensores de red, Figura 2_7

Figura 2_7

Topología de la red en ese momento de la toma de lectura en panel de control

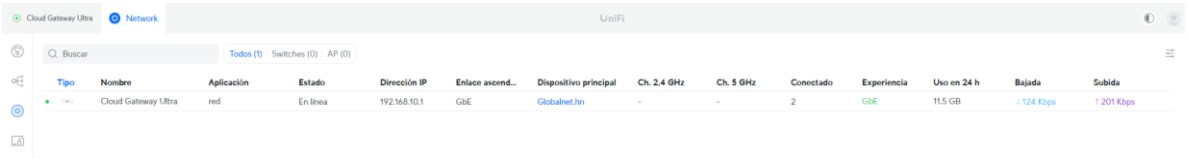


Nota. Como se muestra en la figura se plasma la Topología de red con los equipos conectados. Fuente: UCG-Ultra(2024).

Esta otra pantalla son los dispositivos de la marca Ubiquiti únicamente contando como otros equipos Gateway los que se podrán observar en la figura 2_8

Figura 2_8

Menu de network dispositivos conectados en equipo.

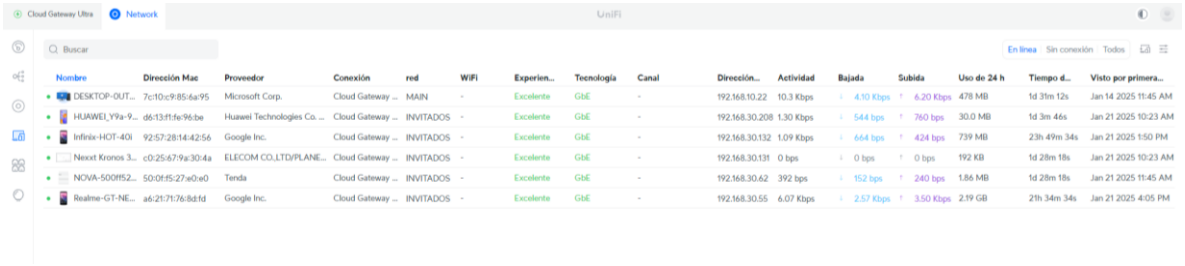


Nota. En la figura se observa los Dispositivos conectados en equipo. Fuente: UCG-Ultra(2024)

En la figura 2_9 se puede ver el siguiente icono podrán observarse la cantidad de clientes conectados por vía wifi o conectados mediante cable de red y se observan en forma de lista.

Figura 2_9

Cantidad de clientes conectados directamente en la red Lan del equipo



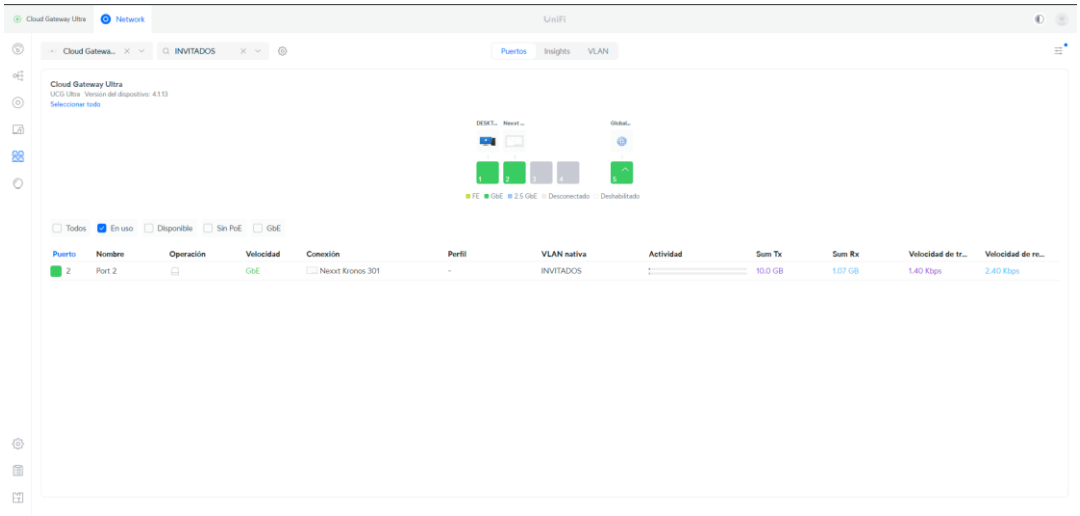
Nota. La figura muestra una Lista de Clientes conectados desde cualquier dispositivo conectado a la red. Fuente: Ucg-Ultra (2024).

En el siguiente icono se podrá observar la administración de puertos del dispositivo, aquí puedes asignar vlans a determinado puerto, por ejemplo, si yo tengo un AP que no es de la marca Ubiquiti puedo ponerlo en modo puente y aislar este puerto asignándole un vlan, solo para ese puerto y claro está desde el firewall evitar el tráfico entre vlans.

Además, se puede limitar el tráfico de red por puerto.

Figura 2_10

Puertos conectados en equipo

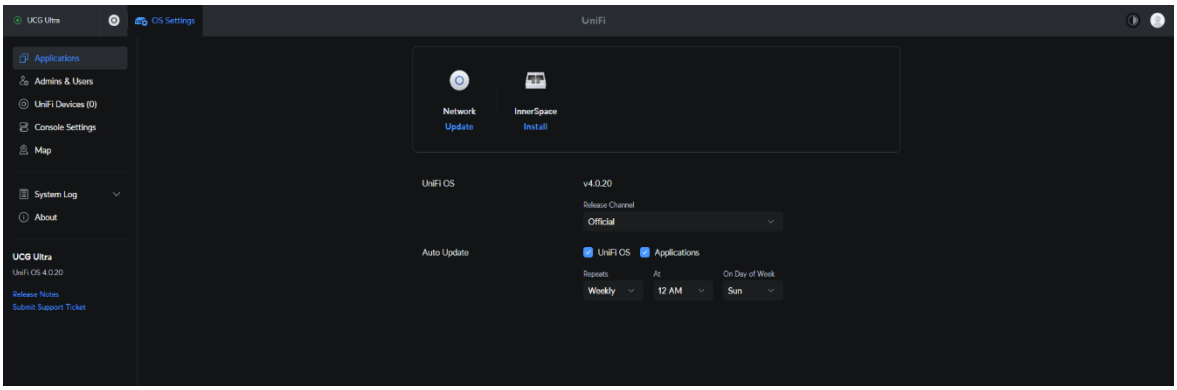


Nota. Como se muestra en la figura se encuentra una administración de puertos en dispositivo. Fuente: UCG-Ultra (2024)

Paso 8. Para finalizar dicha práctica es de saber que al conectar un equipo nuevo siempre puedan tener actualizaciones pendientes debido a que UNIFI saca seguido versiones más actualizadas con pequeñas modificaciones que se harán a continuación mostradas en el apartado de aplicaciones como se muestra en la Figura 2_11

Figura 2_11

Consola mostrando configuración del dispositivo

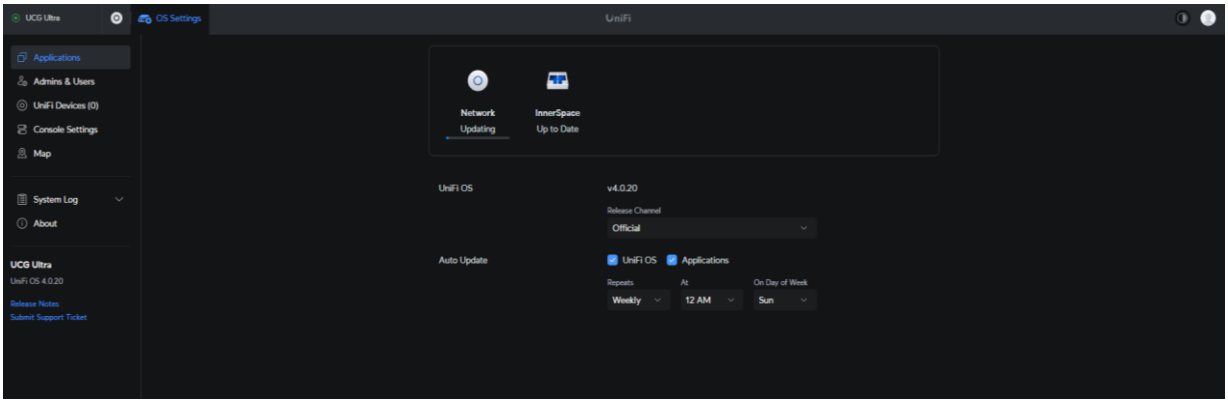


Nota. La figura muestra la consola en el enlace del dispositivo. Fuente: UCG-Ultra(2024)

Pueden pasar uno o dos minutos antes de que la consola haya comprobado si hay actualizaciones disponibles, pero asegúrese de que todas las aplicaciones estén actualizadas a la última versión

Figura 2_12

Cambio de nombre para la consola y actualizarla



Nota. En la figura se puede mostrar cómo se actualiza el sistema en la consola. Fuente: UCG-Ultra (2024)

CONCLUCION

- En la práctica anterior se aprendió a ingresar de manera seguro con las credenciales previas ya registradas para iniciar proceso de configuración
- Se ingreso al equipo UCG-ULTRA y se mostró como configurarla inicialmente hasta llegar al panel de control.
- En esta guía de laboratorio se muestra los menús dentro del equipo UCG-ULTRA

3.3 GUIA # 3 Configuración de la red con VLAN en equipo UNIFI*

INTRODUCCION

En el ámbito de las redes informáticas, la correcta configuración de los dispositivos es fundamental para garantizar un rendimiento óptimo, seguridad y escalabilidad. Los equipos UNIFI Cloud de Ubiquiti se han posicionado como una solución integral para la gestión de redes, ofreciendo herramientas avanzadas y una interfaz intuitiva que simplifica la administración de infraestructuras de red, ya sea en entornos pequeños o de gran escala. En esta guía de laboratorio, exploraremos paso a paso el proceso de configuración de una red utilizando equipos UNIFI Cloud, con el objetivo de familiarizarnos con sus funcionalidades y aprovechar al máximo sus capacidades para crear redes eficientes y seguras.

OBJETIVO GENERAL

Proporcionar los conocimientos y habilidades necesarios para configurar, gestionar y optimizar una red utilizando equipos UCG ULTRA. A través de un enfoque práctico, se busca que los participantes comprendan el funcionamiento de estos dispositivos, dominen las herramientas de administración basadas en la interfaz y sean capaces de implementar una red segura, escalable y de alto rendimiento en entornos reales.

OBJETIVOS ESPECIFICOS

- Aprender sobre la creación de las VLAN y su configuración interna para el uso de los usuarios finales y la visualización en el equipo
- Aprender sobre la conexión de otros equipos UCG- ULTRA.
- Aprender sobre la configuración de la red interna para distribuir en puntos de red

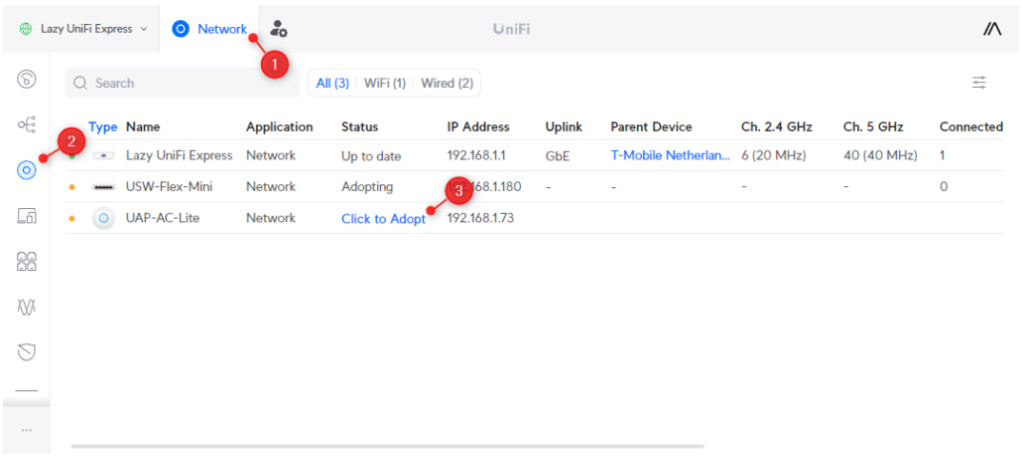
DESARROLLO

En este laboratorio se pretende que el usuario pueda aprender a crear VLAN para asignarla a usuarios finales en su configuración, también qué tipo de usuarios pueden conectarse y sus características y verificarlas en topología.

Paso1. Como primer punto se explicará paso a paso el añadir equipos UCG- ULTRA exclusivamente todo aquel que no sea autoadministrable solamente controlado por usuarios como se muestra en la figura 3_1.

Figura 3_1

Configuración para adicionar equipos UniFi directamente para su uso inmediato



Nota. La figura muestra el Inicio de configuración para incluir equipos UNIFI. Fuente: UCG-Ultra(2024)

Con UniFi Network totalmente actualizado, podemos empezar por adoptar nuestros dispositivos de red:

1. Abre la **aplicación UniFi Network**
2. Haga clic en **Dispositivos**
3. Haga clic en **Clic para adoptar** para cada dispositivo

Puede suceder que un dispositivo no lo adopte. Esto sucede cuando, por ejemplo, el firmware es demasiado antiguo en el dispositivo o cuando es administrado previamente por otro controlador UniFi.

Paso 2. Para el segundo paso entraremos ya que en la creación de VLAN en UCG- ULTRA se realiza en un par de pasos, ya que no solo tenemos que crear las diferentes redes, sino que también tenemos que proteger las VLAN. El “problema” con UniFi es que el tráfico entre VLAN está permitido de forma predeterminada. Por lo tanto, sin ninguna regla de firewall, el tráfico de, para ello se entenderá de mejor manera con un ejemplo el cual servirá de practica para los usuarios:

En este ejemplo, crearemos 3 redes VLAN para:

- Invitados – VLAN 20
- Cámaras – VLAN 30

- Dispositivos IoT – VLAN 40

La VLAN de invitados es un poco diferente de las demás VLAN porque UniFi creará automáticamente las reglas de firewall necesarias para la red de invitados. Todo lo que tienes que hacer es **aislar la red** en la configuración de red.

Entonces, en los pasos a continuación, crearemos la red de invitados, con la configuración correcta, pero más adelante usaré la VLAN de IoT como ejemplo para mostrar la diferencia en 3 diferentes ejemplos.

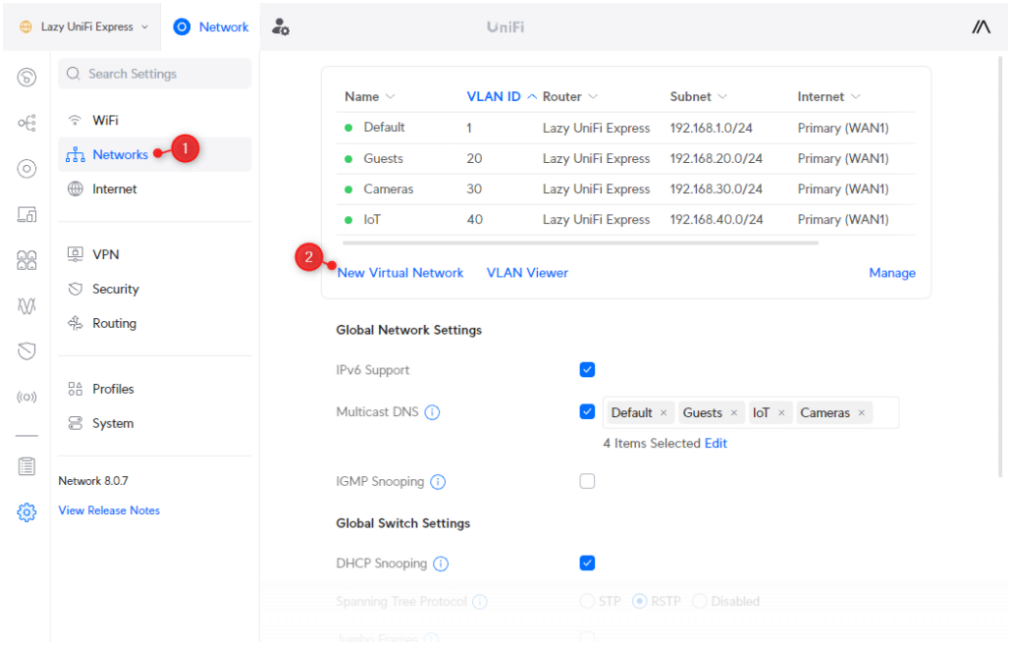
- El primer paso es crear las diferentes redes para las VLAN. He utilizado identificadores de VLAN personalizados en los pasos siguientes, pero también puedes dejar activada la opción Escalado automático de red. De esta manera, UniFi creará automáticamente el rango de IP y el identificador de VLAN.

Abra la consola de su red UniFi y navegue a:

1. **Configuración** > **Redes**
2. Haga clic en **Nueva red virtual**

Figura 3_2

Creación paso a paso para una Vlan a partir de la configuración de redes.



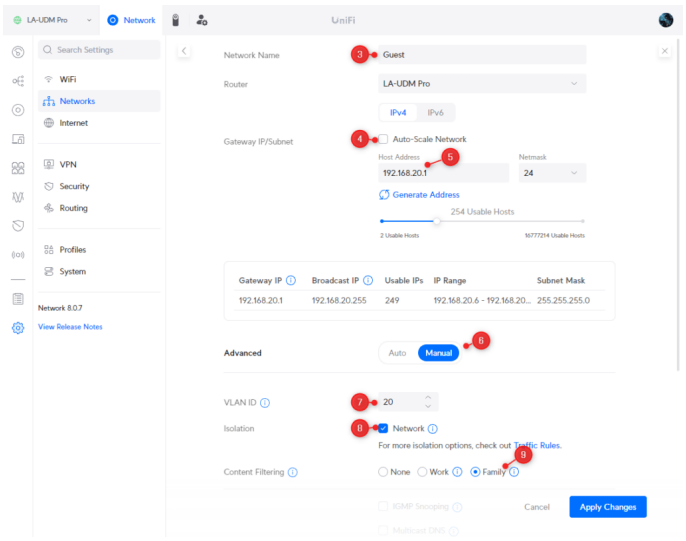
Nota. En la figura podemos observar cómo se Crea una Vlan. Fuente: UCG-Ultra (2024)

Primero vamos a crear la red de invitados:

3. Introduzca **invitados** en el **nombre de la red**
4. Anular la selección de **escala automática de red**
5. Establezca la dirección del host en **192.168.20.1**
6. Cambiar **la configuración avanzada** a **manual**
7. Cambie el **ID de VLAN a 20** para que coincida con el rango de IP
8. Habilite **el aislamiento** marcando **la opción Red**
9. Cambiar el **filtrado de contenido a Familia** (opcional)
10. Haga clic en **Aplicar cambios**

Figura 3_3

Ejemplo de la creación y configuración de una Vlan para red de invitados



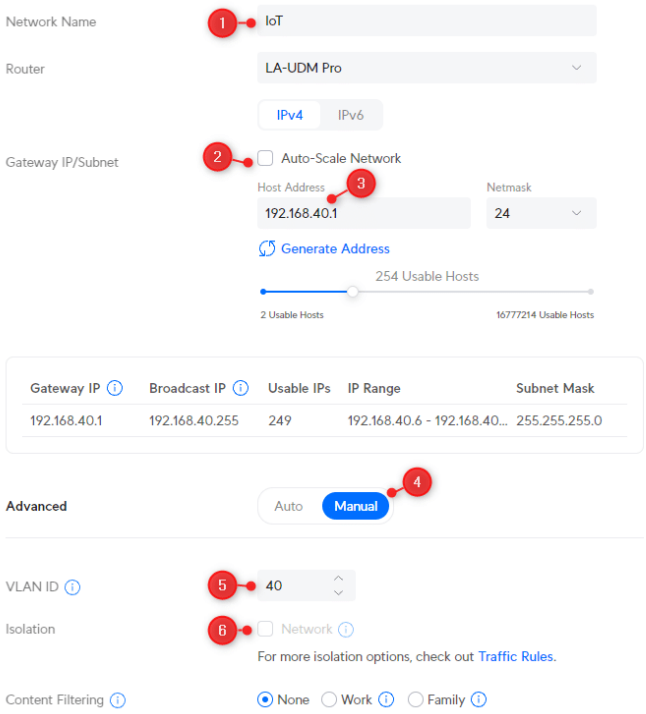
Nora. En la figura se observa la Configuración individual de una Vlan ejemplo 1. Fuente: UCG-Ultra (2024)

- En el segundo ejemplo: Debemos crear la red para las cámaras y los dispositivos IoT. Haga clic nuevamente en **Nueva red virtual** y repita los pasos a continuación para **las cámaras y el IoT**, utilizando la VLAN 30 para las cámaras y la 40 para el IoT:

1. **Nombre de la red:** IoT
2. **Deshabilitar la escala automática de red**
3. Dirección del host: **192.168.40.1**
4. Configuración avanzada: **manual**
5. Identificación de VLAN: **40**
6. Aislamiento: **Desactivado**
7. Haga clic en **Aplicar cambios** (y repita para las cámaras)

Figura 3_4

Creación de una Vlan paso a paso para el ejemplo 2.



Nota. En la figura se observa la Configuración para las cámaras en esta Vlan ejemplo 2. Fuentes: UCG-Ultra (2024)

Paso 3. En el siguiente paso se conocerá un poco más de las VLAN en el equipo UNIFI se nos proporciona también otra forma de crear las VLAN el cual es "VLAN Magic" Si está utilizando UniFi Network 8.0.24 o una versión superior, también puede utilizar la nueva función VLAN Magic para crear redes virtuales. Le permite crear una nueva red virtual desde la descripción general de dispositivos y simplemente asignar dispositivos a la VLAN seleccionándolos.

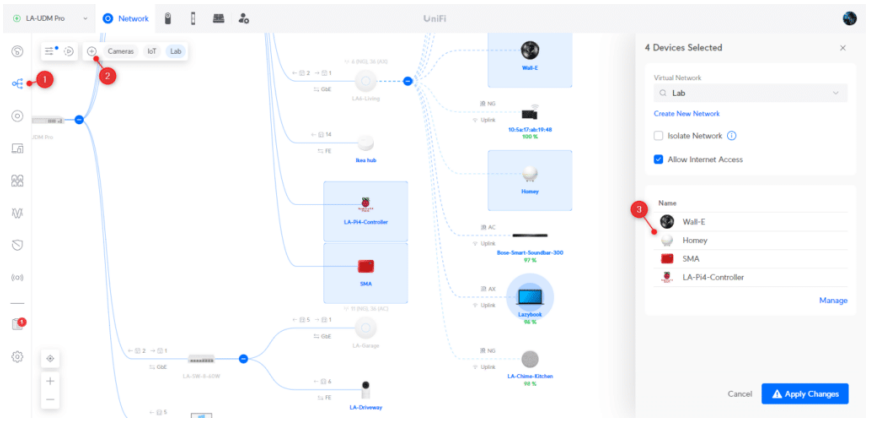
Para crear una nueva VLAN con VLAN Magic:

1. Abrir la vista **de topología**
2. Haga clic en el **ícono más** para crear una nueva VLAN
3. **Seleccione los dispositivos** en la descripción general para asignarlos

Haga clic en Aplicar cambios

Figura 3_5

Topología de las Vlan creadas



Nota. En la figura muestra las Topología de las Vlan creadas. Fuente: UCG-Ultra (2024)

CONCLUCION

- Se pudo realizar creación de VLAN para situaciones específicas y darle al usuario la cantidad de equipos que se pueden conectar y sus limitaciones.
- Se observo que gracias a las VLAN se pudo configurar para que múltiples usuarios finales puedan conectarse un punto de red especifico añadiendo algún switch o algún equipo UCG-ULTRA para alargar su radio de conexión.

3.4 GUIA # 4 Configuración de la seguridad en la red con Firewall basado en zonas.

INTRODUCCION

En el entorno actual de redes, la seguridad es un aspecto crítico para proteger los datos y garantizar la continuidad del negocio. Los firewalls son una de las herramientas más efectivas para controlar el tráfico de red y prevenir accesos no autorizados. En el caso de los equipos UniFi de Ubiquiti, el firewall basado en zonas ofrece una forma flexible y potente de gestionar la seguridad de la red.

OBJETIVO GENERAL

Aprender a entender en el equipo UNIFI el firewall basado en zonas, en el cual se pretende configurar y para que su funcionamiento, también el usuario debe aprender sobre las políticas que se deben asignar a las VLAN creadas directamente o a las restricciones directas.

OBJETIVOS ESPECIFICOS

- Aprender sobre los cortafuegos y la matriz de políticas
- Aprender a bloquear aplicaciones mediante el equipo UNIFI
- Restringir páginas web y también opciones para bloqueos mediante el equipo

ALCANCE

En esta práctica se dedicará a poder configurar redes con Firewall basado en zonas configurando las políticas para poder brindar al usuario final las restricciones que se apliquen según la VLAN para su uso.

DESARROLLO DE PRACTICA

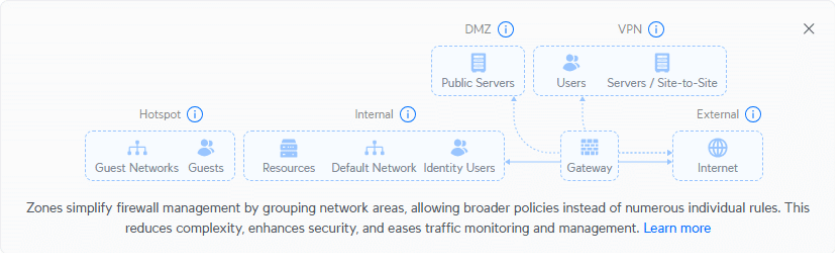
En UniFi Network siempre hemos tenido las reglas de firewall normales (avanzadas). Los nombres de los campos han cambiado un par de veces (y vuelven a cambiar con la versión 9.x), pero permite controlar el acceso en función de las direcciones IP (o rango), las redes y los grupos de puertos.

Se agregaron reglas de tráfico para facilitar la creación de reglas de firewall y también nos permitió bloquear fácilmente dispositivos individuales, aplicaciones, dominios, etc. Pero las reglas de tráfico nunca reemplazaron por completo las reglas de firewall avanzadas.

El problema con las reglas de firewall existentes (en la versión 8.x y anteriores) es la convención de nombres que se utiliza. A muchas personas les resultó difícil entender la convención de nombres que se utiliza para LAN In, LAN Out, WAN In, etc., lo cual entiendo perfectamente.

Figura 4_1

Zonas de firewall con cada una de sus clases



Nota. La figura muestra cada una de las clases en la Zonas de Firewall. Fuente: UCG-Ultra (2024)

Aquí es donde entran en juego las Zonas de Firewall, que permiten agrupar fácilmente las diferentes interfaces de red en grupos lógicos. Ahora podemos tener una zona, externa, con todas las conexiones WAN, o una zona VPN donde residan todas las conexiones VPN.

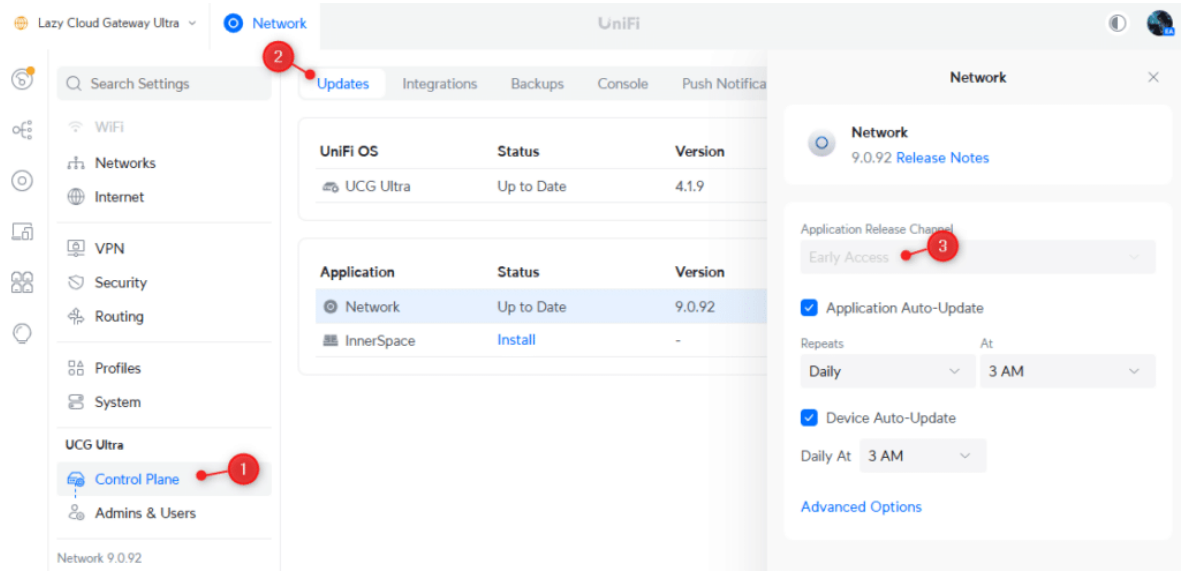
Las zonas ya no tienen reglas (de firewall), pero ahora podemos aplicar políticas a las diferentes zonas. Al igual que las reglas, las políticas permiten bloquear o permitir el tráfico entre diferentes zonas. La política no solo se aplica entre zonas, sino que también se puede aplicar a un dispositivo específico o a un rango de IP en una zona.

Paso 1. Como primer punto Como se mencionó al principio, ZBF es parte de la nueva versión UniFi Network 9.x, que actualmente se encuentra en acceso anticipado. Esto significa que, si desea utilizarla ahora mismo, deberá cambiar el canal de lanzamiento de UniFi Network a acceso anticipado:

1. Abra **Configuración** > **Plano de control**
2. Haga clic en **Actualizaciones**
3. Seleccione **Red** y asegúrese de que esté seleccionado **Acceso anticipado**

Figura 4_2

Actualización en las redes LAN



Nota. En la figura se muestra las actualizaciones de panel de control. Fuente: UCG-Ultra (2024)

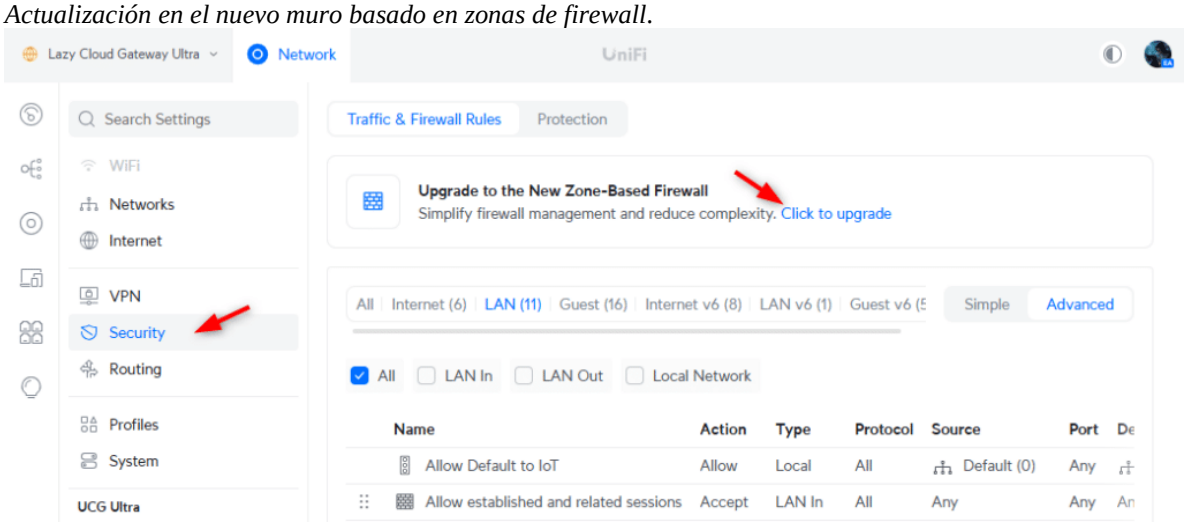
Paso 2. A continuación, tendremos que habilitar el firewall basado en zonas. Tenga en cuenta que no se puede volver atrás. Cuando habilite el firewall basado en zonas, todas las reglas de tráfico y firewall existentes se migrarán automáticamente a las nuevas políticas de firewall basado en zonas.

Y es bueno saber que terminarás con muchas más políticas de las que tenías. Terminé con alrededor de 100 políticas después de tener solo 5 reglas de firewall personalizadas en este dispositivo.

- Vaya a **Configuración** y abra **Seguridad**
- Haga clic en **Actualizar** en la notificación.

Figura 4_3

Actualización en el nuevo muro basado en zonas de firewall.

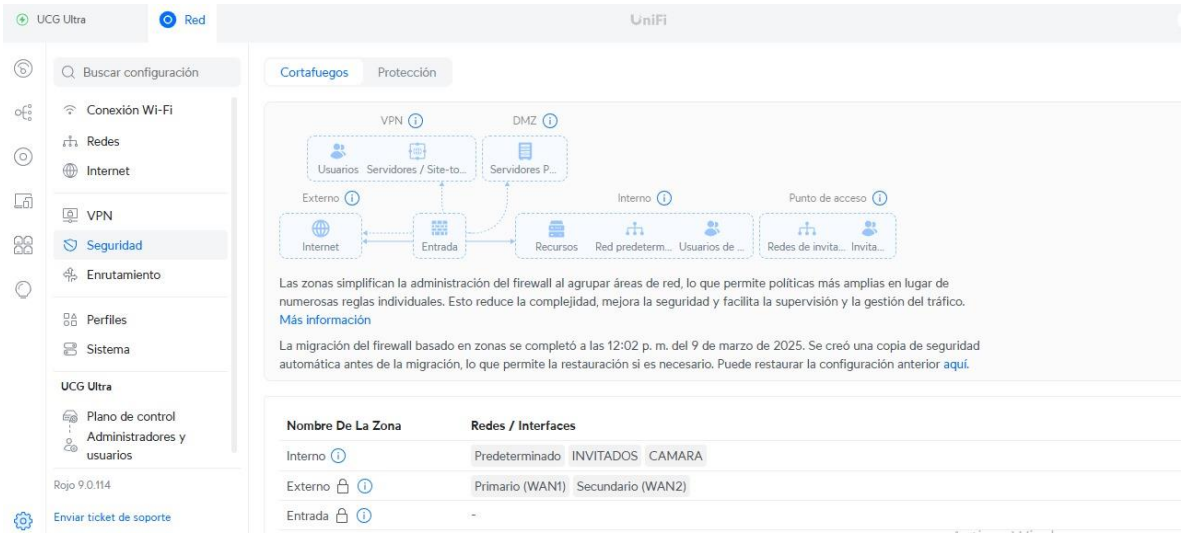


Nota. En la figura muestra la Actualización en notificación zona firewall. Fuente: UCG-Ultra (2024)

Paso 3. Como siguiente paso entraremos para el inicio de la configuración de firewall basado en zonas ingresaremos al apartado de configuración luego en seguridad y se abrirá el apartado de Cortafuegos y veremos a primera instancia la figura 4_1.

Figura 4_4

Corta fuegos en menú de seguridad.



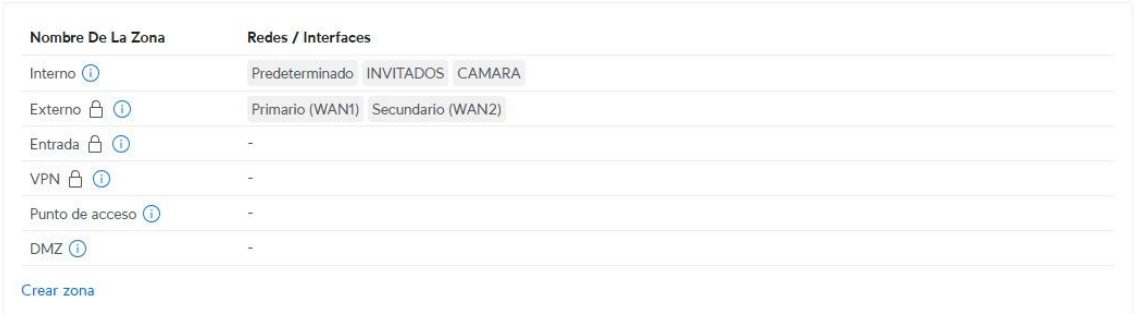
Nota. La figura muestra el Apartado de Corta Fuegos. Fuentes: UCG-Ultra (2024)

Así mismo si seguimos bajando podremos observar los nombres de las zonas de la siguiente manera:

- **Interno**: para el tráfico de confianza local. Las redes que crea se ubican de manera predeterminada en la zona interna, excepto las redes de invitados.
- **Externo**: tráfico entrante no confiable proveniente de sus conexiones WAN.
- **Puerta de enlace**: tráfico desde y hacia su puerta de enlace UniFi (gestión de DNS, DHCP, HTTPS/SSH)
- **VPN**: todo el tráfico VPN, incluidos Teleport, servidor VPN Wireguard/OpenVPN/L2TP, Site-Magic, etc.
- **Punto de acceso** – Red de invitados
- **DMZ**: se utiliza para colocar un servidor en el borde de su red, haciéndolo accesible desde Internet.

Figura 4_5

Lista de las zonas puestas en las interfaces creadas por las clases

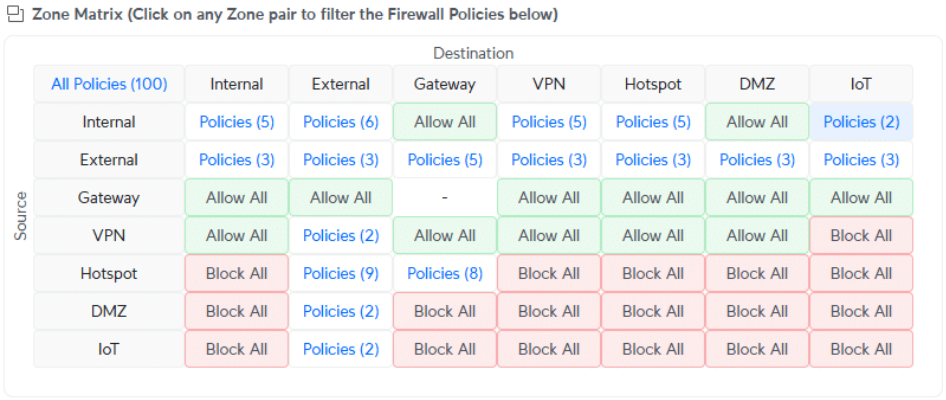


Nota. La figura muestra el Nombre de las zonas en las interfases. Fuente: UCG-Ultra (2024)

A continuación, podremos observar la zona matricial de políticas la cual pone el Nombre de las zonas puedan estar en otro orden como en la figura 4_3

Figura 4_6

Matriz de las zonas con cada una de sus políticas



Nota. En la figura se muestra Matriz de zonas. Fuente: UCG-Ultra (2024)

De manera predeterminada, una zona no puede acceder a ninguna otra zona, excepto, por supuesto, a la puerta de enlace, y el tráfico establecido se permite hacia la zona externa. Puede hacer clic en Políticas (n) para ver y administrar las políticas que se aplican entre las dos zonas.

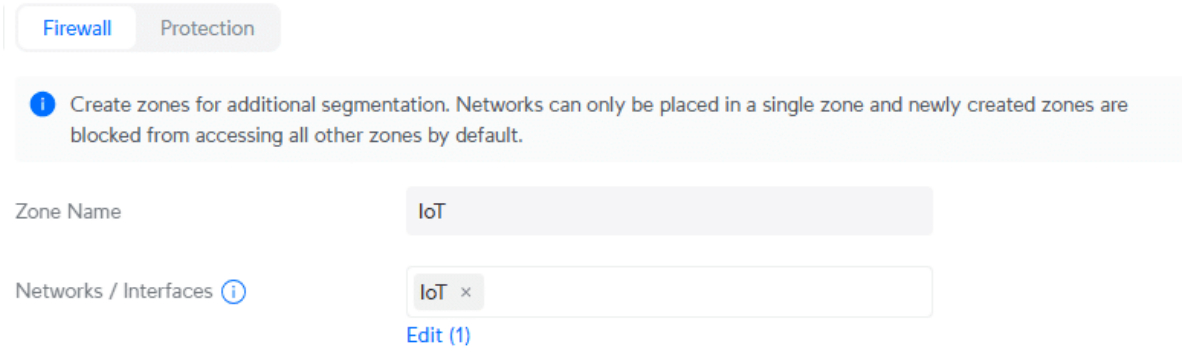
Las zonas realmente ayudan a segmentar su red y le permiten establecer fácilmente límites claros entre ellas.

Una interfaz de red, por ejemplo, el puerto WAN1 o su red IoT, solo se puede asignar a una zona. Ahora no puede eliminar las zonas predefinidas, pero puede crear zonas personalizadas y asignarles una interfaz de red. De esta manera, puede personalizar las políticas asignadas.

Paso 4. Para el siguiente paso iniciaremos con la creación de zonas para eso en la figura 4_3 podemos observar en la parte inferior izquierda un apartado donde dice “Crear zonas”.

Figura 4_7

Creación de las zonas en el firewall



Nota. En la figura se puede mostrar cómo se crea el Nombre de la zona. Fuente: UCG-Ultra

Crear una nueva zona es bastante fácil, simplemente haga clic en Crear zona en la pestaña de seguridad, dé un nombre a la zona y seleccione la red y/o interfaz que desea asignarle. Tenga en cuenta que no es necesario crear zonas para cada VLAN. Si desea bloquear el tráfico entre VLAN, simplemente cree una política para ello en la zona interna.

Figura 4_8

Creación de una zona llamada CAMARA con la misma política.

Nota. En la figura se puede mostrar la Zonas ya configuradas con la política de cámara. Fuente: UCG-Ultra (2024)

Como pueden ver en la matriz ya se agregó la póliza de cámara y se crearon todas las políticas de manera automática

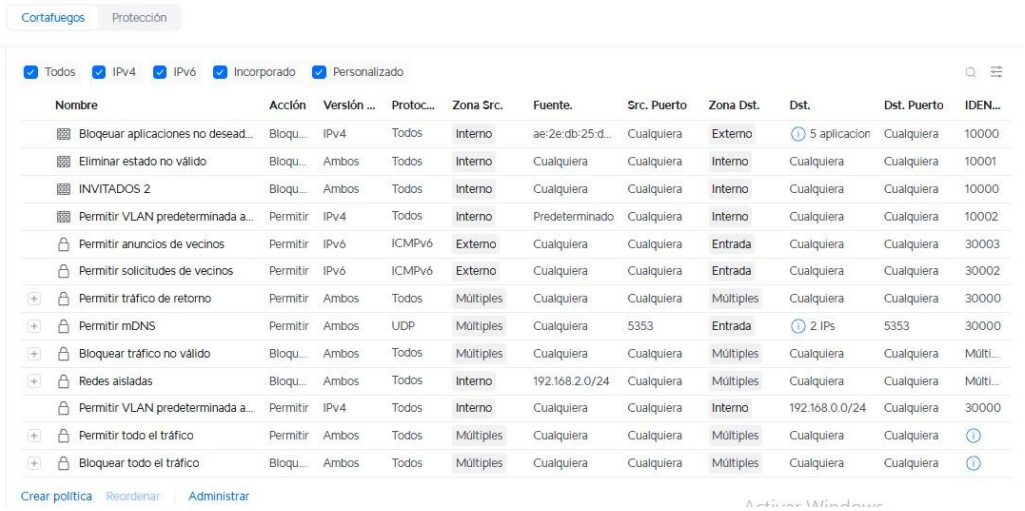
Paso 5. Para el siguiente paso crearemos una política dentro de la zona cabe mencionar que, dentro de una zona, puede haber varias redes (VLAN). Ahora, estas redes pueden comunicarse entre sí de manera predeterminada, no hay bloqueo entre VLAN dentro de una zona.

Sin embargo, también podemos crear políticas para filtrar el tráfico dentro de la misma zona. De esta forma, podemos bloquear todo el tráfico entre VLAN y permitir solo el tráfico predeterminado para IoT, por ejemplo. O crear una excepción para un dispositivo específico.

Nos iremos al final del mismo apartado de los cortafuegos y haremos clic en Crear Política:

Figura 4_9

Se observa con claridad cada una de las políticas creadas a partir de las zonas.



Nota. En la figura se puede observar las Listas de VLAN con políticas creadas. Fuente: UCG-Ultra (2024)

Luego nombraremos una política y podremos configurarla al gusto de uno y haremos lo siguiente:

i. Nombre: Bloqueo de aplicación
ii. Zona de origen: Interno y Dispositivos (Mi PC)
iii. Paseo: Cualquiera
iv. Acción: Bloquear
v. Zona de destino: Externo y especificaremos (Whats app)
vi. Versión Ip: Ambos
vii. Estado de conexión: Todos
viii. Horario: Siempre
ix. Descripción: Pondremos bloqueo de aplicación WhatsApp

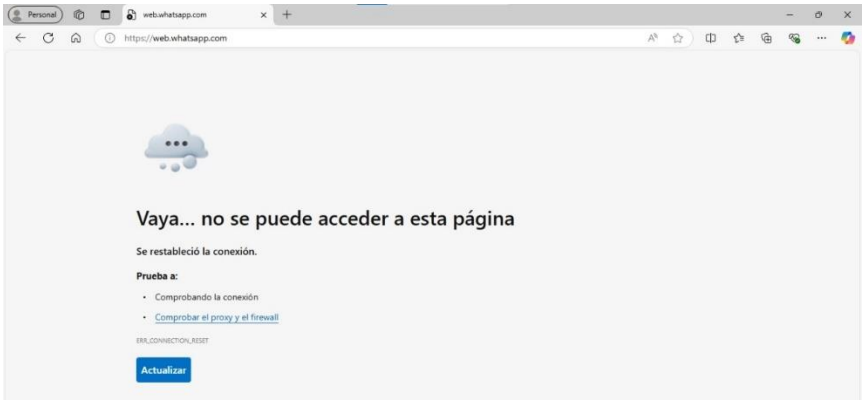
Figura 4_10

Políticas creadas para ejemplo en ejercicio de laboratorio.

Nota. En la figura se puede observar las Políticas creadas para equipo especifico. Fuente: UCG-Ultra (2024)

Figura 4_11

Intento de ingresar a sitio bloqueado por la política



Nota. En la figura se puede observar que Todo acceso externo está bloqueado sobre la aplicación WhatsApp. Fuente: UCG-Ultra (2024)

Como podemos observar acá ya se creó una nueva política el cual bloquea específicamente el distintivo que se añade, pueden ser páginas web, direcciones Ip, otras políticas, etc.

Y se puede observar en la figura 4_9 se bloqueó con éxito aplicación de WhatsApp.

Paso 6. Para el siguiente paso. Después de la migración, probablemente desees mover una o más VLAN a una zona diferente. Hay dos formas de mover una red (VLAN) a una zona diferente, podemos hacerlo en la configuración de Redes o en la configuración de **Seguridad** > **Firewall**. Cuando intenté cambiar la zona en la configuración de red, no funcionó, el controlador de red arrojó un error.

Pero cambiar la zona en la configuración del Firewall parece funcionar bien:

1. Abra la **configuración del Firewall**
2. Seleccione la **zona de Hotspot**
3. Haga clic en **Editar**
4. **Seleccione la red IoT** y haga clic en **Guardar**

Ahora, la pregunta que me hacen con frecuencia es dónde colocar la red IoT. Puede que sienta la tentación de colocarla en la zona de puntos de acceso, porque son dispositivos que no son de confianza. Pero cuando coloca la red IoT en la zona de puntos de acceso, se activará el portal cautivo, lo que provocará problemas de conexión para sus dispositivos.

La red IoT puede residir perfectamente en la zona interna, siempre que bloquees el tráfico entre las VLAN. Realmente no es necesario trasladarla a la zona Hotspot para que sea más segura.

CONCLUCION

- Se realizo una explicación breve del apartado de seguridad en el equipo UCG-ULTRA
- Se pudo realizar las pruebas de bloqueo en aplicaciones mediante la política basado en creación de zonas a un equipo especifico
- Se demostró que el equipo UCG-ULTRA es bastante eficiente en apartados en los que se tenga que brindar limitación en cuanto a la búsqueda de aplicaciones y paginas específicas y generales

3.5 GUIA#5 Configuración de red inalámbrica

INTRODUCCION

El UniFi Cloud Gateway Ultra (UCG-ULTRA) es un potente dispositivo de gestión de redes diseñado para entornos UniFi. Aunque no cuenta con un punto de acceso WiFi integrado, permite administrar y optimizar redes inalámbricas a través de la aplicación UniFi Network.

Para configurar una red inalámbrica con el UCG-ULTRA, es necesario conectarlo a uno o más Access Points (APs) UniFi, los cuales serán gestionados centralmente desde su interfaz de administración. Este proceso garantiza una cobertura WiFi eficiente, segura y con funciones avanzadas como balanceo de carga, segmentación de tráfico y seguridad mejorada. A continuación, se detallarán los pasos para integrar el UCG-ULTRA con puntos de acceso UniFi y configurar correctamente la red inalámbrica.

OBJETIVO ESPECIFICO

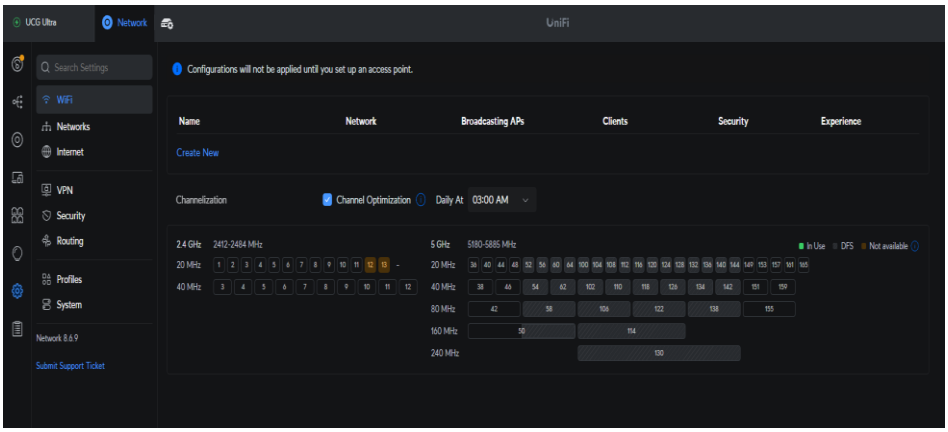
- Demostrar de qué manera puede funcionar como punto de acceso en red inalámbrica y que componentes necesita para poder funcionar de manera correcta
- Indagar con los puertos de Acceso que tiene el equipo UCG-ULTRA y su configuración
- Tener una explicación para la forma en que se puede acceder a puntos de acceso inalámbrico.

DESARROLLO DE PROBLEMA

Paso 1. Para iniciar se debe tener en claro que está sección igual va dirigida a quienes cuenten con un AP de la marca Ubiquiti con controlador UniFi. Cuando abra la **Configuración** > **WiFi** y seleccione su red inalámbrica, tendrá la opción de habilitar la **configuración avanzada**.

Figura 5_1

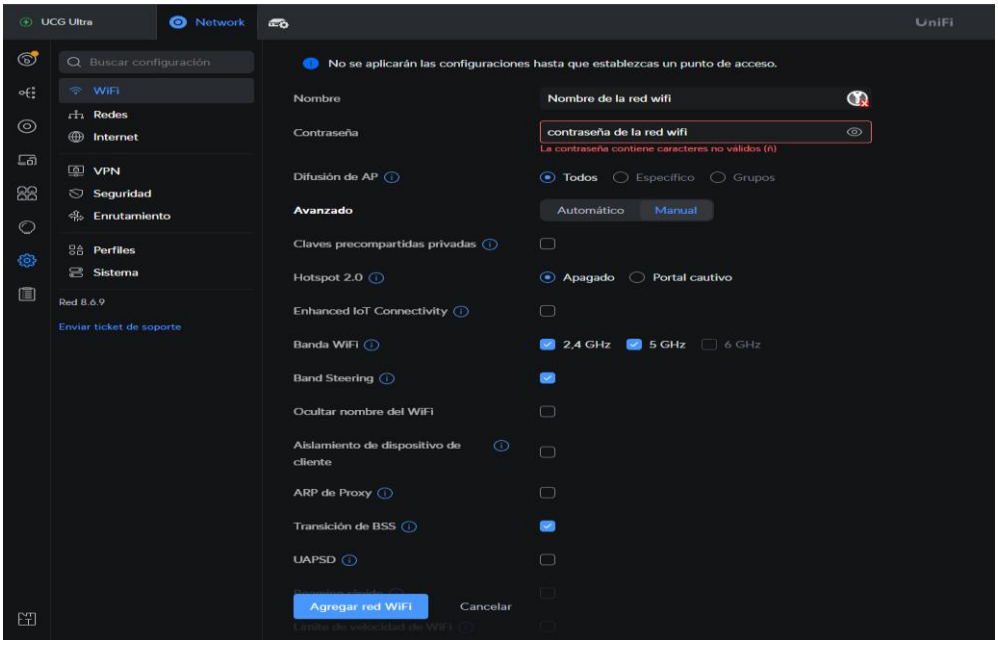
Apartado de red inalámbrica con equipo UniFi



Nota. En la figura se pude observar el Inicio de configuración de red inalámbrica Fuente: UCG-Ultra (2024)

Figura 5_2

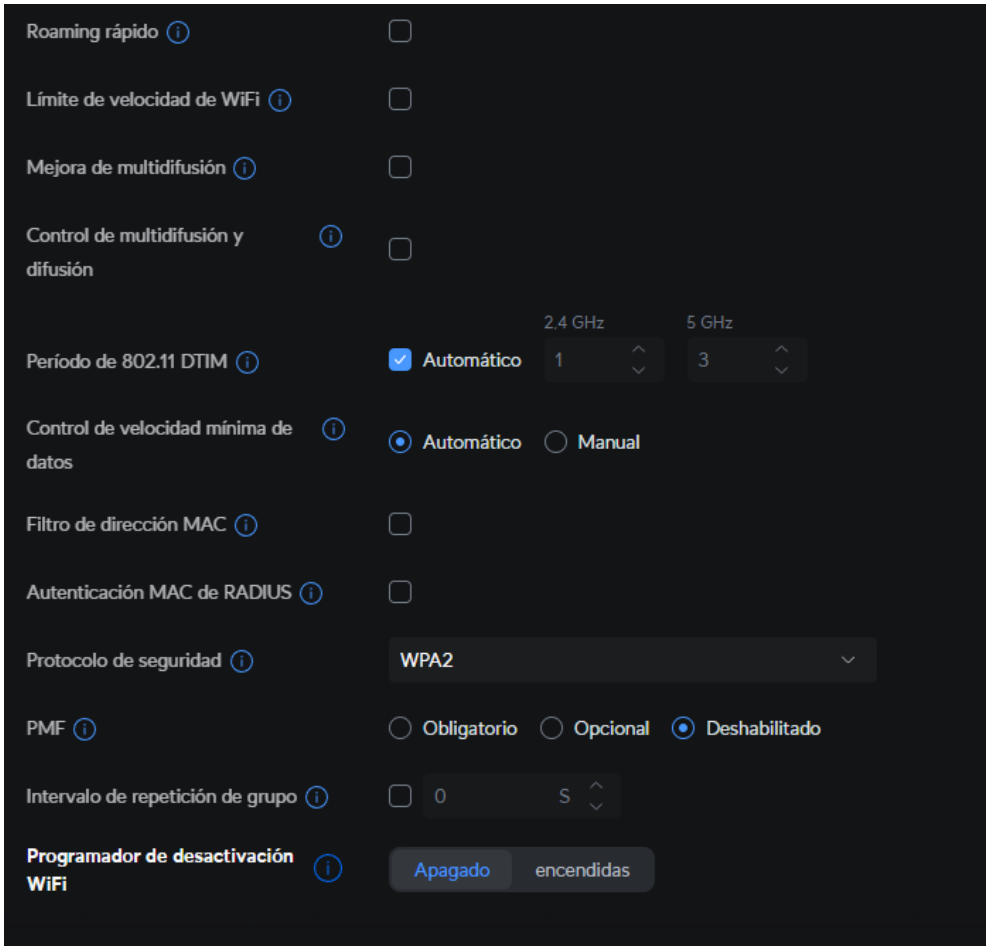
Configuración de la red inalámbrica con equipo UniFi



Nota. En la siguiente figura se encuentro la Configuración de red inalámbrica. Fuente: UCG-Ultra (2024)

Figura 5_3

Configuración avanzada para una red Wifi con ancho de banda 2.4 Ghz y 5Ghz



Nota. En la figura se puede apreciar la Configuración avanzada de redes wifi. Fuente: UCG-Ultra (2024)

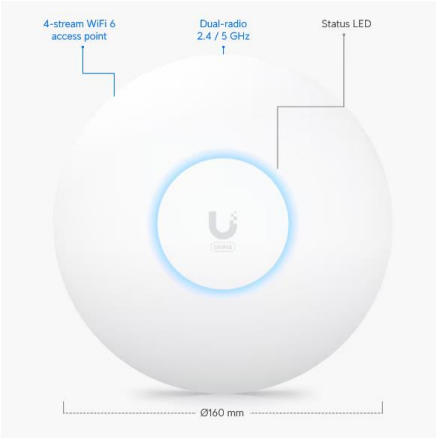
La configuración avanzada predeterminada es perfecta para la mayoría de las redes inalámbricas. Solo cuando tenga una red de alta densidad o muchos usuarios invitados, es posible que desee optimizar algunas configuraciones. Además, si tiene problemas de conectividad con Sonos o Chromecast, aquí hay algunas configuraciones que puede cambiar.

En este caso enlistaremos un par de equipos que podrían ser anexados en este apartado para que funcione como emisor de la red WI-FI.

Para el proceso anterior solo es aplicable única y exclusivamente para los equipos Unifi que replican señal WiFi como lo es el equipo más básico que tiene UniFi para replicar señal Wifi en bandas 2.4Ghz y 5Ghz, El Equipo que se muestra en la figura 5_4 llamado U6-Plus.

Figura 5_4

Equipo UniFi replicador de Señal WiFi



Nota. En la figura se observa un Equipo Replicador WiFi U6-PLUS un equipo propio de la línea UniFi. Fuente: UCG-Ultra (2024)

Paso 2. Como segundo punto se explica punto a punto el apartado Wifi que se mostró en el punto. Explicaré brevemente la configuración, pero puede dejarla predeterminada para las redes normales y simplemente saltar al siguiente paso:

- **Claves privadas precompartidas**: le permite utilizar una red inalámbrica para todas sus VLAN. De esta manera, no necesita crear una red inalámbrica separada para sus cámaras o dispositivos IoT.
- **Portal de puntos de acceso**: se utiliza para redes de misiones. Le permite mostrar una página de inicio de sesión de marca y utilizar diferentes opciones de autenticación para los huéspedes, incluidos cupones u opciones de pago
- **Banda WiFi**: desea habilitar todas las bandas WiFi para su red. Si tiene un punto de acceso UniFi 6 Enterprise, también puede habilitar la banda de 6 GHz si está permitida en su región.
- **Dirección de banda**: anima a los clientes a usar 5 GHz en lugar de 2,4 GHz, que es más lento. Déjalo activado, pero apágalo si tienes muchos problemas de conectividad.
- **Aislamiento de dispositivos cliente**: habilítelo para redes de invitados o IoT. Evita que los dispositivos conectados se comuniquen entre sí.
- **Proxy ARP**: solo se utiliza en redes de alta densidad. Permite puntos de acceso a solicitudes ARP de proxy que reducen el tráfico de difusión.
- **Transición BSS**: permite que los puntos de acceso compartan información de topología de red con los clientes. Esto reduce el uso de energía para dispositivos móviles y puede ayudar con el roaming.

- **UAPSD**: cuando está habilitado, los clientes pueden mantener su WiFi durante más tiempo en modo de suspensión. Es posible que desee habilitar esto en una red de IoT, donde ayudará a ahorrar consumo de batería.
- **Roaming rápido**: permite a los clientes desplazarse más rápido entre puntos de acceso. Habilite esta opción solo cuando se desplace mucho entre puntos de acceso durante llamadas de VoIP o videoconferencia.
- **Límite de velocidad WiFi**: limita el ancho de banda de carga y descarga para los clientes. Útil para redes de alta densidad o redes de invitados.
- **Mejora de multidifusión**: mejora el acceso a los clientes de registro y convierte el tráfico de multidifusión en unidifusión. Puede mejorar el rendimiento de productos domésticos inteligentes como Chromecast o Airplay.
- **Control de multidifusión y difusión**: restringe el tráfico múltiple y de difusión, excepto para los dispositivos definidos. Puede ayudar a reducir el tráfico aéreo en redes de alta densidad
- **802.11 Período DTIM** – Dejar en auto.
- **Control de velocidad de datos mínima**: establece una velocidad de red mínima que los clientes deben poder alcanzar. Si lo estableces como si estuvieras demasiado bajo, puedes causar problemas de conexión. Solo se utiliza en redes de alta densidad.
- **Filtro de direcciones MAC**: le permite especificar una lista de permitidos o denegados en función de la dirección MAC con dispositivos
- **Autenticación MAC RADIUS**: le permite utilizar un servidor RADIUS para la autenticación del cliente
- **Protocolo de seguridad**: se debe usar WPA2 como mínimo. WPA3 es más seguro y necesario para redes de 6 GHZ. Déjalo en WPA2/WPA3 para que también sea compatible con dispositivos más antiguos.
- **PMF**: necesario para WPA3, pero opcional cuando WPA3 está habilitado para admitir dispositivos más antiguos.
- **Programador de WiFi**: le permite establecer las horas en las que se debe encender la red inalámbrica.

Paso 3. Como siguiente punto iniciaremos y podremos crear y configurar redes. Siempre se tiene la red predeterminada, que se crea automáticamente, pero podemos agregar redes virtuales adicionales a nuestro entorno.

Las redes virtuales se utilizan cuando se desea crear una separación entre dispositivos, de tal manera que no puedan interactuar entre sí. Por ejemplo, los invitados pueden usar su conexión a Internet, pero no desea que puedan acceder a sus dispositivos de red.

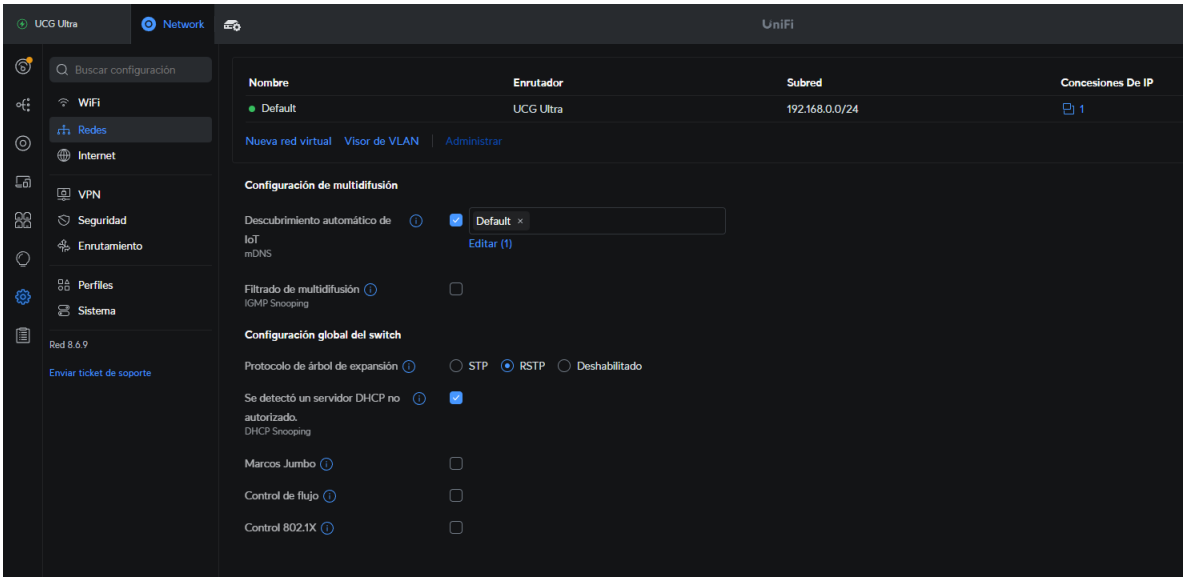
O cuando tiene muchos dispositivos IoT, debe colocarlos en una red separada por razones de seguridad. Entonces, cuando un dispositivo se ve comprometido debido a una vulnerabilidad, por ejemplo, no podrá acceder a otros dispositivos de su red.

Cuando abra la **configuración de red (Redes),** verá la **Configuración de red global**. Podemos dejar esa configuración en los valores predeterminados en nuestra configuración de

UniFi. IGMP Snooping o Jumbo Frames, por ejemplo, solo son necesarios en situaciones específicas, para la mayoría de las redes domésticas.

Figura 5_5

Configuración de la red global ante una red creada como Vlan

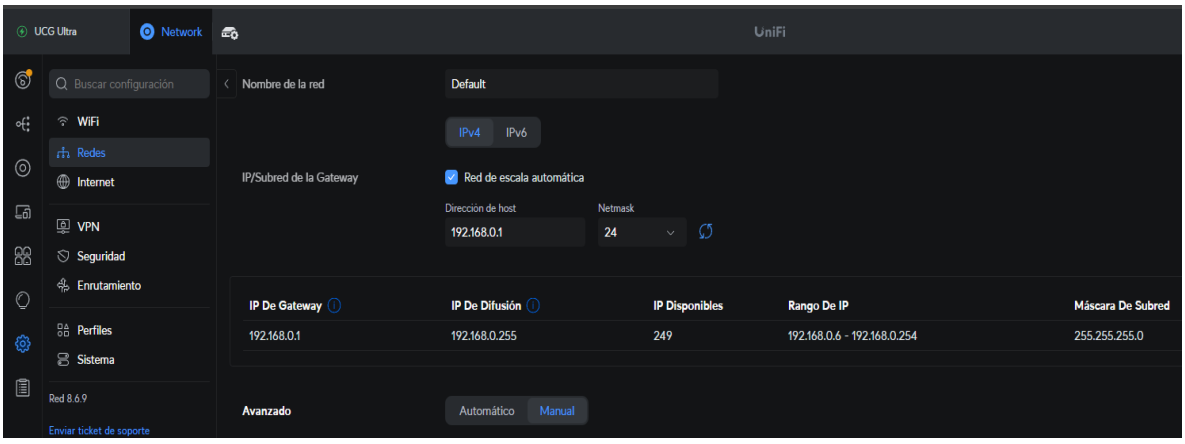


Nota. Configuración de red Global para una red WiFi. Fuente: UCG-Ultra (2024)

Si hace clic en la **red predeterminada**, puede configurar los ajustes de la red, como el **rango de IP, el alcance de DHCP, DNS, el filtrado de contenido** y más:

Figura 5_6

Configuración por Ip para acceso a redes WiFi



Nota. En la figura se puede observar como de manera Manuel se Configura la Ip del host. Fuente: UCG-Ultra (2024)

La **configuración predeterminada de** IP/subred de puerta de enlace **(1)** es correcta para la mayoría de las redes. Le permite usar 249 direcciones IP de forma predeterminada, lo cual es suficiente para la mayoría de las redes pequeñas.

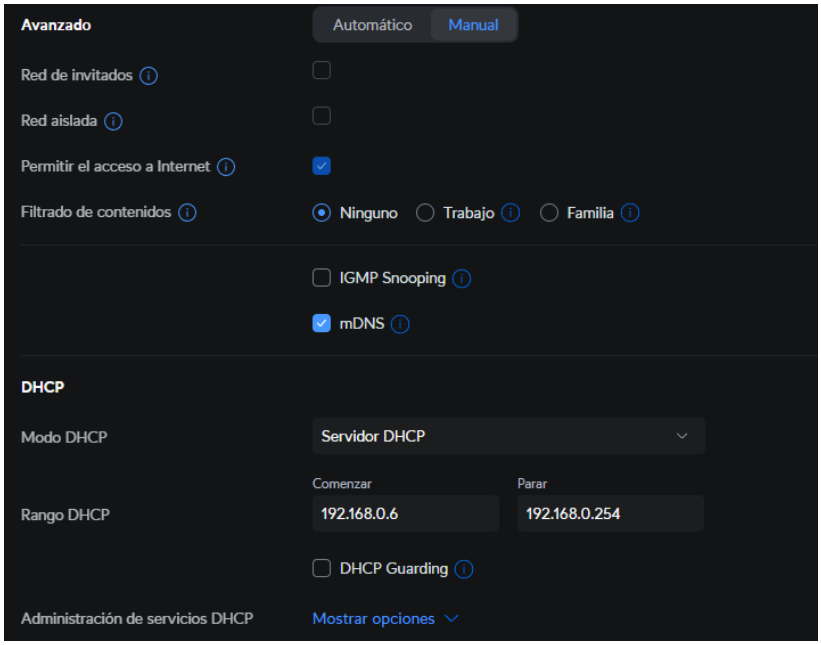
Paso 4. Con el siguiente punto seguiremos con la configuración avanzada siguiendo:

Si se habilita la **configuración avanzada (2),** puede cambiar la configuración de DHCP y DNS. Si su puerta de enlace en la nube admite la detección de actividades sospechosas, también puede configurar el filtrado de contenido para la red aquí.

El ámbito DHCP predeterminado comienza en 192.168.0.6 y termina en 0.254. Esto no le dará mucho espacio para direcciones IP fijas. Prefiero configurar direcciones IP estáticas (fijas) para dispositivos de red conocidos, como impresoras, concentradores domésticos inteligentes o inversores solares. Para ello, tendrás que desactivar la **red de Auto-Scale (1),** tras lo cual podrás personalizar el **Rango DHCP (3)**

Figura 5_7

Configuración avanzada para una red inalámbrica de conexión automática o Manual



Nota. En la siguiente figura se observa el Panel de configuración avanzada. Fuente: UCG-Ultra (2024)

Paso 5. Como siguiente punto A pesar de que su Internet ya está funcionando, necesitamos optimizar algunas configuraciones en nuestra configuración de UniFi para obtener el mejor rendimiento. Si abre la Configuración de Internet, verá la conexión principal (WAN1).

Cuando tienes un UDM Pro, por ejemplo, también ves la opción de configurar tu conexión principal y configurar la conmutación por error o el equilibrio de carga.

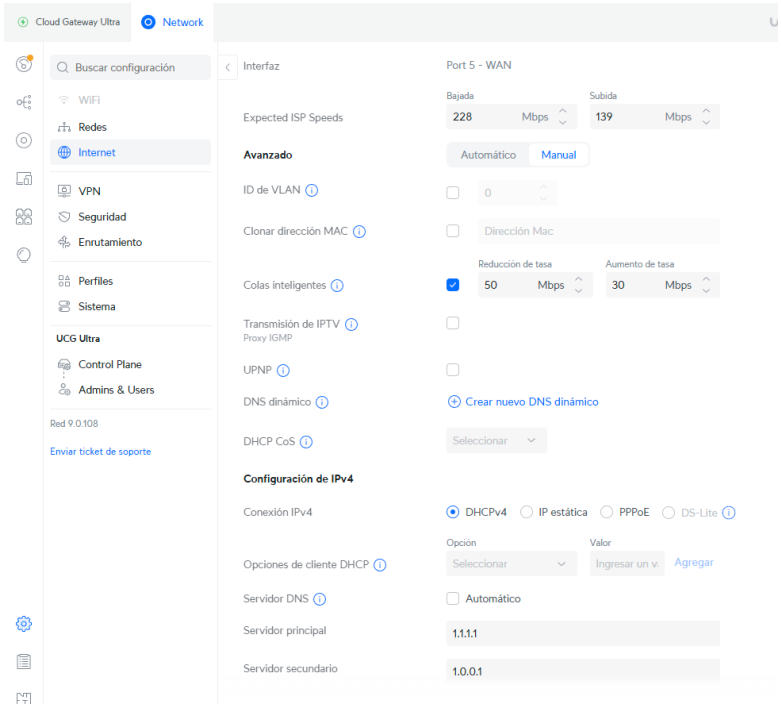
Hay algunas cosas que necesitamos configurar. La más importante es habilitar las colas inteligentes si la velocidad de su conexión a Internet es inferior a 300 Mbps. Esto evitará la hinchazón del búfer, que ocurre cuando su enrutador envía más datos a la línea de Internet de los que su conexión puede manejar.

Además, queremos usar un servidor DNS bueno y rápido, no el de tu ISP, y configurar la velocidad esperada del ISP: **Configuración,** vaya a **Internet**

1. En **Configuración,** vaya a **Internet**
2. Abra su conexión **primaria (WAN1)** haciendo clic en ella.
3. Introduzca las **velocidades esperadas del ISP**
4. Establecer **avanzado** en **Manual**
5. **Habilite las colas inteligentes** cuando la velocidad de su conexión a Internet sea inferior a 300 Mbps
    1. Configura tu **Down y Uprate unos Mbit** por debajo de tu velocidad de conexión (más información)
    2. **Pruebe** su conexión aquí
    3. **Ajusta las velocidades** hasta que obtengas una **A+** para Bufferbloat en la prueba
6. En Configuración de IPv4, **deshabilite Auto** para el **servidor DNS**
7. Introduzca los siguientes servidores DNS
    1. **Principal: 1.1.1.1**
    2. **Secundario: 1.0.0.1**
8. Haga clic en **Aplicar cambios**

Figura 5_8

Configuración y división de ancho de banda para múltiples clientes

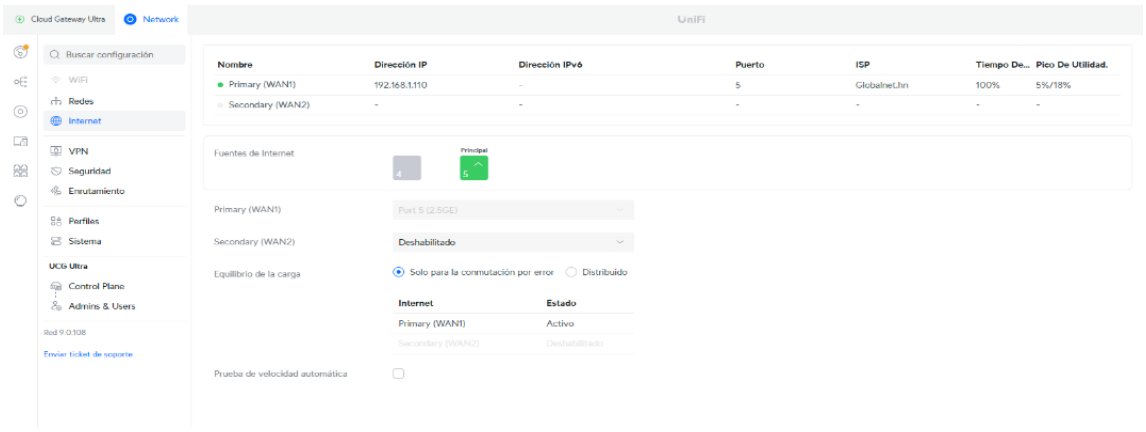


Nota. En la figura observamos la Configuración para navegación internet. Fuente: UCG-Ultra (2024)

Su Gateway también cuenta con la posibilidad de poner un segundo ISP, para hacer eso primero debe activar Secondary (WAN2), el cual será el puerto #4, luego proceda a conectar el cable ethernet de su segundo ISP.

Figura 5_9

En el menú de internet se activará la WAN para otros puertos

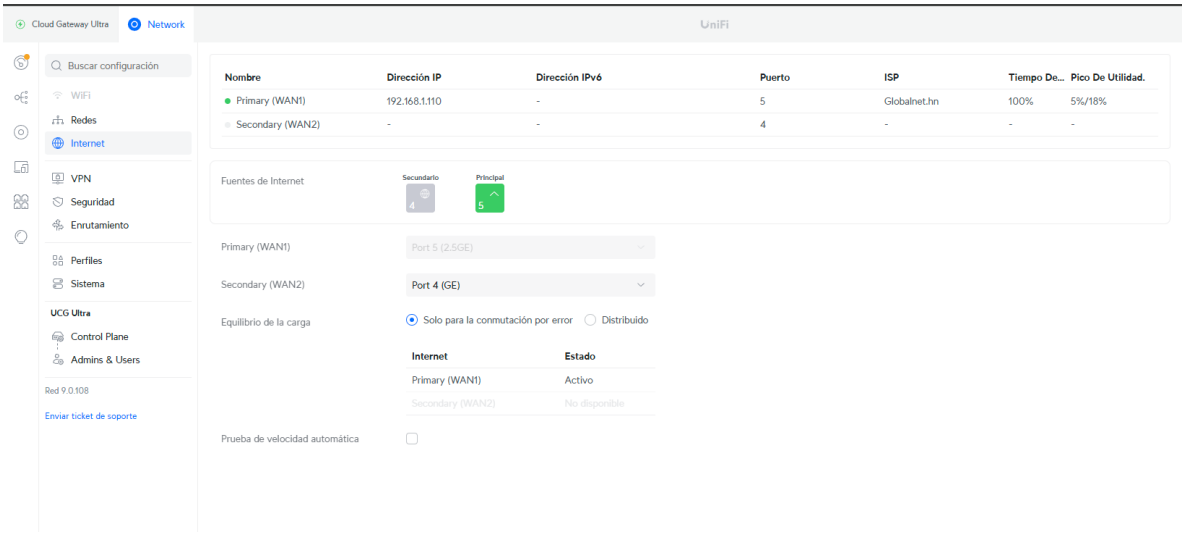


Nota. En la figura veremos en su panel la Activación del WAN. Fuente: UCG-Ultra (2024)

En este punto usted tendrá dos opciones, en Equilibrio de carga ustedes pueden dejarla en conmutación de erros, si uno de los ISP llega a fallar, se cae el servicio, el otro entra inmediatamente para sustituirlo.

Figura 5_10

Configuración para el ISP en los puertos

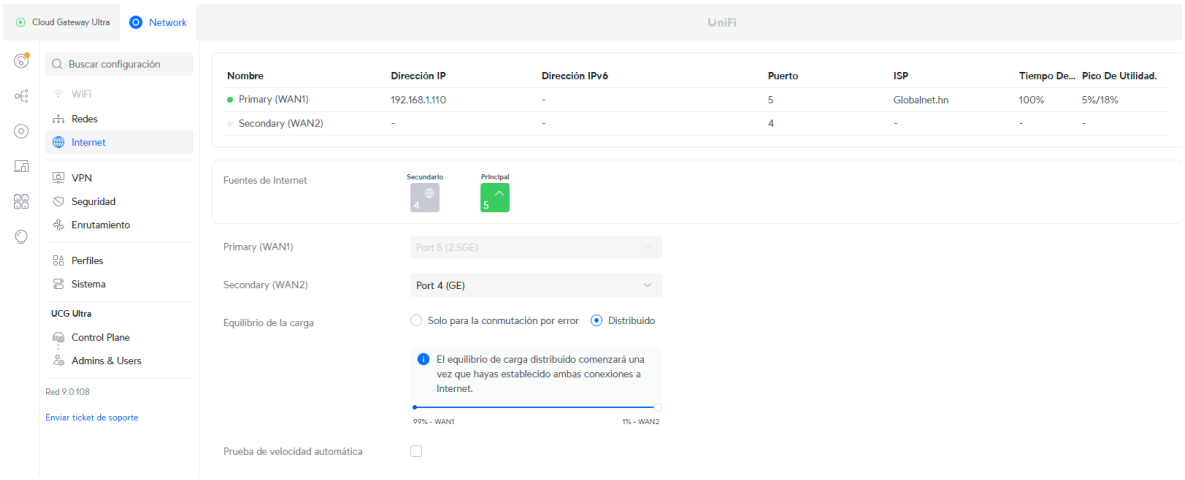


Nota En la figura anterior se observa el Respaldo en ISP. Fuente: UCG-Ultra (2024)

Si se deja en distribuido, se hará uso de los dos ISP, dependiendo del balance que se establezca en el deslizador, como recomendación dejarle más porcentaje al ISP con mayores megas o que se determine que no tiene tantos problemas de conexión, para saber esto se pueden leer los mensajes en el dashboard.

Figura 5_11

Distribución de dos ISP en WAN

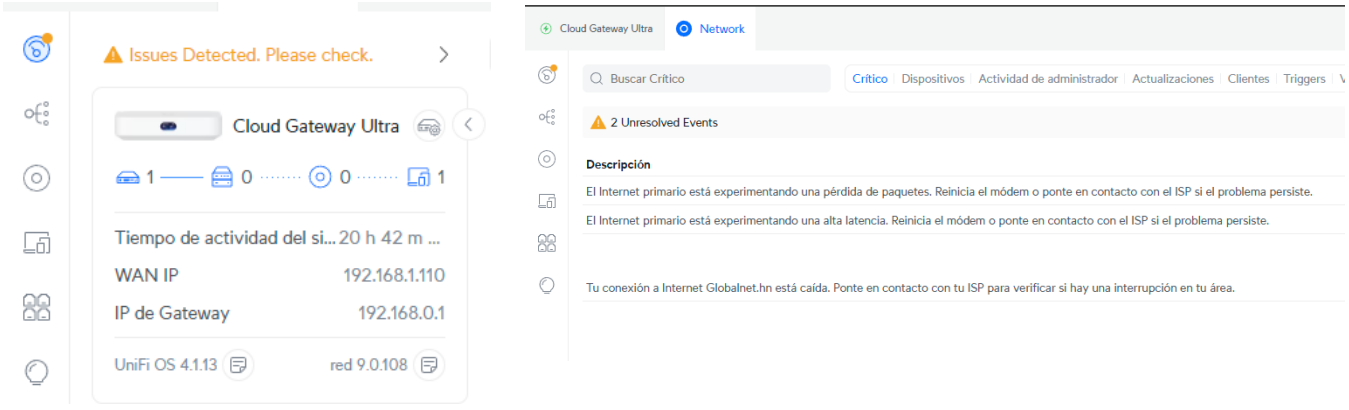


Nota. En la figura se puede observar la Distribución de dos ISP. **Fuente: UCG-Ultra (2024)**

Normalmente aparecen arriba a la izquierda del dashboard.

Figura 5_12.

Se configura ISP de manera más general.



Nota. La figura se observa cómo es la Configuración ISP. Fuente: UCG-Ultra (2024)

CONCLUCION

- Se demostró la configuración de otro equipo UniFi para poder tener acceso a redes wifi funcionales con la configuración interna del equipo UCG-ULTRA en uno de sus puertos y si se conecta a un switch haremos todo el switch estará configura según ese puerto.
- Como se demostró se puede acceder a un replicador WiFi, así como lo es el AX3 de Huawei es decir un equipo ajeno con la diferencia que se configura con VLAN.

3.6 GUIA# 6 Configuración en UCG-ULTRA con VPN

INTRODUCCION

A través de la aplicación UniFi Network, los administradores pueden establecer túneles VPN seguros para conectar sucursales, permitir el acceso remoto a la red local y mejorar la privacidad de las conexiones.

OBJETIVO GENERAL

- Configurar y optimizar una red privada virtual (VPN) en el UniFi Cloud Gateway Ultra (UCG-ULTRA) para permitir conexiones seguras y eficientes entre redes remotas, usuarios externos y la infraestructura local, garantizando confidencialidad, integridad y disponibilidad de los datos.

OBJETIVO ESPECIFICO

- Configurar y habilitar la VPN en la interfaz de administración de UniFi, estableciendo los parámetros esenciales como direcciones IP, autenticación y cifrado.
- Aprender de la opción de Teleport y como aporta o ayuda al usuario final a quien ingrese por VPN

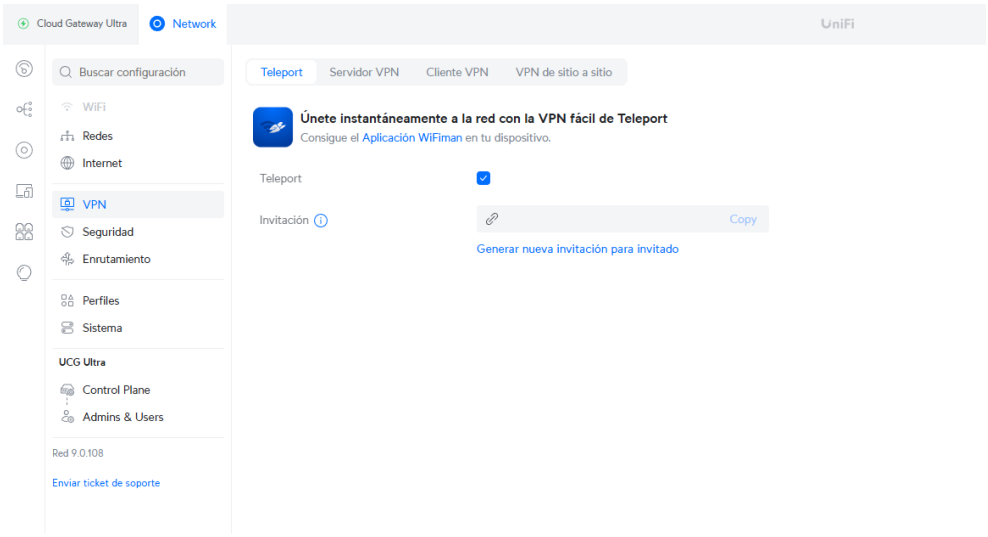
Desarrollo de practica

Paso1. Para la siguiente guía de laboratorio se explica que UniFi Cloud Gateway viene con un servidor VPN incorporado que le permite conectarse con su red doméstica con un solo clic. Ahora podrías pensar, ¿cuándo necesito esto? Para cuando estás conectado a una red pública y necesitas acceder a tu cuenta bancaria, por ejemplo, entonces es mejor utilizar tu propia conexión a Internet.

Accederemos de la siguiente manera: Nos iremos en **configuración** y dentro de configuración ingresaremos a **VPN** el cual nos aparecerá un apartado de un pequeño icono el cual es llamado “Únete instantáneamente a la red con la VPN de Teleport” como se muestra en la figura 6_1.

Figura 6_1

Configuración VPN mediante Teleport



Nota. En la figura se puede observar la Opción con VPN Teleport. Fuente: UCG-Ultra (2024)

Paso 1.2 Con una pequeña explicación de Teleport:

Teleport se lanzó originalmente en 2018 para la línea de productos AmpliFi de Ubiquiti. Pero ahora también está disponible en todas las puertas de enlace en la nube de UniFi y las puertas de enlace de próxima generación. Le permite crear una conexión VPN con un solo clic desde su dispositivo móvil o computadora de escritorio a su red doméstica.

Con una VPN tradicional, deberá configurar su red, tal vez abrir puertos, crear un nombre de usuario y una contraseña, etc., antes de poder establecer una conexión VPN. Con UniFi Teleport, solo necesita crear un enlace de invitación en su controlador.

UniFi Teleport le permite establecer una conexión VPN a su propia red con un solo clic. Utiliza el protocolo VPN WireGuard, que suelen utilizar los grandes proveedores de VPN, como NordVPN o Surfshark.

La diferencia con respecto a estos proveedores de VPN es que con el teletransporte creas un túnel VPN a tu propia red. Esto es ideal cuando se encuentra en una red inalámbrica pública y desea acceder de forma segura a su cuenta bancaria u otra información confidencial.

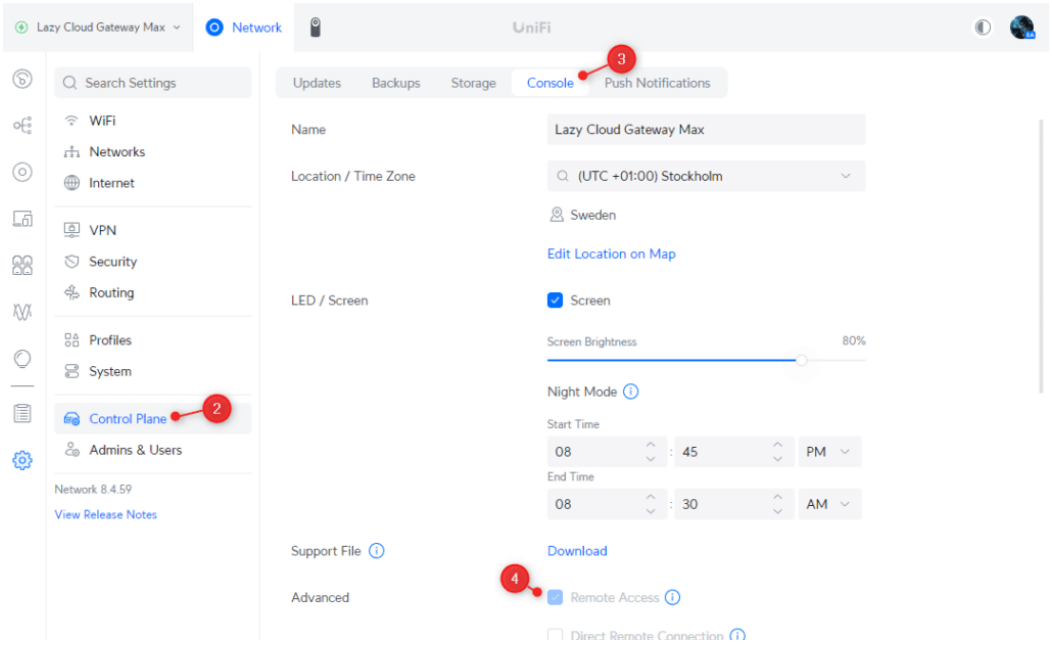
Con Teleport no solo puedes navegar por Internet de forma segura, sino que también puedes acceder a tu red doméstica. Una vez que haya realizado la conexión VPN, puede acceder a todos los dispositivos de su red doméstica como cuando está conectado a su red inalámbrica en casa.

Paso 2. Para el siguiente paso verificaremos el acceso remoto a la consola UniFi debe estar habilitado para usar Teleport. Puede habilitar el acceso remoto en el plano de control. Si está utilizando una versión anterior, encontrará el acceso remoto en la configuración del sistema operativo UniFi.

1. Abre la **aplicación UniFi Network**
2. Vaya a **Configuración** > **plano de control**
3. Abra la **pestaña Consola**
4. Compruebe si **el acceso remoto está habilitado.**

Figura 6_2

Habilitando el acceso remoto para la actualización del sistema en consola



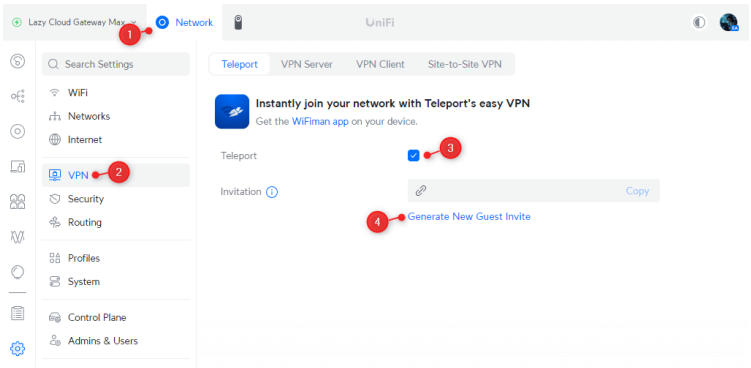
Nota. En la figura se observa Habilitar Acceso Remoto para la actualización del sistema. Fuente: UCG-Ultra (2024)

Paso 3. Para habilitar Teleport es realmente fácil después de haberte asegurado de que todo esté actualizado. Todo lo que tenemos que hacer es habilitar la función en la aplicación UniFi Network.

1. Abre la **aplicación UniFi Network**
2. Ir a **Configuración** > **VPN**
   Habilitar Teletransporte

Figura 6_3

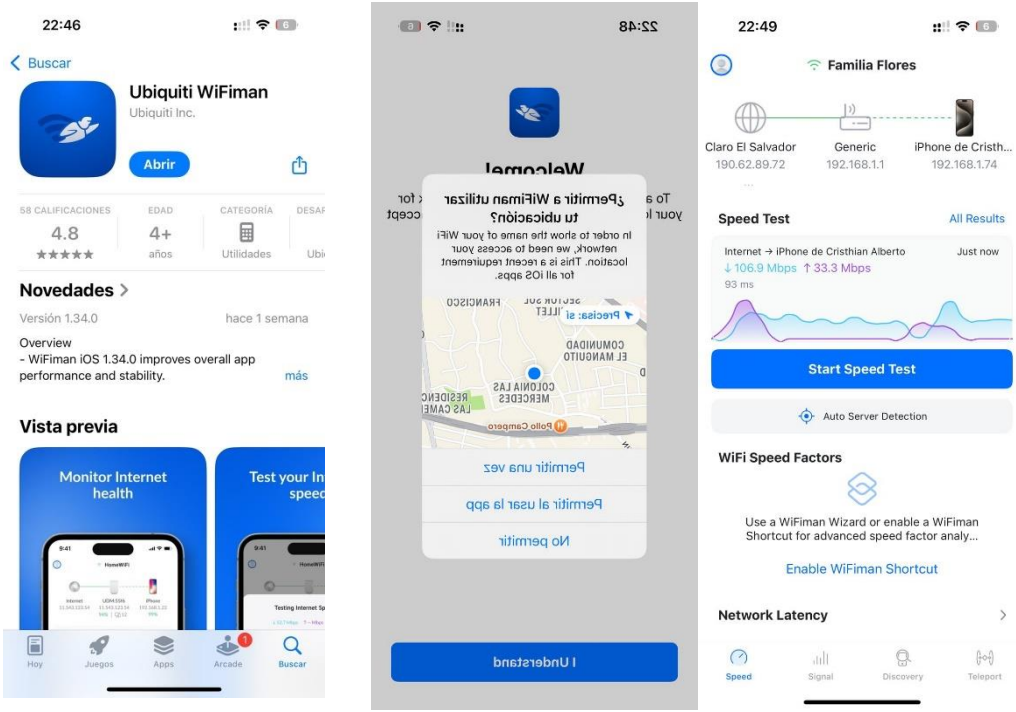
Instalación de aplicación WiFman en celular o PC para funcionamiento de Teleport



Nota. En la figura se observa la Instalación de WIFman y generación de link. Fuente: UCG-Ultra (2024)

Figura 6_4

Instalación directa de aplicación en IOS



Nota. En la figura se puede observar cómo es la Instalación de aplicación WiFman para Sistema operativo iOS. Fuente: UCG-Ultra (2024)

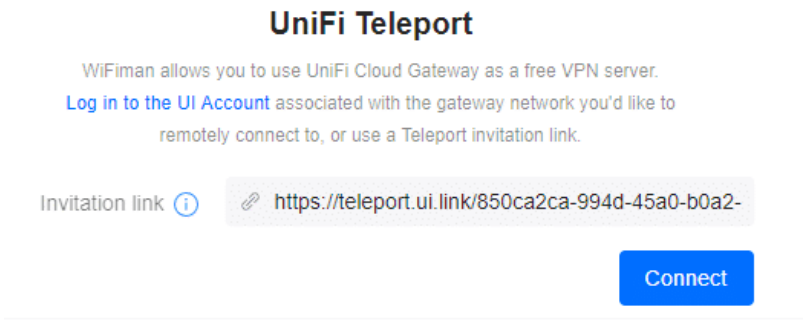
Como se puede observar en la Figura 6_2 Ya está instalada la aplicación así que regresamos a la página de UniFi y generaremos el link para conexión VPN.

Otra opción para conectarse a UniFi Teleport es iniciar sesión con su cuenta de Ubiquiti. Para que esto funcione, debe ser un administrador del sitio y Teleport debe estar habilitado. Si desea ofrecer Teleport a varios usuarios, UniFi Identity también podría ser una buena opción.

Solo necesita generar un nuevo enlace de invitación **(4)** después de haber habilitado Teleport. Ten en cuenta que el **enlace caduco a las 24 horas**. Copie el enlace y envíelo a su dispositivo móvil, como se muestra en la figura

Figura 6_5

Generación de Link mediante Teleport

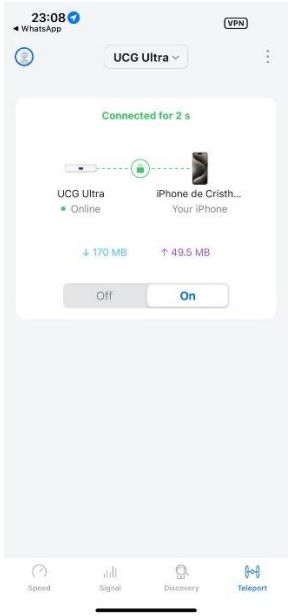


Nota. En la figura se observa cómo es la Generación de Link para iniciar Teleport en WIFman generando conexión VPN. Fuente: UCG-Ultra (2024)

A continuación, veremos cómo se inicia la conexión VPN en nuestro dispositivo móvil

Figura 6_6

Dispositivo móvil ya listo con VPN activada brindada por equipo UniFi UCG-Ultra



Nota. En la figura se muestra la Conexión VPN mediante WIFman. Fuente: UCG-Ultra (2024)

Ahora ya estamos conectados a la VPN creada por UCG-ULTRA mediante Teleport directamente del dispositivo móvil sin embargo Como se mencionó, hay dos formas de usar UniFi Teleport, pero para ambos casos, primero necesitaremos instalar la aplicación WiFiman. Esta aplicación está actualmente disponible para todos los sistemas operativos y dispositivos móviles y de escritorio.

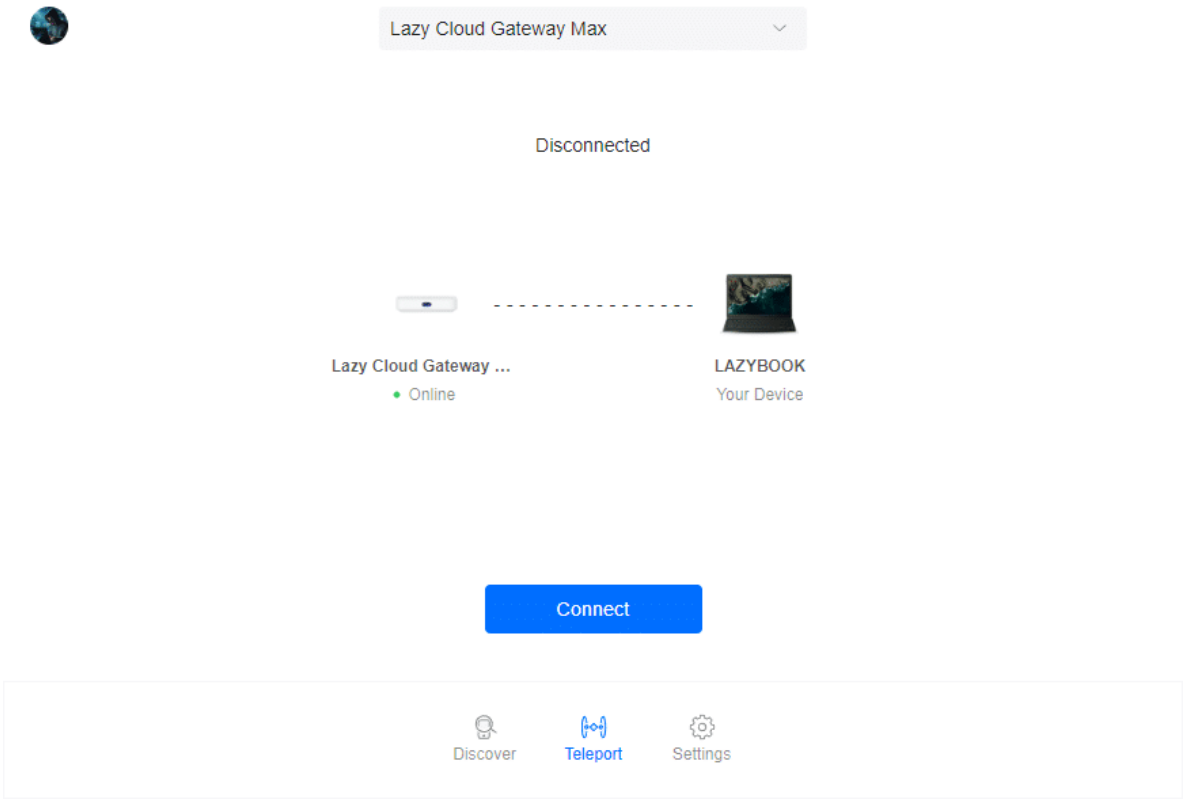
Paso 4. Haremos el segundo paso para la conexión con Teleport. Puede descargar la aplicación WiFiman para aplicaciones de escritorio aquí en la página de descarga de UniFi. Para dispositivos móviles, puede encontrar la aplicación en las tiendas de aplicaciones o usar el código QR del enlace de invitación.

Una vez que haya descargado e instalado WiFiman Desktop, verá la opción de conectarse a UniFi Teleport cuando abra la aplicación. Desde aquí tienes dos opciones, iniciar sesión con la cuenta de administrador del sitio o utilizar el enlace de invitación.

Para iniciar sesión, haga clic en el enlace azul "**Iniciar sesión en la cuenta de UI**" o haga clic en la esquina superior izquierda del icono de usuario y elija **Iniciar sesión**. Esto abrirá el navegador y te permitirá iniciar sesión con tu cuenta de Ubiquiti.

Figura 6_7

Conexión de Teleport mediante PC



Nota. En la figura se observa Conectar a VPN mediante Teleport en PC. Fuente: UCG-Ultra (2024)

Una vez que haya iniciado sesión con éxito, puede seleccionar su UniFi Cloud Gateway de la lista y hacer clic en **Conectar**. Una vez conectado, verá una línea de conexión verde entre su dispositivo y la puerta de enlace en la nube y la cantidad de datos que pasan por la conexión.

Figura 6_8

Link de invitación para Teleport en creación de la VPN

Nota. Link te invitación unifi. Fuente: UCG-Ultra (2024)

Otra opción para conectar la aplicación de escritorio WiFiman es usar el enlace de invitación. Simplemente copie y pegue el enlace en el campo de enlace y haga clic en Conectar. La conexión se recordará, lo que le permitirá volver a conectarse en cualquier momento cuando sea necesario.

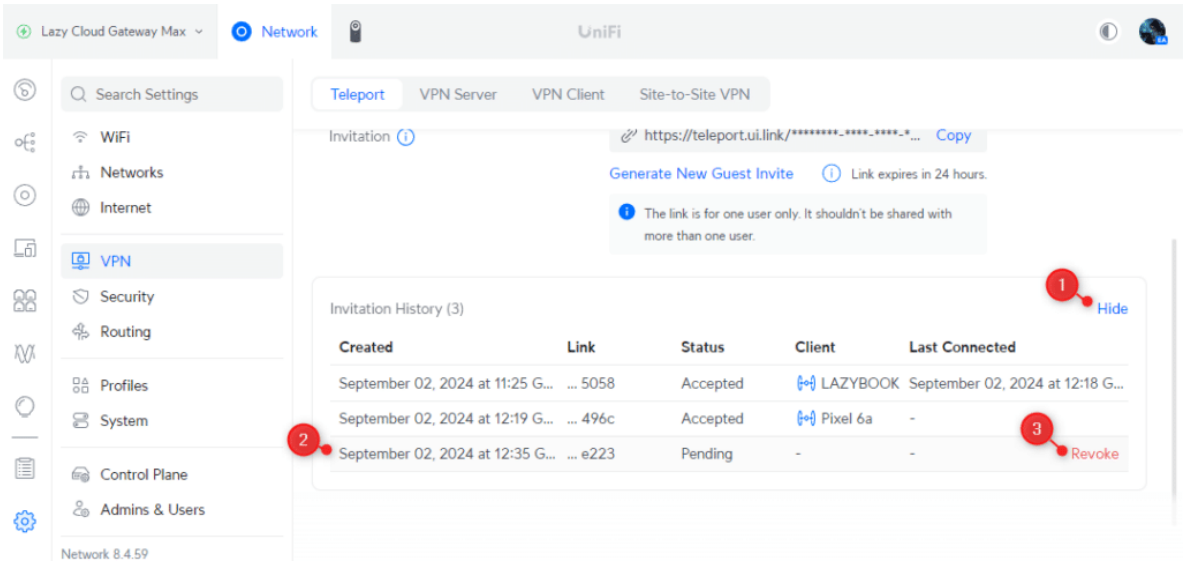
Paso 5. Ahora revocaremos el acceso a Teleport, hay dos formas de revocar el acceso al Teleport UniFi. El método depende del estado de la invitación. Cuando la invitación ya esté aceptada, deberá ir a **Dispositivos cliente** en la red UniFi, seleccionar el dispositivo y **Revocar acceso** en **Configuración**.

Si la invitación aún no ha sido aceptada, puede revocar la invitación desde la pantalla de configuración de Teletransporte.

1. Expanda el **historial de invitaciones** (haga clic en Mostrar)
2. Coloca el cursor sobre una invitación
3. Haga clic en **Revocar**

Figura 6_9

Desconectar conexión VPN



Nota. En la figura se puede observar como Revocar acceso de VPN. Fuente: UCG-Ultra (2024)

Así revocaremos el acceso del usuario al cual se le brindo el link para conectarse mediante VPN y haciendo deficiente el link creado por Teleport.

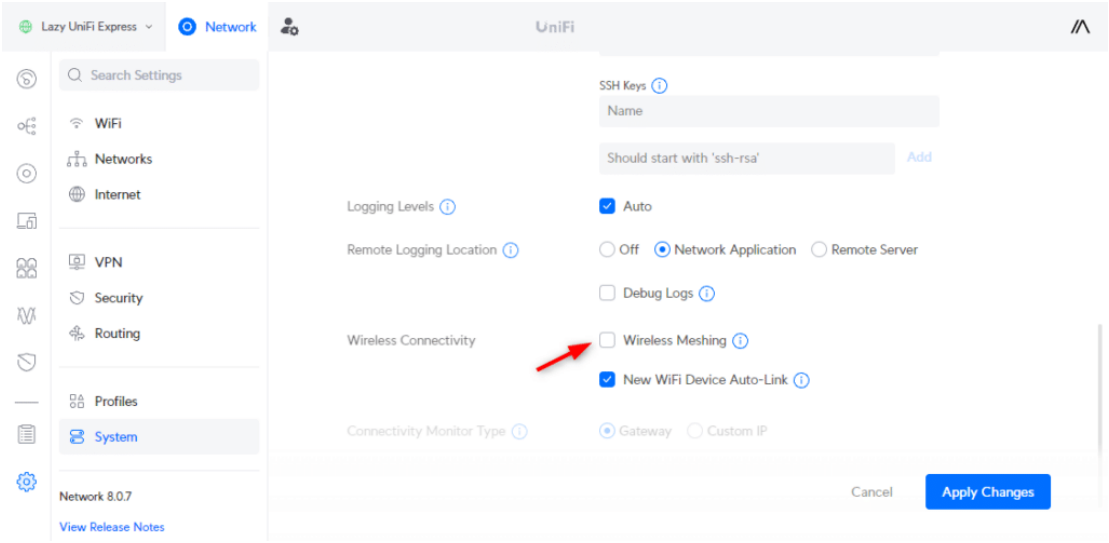
Paso 6. Para El último paso en nuestra configuración de UniFi es verificar la configuración del sistema. Solo hay unas pocas configuraciones que necesitamos verificar/cambiar. Si abre Configuración, asegúrese de verificar primero la configuración del formato de país y hora.

Haga clic en Copias de seguridad y asegúrese de que la copia de seguridad automática esté habilitada. Te recomiendo que cambies el horario a Semanal, para que siempre puedas volver a una versión de copia de seguridad reciente de tu configuración de red UniFi.

Si todos sus puntos de acceso están conectados con un cable Ethernet, entonces no necesita malla inalámbrica. La malla permite que los puntos de acceso se conecten de forma inalámbrica y amplíen su red inalámbrica sin necesidad de tirar de cables Ethernet adicionales.

Figura 6_10

Configuración sobre la copia de seguridad del sistema



Nota. En la figura podemos observar como la Configuración en copia de seguridad se respalda. Fuente: UCG-Ultra (2024)

Si no lo usa, deshabilite la opción Malla inalámbrica en la configuración avanzada.

CONCLUCION

- Se logro aprender a hacer conexiones VPN median te Teleport conociendo su uso y también sus funciones
- Se conocieron las VPN que puede generar por usurario en este apartado, haciendo que el usurario pueda navegar de forma segura añadiendo a sus datos sin dejar rastro por ningún usuario ajeno a la red y dentro del equipo UCG-ULTRA
- Se aprendió de qué manera se puede crear copia de seguridad para que la información quede guardada en el dispositivo UCG-ULTRA

CAPITULO 4. COSTOS DE EQUIPO Y SERVICIOS

4.1 Conexión física de equipo UGC-ULTRA con servicio de internet CLARO

Cuando se menciona hablar del equipo propuesto como una alternativa para la seguridad interna de los negocios en El salvador cabe mencionar la instalación de dichos equipos conlleva un proceso comenzando desde el suministro de nuestra red local con un proveedor de confianza en este caso se escogió a la red Local De claro mediante tecnología HFC para proveer el Cable Modem con la velocidad US y DS adecuadas para la instalación de dicho equipo y garantizar la conectividad para trabajadores y clientes.

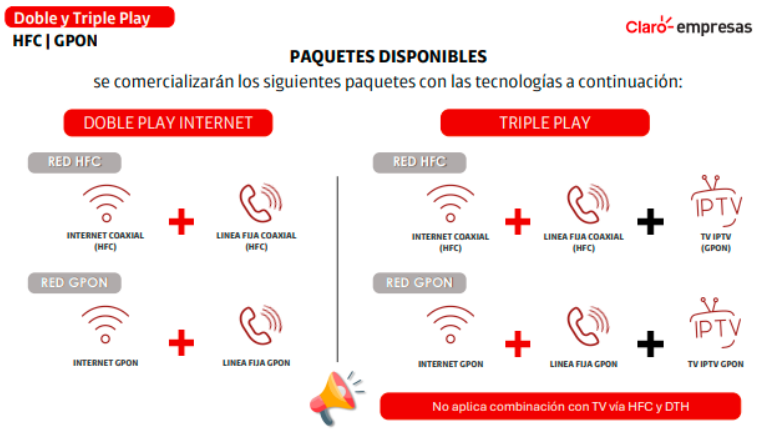
4.1.1 Detalles de Router principal

Para este proyecto se utilizó un Cable Modem CG2200 marca ----- El cual provee una velocidad máxima contratada de 100Mb/s en Subida y 20 Mb/s en bajada, cabe destacar la importancia de saber la velocidad de internet para poder tener un servicio correcto a la hora de proveer un servicio.

En cuanto al servicio contratado lo ideal sería escoger siempre un plan empresarial ya que es más directo en cuanto atención al cliente y más inmediato con reparaciones técnicas sin embargo se optará colocar los planes más accesibles y funcionales para las empresas.

Figura 3

Paquetes combinados HFC y Fibra óptica.



Nota. Información de internet CLARO. Fuente: Claro(2025)

Para esta ocasión a la hora de escoger plan nos será Útil Tecnología HFC o Fibra Óptica sin problema.

Tabla 2

Tabla de precios ante paquetes de velocidad CLARO

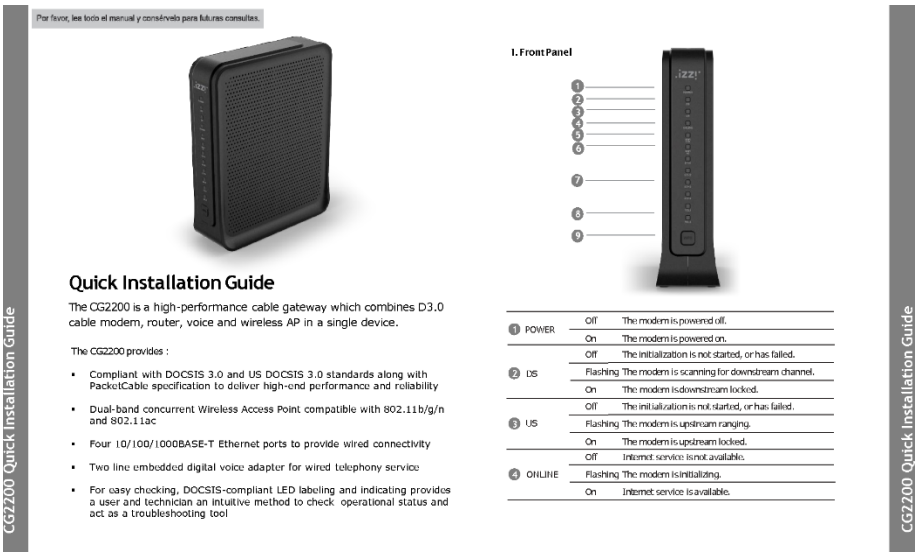
TECNOLOGIA	VELOCIDAD	PRECIO
FIBRA OPTICA/ HFC	100 Mb/s	$25
FIBRA OPTICA/ HFC	200 Mb/s	$31
FIBRA OPTICA/ HFC	300 Mb/s	$38
FIBRA OPTICA/ HFC	400 Mb/s	$45
FIBRA OPTICA/ HFC	500 Mb/s	$60

Nota. Tabla de velocidades y precios contratados Fuente: Claro (2025)

Basado en estos precios optaremos por el mejor precio que nos funcionara de manera más óptima.

Figura 4.

Guía de características para Cable Modem CG2200



Nota. Router CG2200. Fuente: Kaon(2018)

Este modem modelo CG2200 nos permite tener acceso a la navegación asimétrica para los usuarios a conectarse o también podría ser la conexión a un Router de Fibra óptica con las mismas características a diferencia que se tiene un ping más estable y una conexión más estable

Figura 5

ONT de fibra óptica para emisión de internet

Nota. Router ONT Huawei modelo HG8245W5-6T. Fuente: Huawei(2020)

Como el que se presenta en la Figura 43, este es un Router con tecnología GPON es alimentado por un hilo de fibra óptica quien garantiza una conexión mucho más eficiente.

Se interconectan entre el equipo **Ubiquiti Cloud Gateway Ultra** mediante un cable de red para su comunicación de la siguiente manera:

Figura 6

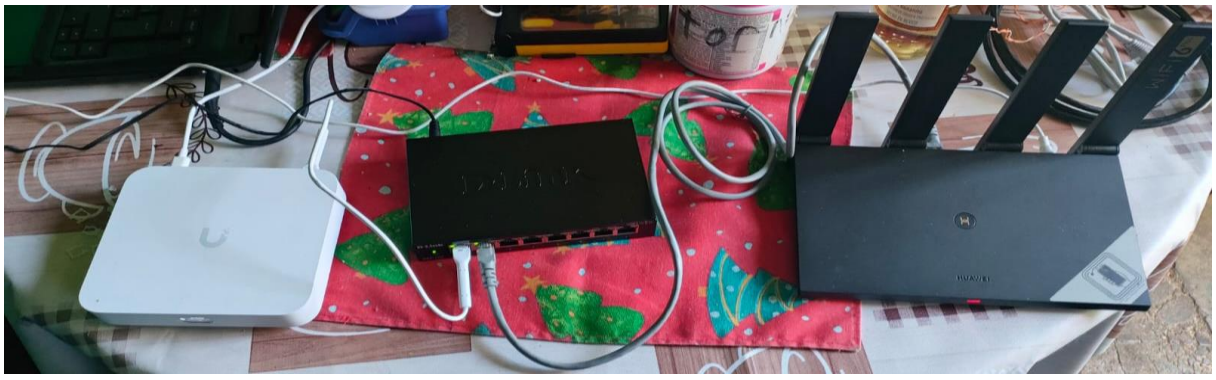
Equipo UCG-Ultra conectado a un Cable Model CG2200

Nota. Conexión entre Router y Ubiquiti Cloud Gateway ultra. Fuente: Propia (2024)

Ya enlazado y configurado para tener acceso a la red se interconecta en la salida del Equipo mediante cable de red un Amplificador de redes wifi para garantizar conexión directa al equipo mediante cable ETHERNET o Wifi para los clientes de la siguiente manera:

Figura 7

Interconexión con UCG-Ultra a switch y a replicador AX3-Pro



Nota. Conexión de equipo Ubiquiti Cloud Gateway Ultra a Replicador Huawei AX3. Fuente: Propia(2024)

Siguiendo a la instalación se tiene que configurar el Replicador de señal instalado de manera en que replique la señal internet con las restricciones que fueron configuradas en el equipo

Ubiquiti controlando cada uno de los equipos en los que se enlazaran a la red en él se utilizará el equipo Huawei Ax3 debido a que este cumple con las características esperadas.

Figura 8

Switch 100/1000/10000 marca Cisco

Nota. Switch Marca Cisco 10/100/1000 de 8 Puertos. Fuentes: Cisco(2018)

4.2 Precios de instalación de equipo completo

Cuando se habla de la seguridad en la red interna de una empresa cabe destacar que toda la información está en ella, cuentas, dinero, datos importantes, etc.

Por eso es importante invertir en un equipo que proteja la información total, en el que limite y controle lo que se busca en la red o a lo que se quiere acceder, se pretende demostrar que de manera económica se puede optar por un par de alternativas en equipos que nos funcionen para dicha acción.

En esta tesis se habla del equipo **Ubiquiti Cloud Gateway Ultra** como una alternativa para la seguridad de una empresa, se cotizo el equipo en si dándonos un precio total $147.82 + IVA.

Figura 9

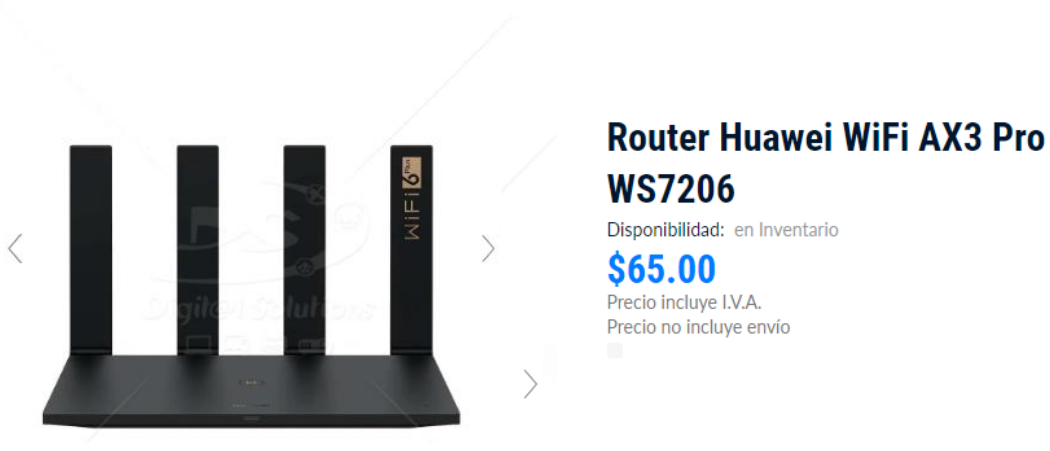
Precio de UCG-Ultra

Nota. Cotización de equipo Ubiquiti cloud Gateway. Fuente: UniFi (2022)

Cuando se trata del replicador que se utilizara se cotiza en diferentes áreas para conseguir el mejor precio

Figura 10

Replicador de internet AX3 marca Huawei modelo WS7206



Nota. Cotización de Replicador Huawei Ax3. Fuente: Huawei(2015)

Se toma en cuenta también El precio del switch 10/100/1000 cotizándolo y de la siguiente manera se consiguió

Figura 11

Precio para switch Cisco 100/1000/10000

Nota. Cotización de Equipo switch cisco 8 puertos 10/100/100. Fuente: Cisco(2015)

El metraje del cable es importante también y se cotizo de la siguiente manera junto a sus conectores:

Figura 12

Cotización de cable UTP Cat 6 y conector RJ45

Nota. Cotización de Cable UTP CAT 6 y Conectores RJ45 Fuente: Freund(2025)

En total estaríamos hablando de una inversión en seguridad

Tabla 3

Suministración e instalación de equipo UCG-Ultra con su respectiva LAN

ITEM	DESCRIPCION	CANT.	UNIDAD	PRECIO UNIT	SUB TOTAL
Obras Eléctricas -Suministro e instalación					
COSTO FIJO					
1	Equipo Ubiquiti Cloud Gateway Ultra - Router y Gateway	1	UN	$ 147.82	$ 147.82
2	Replicador de internet Huawei Ax3 Pro WS7206	1	UN	$ 65.00	$ 65.00
3	Switch marca CISCO 10/100/1000 Mbps de 8 puertos	1	UN	$ 31.00	$ 31.00
4	Metraje de Cable UTP CAT 6 Color azul	7	ML	$ 2.25	$ 15.75
COSTO VARIABLE					
1	Servicio de Internet Mensual Claro de 100 Mbps (Mensual con instalación gratis de parte de empresa)	1	UN	$ 25.00	$ 25.00
	TOTAL	**TOTAL, SIN IVA**			**$ 284.57**

Nota. Tabla de Precio final. Fuente: Construcciones Barrera (2025)

Se debe tener en cuenta que la instalación realizada por contratación a otra empresa incrementaría el precio significativamente dependiendo de la empresa sin embargo se estipula instalación propia cotizada por otra empresa y que se consiguiera todo.

También se toma en cuenta que la inversión solamente sería el equipo de seguridad y lo que conlleva su instalación ya si se quisiera tener un switch más grande o también mayor cantidad de amplificadores de señal según el tamaño de la empresa el precio incrementaría y mayor velocidad de internet, sin embargo, se ha tomado en cuenta teniendo lo más básico para poder proteger de manera óptima la red según las especificaciones ya mencionadas en esta tesis.

CAPITULO 5. MANUAL DE IMPLEMENTACIÓN DE ISO/IEC 27001:2022 APLICADO EN PYMES

5.1 INTRODUCCION ISO/IEC 27001:2022

Se presente como una guía práctica para ayudar a las medianas y pequeñas empresas (PYMES) a establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La norma ISO/IEC 27001:2022 proporciona un marco para gestionar la seguridad de la información, protegiendo los datos críticos de la organización y garantizando la confidencialidad, integridad y disponibilidad de la información.

- La norma es aplicable a organizaciones de cualquier tamaño y sector.
- Su enfoque principal es proteger la información mediante la identificación de riesgos y la implementación de controles adecuados.
- Para PYMES en El Salvador, es especialmente relevante debido al creciente uso de tecnologías digitales y la necesidad de proteger datos sensibles en un entorno de ciber amenazas en aumento.

Figura 12

Logo oficial de la regla ISO 27001:2022

Nota. Representación de ISO 27001:2022. Fuente: Udemy (2025)

5.2 Beneficios para PYMES

- Protección de datos: Garantiza la seguridad de la información crítica de la empresa siendo uno de los pilares fundamentales del Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo principal es garantizar la seguridad de la información crítica de la empresa, asegurando su confidencialidad, integridad y disponibilidad. A continuación, se presenta un resumen detallado de cómo la norma aborda la protección de datos:

- Cumplimiento legal: Ayuda a cumplir con regulaciones locales e internacionales.

  es un aspecto crítico dentro del Sistema de Gestión de Seguridad de la Información (SGSI). La norma exige que las organizaciones identifiquen y cumplan con las obligaciones legales, regulatorias y contractuales relacionadas con la seguridad de la información. A continuación, se presenta un resumen detallado de cómo la norma aborda el cumplimiento legal.

  El cumplimiento legal no solo es una obligación, sino también una forma de proteger a la organización de sanciones, multas y daños reputacionales. La ISO/IEC 27001:2022 ayuda a las empresas a:

  1. Identificar las leyes y regulaciones aplicables.
  2. Implementar controles para cumplir con estos requisitos.
  3. Demostrar conformidad ante auditores, clientes y autoridades.

Controles Relacionados con la Protección de Datos

El Anexo A de la norma proporciona una lista de controles que las organizaciones pueden implementar para proteger los datos. Algunos de los controles más relevantes incluyen:

- **A.8.2 - Gestión de activos de información:**
- Identificar y clasificar los activos de información (por ejemplo, datos críticos, sensibles o públicos).
- Asignar responsabilidades para la protección de cada activo.

- **A.8.3 - Protección de la información en medios:**
- Implementar medidas para proteger datos almacenados en dispositivos físicos (por ejemplo, discos duros, USB).
- Asegurar la eliminación segura de datos cuando ya no sean necesarios.

A.8.4 - Control de acceso:

- Restringir el acceso a la información solo a personal autorizado.

- Implementar autenticación fuerte (por ejemplo, contraseñas complejas, autenticación de dos factores).

A.8.10 - Cifrado:

- Utilizar técnicas de cifrado para proteger datos en tránsito (por ejemplo, correos electrónicos, transferencias de archivos) y en reposo (por ejemplo, bases de datos, archivos).

A.8.12 - Prevención de fuga de datos:

- Implementar soluciones para detectar y prevenir la filtración de información sensible (por ejemplo, sistemas DLP - Data Loss Prevention).

A.8.23 - Seguridad en redes:

- Proteger la red local mediante firewalls, segmentación de red y monitoreo de tráfico.

A.8.31 - Copias de seguridad:

- Realizar copias de seguridad regulares de datos críticos y asegurar su restauración en caso de incidentes.

La norma exige que las organizaciones realicen una evaluación de riesgos para identificar amenazas a la protección de datos (por ejemplo, ciberataques, errores humanos, desastres naturales). Con base en esta evaluación, se deben seleccionar e implementar controles adecuados para mitigar los riesgos identificados.

- Confianza del cliente: Demuestra compromiso con la seguridad de la información.

  La ISO/IEC 27001:2022 no solo es una herramienta para mejorar la seguridad de la información, sino también un mecanismo para generar confianza del cliente. Al implementar la norma, las organizaciones demuestran su compromiso con la protección de datos, lo que se traduce en relaciones más sólidas y duraderas con los clientes. Para PYMES, esto puede ser un factor clave para diferenciarse en el mercado y acceder a nuevas oportunidades de negocio.

- Reducción de riesgos: Minimiza el impacto de posibles brechas de seguridad.

la reducción de riesgos es uno de los objetivos centrales del Sistema de Gestión de Seguridad de la Información (SGSI). La norma proporciona un enfoque sistemático para identificar, evaluar y tratar los riesgos asociados a la seguridad de la información, con el fin de minimizar el impacto de posibles brechas de seguridad.

La norma establece requisitos específicos para la gestión de riesgos:

La organización debe identificar los riesgos asociados a la pérdida de confidencialidad, integridad o disponibilidad de la información.

Cláusula 6.1.3 - Evaluación de riesgos:

- Se debe evaluar la probabilidad y el impacto de cada riesgo identificado.
- Esto permite priorizar los riesgos que requieren atención inmediata.

Cláusula 6.1.3 - Tratamiento de riesgos:

- La organización debe seleccionar e implementar controles para tratar los riesgos. Estos controles pueden incluir medidas técnicas, organizativas o físicas.

Anexo A - Controles de Seguridad:

- El Anexo A proporciona una lista de 93 controles organizados en 4 categorías (organizativos, de personas, físicos y tecnológicos) que ayudan a reducir los riesgos. Algunos ejemplos incluyen:

A.5.1 - Políticas para la seguridad de la información.

A.8.2 - Gestión de activos de información.

A.8.3 - Protección de la información en medios.

A.8.4 - Control de acceso.

A.12.6 - Gestión de vulnerabilidades técnicas.

4.3 Implementación

Definir el alcance del SGSI:

Identificar los activos de información críticos (por ejemplo, datos de clientes, financieros, propiedad intelectual). Delimitando el ámbito de aplicación (por ejemplo, la red local, servidores, dispositivos móviles).

Realizar una evaluación de riesgos:

- Identificar amenazas (por ejemplo, malware, phishing, acceso no autorizado).
- Evaluar vulnerabilidades en la red local (por ejemplo, contraseñas débiles, falta de cifrado).

Seleccionar controles de seguridad:

Basarse en el Anexo A de la norma, que incluye 93 controles organizados en 4 categorías:

1. Controles organizativos: Políticas de seguridad, roles y responsabilidades.
2. Controles de personas: Concientización y capacitación del personal.
3. Controles físicos: Protección de equipos y accesos físicos.
4. Controles tecnológicos: Firewalls, antivirus, cifrado de datos.

Implementar controles en la red local:

- Firewalls: Para filtrar tráfico no autorizado.
- Cifrado de datos: Para proteger información sensible en tránsito y en reposo.
- Autenticación fuerte: Uso de contraseñas complejas y autenticación de dos factores (2FA).
- Actualizaciones de software: Mantener sistemas y aplicaciones actualizados para evitar vulnerabilidades.

Copias de seguridad: Realizar backups regulares de datos críticos.

- Documentar políticas y procedimientos Creando un manual de seguridad que incluya políticas de acceso, uso aceptable de recursos y respuesta a incidentes.

Monitoreo y mejora

Realizar auditorías internas para verificar el cumplimiento del SGSI y Revisando las actualizaciones periódicamente con sus controles de seguridad.

4.4 Alternativas de Seguridad de Datos en la Red Local

Para PYMES en El Salvador, las siguientes alternativas son viables y efectivas:

- Firewalls de próxima generación (NGFW): Protegen la red local contra amenazas avanzadas.

- Soluciones de cifrado: Herramientas como BitLocker (Windows) o VeraCrypt para cifrar discos y archivos.
- Antivirus y antimalware: Soluciones como ESET, Kaspersky o Avast para proteger dispositivos.
- Redes privadas virtuales (VPN): Para asegurar conexiones remotas a la red local.
- Segmentación de red: Dividir la red en subredes para limitar el acceso a áreas críticas.
- Sistemas de detección de intrusos (IDS): Monitorean la red en busca de actividades sospechosas.

4.5 Consideraciones para PYMES en El Salvador

- Recursos limitados: Priorizar controles de seguridad según el presupuesto y los riesgos identificados.
- Concientización local: Adaptar las políticas de seguridad al contexto cultural y operativo del país.
- Proveedores locales: Buscar soluciones de seguridad ofrecidas por empresas locales con soporte en español.

La implementación de ISO/IEC 27001:2022 en PYMES de El Salvador no solo mejora la seguridad de la información, sino que también fortalece la competitividad y la confianza de los clientes. Al adoptar alternativas de seguridad adecuadas para la red local, las empresas pueden proteger sus datos críticos y reducir el riesgo de ciberataques.

CAPITULO 6. MANUAL DE RECOMENDACIONES DE BUENAS PRACTICAS DE SEGURIDAD DE LA INFORMACION

6.1 Manual de buenas practicas

INTRODUCCION

Al igual que las amenazas informáticas en general, los códigos maliciosos fueron evolucionando al mismo tiempo de las tecnologías de información y comunicación, aumentando considerablemente el nivel de complejidad y agresión. Es por eso que la visión y la filosofía de CFP VERGE DE CORTES consideran la protección de manera proactivo, no sólo a través de sus soluciones de seguridad sino también a través de la educación. Es necesario que los usuarios incorporen buenas prácticas para proteger el ámbito de información, y prevenir más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan tirar provecho de las debilidades humanas. Pero para eso inevitablemente se deben conocer los peligros latentes, y como detenerlos a través de mecanismos de prevención. El presente documento expone medidas de seguridad tendentes a minimizar el volumen de "potenciales víctimas", brinda herramientas preventivas para cada una de las tecnologías y servicios más populares y más utilizados por los usuarios y aborda en cada punto los mecanismos de prevención que permiten detectar, de manera tempranera y sin acciones complejas, las acciones maliciosas más comunes. El presente código de buenas prácticas en seguridad informática está orientado a todo el personal que trabaja para lo en nombre de las PYMES

OBJETIVOS GENERALES

- El principal objetivo para el usuario es poder leer y comprender a detalle este pequeño manual el cual se aclara puntos importantes en los cuales puede estar amenazada su información con soluciones firmes para tener buenas prácticas a la hora del maneje de datos e informaciones delicadas.

OBJETIVOS ESPECIFICOS

- Promover el uso de contraseñas seguras mediante la adopción de buenas prácticas de gestión y autenticación multifactorial.
- Fomentar la actualización y protección de dispositivos para mitigar vulnerabilidades y prevenir accesos no autorizados.
- Garantizar el uso seguro de redes e internet, reduciendo el riesgo de ataques y filtraciones de información.
- Reducir el riesgo de ataques de phishing y malware mediante buenas prácticas en la gestión del correo electrónico.

- Proteger la información sensible a través de políticas de cifrado, clasificación y control de acceso.
- Implementar estrategias de respuesta ante incidentes de seguridad, estableciendo protocolos de detección, reporte y mitigación de amenazas.

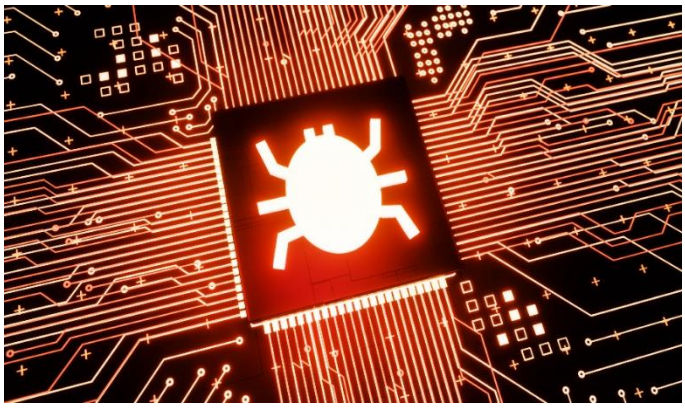
6.2 MANTENER ACTUALIZADO SISTEMA OPERATIVO Y LAS APLICACIONES

Malware (del inglés malicious software), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar un ordenador sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones para referirse a todos los tipos de malware, incluyendo los verdaderos virus. La historia del malware los brinda la respuesta de por qué es importante mantener actualizados los sistemas operativos (SO) y las aplicaciones con sus correspondientes parches de seguridad. En cuanto a este aspecto de la seguridad, las medidas prácticas de prevención se enfocan en:

- No descargar actualizaciones desde sitios de dudosa reputación y hacerlo sólo desde sitios de confianza. Descargar las actualizaciones desde sitios no oficiales implica un potencial riesgo de infección.
- Descargar las actualizaciones a través de los mecanismos ofrecidos por el fabricante.
- Para las plataformas Microsoft se pode: o Acceder al sitio web de Windows Update para obtener los últimos parches de seguridad. o Configurar en el Centro de Seguridad de Windows la automatización, o no, de descarga de actualizaciones. o Implementar (en ámbitos corporativos) los WSUS (Windows Server Update Services) de Microsoft.

Figura 13

Representación Malware.



Nota. Malware. Fuente: Apunts (2020)

6.3 Aseguramiento del sistema operativo

Otro de los aspectos importantes en materia de prevención, radica en configurar el sistema operativo para hacerlo más seguro. Entre las buenas prácticas que se pueden tener en cuenta se encuentran:

- Utilizar contraseñas fuertes. El empleo de contraseñas donadas de recordar es otra de las debilidades que los códigos maliciosos suelen aprovechar para propagarse por los recursos de información.
- Crear un perfil de usuario con privilegios restringidos. Por defecto, usuario que crean las plataformas Windows al punto de su implementación posee privilegios administrativos. Esto es un factor que aumenta la probabilidad de infección.
- Deshabilitar la ejecución automática de dispositivos USB. Los dispositivos de almacenamiento que se conectan al puerto USB constituyen un vector de ataque muy empleado por el malware para la propagación, sobre todo, de vermes.
- Configurar la visualización de archivos ocultos ya que la mayoría de los códigos maliciosos se esconden en el sistema con este tipo de atributos.
- Configurar la visualización de las extensiones de archivos para poder identificar las extensiones de los archivos descargados y no ser víctimas de técnicas como la doble extensión

Figura 14

Representación de peligro en PC

Nota. Representación de peligro en PC. Fuente: Apunts (2020)

6.4 Protección de correo Electrónico

El correo electrónico constituye una de los canales de propagación/infección de malware más utilizados por atacantes; por lo tanto, es importante que los usuarios incorporen como hábito determinadas prácticas que permitan prevenir los ataques realizados a través de que códigos maliciosos. En consecuencia, a continuación, se presenta una serie de medidas preventivas orientadas a aumentar la seguridad durante lo uso del correo electrónico

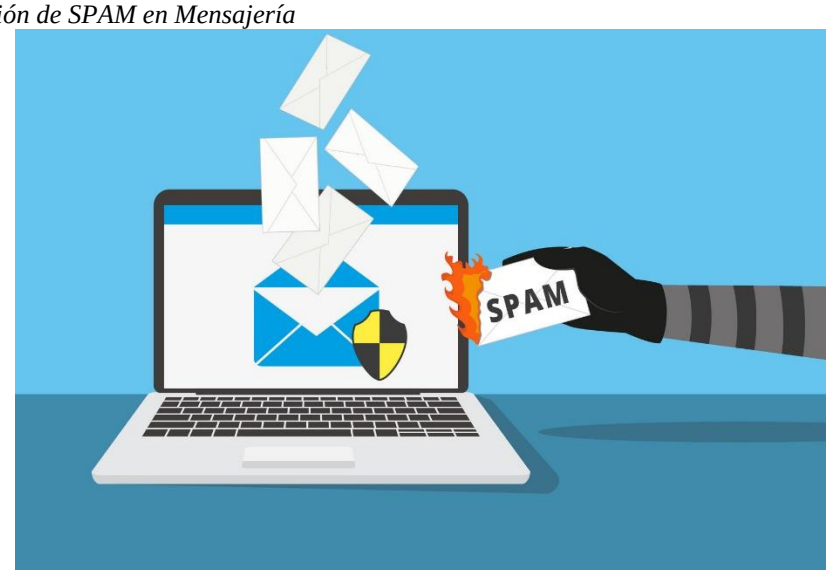
6.4.1 Spam

Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican, de alguna o varias maneras al receptor. Constituye uno de los principales medios de propagación de una importante cantidad de códigos maliciosos y por lo tanto se recomienda:

- No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Esto asegura que no se ejecutará un malware.
- Cuando se reciben adjuntos, prestar especial atención a las extensiones de estos, ya que suelen utilizar técnicas de engaño como la doble extensión o espacios entre el nombre del archivo y la extensión de este
- Evitar publicar las direcciones de correo en sitios web de dudosa reputación como foros, chats, entre otros.
- Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.
- No responder jamás el correo spam. ES preferible ignorarlos y/o borrarlos, ya que se responde se confirma que la dirección de correo se encuentra activa.
- Dentro de lo posible, evitar el re-envío de mensajes en cadena, ya que suelen ser utilizados para recoger direcciones de correo activas.
- Si de todas formas se desea enviar mensajes en cadena, es recomendable hacerlo siempre con copia oculta para que quien lo recibe léela sólo la dirección del emisor.
- Utilizar claves seguras y cambiar la contraseña con periodicidad.
- Configurar la pregunta secreta, además, de una forma que no sea adivinable para fortalecer aún más la seguridad de la cuenta.
- Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino.

Figura 15

Representación de SPAM en Mensajería



Nota. Representación de SPAM. Fuente: Apunts (2020)

6.4.2 PUSHING

El phishing es una modalidad delictiva encuadrada en la figura de estafa realizada a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico caracterizado por intentar adquirir información confidencial de forma fraudulenta (cómo puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). Entre las buenas prácticas de seguridad que se recomiendan a los usuarios, para que estos eviten ser víctimas del phishing, están las siguientes:

- Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio.
- Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles.
- No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden re-direccionar hacia sitios web clonados o hacia la descarga de malware.
- Asegurarse de que la dirección del sitio web al cual se accede comience con el protocolo https. La "s" final, significa que la página web es segura y que toda la información depositada en esta viajará de manera cifrada.
- Verificar la existencia de un certificado digital en el sitio web. El certificado digital se despliega en pantalla al hacer clic sobre la imagen del candado.
- Revisar que el certificado digital no caducara, ya que este podría haber sido manipulado intencionalmente con fines maliciosos
- Comunicarse telefónicamente con la compañía para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo.
- Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.

Figura 16

Representación de Pushing en ataques

Nota. Representación de Pushing. Fuente: Apunts (2020)

6.5 Seguridad en la NAVEGACION

Nos últimos años, Internet se transformó en una plataforma de ataque donde acciones delictivas se llevan a cabo a través de diferentes técnicas como por ejemplo el Drive-by-Download que permite infectar masivamente los usuarios simplemente ingresando a un sitio web determinado. Mediante esta técnica, los creadores y diseminadores de malware propagan sus creaciones aprovechando las vulnerabilidades existentes en diferentes sitios web e inyectando código dañino entre su código original.

Figura 17

Representación de la seguridad informática

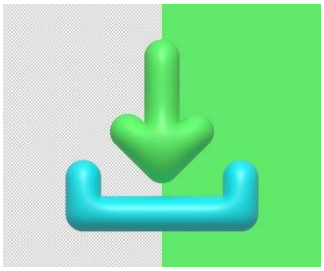
Nota. En la figura podemos observar la Seguridad de información. Fuente: Apunts (2020)

En consecuencia, es fundamental navegar con cautela y tener presentes las recomendaciones más importantes. Entre ellas:

- Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser. ES importante no hacer clic sobre el botón ejecutar ya que esto provoca que el archivo se ejecute automáticamente después de descargado, dejando a la margen a posibilidad de verificar su integridad.
- Descargar programas de seguridad solamente desde lo sitio oficial de este, para evitar la descarga de archivos que pudiesen previamente ser manipulados con fines delictivos.
- A ser posible, leer atentamente las políticas de privacidad de las aplicaciones descargadas desde sitios web no oficiales o de dudosa reputación, antes de instalarlas.
- No realizar la instalación de complementos extras como barras de tareas o protectores de pantallas sin verificar previamente su autenticidad.
- Configurar el navegador web para minimizar el riesgo de ataques a través de este.

Figura 18

Representación de la descarga en PC.



Nota. Figura de la presentación de las Descargas. Fuente: Apunts (2020)

6.6 Seguridad en las redes sociales

En la actualidad, las redes sociales son muy populares y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware. Por tal motivo, se torna necesario tener en cuenta y aplicar las siguientes medidas preventivas:

- Intentar no publicar información sensible y confidencial, debido la que personas extrañas pueden aprovechar esta información con fines maliciosos.
- También es recomendable evitar la publicación de fotografías propias y de familiares.
- Mantener la privacidad del perfil; es decir, configurar el perfil para que no sea público.
- No responder a las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o pueden formar parte de actividades delictivas.
- No abrir contenidos con spam a través de este medio. De este modo se evita formar parte del ciclo de vida del spam.
- Cambiar periódicamente la contraseña para evitar que esta sea descubierta fácilmente.
- Antes de aceptar contactos espontáneos, es recomendable verificar su existencia y que realmente provienen de quien dice ser.

Figura 19

Representación de las redes sociales en PC y aplicaciones

Nota. En la figura siguiente se observa Redes sociales. Fuente: Apunts (2020)

6.7 Seguridad en mensajería instantánea

Otro medio de comunicación popular, y que se emplea masivamente, es la mensajería instantánea, que, en consecuencia, constituyen uno de los vehículos más explotados por diferentes amenazas, dentro de las cuales una de las más activas es el malware. Para prevenir ser víctimas de acciones maliciosas llevadas a cabo a través de esta tecnología, se recomienda aplicar alguna de las medidas de seguridad que a continuación se describen:

- Evitar aceptar cómo contacto cuentas desconocidas sin verificar a quien pertenece, ya que en la mayoría de los casos se trata de intentos de engaños con fines maliciosos.
- No descargar archivos sospechosos, sobre todo cuando vienen acompañados de mensajes genéricos o en otro idioma. Esto constituye una de las características principales de los códigos maliciosos que se propagan a través de este canal de comunicación.
- En caso de descargar archivos, explorarlos con una solución antivirus.
- Configurar en la mensajería a exploración automática de archivos en el momento de su recepción. La mayoría disteis clientes consideran la posibilidad de configurarlos con un antivirus.
- Es recomendable, al igual que con el correo electrónico, no hacer clic sobre los enlaces incrustados en el cuerpo del mensaje, ya que pueden direccionar las páginas con contenido malicioso o hacia la descarga de malware.
- En el compartir información confidencial a través de este medio ya que esta puede ser interceptada y robada con fines delictivos.
- Cuando se reciben mensajes conteniendo uno enlace no esperado, es recomendable preguntar si la otra persona realmente lo envió; de este modo se pode verificar la autenticidad de este

Figura 20

Representación de la mensajería instantánea en los dispositivos móviles

Nota. Figura de Mensajería instantánea. Fuente: Apunts (2020)

6.8 Seguridad en dispositivos de almacenamiento

Los dispositivos de almacenamiento que se conectan a través del puerto USB (memorias, cámaras digitales, teléfonos móviles, etc.), constituyen otro de los mayores focos de propagación/infección de códigos maliciosos. Por lo tanto, es necesario tener presente alguna de las siguientes medidas que ayudan a mantener el ámbito de información con un nivel acomodado de seguridad, ya sea en ámbitos corporativos como en ámbitos caseros:

- Establecer políticas que definan el uso correcto de dispositivos de almacenamiento. Esto ayuda a tener claro las implicancias de seguridad que lleva consigo el uso de estos dispositivos.
- Brindar acceso limitado y controlado de los usuarios que utilizan estos dispositivos, para controlar la propagación de potenciales amenazas y el robo de información.
- De ser necesario, registrar el uso de estos y/o habilitar/deshabilitar puertos del tipo USB.
- Si se transporta información confidencial en estos dispositivos, es recomendable cifrarla. De esta manera, en caso de robo o extravío, la información no podrá ser vista por terceros.
- ES recomendable explorar con el antivirus cualquier dispositivo que se conecte el ordenador para controlar a tiempo una posible infección.
- Deshabilitar la ejecución automática de dispositivos en los sistemas operativos Microsoft Windows, ya que muchos códigos maliciosos aprovechan la funcionalidad de ejecución automática de dispositivo s de las plataformas Microsoft para propagarse a través de un archivoAutorun.inf.

6.9 CONCLUCION

Implementar estas buenas prácticas contribuye significativamente a reducir los riesgos de seguridad de la información. La concienciación y el cumplimiento de estas recomendaciones ayudan a crear un entorno digital más seguro y confiable.

CAPITULO 7. CONCLUCION DE TRABAJO DE GRADUACION

CONCLUCION

La seguridad de los datos en la red local es un desafío crítico para las medianas y pequeñas empresas (PYMES) en El Salvador, especialmente en un entorno donde las ciber amenazas son cada vez más sofisticadas y frecuentes. Esta tesis ha explorado alternativas de seguridad viables y efectivas, centrándose en la implementación del equipo Ubiquiti Cloud Gateway Ultra como una solución integral para proteger los activos de información en redes locales.

A lo largo de la investigación, se demostró que el Ubiquiti Cloud Gateway Ultra es una herramienta robusta y escalable que ofrece múltiples funcionalidades de seguridad, como firewalls avanzados, control de acceso, segmentación de red y monitoreo en tiempo real. Estas características lo convierten en una opción ideal para PYMES que buscan proteger sus datos sin incurrir en costos excesivos o complejidades técnicas innecesarias. Además, su integración con el ecosistema Ubiquiti permite una gestión centralizada y remota, lo que facilita su administración incluso para empresas con recursos limitados.

La implementación de este equipo, junto con buenas prácticas de seguridad como el cifrado de datos, la actualización regular de software y la capacitación del personal, permite a las PYMES salvadoreñas fortalecer su postura de seguridad y reducir significativamente los riesgos de ciberataques. Asimismo, se evidenció que la adopción de soluciones como el Ubiquiti Cloud Gateway Ultra no solo protege los datos críticos, sino que también contribuye al cumplimiento de estándares internacionales como la ISO/IEC 27001:2022, mejorando la confianza de clientes y socios comerciales.

En el contexto de El Salvador, donde muchas PYMES carecen de recursos técnicos y financieros para implementar soluciones de seguridad complejas, el Ubiquiti Cloud Gateway Ultra emerge como una alternativa accesible y efectiva. Su capacidad para adaptarse a las necesidades específicas de cada empresa, junto con su costo-beneficio, lo posiciona como una opción viable para mejorar la seguridad de la información en un entorno empresarial cada vez más digitalizado.

Para PYMES se ha podido demostrar que utilizando el equipo ya mencionado como una alternativa a la propuesta mencionada en esta tesis puede tener todo lo necesario con una inversión económica bastante baja en cuanto a seguridad se refiere siendo una opción Aceptable y al alcance del usuario quien brinda sus servicios como es el caso en PYMES

Se puede demostrar en esta tesis ha demostrado que la combinación de tecnologías avanzadas como el Ubiquiti Cloud Gateway Ultra con un enfoque proactivo hacia la gestión de riesgos y la concientización del personal puede transformar la seguridad de las redes locales en las PYMES salvadoreñas. Se recomienda a las empresas considerar la implementación de este tipo de soluciones, junto con un compromiso continuo con la mejora de sus prácticas de seguridad, para garantizar la protección de sus datos y la sostenibilidad de sus operaciones en el largo plazo.

CAPITULO 8. BIBLIOGRAFIA

REFERENCIAS

ISACA (2022) Guía práctica para la implementación de gestión de seguridad de la información según ISO/IEC 27001:2022 Consultado el 10 de octubre 2024. https//:www.edirama.it/wp-content/upload/2023/10/document-2.pdf (Guía V) (5) (81-86)

UNIFI (2024) Configuración y actualización en los sistemas operativos internos de Cloud Gateway. Consultado 25 de enero

https://help.ui.com/hc/en-us/sections/27826487543447-VPN-Configurations

(Configuración VPN) (1) (64-72)

HG8245W5 HUAWEI (2025) Equipo ONT con alimentador fibra óptica. Consultado 20 de febrero 2025

HG8245W5 (huawei.com) (AX3) (1) (77)

Equipo Huawei WiFiAx3 Pro (2023) Características técnicas de equipo WifiAX3, Consultado 15 de diciembre de 2024

Router Huawei WiFi AX3 Pro WS7206 (digitalsolutions.com.sv) (AX3 PRO) (1) (100-104)

Cleri, C. (2007). *El libro de las PYMES* (1.ª ed., pp. 1 - 44). Buenos Aires: Cleri Carlos A.R. Buenos Aires: Cleri Carlos A.R.

Equipo Switch D-links108 8 puertos 10/100/1000(2019) Características y Precio. Consultado 1 de febrero de 2025.

D-link DGS-108 Switch 8 Puertos 10/100/1000Mbps | PcComponentes.com

(CARACTERISTICAS) (1) (76)

Rudy Mens. (2024). Unifi Cloud Gateway Ultra review. Consultado 17 de septiembre de 2024.

https://lazyadmin.nl/network/unifi-cloud-gateway-ultra/

CFP VERCE DE CORTES (2021). Manual de buenas prácticas en seguridad de la información. Consultado 1 de marzo de 2025.

MBPSI.pdf (cfpvergedecortes.es) (UCG-Ultra REVIEW) (1) (22-24)

Xavi Gómez (2020). Manual de seguridad informática y buenas prácticas en el uso de las nuevas tecnologías para empresas y usuarios particulares. Consultado 10 de febrero 2025.

MANUAL-DE-SEGURIDAD-INFORMATICA-Y-BUENAS-PRACTICAS-PARA_EMPRESAS-Y-USUARIOS-JUNIO-2020-2.pdf(grupapunts.es)
(INTRODUCCION Y ALCANCES) (1) (87-95)

ANEXOS

DATA SHEET EQUIPO HUAWEI AX3

HUAWEI WIFI AX3 (Dual-core)
Product Description

Issue 03

Date 2020-07-10

HUAWEI DEVICE CO., LTD.

HUAWEI

1.1 Introduction

Figure 1-1 Appearance

HUAWEI Wi-Fi 6 plus

HUAWEI unique Dynamic Narrow Bandwidth technology, the chipset level synergy between routers and devices, improves the signal of HUAWEI Wi-Fi 6 smartphones to new height.

3x Speed: Not only 1024 QAM but also 160Mhz Channel bandwidth, which maximizes the speed of Wi-Fi 6 and even the Wi-Fi 5 phones or tablets supporting 160Mhz channel bandwidth.

4x Capacity: OFDMA from Mobile Telecommunication field allows sharing the spectrum resources simultaneously.

2/3 Latency Cut: OFDMA and the latest spatial reuse technology BSS coloring increase your network efficiency and decrease interference.

30% Power Saved: On-demand waked-up functionality saves battery for all Wi-Fi 6 connected devices.

Dual-core 1.2GHz CPU

Figure 1-2 Button/Ports

Table 1-1 Buttons and ports

No.	Button/Port	Description
1	H button	The indicator will flash when the router discovers a device that supports HUAWEI HiLink. You can press the H button to connect the device to the router's Wi-Fi. By pressing the H button, you can also enable WPS to connect a WPS device to the router. **NOTE** *Devices that support HUAWEI HiLink include: HUAWEI routers, HUAWEI mobile phones (EMUI 5.1 or later), etc.*
2	Power port	Connect the power adapter to this port.
3	WAN port	The port that connects to the Internet (e.g., a fiber optic modem/broadband modem/cable modem).
4	LAN ports	The ports that connect to network devices such as a computer.
5	Reset button	When the router is powered on, you can use a pointed object to press and hold the reset button for more than two seconds until the indicator turns off. The router should now be restored to factory settings.
6	Power button	Press once to power on the device, or press and hold for at least three seconds to power it off.

1.4 Network Architecture

Figure 1-4 Network architecture

NOTE

Optical fiber (or telephone line/Ethernet cable)

Ethernet cable

3.2 Ports

3.2.1 WAN Ethernet Port

100/1000 Mbit/s self-adaptive Ethernet port: 1

3.2.2 LAN Ethernet Port

100/1000 Mbit/s self-adaptive Ethernet ports: 3

3.3 Power Supply Specification

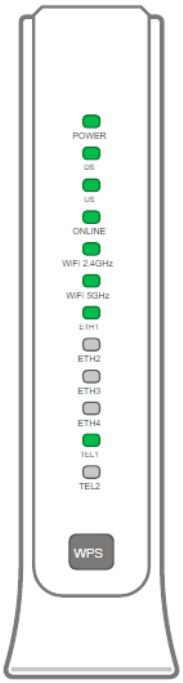
- Power supply: 12V DC, 1A
- Power consumption: < 12W
- Input voltage: 100 - 240V AC
- Input voltage frequency: 50 – 60 Hz

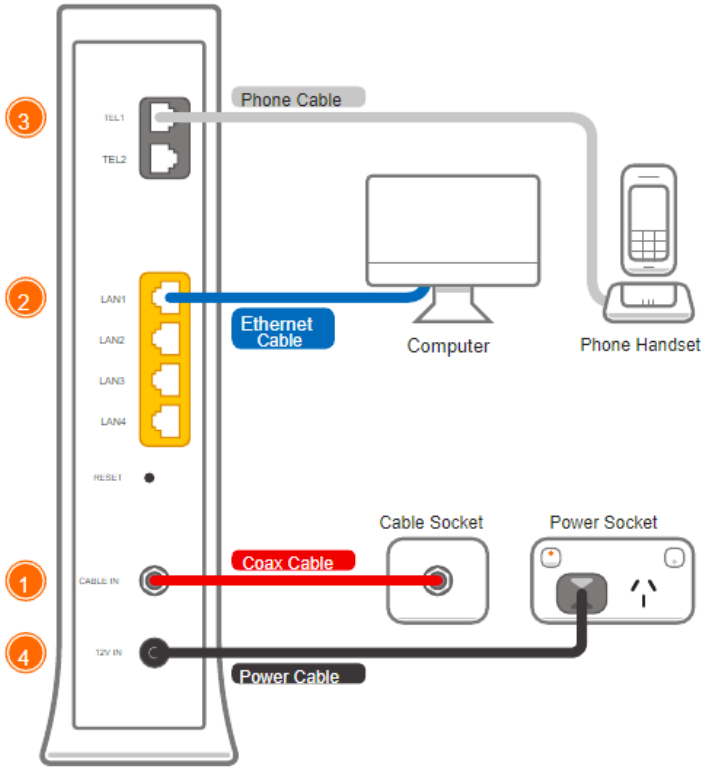
3.4 Physical Specifications

- **Dimensions (Height x Width x Depth):**
  The product with folded external antennas: 39.7mm x 225mm x 159.2mm
  The product with vertical external antennas: 165.2 mm x 225 mm x 144.4mm
  The packaging of EU/UK version: 56mm x 313mm x 212mm
- **Weight:**
  The product without packaging: about 387g
  The EU version weight: about 710g
  The UK version weight: about 720g
- Operating temperature: 0 ℃ to 40 ℃ (32 ℉ to 104 ℉)
- Storage temperature: –40 ℃ to +70 ℃ (–40 ℉ to +158 ℉)
- Operating humidity: 5% to 95% RH (non-condensing)
- Storage humidity: 5% to 95%, non-condensing

DATA SHEET CG2200

Light	State	Meaning
Power	On	Modem is turned on
	Off	Modem is turned off or has no power supply
DS	On	Modem is receiving data from the Cable network
	Blinking	Modem is searching for downstream channel or a firmware upgrade is in progress
	Off	Modem has no power or it cannot connect to the Cable network
US	On	Modem is sending data via the Cable network
	Blinking	Modem is searching for upstream channel or a firmware upgrade is in progress
	Off	Modem has no power or it cannot connect successfully to the cable network
Online	On	Modem is registered to the Cable Network and fully operational
	Blinking	Modem is booting up
	Off	Modem is not registered/online on the cable network
WiFi	On	2.4GHz or 5GHz WiFi network enabled
	Blinking	Network activity
	Off	2.4GHz or 5GHz WiFi disabled
Eth	On	An ethernet device is connected to the corresponding ETHERNET port
	Blinking	Network activity
	Off	No ethernet device detected
Tel	On	Netphone (VoIP) service available
	Blinking	Phone in use
	Off	Netphone (VoIP) service not available
WPS		Press this button to enable WPS Mode when connecting compatible devices



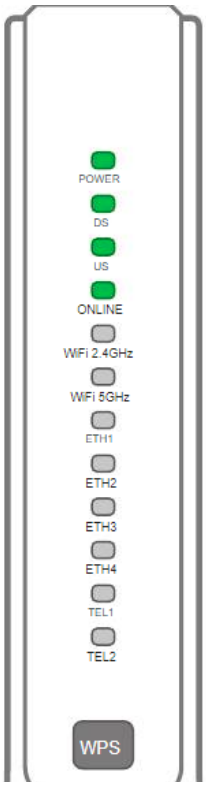


Lights to look out for

If both the US and DS lights are BLINKING and the Online light is ON, your modem is upgrading its firmware. You don't need to do anything; simply wait for the upgrade to complete.

If both the US and DS lights are BLINKING but the Online light is OFF, your Cable service may not be fully activated on our end. Make sure you've received a confirmation from us advising that your Cable service is active, or call us for assistance.

We'll need your modem's MAC and Serial Number to investigate - these are printed on your modem's barcode sticker.



Warranty Info

1. How to claim under the warranty and your rights

1.1 In order to claim under the warranty, you should contact us to advise that you wish to claim under the warranty and answer any questions we have. We will assess whether you are eligible to claim under the warranty and determine, at our option and in accordance with any specific terms that apply to the relevant equipment, whether to repair or replace your equipment, or provide a credit.

iiNet:
Phone: 13 22 58
Email: support@iinet.net.au

Westnet:
Phone: 1300 786 068
Email: support@westnet.com.au

1.2 If we determine that your equipment needs to be returned, you will be sent replacement equipment and a return freight bag in which to return the faulty equipment.

1.3 If the faulty equipment is not returned to us, with all cables, accessories and components, within 21 days of you receiving the replacement equipment and return freight bag, you will be charged the full price for the purchase of the equipment that we sent to you, plus any shipping costs relating to the prepaid satchel that was sent to you. You will also still be charged for the original equipment and if the original equipment has already been paid for, you will not be entitled to a refund.

1.4 The warranty does not apply to faults caused by any of the following (Non Covered Events):

a) any equipment not supplied by us;

b) any interference with or modification to the equipment or a failure to use it in accordance with instructions; or

c) damage caused by you or someone who has used the equipment (for example misuse or exposure to liquid or excessive heat); or

d) an external event (for example a fire or flood).

1.5 If on inspection of the returned equipment we determine that the fault was caused by a Non Covered Event, you will be charged for the original equipment (or if the original equipment has already been paid for, you will not be entitled to a refund) and the replacement equipment, unless:

a) you have not used the replacement equipment;

b) and you return it to us in its unopened packaging, in which case, you will not be charged for the replacement equipment.

1.6 The repair or replacement of equipment may result in loss of data (such as loss of telephone numbers stored on your handset).

AGREGADO EXTRA

CUMPLIMIENTO DE LA NORMA ISO/IEC27001:2022 EN EQUIPO UCG-ULTRA

El equipo UCG-ULTRA de UniFi (Ubiquiti) es una pasarela (Gateway) avanzada diseñada para redes empresariales y gestionada a través del UniFi Network Controller. Aunque Ubiquiti no certifica específicamente sus dispositivos bajo ISO/IEC 27001:2022, muchos de sus productos (incluyendo el UCG-ULTRA) incorporan funciones de seguridad alineadas con los controles del Anexo A de esta norma.

CONTROLES DE CUMPLIMIENTO

Basándonos en sus capacidades técnicas, estas son algunas áreas de alineación:

1. **Controles Organizacionales (A.5)**

A.5.1: Políticas para la seguridad de la información

- Soporta políticas de firewall, filtrado de tráfico y gestión centralizada.

A.5.23: Seguridad en la nube

- Integración con UniFi Cloud para gestión remota (con autenticación MFA).

2. **Controles de Personas (A.6)**

A.6.1: Asignación de responsabilidades

- Permite roles de administrador con distintos niveles de acceso (RBAC).

A.6.8: Concienciación sobre seguridad

- Registros (logs) y alertas para monitorear actividades sospechosas.

3. **Controles Físicos (A.7)**

A.7.1: Protección física

- El hardware incluye TPM (Trusted Platform Module) para proteger claves criptográficas.

4. **Controles Tecnológicos (A.8)**

A.8.1: Gestión de endpoints

- Filtrado de dispositivos mediante MAC filtering, VLANs y segmentación de red.

A.8.2: Cifrado

- Soporta IPSec VPN, SSL/TLS para comunicaciones seguras.

A.8.10: Monitoreo de actividades

- Registros detallados (syslog), detección de intrusiones (IDS/IPS) y análisis de tráfico.

A.8.23: Seguridad en redes

- Firewall avanzado, protección DDoS y QoS para priorizar tráfico crítico.