FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“DISEÑO E IMPLEMENTACIÓN DE FIREWALL PALO ALTO PARA MEJORAR EL CONTROL DE SEGURIDAD Y ACCESO A INTERNET”

Trabajo de suficiencia profesional para optar el título profesional de:

INGENIERO DE SISTEMAS COMPUTACIONALES

Autor:

Esau Esmael Campomanes Asencios

Asesor:

Ing. Deivhy Paul Torres Vargas

Lima - Perú

2022

DEDICATORIA

Dedicado a mis padres y hermanos, quienes son parte importante en mi vida, a mi enamorada Elizabeth, quien fue la persona que me motivo en este logro, a ellos mi eterno agradecimiento.

AGRADECIMIENTO

A Dios por todos los logros en mi vida.

A mis padres por el apoyo y amor incondicional A mi asesor el Ing. Ing. Deivhy Paul Torres Vargas por el apoyo y orientación.

A la Universidad Privada del Norte, autoridades, docentes y compañeros de estudios por contribuir de manera exigente y solidaria en nuestra formación académica.

TABLA DE CONTENIDOS

INDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente trabajo de suficiencia describe la implementación del nuevo sistema de seguridad del firewall Palo Alto dentro de la Cooperativa de Ahorro y Crédito Abaco, el cual permite aumentar la seguridad y las diferentes prestaciones de servicios dentro de la red de la cooperativa.

Este estudio analizó las diferentes clasificaciones de las redes de datos, así mismo los diferentes tipos de firewall, sus fundamentos teóricos de las redes de área local y amplia, también la seguridad y sus funcionalidades del firewall. Para llevar a cabo la implementación del firewall Palo Alto, se basó en la problemática de la cooperativa, en el cual se buscó el objetivo y las estrategias para llevar a cabo la metodología el cual estuvo dividido en 8 etapas desde el diseño de la propuesta, planeamiento, costo, diagrama, matriz de riesgo, hasta realizar la configuración del firewall.

Como resultado se obtuvo un nuevo firewall el cual brinda mayor seguridad de la información de los diferentes tipos de ataques hacia la zona DMZ y zona LAN, así mismo se obtuvo mayor disponibilidad para garantizar el acceso a los diferentes servicios internos, de la misma manera garantizar el acceso hacia internet y mejorar la rapidez de acceso a los servicios requeridos por las diferentes áreas de trabajo.

CAPITILO I. INTRODUCCIÓN

En la actualidad las empresas son más dependientes de las redes informáticas, es por ello que el mundo de infraestructura tecnológica ha cambiado y ha ido avanzando a tal punto que los firewalls se han convertido en un aspecto primordial para las operaciones de las empresas.

Al 80% de las Pymes de Latinoamérica les preocupa la seguridad, a pesar de ello, el 98% no considera este aspecto como una prioridad dentro de sus organizaciones, indica un estudio elaborado por IDC, y es que no saben cómo están siendo atacadas ni cómo se comportan los códigos maliciosos. (Anon, 2015)

Así mismo un estudio realizado en Colombia de un firewall para dar solución de seguridad informática para empresas fue muy efectivo de acuerdo a las exigencias de las políticas de seguridad creadas. (Martínez et, al. 2009)

También un estudio realizado a nivel nacional acerca de la implementación de firewall para el control de servicio de internet en la universidad peruana de los andes nos relata lentitud en la transmisión de la información, perdida de paquetes y quejas de los trabajadores administrativos, donde se realizó una implementación de un firewall para controlar el uso de internet los cuales llegaron a un nivel de funcionamiento aceptable. (Joaquín, 2019)

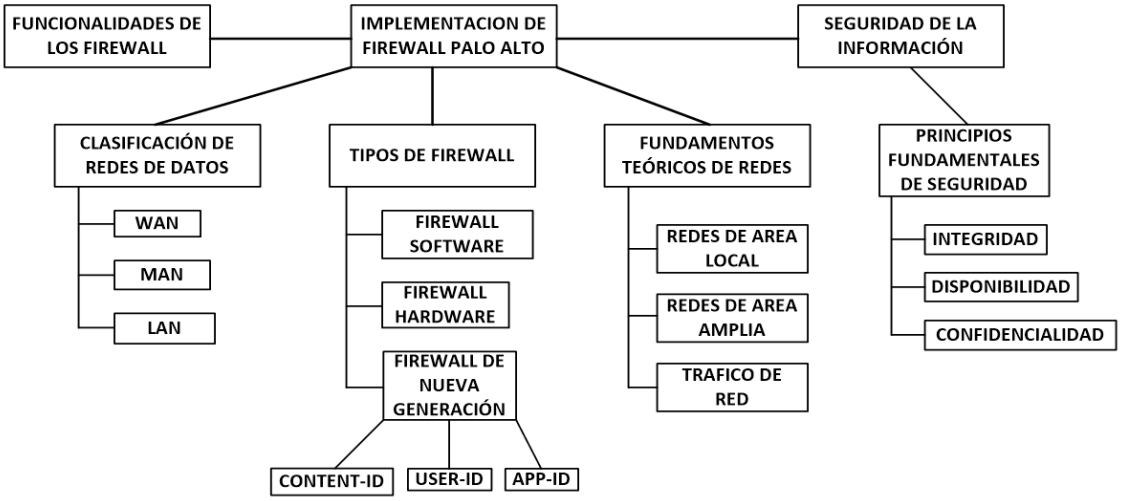
En el presente trabajo se realizó el diseño e implementación del firewall palo alto para mejorar el control de seguridad y acceso a internet, en la Cooperativa de Ahorro y Crédito Abaco. Esta nueva implementación nos permitirá mejorar el sistema de seguridad, contra los diversos ataques que se dan desde internet, así como desde la zona local, de la misma forma este sistema realiza el análisis y la inspección del tráfico cifrado incluso si está cifrado, de la misma forma obtener mayor capacidad de rendimiento del hardware.

CAPITULO II. MARCO TEÓRICO

A continuación, se presentan los conceptos más importantes para el diseño e implementación de Firewall Palo Alto para mejorar el control de seguridad y acceso a internet descrito en el capítulo 3.

Figura 1.

Mapa conceptual



Fuente: Elaboración propia

Es importante mencionar los diferentes conceptos para la implementación de un firewall por tanto tenemos a Lopez (2020) quien refiere que un firewall es un sistema que controla el tráfico saliente y entrante no autorizado en una red LAN. Las redes LAN (Local Access Network) son aquellas que tenemos en casa, contando desde el router hacia los distintos dispositivos que podamos tener conectados a él, tanto por cable como por WiFi. El término firewall, o cortafuegos, hace referencia a un sistema de seguridad informática que previene del acceso no autorizado a nuestra LAN, es decir, el proveniente desde el exterior (WAN).

Así mismo Guzmán (2018) refiere que los firewalls son usados como una estrategia de la seguridad en una compañía, generalmente posicionados en el borde de la red entre redes públicas y privadas; en el transcurrir de los años se

han planteado diferentes desafíos ya que inicialmente no se pensó que el internet fuera a crecer desmedidamente.

Según Cisco (2020) Los cortafuegos han sido una primera línea de defensa en seguridad de redes durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas en las que se puede confiar y las redes externas no confiables, como Internet.

2.1 Clasificación de redes de datos

LAN (Local Área Networks, Redes de Área Local)

De acuerdo con Cyberprimo (2008) “las redes de área local suelen ser una red limitada a la conexión de equipos dentro de un único edificio, oficina o campus, la mayoría son de propiedad privada”.

WAN (Wide Área Networks, Redes de Área Amplia)

Así mismo Cyberprimo (2008) las Redes de área extensa son aquellas que proporcionen un medio de transmisión a lo largo de grandes extensiones geográficas (regional, nacional e incluso internacional). Una red WAN generalmente utiliza redes de servicio público y redes privadas y que pueden extenderse alrededor del globo.

MAN (Metropolitan Área Networks, Redes de Área Metropolitana)

wikitel (s.f.) las redes de área metropolitanas están diseñadas para la conexión de equipos a lo largo de una ciudad entera. Una red MAN puede ser una única red que interconecte varias redes de área local LAN’ resultando en una red mayor. Por ello, una MAN puede ser propiedad exclusivamente de una misma compañía privada, o puede ser una red de servicio público que conecte redes públicas y privadas.

2.2 Funcionalidades básicas de los firewalls

Dentro de sus funcionalidades Pacheco y Martínez, (2009) refieren lo siguiente:

- Bloqueo de paquetes que se originan en un determinado rango de IP, puertos, dominios, direcciones de correo, etc.
- Bloqueo de paquetes formados por determinados protocolos o aplicaciones.
- Bloqueo de paquetes que sean reconocidos como firmas de ataques a sistemas o redes.
- Herramienta de análisis del comportamiento de sistemas y de red.
- Herramienta de análisis forense.
- Sistema de defensa contra virus, troyanos y malware en general.
- Bloqueo del uso de la red que protegen como origen de ataques.

2.3 Tipos de Firewall

Firewall por Software

De acuerdo con Castillo et al. (2017) los cortafuegos permiten poner en funcionamiento a través de hardware, lo que sería más preferible, aunque es algo costoso en comparación a un firewall por software. Los Firewalls personales o de software son programas que depuran la circulación de datos que entra y sale de una computadora. Una vez asentados, el cliente necesita establecer el nivel de protección, aprueba o niega la entrada de cierto software a Internet y concede o no la entrada desde el exterior.

Firewall por Hardware

También Castillo et al. (2017) mencionan que un cortafuego es un hardware específico con un sistema operativo que filtra el tráfico y resuelve si la información ingresa, se cambia, o se suprime. Es necesario tener como mínimo dos tarjetas de red para que así un firewall se desempeñe con total normalidad. El bosquejo tradicional de un firewall para custodiar una red local que se encuentra enlazada a internet por intermedio de un router Los cortafuegos tiene que ir entre el router, con un solo cable y la red local, conectado al dispositivo

hub. Si se tienen otras necesidades para con cada red, también es posible colocarse más de un Firewalls para instalar diversos cercos de seguridad con respecto al sistema que se desea resguardar. Es muy común que se requiera exponer un servidor a internet, podría ser un servidor web, un servidor de correo, u otro. Es ahí precisamente que se permite todo tipo de conexión con ellos.

Aconsejamos en estos casos situar el servidor en un sitio muy aparte de la red, llamamos ese lugar DMZ o también conocida como zona desmilitarizada.

2.4 Firewall de nueva generación

Según Palo alto (2016) los firewalls de nueva generación inspeccionan todo el tráfico (aplicaciones, amenazas y contenido), lo vincula al usuario, sin importar la ubicación o el tipo de dispositivo. La aplicación, el contenido y el usuario, se convierten en componentes integrales de su política de seguridad empresarial.

App-ID:

De acuerdo a Palo alto (2011) App-ID hace frente a las limitaciones de visibilidad en la clasificación del tráfico que afectan a los firewalls tradicionales mediante la aplicación de varios mecanismos de clasificación al flujo de tráfico, tan pronto como lo detecta el firewall, para determinar la identidad exacta de las aplicaciones que recorren la red. App-ID supervisa continuamente el estado de la aplicación, reclasificando el tráfico e identificando las diferentes funciones que se están utilizando. La política de seguridad determina cómo tratar la aplicación: bloquear, permitir o habilitar de forma segura (explorar y bloquear amenazas, inspeccionar la transferencia no autorizada de archivos y patrones de datos o moldear el tráfico mediante QoS (Quality of Service o calidad de servicio).

User-ID:

Palo alto (2011) un User-ID permite que las organizaciones extiendan políticas de habilitación de aplicaciones basadas en usuarios o en grupos entre usuarios de Microsoft Windows, Apple Mac OS X, Apple iOS y Linux. La información de los usuarios se puede recoger de directorios empresariales

(Microsoft Active Directory, eDirectory y Open LDAP) y de ofertas de servicios de terminal (Citrix y Microsoft Terminal Services), mientras que la integración con Microsoft Exchange, un Portal cautivo y una API XML permite a las organizaciones extender la política a usuarios de Apple Mac OS X, Apple iOS y UNIX que residen habitualmente fuera del dominio.

Content-ID:

Palo alto (2011) donde Content-ID, junto con App-ID, proporciona a los administradores una solución de dos frentes para proteger la red. Después de utilizar App-ID para identificar y bloquear aplicaciones no deseadas, los administradores pueden habilitar de manera segura las aplicaciones autorizadas evitando que exploits de vulnerabilidad, software malicioso moderno, virus, botnets y otros tipos de software malicioso se propaguen a través de la red, todo ello independientemente del puerto, el protocolo o el método de evasión. Como complemento de los elementos de control que ofrece Content-ID, existe una extensa base de datos URL para controlar la navegación por Internet y las funciones de filtrado de datos.

2.5 Fundamentos teóricos de Redes

Dentro de los fundamentos tenemos lo siguiente:

Redes de área local:

De acuerdo a Cabanillas (2015) son conocidas como LAN, son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información.

Redes de área Amplia:

También Cabanillas (2015) “refiere que son conocidas como WAN, abarca grandes áreas geográficas, con frecuencia un país o un continente. Contiene un conjunto de dispositivos diseñado para programas de usuario”.

Trafico de red:

Duarte y Paredes (2016) refieren que el tráfico es un concepto que tiene su origen en un vocablo italiano que se refiere al tránsito o desplazamiento de medios de transporte por algún tipo de camino o vía. El concepto de tráfico puede hacer mención tanto a la acción del movimiento como a las consecuencias de dicha circulación. Por lo tanto, el tráfico de red se puede definir como la cantidad de información o datos enviados y recibidos por todos aquellos equipos de una red de computadoras.

2.6 Seguridad de la información

Ibero (2020) La seguridad de la información es todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de una institución; y asegurarnos que esa información no salga del sistema de la empresa y caigan en las manos equivocadas. Por lo tanto, la seguridad de la información resguardará los datos que están a disposición del sistema de cada empresa y mantendrá el acceso limitado únicamente a los usuarios con autorización.

2.6.1 Principios Fundamentales de Seguridad

Los principios de seguridad son clasificados de la siguiente manera.

Confidencialidad:

Caballa y Torres (2010) refiere que la confidencialidad, asegura el nivel necesario de secreto y se encuentra asegurado en cada instancia del procesamiento de datos, de manera tal de prevenir su divulgación a personas no autorizadas a conocer los mismos. La Confidencialidad, a menudo puede ser provista o reforzada, mediante la implementación de un estricto control de acceso, por medio de la encriptación de datos (ya sea al momento de almacenar o transmitir los mismos), la puesta en marcha de procesos de clasificación de la Información, concientización y entrenamiento del personal.

Integridad:

De acuerdo a Walkowski (2019) la integridad consiste en garantizar que los datos no hayan sido manipulados y, por lo tanto, sean confiables. Garantizar la integridad implica proteger los datos en uso, en tránsito (por ejemplo, al enviar un correo electrónico o al cargar o descargar un archivo) y al almacenarlos, ya sea en aparatos físicos o en la nube. Las contramedidas que protegen la integridad de los datos incluyen: encriptación, la función hash, firmas digitales, certificados digitales, sistemas de detección de intrusos, auditorías, control de versiones, mecanismos de autenticación y controles de acceso

Disponibilidad:

Caballa y Torres (2010) la disponibilidad de la Información es la capacidad de encontrarse siempre disponible, para ser utilizada por las personas autorizadas. A fin de cumplir con este principio, los sistemas y redes deben proveer la capacidad adecuada de procesamiento, actuar de modo previsible y brindar un adecuado nivel de performance. Entre las amenazas que afectan el principio de Disponibilidad, se encuentran las fallas relacionadas con el software y hardware, aspectos relacionados con el entorno (calor, frío, humedad, electricidad estática, etc.), desastres naturales, denegaciones de servicios (DoS, DDoS), etc.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

En el año 2008 comencé con mi formación profesional en la carrera de redes y comunicaciones en el Instituto IDAT (Instituto de Investigación y Desarrollo de Administración y Tecnología), oportunamente fui contratado por recomendación a la empresa DISEC S.R.L., donde me desempeñé realizando funciones de implementación de cableado estructurado e implementación de red. Transcurrido el tiempo en el año 2013 la empresa DISEC S.R.L., me envió a brindar los servicios de soporte técnico en el área de networking en la Cooperativa de Ahorro y Crédito Abaco.

Por tal motivo en el año 2014 decidí continuar una carrera universitaria de ingeniería de sistemas computaciones, en el transcurso de estos años tuve la oportunidad de realizar diversas funciones relacionadas a mi carrera y a la par aplicar todos los conocimientos aprendidos en la universidad UPN (Universidad Privada del Norte), todas estas actividades fueron ejecutados con supervisión de un ingeniero especializado.

Funciones realizadas

Dentro de las funciones realizadas durante estos años de trabajo en la Cooperativa de Ahorro y Crédito Abaco SAC, estuvieron enfocadas en:

- Implementación de sistemas de seguridad firewall.
- Implementación y administración de switch en capas 2 y 3.
- Implementación de Wireless LAN Controller.
- Supervisión en la implementación de balanceadores de carga para los ISP.
- Supervisión en la implementación de centrales de telefonía IP.
- Supervisión en la implementación de Event Log Analizer.
- Implementación de sistema NTP.

3.1. Definición de la empresa DISEC S.R.L.

La empresa DISEC SRL. inició sus operaciones en el año 1993, actualmente se dedica exclusivamente a diversos trabajos de implementación de sistemas TI, así como implementaciones de sistemas de energía eléctrica, la sede principal se encuentra en el distrito de Jesús María. Con el pasar del tiempo, la empresa también se ha certificado en ISO 45001. A continuación, se muestra la información de la empresa.

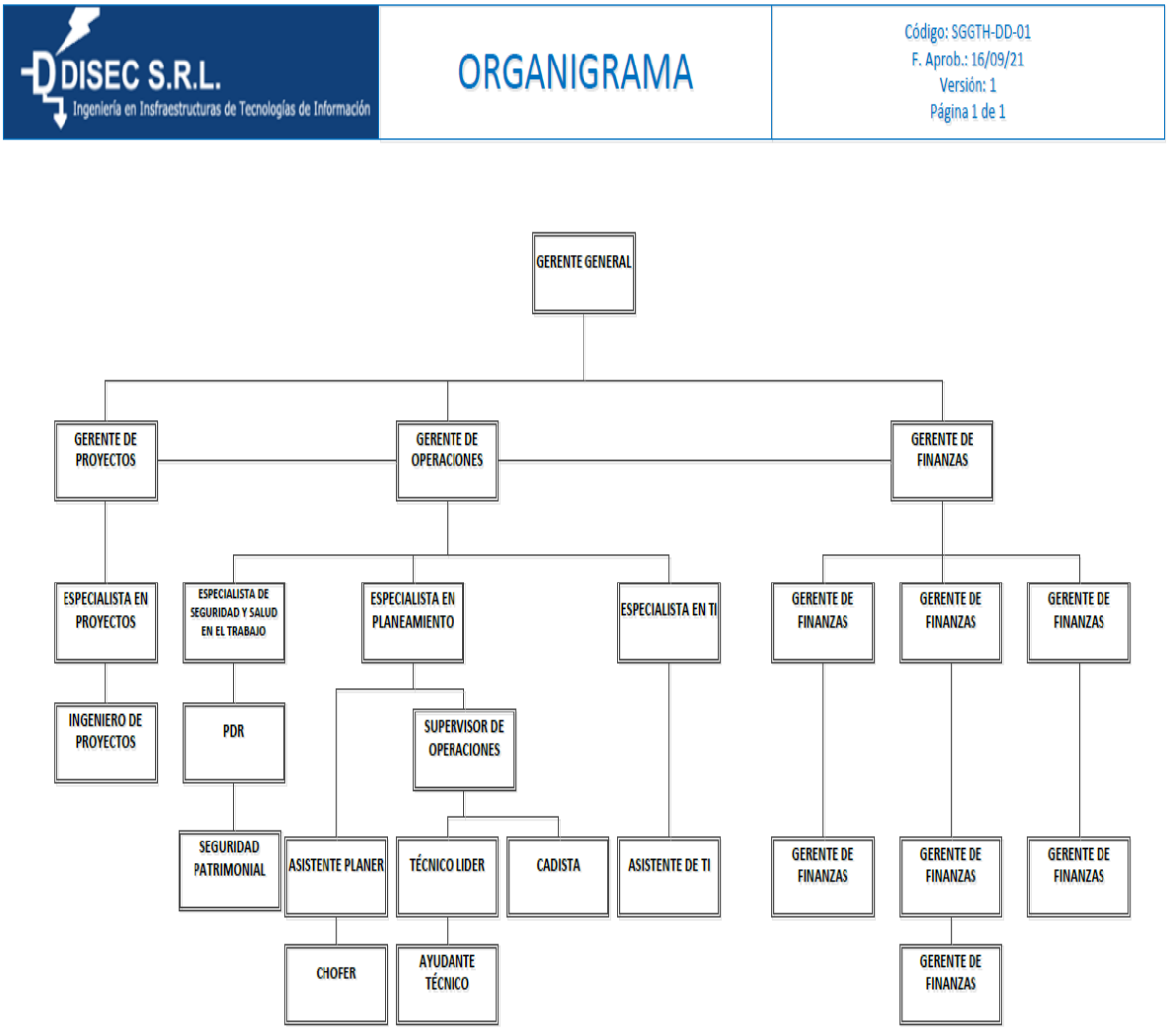
- Razón Social: DISEC SOCIEDAD COMERCIAL DE RESPONSABILIDAD LIMITADA DISEC SRL.
- Nombre comercial: Disec Sociedad Responsab Ltda.
- RUC: 20111328804.
- Tipo de empresa: Soc.Com. Respons. Ltda.
- Actividad comercial: Telecomunicaciones y otras actividades de informática.
- Dirección Legal: Av. Húsares de Junín Nro. 311 Fnd. Oyague Jesus María Lima, Perú.
- Misión: Brindar soluciones integrales de infraestructura en tecnologías de información para un adecuado funcionamiento de los equipos eléctricos. Brindar servicio eficiente por nuestros servicios. Ser una empresa líder en nuestro rubro, con el reconocimiento de nuestros clientes para poder extendernos a nivel nacional.
- Visión: Ser una empresa líder en infraestructura requerida por las TICs, basados en estándares internacionales de calidad. Innovación y el mejoramiento continuo.
- Valores: Satisfacción, Calidad, Puntualidad, Responsabilidad, Soluciones rápidas, Garantía y compromiso de cubrir las necesidades de nuestros clientes.
- Servicios.
    - Sistemas de Energía Eléctrica.
    - Cableado Estructurado e Infraestructura para TICs

- Mantenimiento Preventivo y Correctivo.
- Diseño y Elaboración de Expediente Técnico.
- Seguridad de Infraestructura.
- Supervisión de Proyectos.
- Auditoria de Red.
- Instalación de Sistemas Inalámbricos.

En la siguiente imagen se muestra el organigrama de la empresa DISEC S.R.L

Figura 2.

Organigrama de la empresa DISEC S.R.L



Fuente: Empresa DISEC S.R.L.

3.2 Definición de la Cooperativa de Ahorro y Crédito Abaco.

El 28 de octubre de 1981 fue fundada la Cooperativa Abaco gracias a la iniciativa de 32 personas que tenían como objetivo "practicar la ayuda mutua entre los amigos". Hoy, mantenemos esa filosofía razón por la cual muchas de las empresas y personas que pertenecen a Abaco se han desarrollado y crecido con nosotros. A continuación, se mostrará la información de la empresa.

- Razón Social: COOPERATIVA DE AHORRO Y CREDITO ABACO.
- Nombre comercial: Abaco.
- RUC: 20101091083.
- Tipo de empresa: Cooperativas, Sais, Caps
- Actividad comercial: Otros Tipos Intermediación Monetaria
- Dirección Legal: Av. Coronel Andrés Reyes Nro. 420 Int. 301 San Isidro Lima, Perú.

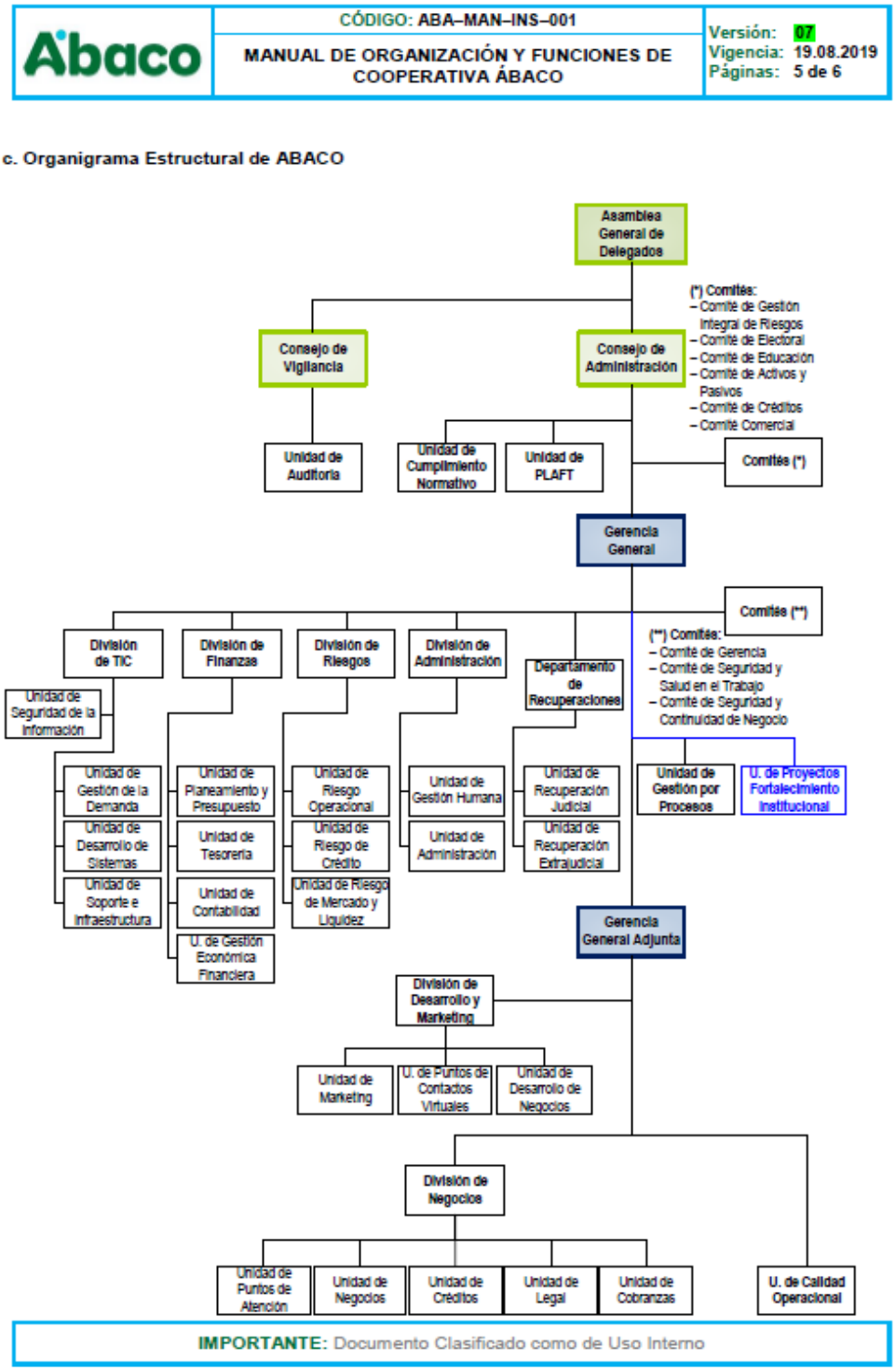
Misión: Contribuir en elevar el bienestar de nuestros socios con soluciones financieras ágiles y adaptables, trabajando por el bien común, enfocados en un desarrollo sostenible.

Visión: Ser reconocidos como la mejor solución financiera para nuestros socios.

En la siguiente imagen se muestra el organigrama de la Cooperativa Abaco:

Figura 3.

Organigrama de la empresa Cooperativa de Ahorro y Crédito Abaco.



Fuente: Empresa Abaco (2019)

3.3 Descripción de la problemática de la Cooperativa de Ahorro y crédito Abaco.

La Cooperativa de Ahorro y Crédito Abaco es una entidad financiera, en los últimos años ha venido creciendo en todas sus áreas por el incremento de socios, es por ello que se decide realizar una mayor inversión en su infraestructura tecnológica para mejorar los diversos servicios con mayor seguridad y así evitar los diversos problemas informáticos para proteger la información.

La problemática de la cooperativa es:

- Tiempo de implementación por falta de renovación de licencias del firewall anterior.
  Esto surge debido a que las licencias del firewall Fortinet se encontraban a punto de culminar la fecha límite de vencimiento.
- Tiempo limitado para la ejecución del cambio.
  Esto debido al corto tiempo para el cambio por el tema de las licencias.
- Inestabilidad del firewall anterior por requerir agentes para la conexión con servidores Windows.
  Esto debido a que el firewall Fortinet tiene inestabilidad de conexión con los servidores Windows ya que al requerir un agente FSSO para la conexión causa cierta inestabilidad.
- Renovación de equipos de seguridad a través del tiempo.
  Esto debido a que los equipos de seguridad se renuevan cada cierto tiempo de la misma forma porque los nuevos sistemas vienes con nuevos parámetros de seguridad.
- Mayor saturación de trafico de red.
  Esto debido a que el firewall Fortinet no abastece la cantidad de carga de red de toda la cooperativa.
- capacidad de equipamiento.
- El firewall Fortinet tiene ciertas limitaciones a nivel de hardware.
- Temas de seguridad.

- Esto debido a que existen diversos riesgos en el tema del aseguramiento de la información.
- Vulnerabilidad en VPN SSL.
  Esto debido a que las conexiones de cliente vpn han tenido vulnerabilidades al momento de las conexiones.
- Vulnerabilidad en Fortiweb.
  Esto debido a la baja protección de ciertas páginas web maliciosas.

3.4 Participantes del proyecto.

Dentro de la implementación del proyecto participaron los siguientes profesionales.

Tabla 1.

Participantes del proyecto

ASISTENTES		
PERSONA	CARGO	EMPRESA
Calos Ataucusi	Coordinador de proyecto	DISEC
Esau Campomanes	Coordinador de proyecto	DISEC
Sergio Morales	Ingeniero de proyecto	DISEC
Oscar Pimentel	Representante del proyecto	ABACO
Carlos Sonan	Coordinador de proyecto	ABACO

Nota. *Personas involucradas en el proyecto. Fuente: Elaboración propia

3.5 Objetivos, estrategias y metodologías del proyecto.

3.5.1 Objetivo del proyecto:

Diseñar e implementar un firewall palo alto para mejorar el control de seguridad y acceso a internet para la Cooperativa de Ahorro y Crédito Abaco.

3.5.2 Estrategias

Para realizar las estrategias del proyecto se propusieron los siguientes puntos.

- Coordinaciones con el jefe de soporte e infraestructura.
  Estas coordinaciones se realizaron mediante reuniones virtuales a través de Microsoft Teams y así formalizando a través de correo electrónico.

- Levantamiento de información de toda la red

  Para realizar el levantamiento de información de la red, se realizó previa coordinación con el jefe de soporte e infraestructura, para ello nos basamos en el diagrama topológico de red, se ingresó vía interfaz gráfica y ssh en los equipos de networking, del mismo modo se realizó las visitas físicas a todos los ambientes en los cuales se encuentran instalados los equipos de redes y comunicaciones.
- Se realiza dentro del data center y gabinetes de comunicaciones y se empieza a verificar la topología y estado de toda la red.
- Fijación de fechas y horarios para implementación.

  Se realizó previa coordinación con el jefe de soporte e infraestructura y la empresa Disec S.R.L.

3.5.3 Metodología

Para realizar la implementación del firewall Palo Alto se realizó lo siguiente:

Diseño de la propuesta para la implementación del firewall palo alto

Para la aplicación de la propuesta para la implementación del firewall palo alto se deben considerar tres etapas importantes como la planificación, ejecución y evaluación para obtener resultados esperados.

Planeamiento de la ejecución mediante el diagrama de Gantt

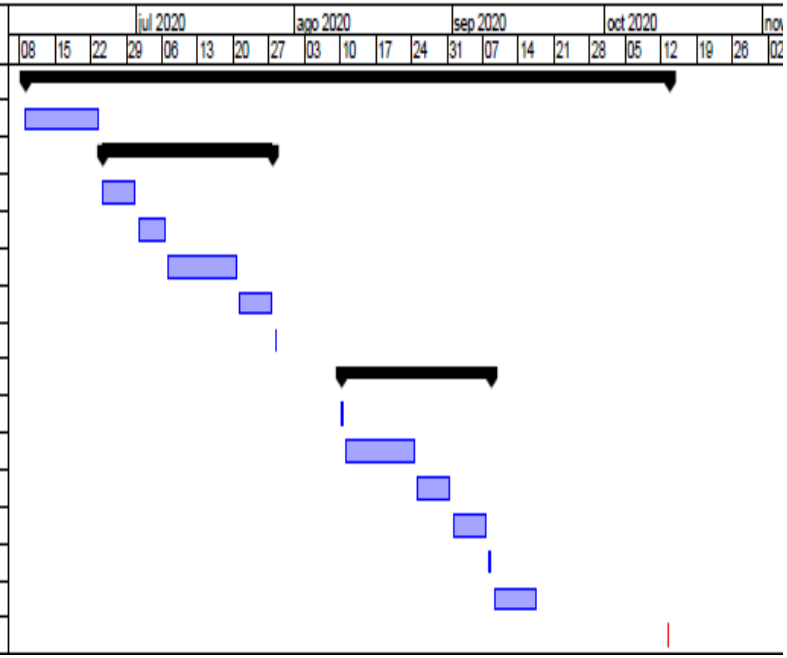
Para realizar el planeamiento de manera eficiente respecto a la implementación del firewall palo alto es importante considerar ciertas acciones que serán plasmadas en el diagrama de Gantt que comprende cinco etapas para la adecuada implementación.

Se elaboró el diagrama de Gantt, para observar gráficamente los procesos de la implementación del firewall palo alto para la cooperativa de ahorro y crédito Abaco.

Figura 4.

Diagrama de Gantt

	Nombre	Duracion	Inicio	Terminado
1	**Proceso de implementación de nuevo sistema de seguridad**	**91 days?**	**09/06/20 08:00 AM**	**13/10/20 05:00 PM**
2	Orden de compra	11 days	09/06/20 08:00 AM	23/06/20 05:00 PM
3	**Inicio de planificación**	**24 days**	**24/06/20 08:00 AM**	**27/07/20 05:00 PM**
4	Topología actual	5 days	24/06/20 08:00 AM	30/06/20 05:00 PM
5	Relación de Vlan de toda la red	4 days	01/07/20 08:00 AM	06/07/20 05:00 PM
6	Políticas actuales de toda la red	10 days	07/07/20 08:00 AM	20/07/20 05:00 PM
7	Relación de servicios publicados actuales	5 days	21/07/20 08:00 AM	27/07/20 05:00 PM
8	Entrega de nuevos firewall	1 day	28/07/20 08:00 AM	28/07/20 05:00 PM
9	**Inicio de implementación**	**22 days?**	**10/08/20 08:00 AM**	**08/09/20 05:00 PM**
10	Instalación de todo el nuevo equipamiento	1 day	10/08/20 08:00 AM	10/08/20 05:00 PM
11	configuración del nuevo sistema	10 days	11/08/20 08:00 AM	24/08/20 05:00 PM
12	Puesta en producción	5 days	25/08/20 08:00 AM	31/08/20 05:00 PM
13	Ajuste de políticas	5 days	01/09/20 08:00 AM	07/09/20 05:00 PM
14	Firma de cierre de implementación	1 day?	08/09/20 08:00 AM	08/09/20 05:00 PM
15	Informe Final	7 days	09/09/20 08:00 AM	17/09/20 05:00 PM
16	Firma de Acta del proyecto	1 day?	13/10/20 08:00 AM	13/10/20 05:00 PM



Fuente: Elaboración propia

Costo de implementación

Se presenta a continuación el costo del proyecto para la implementación del firewall Palo Alto en la cooperativa de Ahorro y Crédito Abaco, tal como se aprecia en el siguiente cuadro:

Tabla 2.

Costo total del proyecto

FAB	MODELO	Descripción	CANT	V UND US$	VV TOTAL US$
PA Networks	PAN-PA-850	Next Generation Firewall Palo Alto Networks PA-850	2	$6,609.21	$13,218.42
PA Networks	PAN-PA-850-TP-3YR-HA2	Licencia para prevención de ataques (malware, etc.)	2	$3,238.01	$6,476.02
PA Networks	PAN-PA-850-URL4-3YR-HA2	Licencia para filtrado URL PANDB URL Filtering	2	$3,238.01	$6,476.02
PA Networks	PAN-PA-850-WF-3YR-HA2	Licencia para prevención de ataques desconocidos (APT, malware polimórfico, etc.)	2	$3,238.01	$6,476.02
PA Networks	PAN-PA-850-DNS-3YR-HA2	Licencia para prevención de ataques desconocidos (APT, malware polimórfico, etc.)	2	$2,957.08	$5,914.15
PA Networks	PAN-PA-850-SDWAN-3YRHA2	Licencia para habilitación de SD-WAN (Mejora de control de tráfico WAN)	2	$3,205.08	$6,410.16
PA Networks	PAN-SVC-BKLN-850-3YR	Licencia de soporte de Palo Alto Networks	2	$4,962.16	$9,924.32
PA Networks	PAN-PA-1RURACK4	Palo Alto Networks PA-820 and PA-850 4 post rack mount kit	2	$128.05	$256.11
PA Networks	FTLX8574D3BCL	Transceiver multimodo 10G BaseSR TXRX SFP+ MULTI 10GB/S 850NM	8	$244.16	$1,953.28
PA Networks	S/N	Servicio de Instalación y configuración (Lima)	1	$1,866.67	$1,866.67
PA Networks	S/N	Soporte local 24x7 por 36 meses	1	$3,240.53	$3,240.53
		Valor de Venta:			$62,211.69
		IGV:			$11,198.10
		Precio venta:			$73,409.80

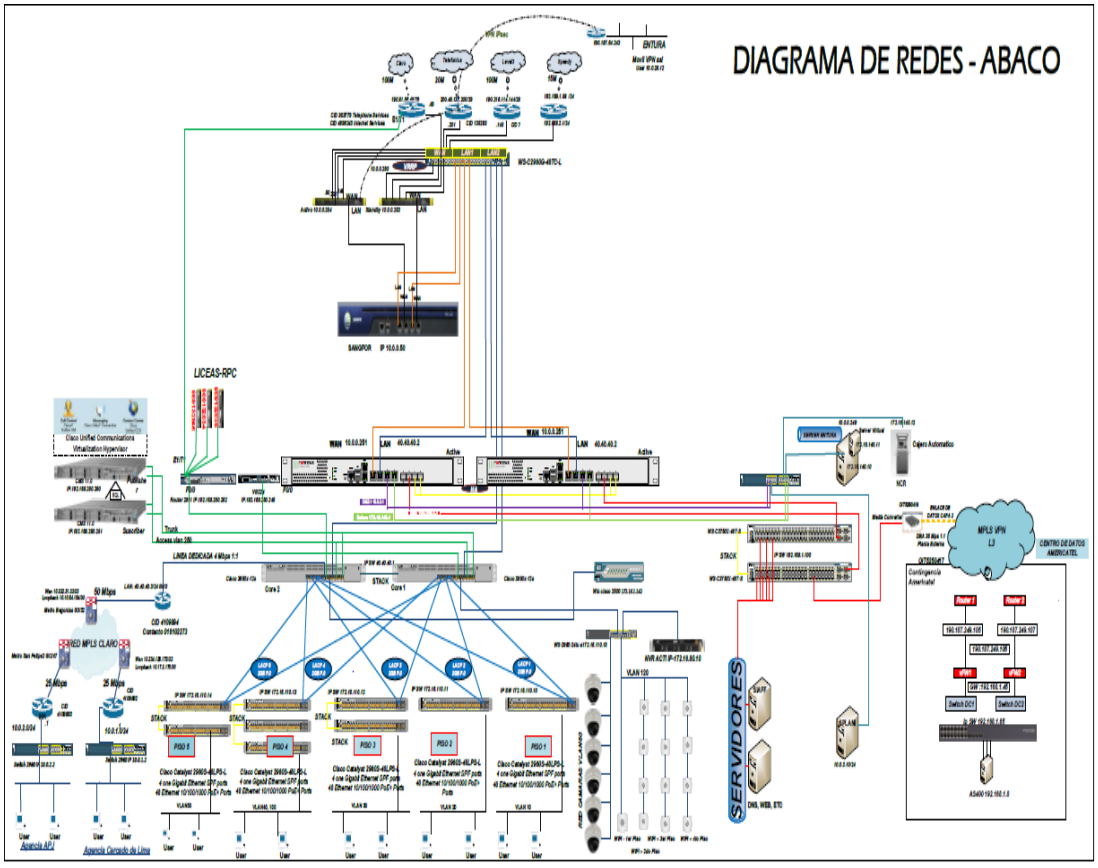
Nota. *Cotización para tres años. Fuente: Disec S.R.L

Diagrama de red antes de la implementación del nuevo firewall Palo Alto.

Anteriormente la Cooperativa de Ahorro y Crédito Abaco contaba con el diagrama de red donde se encuentran diversos equipamientos entre ellos firewall Fortinet, firewall Sangfor y balanceadores Peplink. los cuáles serán reemplazados por el nuevo equipamiento de seguridad en la marca Palo Alto. En la siguiente imagen se muestra toda la topología de red de la cooperativa.

Figura 5.

Topología de red



Fuente: Elaboración propia

Dentro de los componentes de red tenemos los siguiente:

Balanceadores de carga Peplink: Equipamiento que realiza un balanceo de carga para la salida hacia internet ya que la cooperativa cuenta con tres ISP y que a su vez tiene la capacidad para publicar los diferentes tipos de servicios de la cooperativa Abaco.

Figura 6.

Balanceador de carga Peplink

Fuente: Elaboración propia, basado y adaptado de Peplink

Firewall Sangfor: Equipamiento que se encuentra como primer sistema de seguridad de acceso y salida hacia y desde internet. Este sistema de seguridad se encontró en modo transparente.

Figura 7.

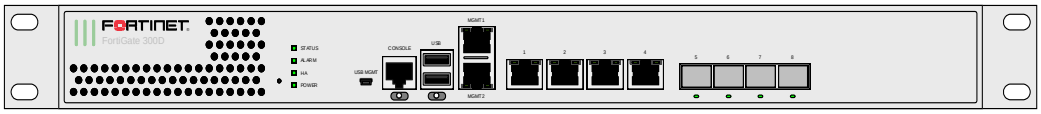
Firewall Sangfor

Fuente: Elaboración propia, adaptado de Sangfor

Firewall Fortinet: Es un sistema de seguridad con funcionalidades de próxima generación además como firewall principal en el cual se encontró configuraciones de diversas políticas de seguridad, así como publicaciones de diferentes servicios propios de la cooperativa.

Figura 8.

Firewall Fortinet

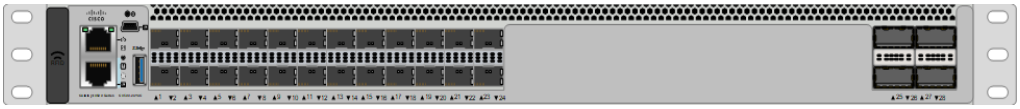


Fuente: Elaboración propia, adaptado de Fortinet

Switch Core: Este equipo es el núcleo principal de toda la red LAN ya que este equipo se encarga de realizar todo el enrutamiento y conmutación de alta velocidad de todas las subredes de la cooperativa de ahorro y crédito Abaco.

Figura 9.

Switch Core

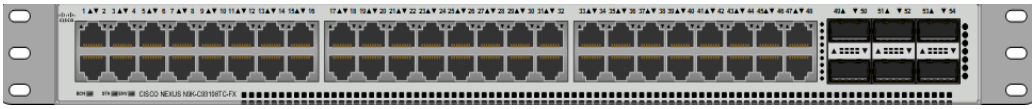


Fuente: Elaboración propia, adaptado de Cisco

Switch servidores: Equipo que se interconecta con todos los servidores para brindar acceso a los diferentes servicios, este equipo se encuentra con HA ubicado en la zona DMZ.

Figura 10.

Switch Servidores

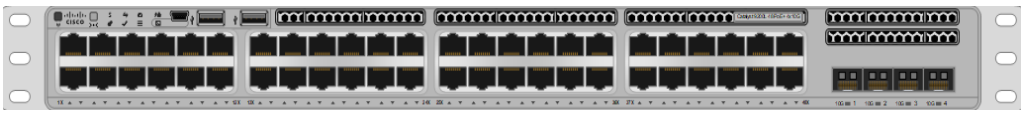


Fuente: Elaboración propia, adaptado de Cisco

Switch para conexión con los ISP: Equipamiento de conmutación para realizar conexiones de alta disponibilidad entre los balanceadores de tráfico de red con los ISP.

Figura 11.

Switch para conexión con los ISP

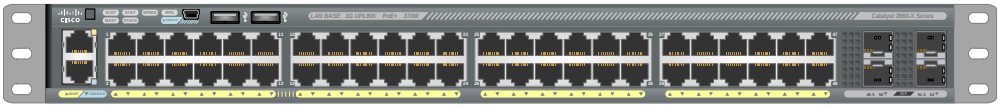


Fuente: Elaboración propia, adaptado de Cisco

Switch Access: Equipamiento de conmutación para realizar conexiones con los usuarios finales ubicados en las diferentes áreas de la cooperativa.

Figura 12.

Switch de Acceso



Fuente: Elaboración propia, adaptado de Cisco

Cisco Unified Communications Manager 11.0: Sistema de tratamiento de llamadas para telefonía IP desarrollado por Cisco Systems.

Figura 13.

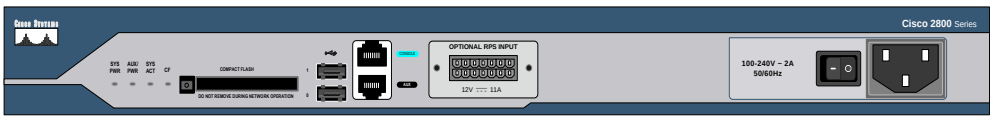
CUCM

Fuente: Elaboración propia, adaptado de Cisco

Router 2800 series: Sistema instalado exclusivamente para realizar enrutamiento para el sistema de telefonía.

Figura 14.

Router 2800



Fuente: Elaboración propia, adaptado de Cisco

VG224: Sistema instalado para interconectar teléfonos analógicos instalados en zonas puntuales.

Figura 15.

VG224

Fuente: Elaboración propia, adaptado de Cisco

Licea: es una línea telefónica o circuito telefónico, para recepción de llamadas y realizar llamadas a números de celular.

Figura 16.

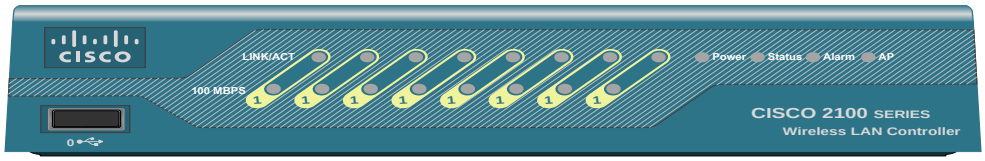
Licea

Fuente: Elaboración propia, adaptado de Cisco

Wireless Lan Controller: Sistema para la administración de varios Access point Cisco instalados en las diversas áreas de la cooperativa.

Figura 17.

WLC



Fuente: Elaboración propia, adaptado de Cisco

Access Point: Equipo inalámbrico para acceso a los diferentes servicios de la cooperativa y navegación web.

Figura 18.

Access Point

Fuente: Elaboración propia, adaptado de Cisco

NVR ACTI: Sistema de almacenamiento de grabación en cual convergen todas las cámaras de la cooperativa.

Figura 19.

NVR ACTI

Fuente: Elaboración propia, adaptado de Acti

Cámara Acti: Equipamiento para realizar el monitoreo correspondiente de todas las actividades que se da en la cooperativa.

Figura 20.

Camara Acti

Fuente: Elaboración propia, adaptado de Acti

Cajero automático: Es un sistema u ordenador que permite realizar operaciones financieras

Figura 21.

Cajero Automático

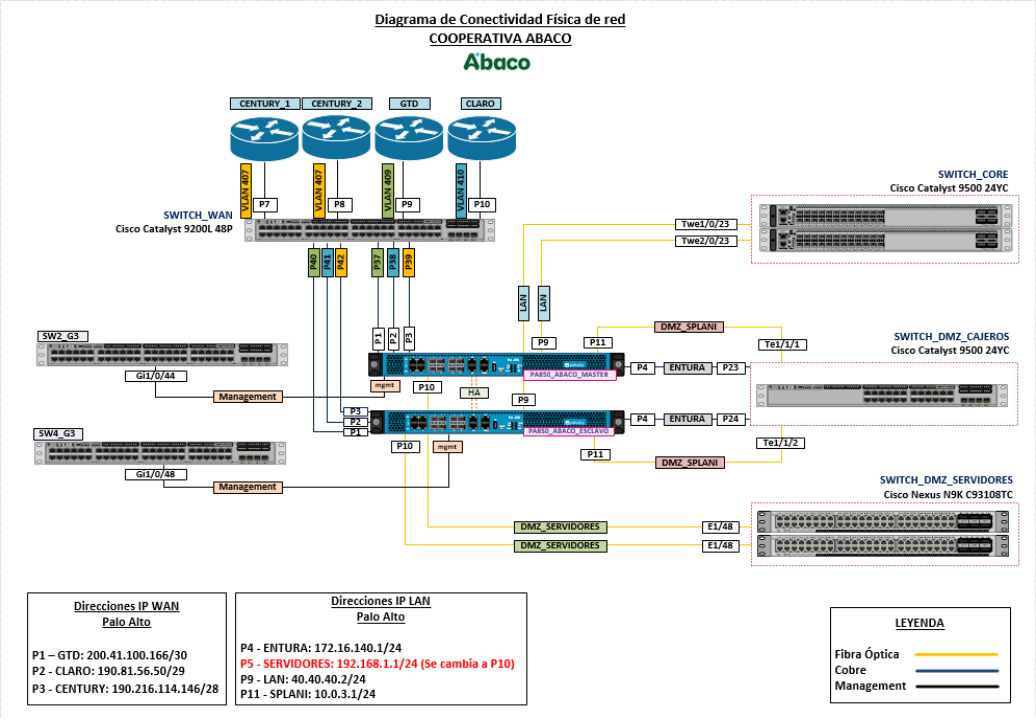
Fuente: Elaboración propia, adaptado de ATM

Diagrama de red de la implementación del firewall Palo Alto.

Se realiza la implementación del nuevo sistema de seguridad palo alto. A continuación, se muestra la nueva topología.

Figura 22.

Diagrama de red nuevo Firewall Palo Alto

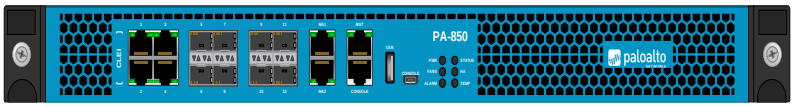


Fuente: Elaboración propia

Firewall Palo Alto: Nuevo sistema de seguridad palo alto en el cual han sido configurados las políticas de seguridad por grupos, publicación de diversos servicios, conexiones de vpn IPsec con diversas empresas y seguridad IPS.

Figura 23.

Firewall Palo Alto



Fuente: Palo Alto Networks

Características propias de la marca

App ID:

Es parte del sistema de seguridad que permite dentro del paquete e identificar la aplicación para así aprender como la aplicación se comporta, sus características y riesgos reales cuando la aplicación se encuentra activa en la red.

Es por ello que para la identificación de aplicaciones utiliza múltiples técnicas entre ellos firmas digitales (signature), des encriptación si es necesario, descifrador de protocolos y de aplicaciones (propia de palo alto), etimología (heurística). Esto permite un control granular del flujo de tráfico. por ejemplo, podemos permitir Facebook, y bloquear Facebook-chat.

En otras palabras, app-id nos permite ver y entender el comportamiento de las aplicaciones en la red. Armado con esta información mejora la seguridad de la red por medio de reglas granulares. (Palo Alto, 2022)

User ID:

Es una forma de identificar a todos los usuarios en la red utilizando una gran variedad de técnicas para identificar a todos los usuarios en todas las ubicaciones usando una variedad de métodos de accesos y sistemas operativos como Microsoft Windows, Apple iOS, Mac OS, Android, y Linux/Unix. de esta

forma identificamos quienes son los usuarios en lugar de solo sus direcciones IP. (Palo Alto, 2022)

DNS Security:

Utiliza el poder de ML para detectar y prevenir las amenazas a través de DNS en tiempo real y proporciona al personal de seguridad la inteligencia y el contexto necesarios para elaborar políticas y responder a las amenazas de forma rápida y eficaz. (Palo Alto, 2022)

Threat Prevention:

Este sistema va más allá de un sistema de Intrusión Prevention (IPS) tradicional para prevenir todas las amenazas conocidas en todo el tráfico en un solo paso, sin sacrificar el rendimiento. (Palo Alto, 2022)

URL Filtering avanzado:

Ofrece protección web de la más alta calidad y maximiza la eficiencia operativa con el primer motor de protección web en tiempo real del sector y una protección contra el phishing líder en el sector. (Palo Alto, 2022)

WildFire:

Garantiza la seguridad de los archivos con la detección y prevención automática de malware desconocido, gracias al análisis basado en la nube gracias a la inteligencia de origen colectivo de más de 42.000 clientes. (Palo Alto, 2022)

Seguridad de IoT:

Proporciona la solución de seguridad de IoT más completa del sector, ya que ofrece visibilidad, prevención y cumplimiento con tecnología ML en una única plataforma. (Palo Alto, 2022)

DLP empresarial:

Ofrece la primera DLP empresarial en la nube del sector que protege sistemáticamente los datos confidenciales en todas las redes, nubes y usuarios. (Palo Alto, 2022)

Seguridad de SaaS:

Ofrece una seguridad SaaS integrada que le permite ver y proteger las nuevas aplicaciones SaaS, proteger los datos y evitar las amenazas de día cero con el menor costo total, de propiedad (TCO). (Palo Alto, 2022)

Matriz de riesgo del proyecto cualitativa del proyecto

En el año en el cual se ejecutó el proyecto se tuvo los siguientes riesgos que se muestra en la tabla.

Tabla 3.

Matriz de riesgo

	1	2	3	4	5
	Insignificante	Menor	Moderada	Importante	Catastrófica
5	5	10	15	20	25
Muy probable	Ausencia por enfermedad de un miembro del equipo	Quejas sobre la empresa			
4	4	8	12	16	20
Probable	Interrupción del suministro eléctrico			Robo de datos del cliente	
3	3	6	9	12	15
Posible			Fraude por parte de un miembro del equipo		
2	2	4	6	8	10
No es probable				Pérdida importante de personal	Incendio o inundación grave
1	1	2	3	4	5
Muy improbable				Riesgo de contagio de COVID 19	Corte prolongado de internet en toda la empresa
	(1-6) Riesgo bajo	(7-12) Riesgo medio		(13-25) Riesgo alto	

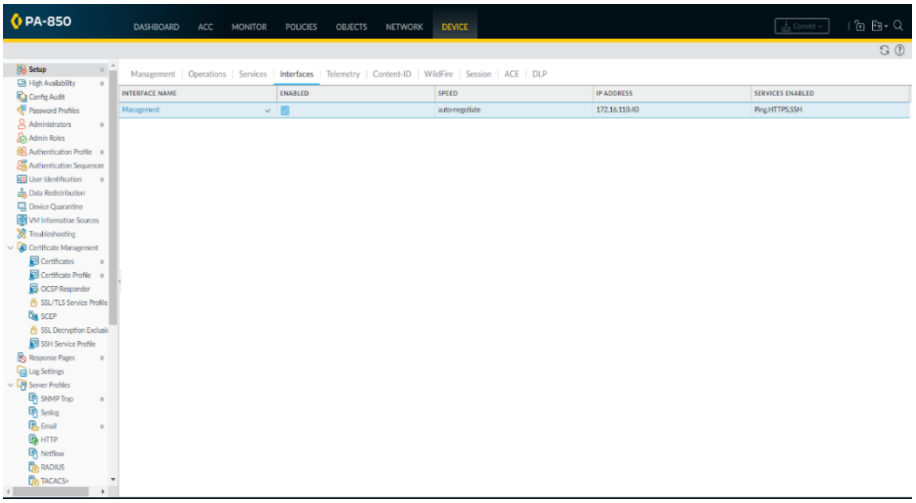
Nota. *Riesgos basados de diferente índole. Fuente: Elaboración propia

Configuración del firewall Palo Alto

Management: En esta interface gráfica del firewall Palo Alto nos permite configurar la interface management para los accesos de los administradores.

Figura 24.

GUI Management Firewall Palo Alto

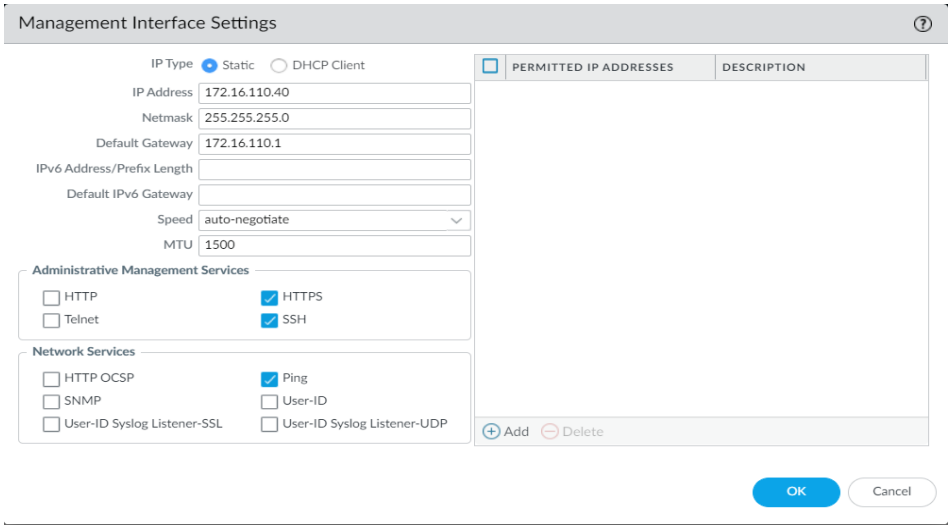


Fuente: Palo Alto Networks

Management interface Setting: Dentro de la opción de interface management colocamos la dirección IP 172.16.110.40 también le ponemos la máscara de red en este caso 24 así como el default Gateway que es 172.16.110.1 así mismo se habilita solamente los servicios que brindan mayor seguridad https, ssh y Ping para los accesos de una forma segura.

Figura 25.

GUI Management Interface Setting

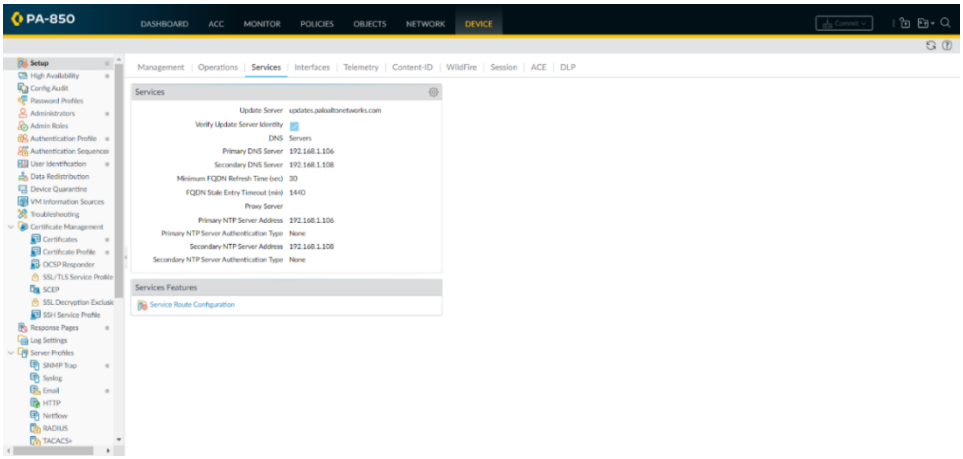


Fuente: Palo Alto Networks

Services: En esta parte se configura diversas direcciones IP de los DNS, así como del servicio NT

Figura 26.

GUI Services

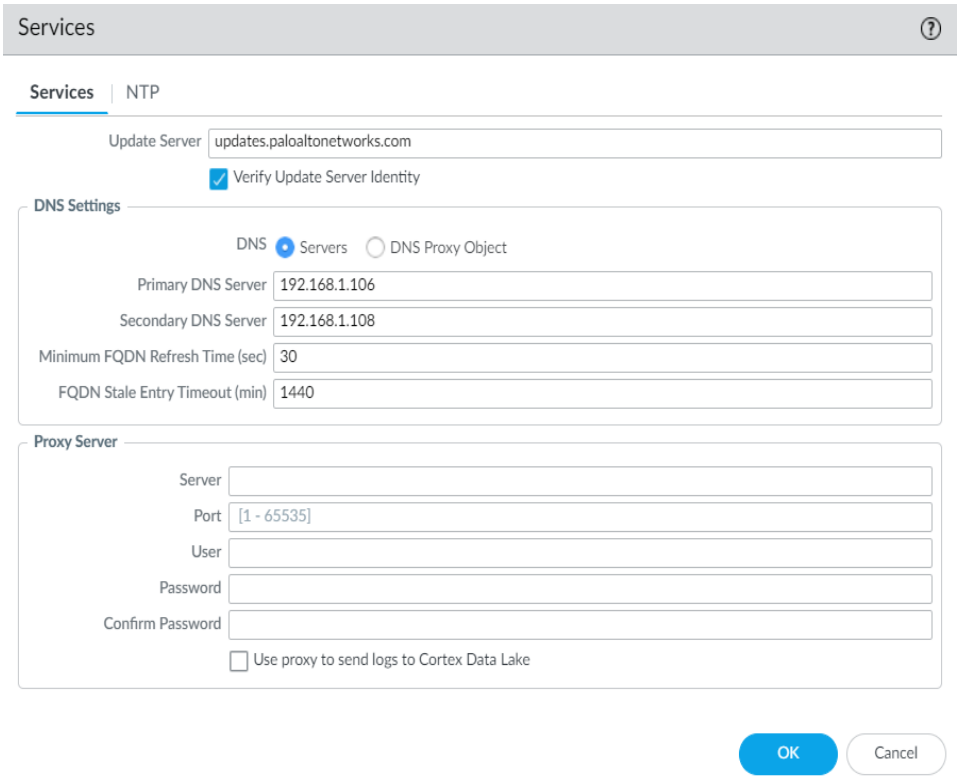


Fuente: Palo Alto Networks

Es así que le vamos colocando las direcciones IP de los DNS internos propios de la cooperativa Abaco.

Figura 27.

GUI Services Update DNS Server

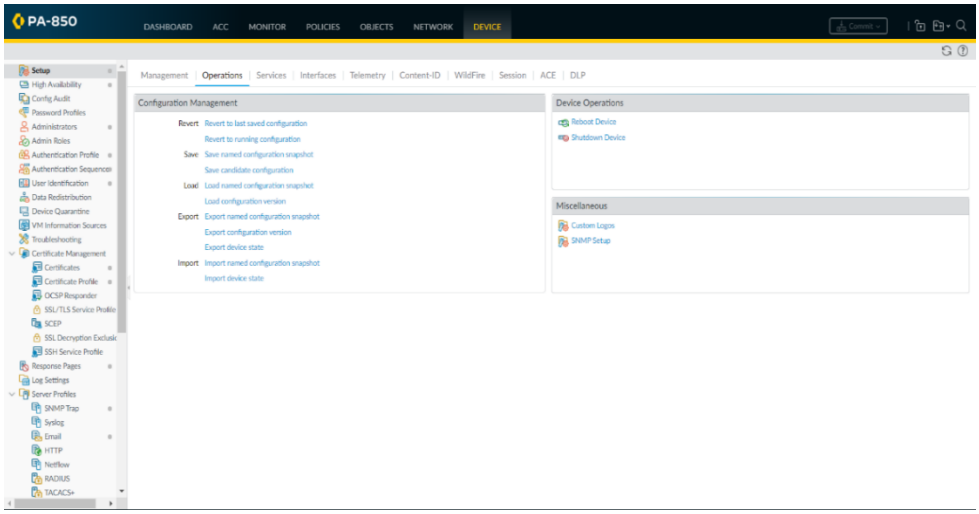


Fuente: Palo Alto Networks

Operations: En esta parte tenemos diversas opciones para configuración, entre ellas para retroceder una configuración, para guardar la configuración en una externa, para cargar una configuración guardada anteriormente, exportar algunos tipos de configuraciones, importar tipos de configuraciones.

Figura 28.

GUI Operations

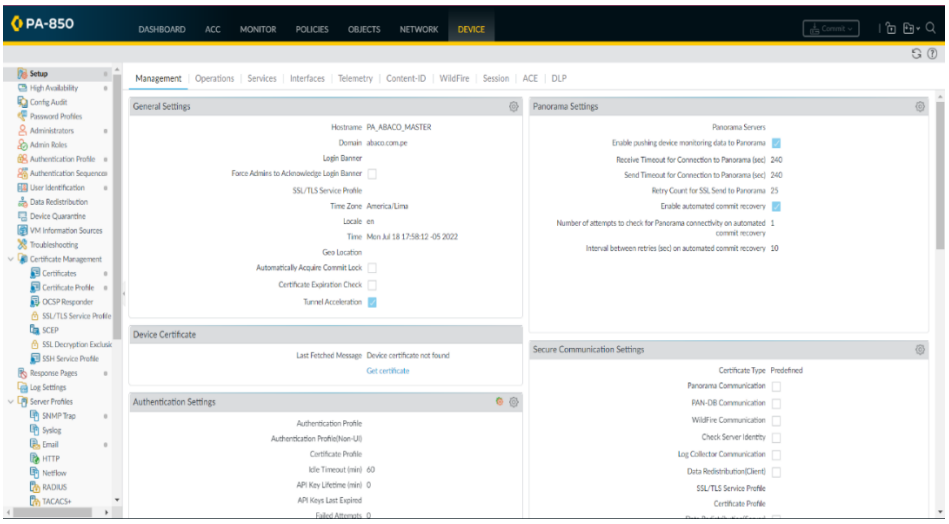


Fuente: Palo Alto Networks

Management: En esta parte se configura el nombre del firewall, así como el dominio de la empresa.

Figura 29.

GUI Management



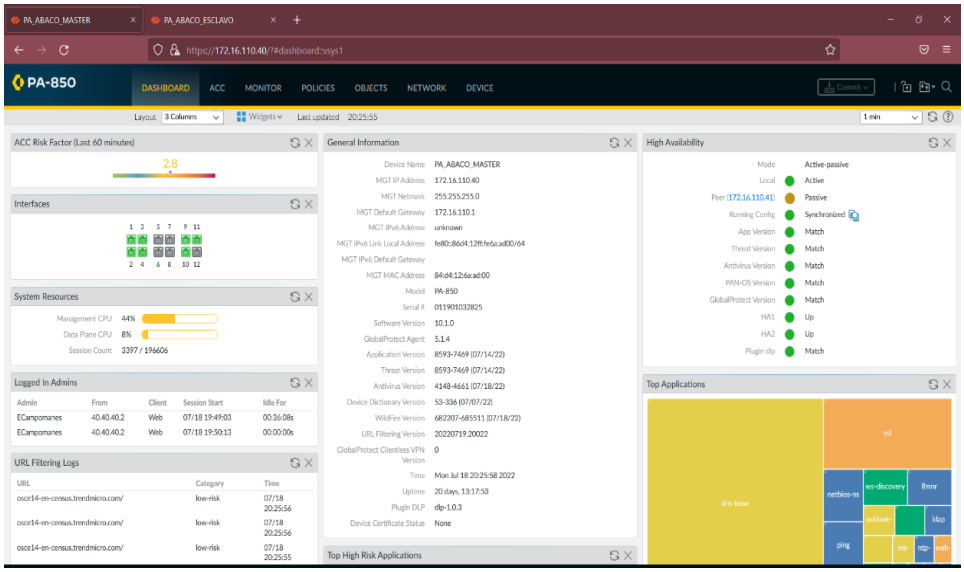
Fuente: Palo Alto Networks

Configuración de Alta Disponibilidad (High Availability): Esta solución de seguridad nos brinda una alta disponibilidad para afrontar diversos riesgos de posibles eventos de caída del firewall Master. Es por ello que se encuentra configurado de la siguiente manera.

Master: El firewall master se encuentra definido con la IP 172.16.110.40/24.

Figura 30.

GUI Dashboard Firewall Activo

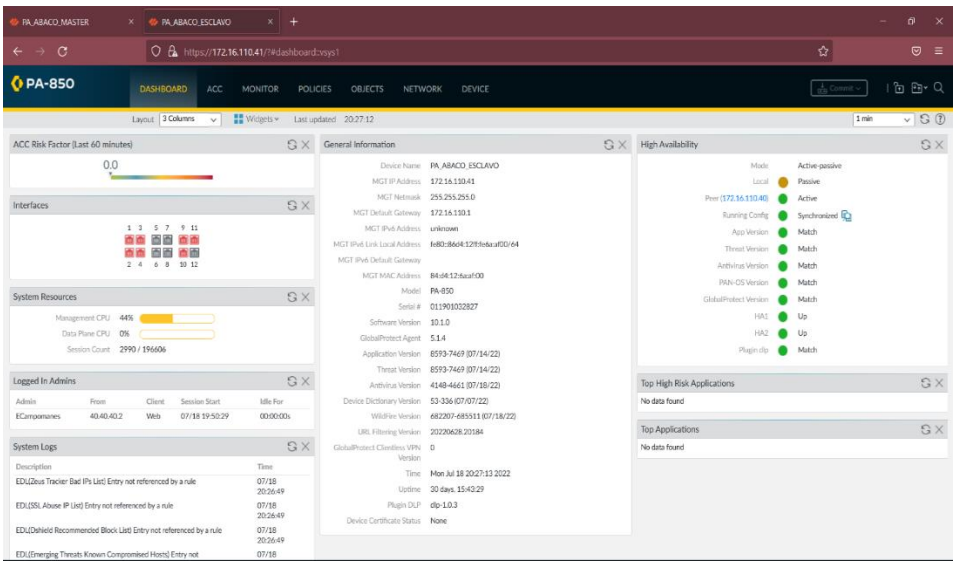


Fuente: Palo Alto Networks

Esclavo: El firewall Esclavo se encuentra definido con la IP 172.16.110.41/24.

Figura 31.

GUI Dashboard Firewall Pasivo

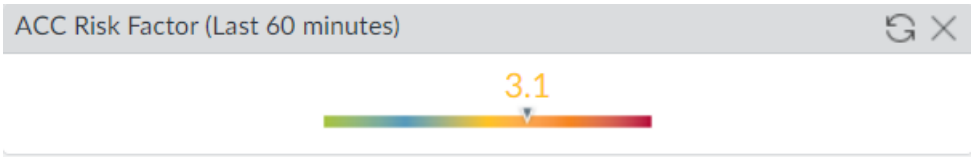


Fuente: *Palo Alto Networks*

Factor de riesgo: Esta parte del sistema nos muestra el nivel de riesgo que existe durante los últimos 60 minutos, los niveles de riesgo son (1=menor a 5=mayor).

Figura 32.

GUI Factor de riesgo

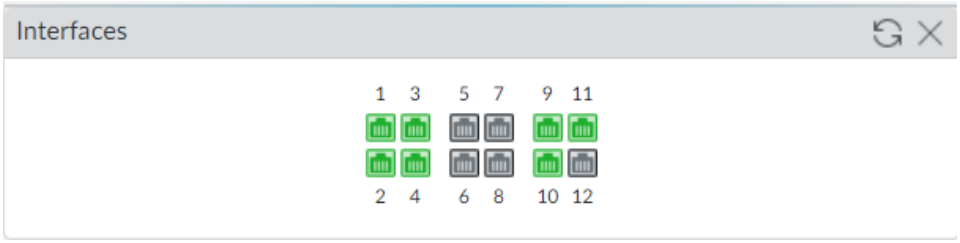


Fuente: Palo Alto Networks

Interfaces: En esta parte observamos todas las interfaces del firewall, de las cuales los que se encuentran activos “funcionando” son los de color verde y los que se encuentran desactivados son los de color gris.

Figura 33.

GUI Interfaces Firewall Activo

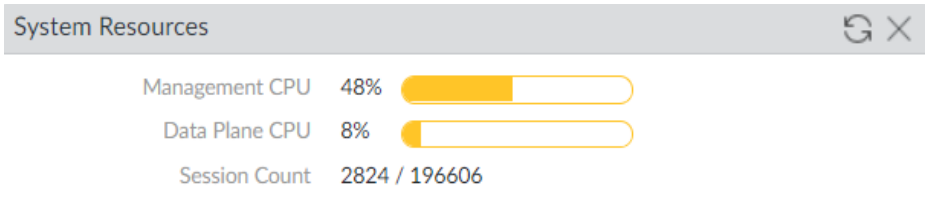


Fuente: Palo Alto Networks

System Resources: El firewall palo alto tiene dos CPU uno asignado específicamente para el tema de gestión y el otro asignado para el tema de datos.

Figura 34.

GUI System Resorces

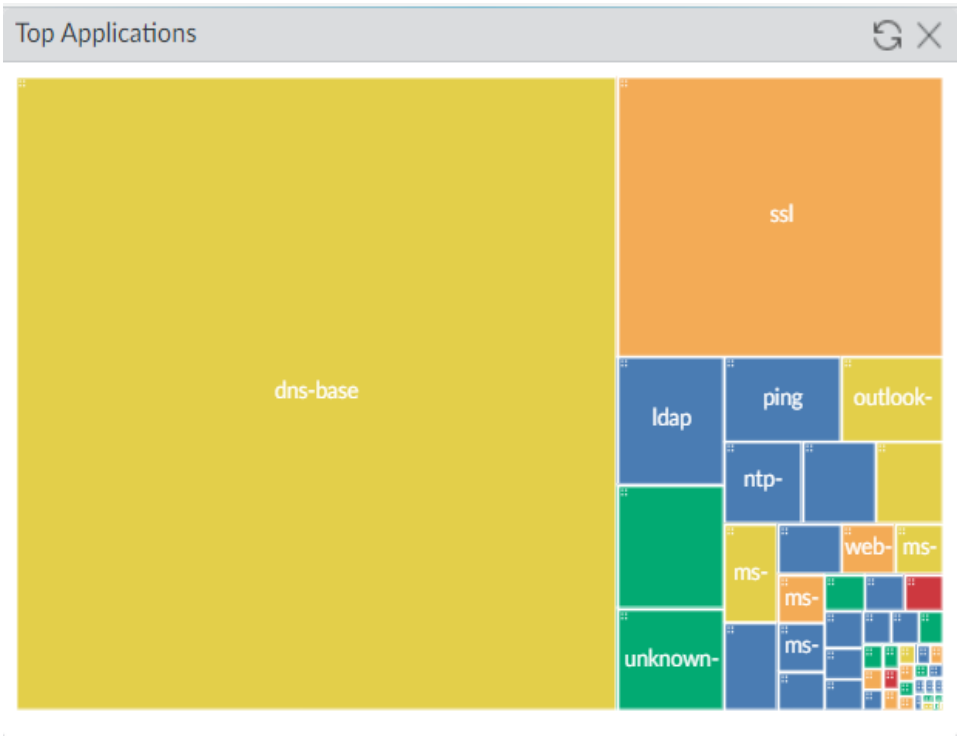


Fuente: Palo Alto Networks

Top Applications: Este gráfico muestra las aplicaciones con la mayoría de las sesiones o de mayor consumo del ancho de banda.

Figura 35.

GUI Top Applications

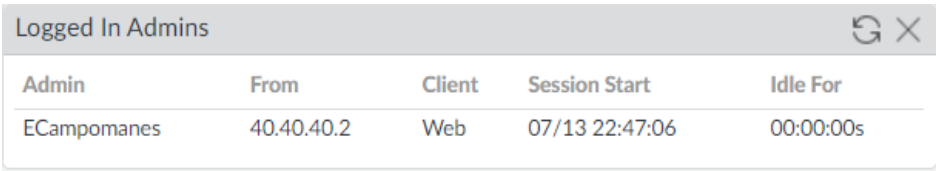


Fuente: Palo Alto Networks

Logged In Admins: En esta parte se observa todas las conexiones al firewall en tiempo real, de todos los usuarios admitidos o creados en el firewall.

Figura 36.

Logged In Admins

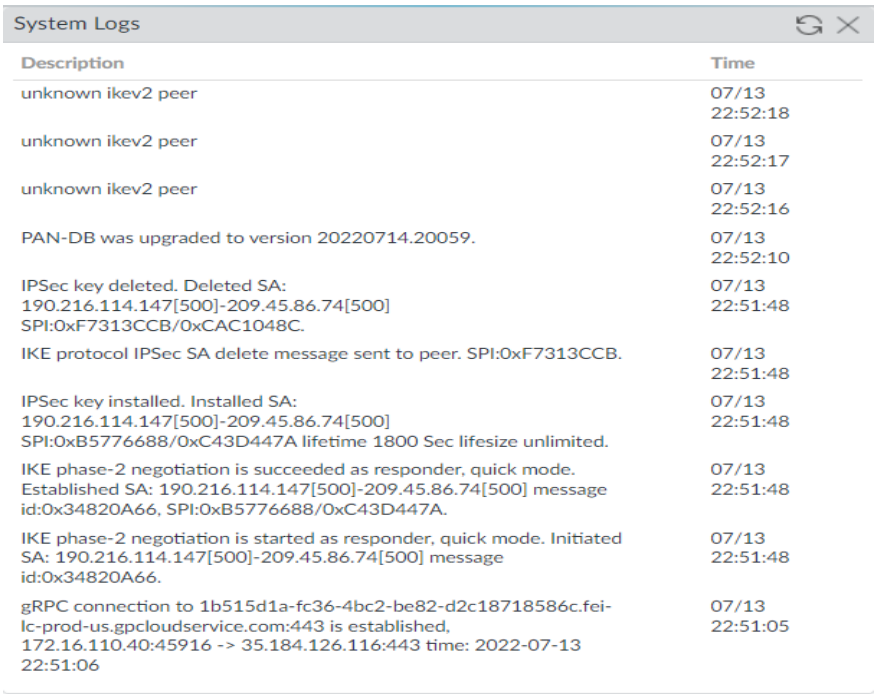


Fuente: Palo Alto Networks

Systems Logs: Interface en el cual se observa todos los acontecimientos del sistema en tiempo real.

Figura 37.

Systen Logs

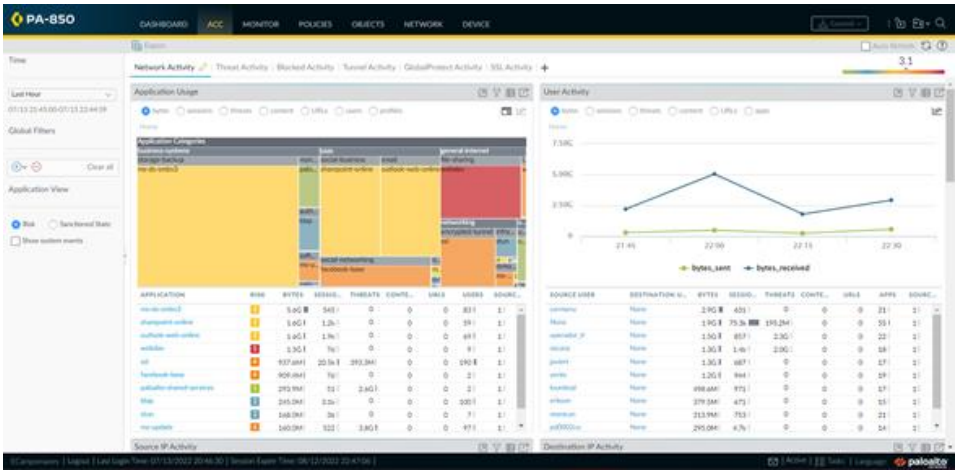


Fuente: Palo Alto Networks

Network Activity: En estas imágenes se observan el tráfico de red por aplicación con su respectiva asignación de riesgos; también se observa el tráfico de red por parte d los usuarios de la cooperativa.

Figura 38.

Network Activity

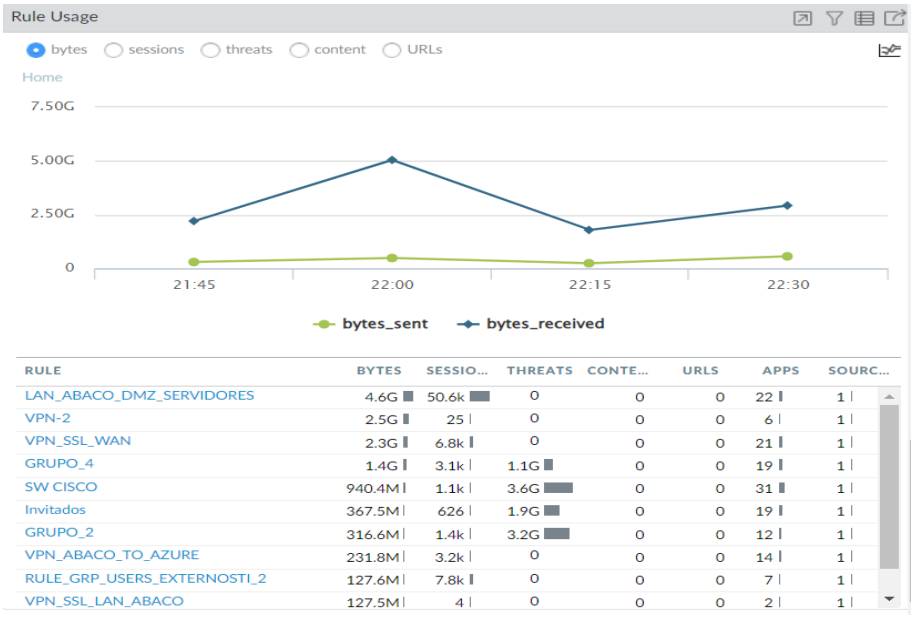


Fuente: Palo Alto Networks

Rule Usage: Interface en el cual se observa las sesiones y amenazas desde las zonas creadas y aplicados en las reglas.

Figura 39.

Rule Usage



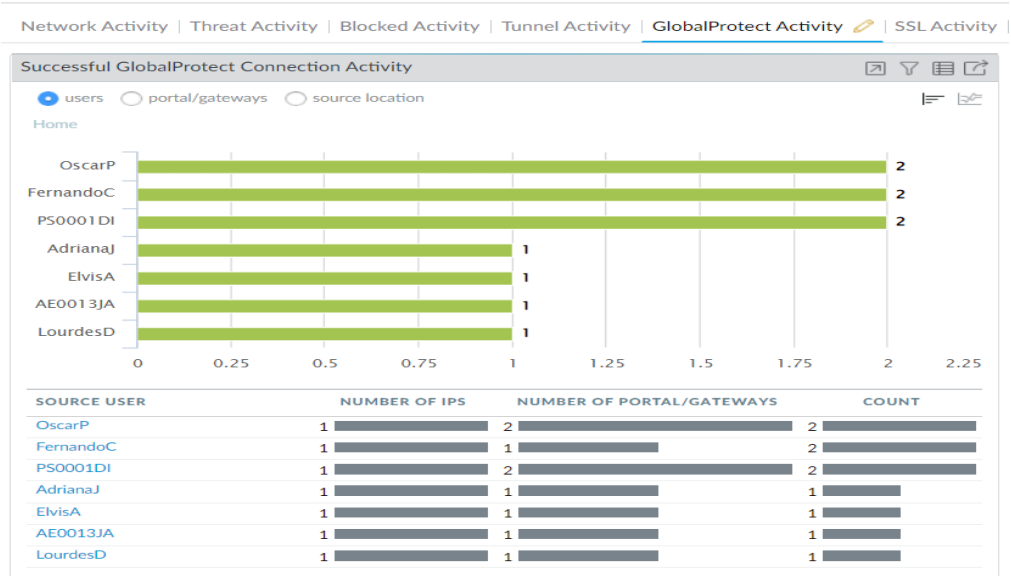
RULE	BYTES	SESSIO...	THREATS	CONTE...	URLS	APPS	SOURC...
LAN_ABACO_DMZ_SERVIDORES	4.6G	50.6k	0	0	0	22	1
VPN-2	2.5G	25	0	0	0	6	1
VPN_SSL_WAN	2.3G	6.8k	0	0	0	21	1
GRUPO_4	1.4G	3.1k	1.1G	0	0	19	1
SW CISCO	940.4M	1.1k	3.6G	0	0	31	1
Invitados	367.5M	626	1.9G	0	0	19	1
GRUPO_2	316.6M	1.4k	3.2G	0	0	12	1
VPN_ABACO_TO_AZURE	231.8M	3.2k	0	0	0	14	1
RULE_GRP_USERS_EXTERNOSTI_2	127.6M	7.8k	0	0	0	7	1
VPN_SSL_LAN_ABACO	127.5M	4	0	0	0	2	1

Fuente: Palo Alto Networks

Global Protect Activity: en esta interface grafica observamos las conexiones exitosas de los usuarios con cuenta VPN (clientes vpn).

Figura 40.

GUI Global Protect Activity

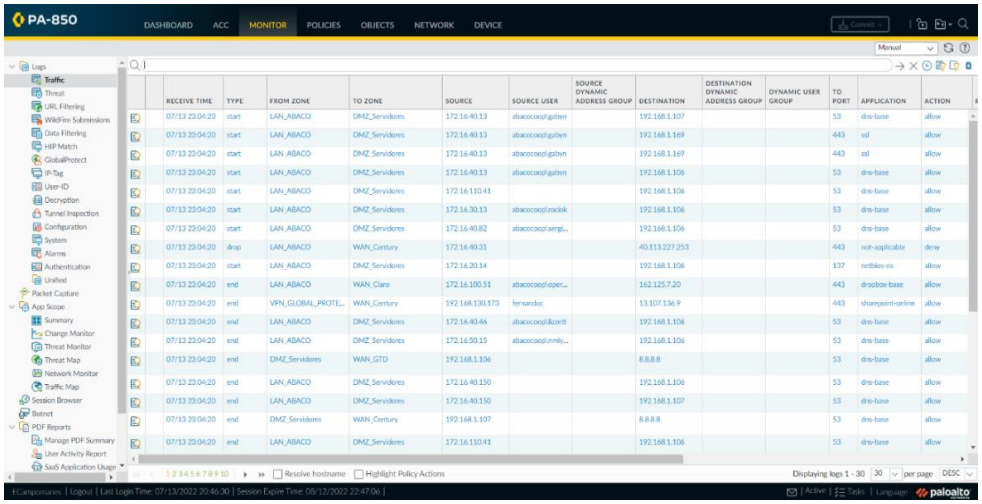


Fuente: Palo Alto Networks

Monitor: en esta GUI se realiza el monitoreo de todo el tráfico de las zonas que pasan a través del firewall Palo Alto.

Figura 41.

GUI Monitor

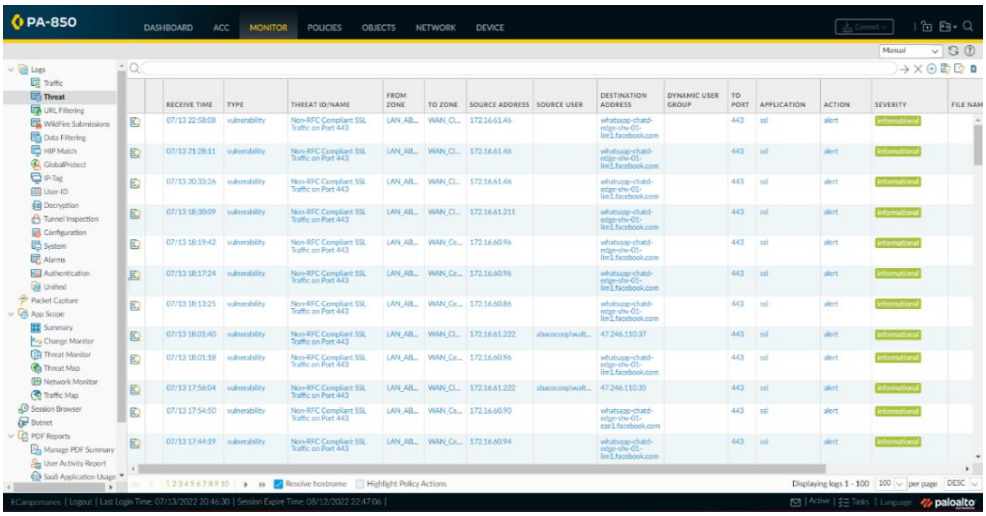


Fuente: Palo Alto Networks

Monitor Threat: En esta GUI muestra un recuento de las principales amenazas durante el periodo de tiempo seleccionado.

Figura 42.

GUI Monitor Threat

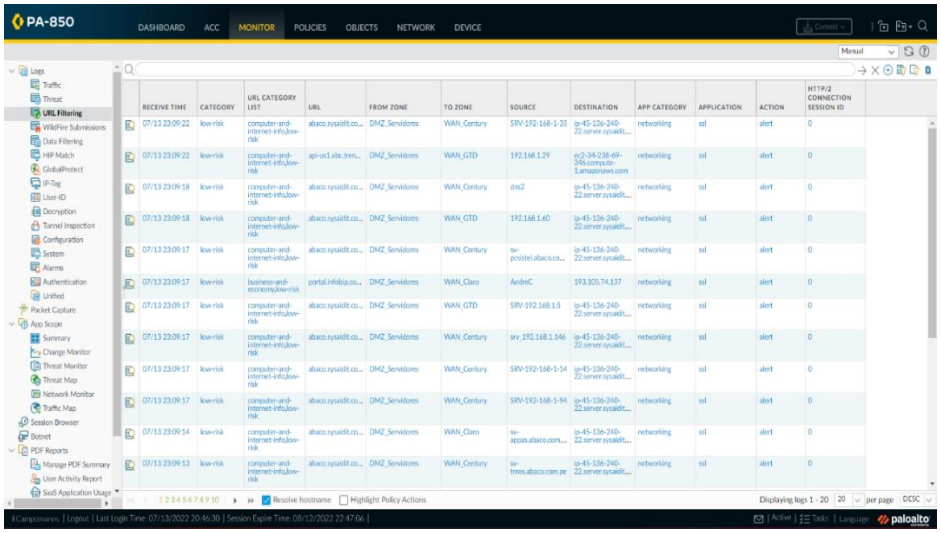


Fuente: Palo Alto Networks

URL Filtering: Muestra información completa sobre el tráfico a las categorías de URL supervisadas en las reglas de las políticas de seguridad.

Figura 43.

URL Filtering

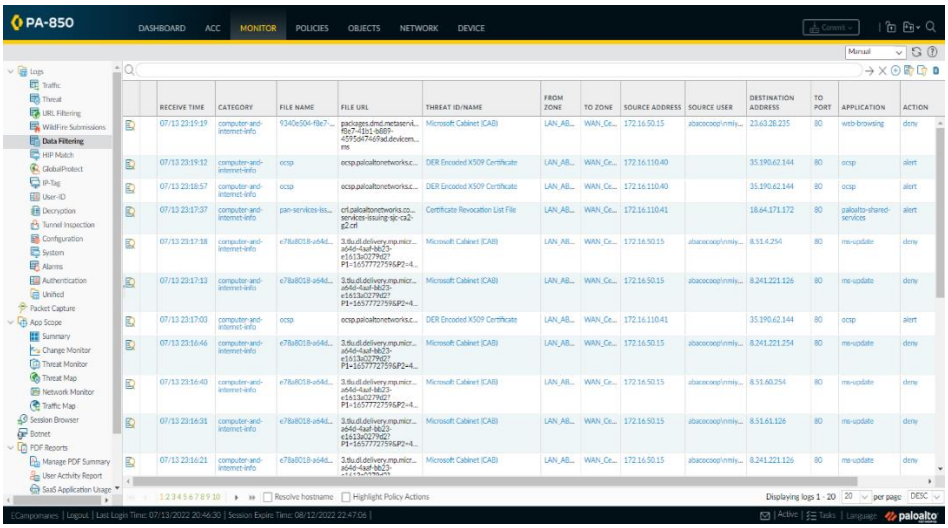


Fuente: Palo Alto Networks

Data Filtering: Los registros de filtrado de datos muestran entradas para las reglas de seguridad que ayudan a evitar que la información confidencial, como números de tarjetas de crédito, salga del área que protege el firewall.

Figura 44.

GUI Filtering

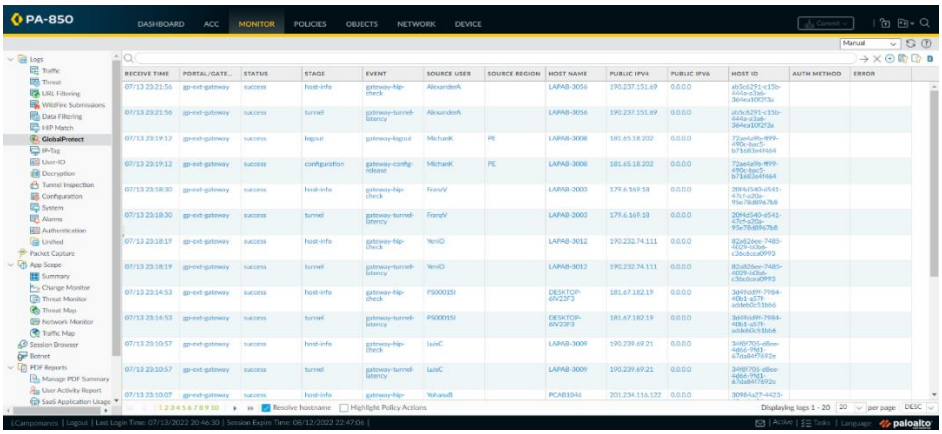


Fuente: Palo Alto Networks

Global Protect: Muestra el método de autenticación utilizado para los inicios de sesión.

Figura 45.

GUI Global Protect

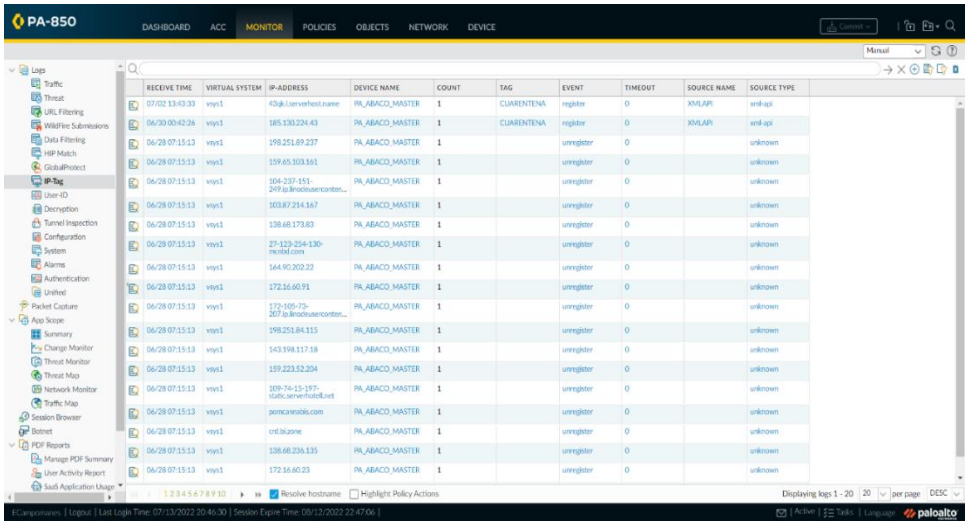


Fuente: Palo Alto Networks

IP-Tag: Los registros de etiqueta s IP muestran cómo y cuándo una dirección IP de origen se registra o cancela en el firewall y qué etiqueta aplicó el firewall a la dirección.

Figura 46.

GUI IP TAG

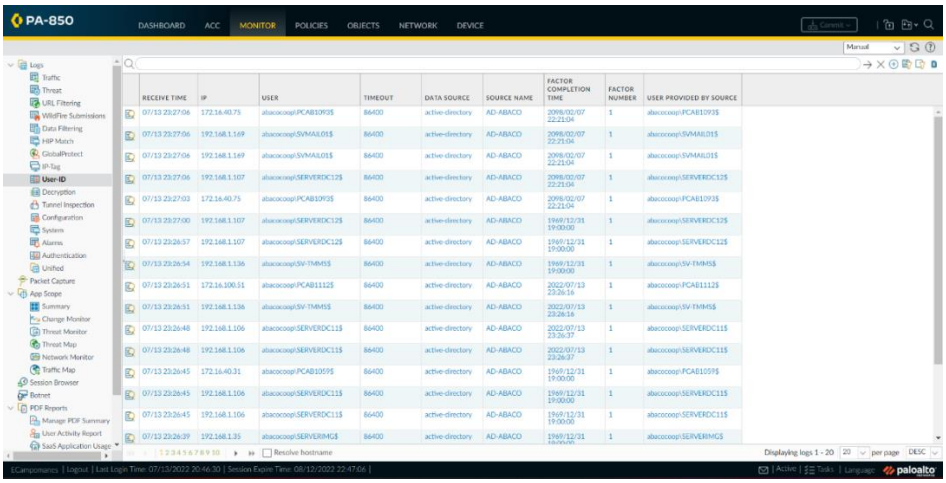


Fuente: Palo Alto Networks

User-ID: Los registros de ID de usuario muestran información sobre asignaciones de dirección IP a nombre de usuario y marcas de tiempo de autenticación, como las fuentes de asignación de la información y las horas en que los usuarios se autenticaron.

Figura 47.

GUI User ID

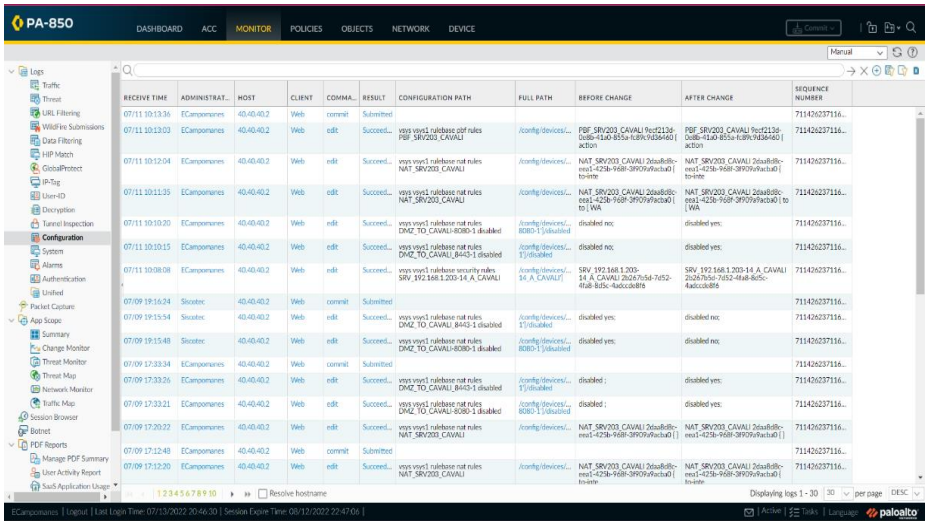


Fuente: Palo Alto Networks

Configuración: Los registros de las configuraciones realizados por los administradores del sistema de seguridad firewall son guardados en una base de datos del firewall palo alto.

Figura 48.

GUI Configuración

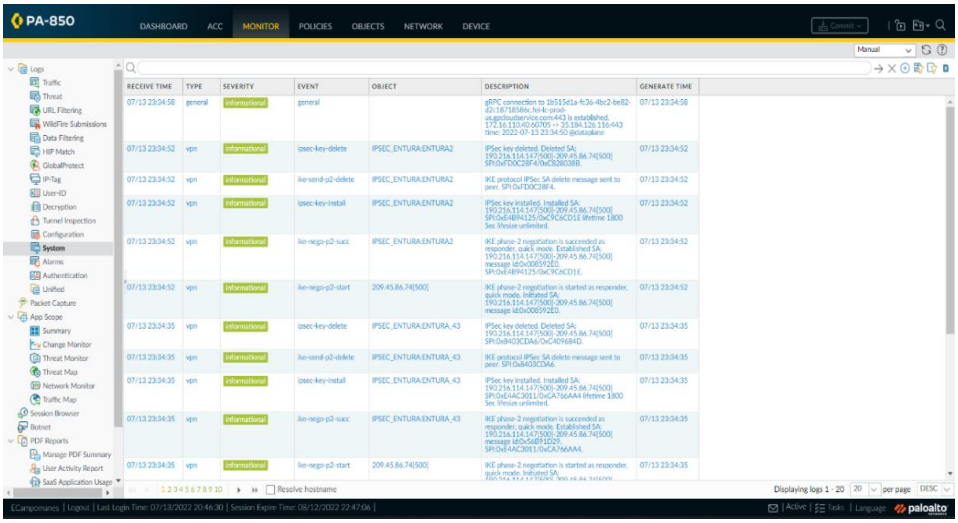


Fuente: Logs Descryption

System: Los eventos con su respectivo nivel riesgo son almacenados en esta unidad del firewall palo alto.

Figura 49.

GUI Logs Systems

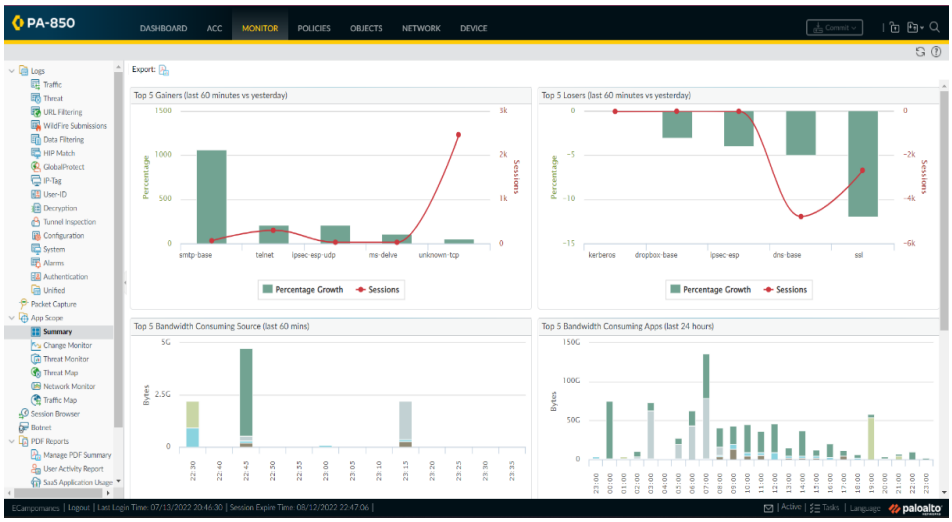


Fuente: Palo Alto Networks

Summary: El informe top de las cinco principales aplicaciones ganadoras, perdedoras y consumidoras de ancho de banda, categorías de aplicaciones, usuarios y fuentes.

Figura 50.

GUI Scope Summary

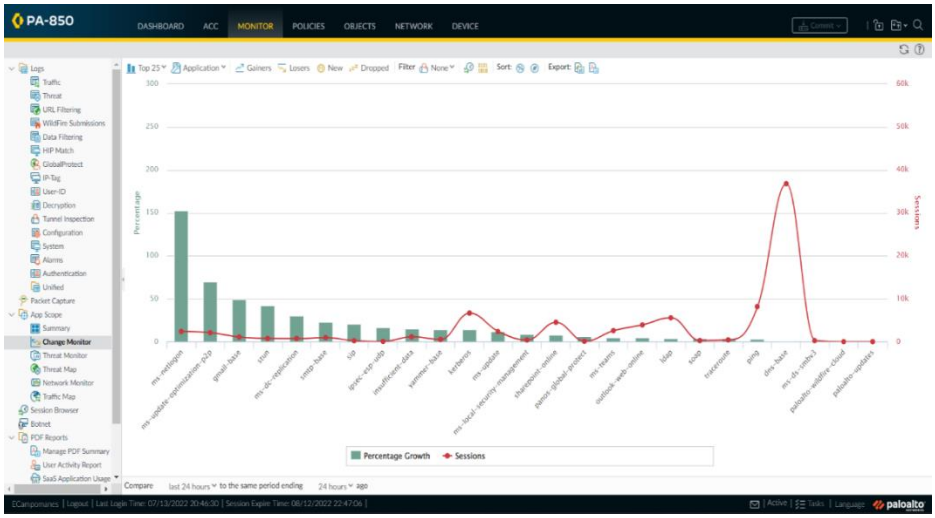


Fuente: Palo Alto Networks

Change Monitor: El informe del monitor de cambios muestra los cambios durante un periodo de tiempo específico.

Figura 51.

GUI App Change Monitor

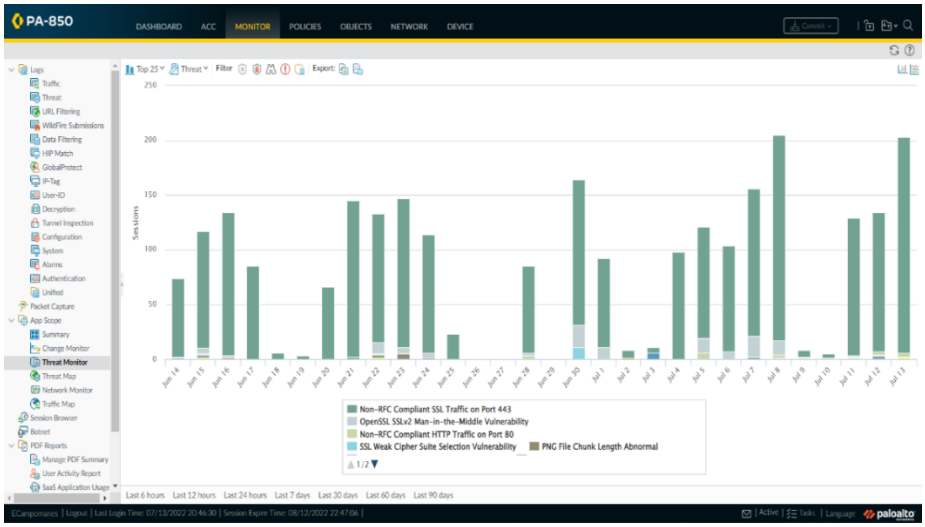


Fuente: Palo Alto Networks

Threat Monitor: El informe del monitor de amenazas muestra un recuento de las principales amenazas durante el periodo de tiempo seleccionada.

Figura 52.

GUI App Scope Threat Monitor

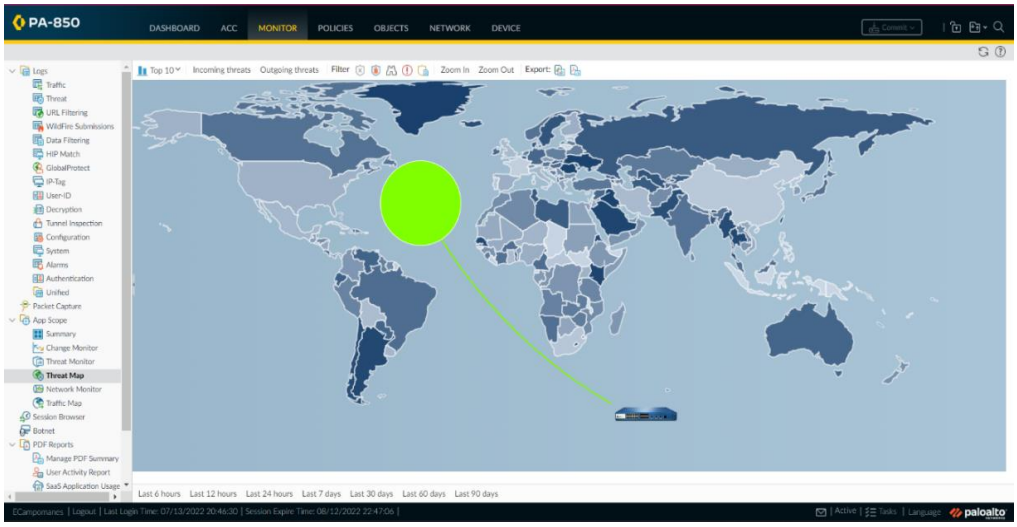


Fuente: Palo Alto Networks

Threat Map: El informe threat Map muestra una vista geográfica de las amenazas, en el cual **incluye el nivel de riesgo.**

Figura 53.

GUI App Scope Map

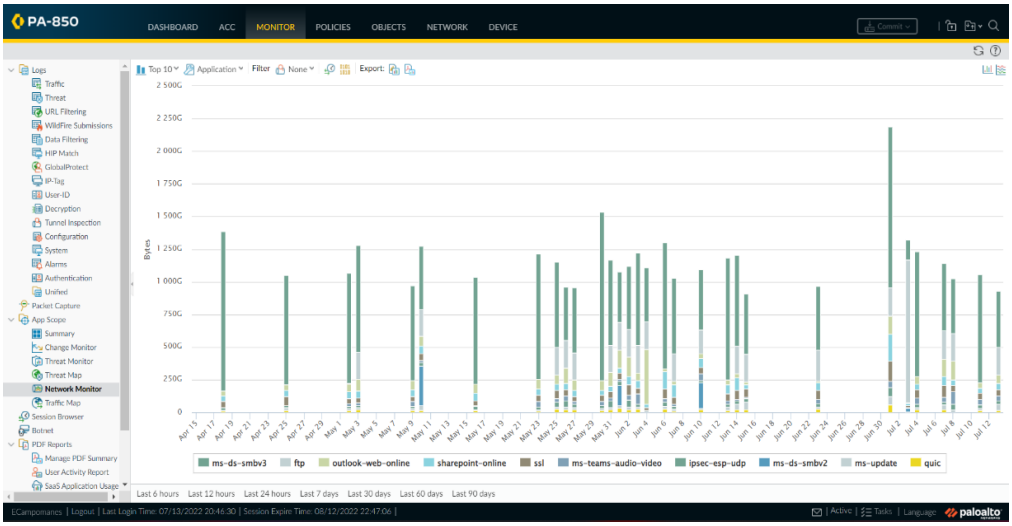


Fuente: Palo Alto Networks

Network Monitor: El informe Network monitor muestra el ancho de banda dedicado a diferentes funciones de red durante el periodo de tiempo especificado, en la cual cada función de red se encuentra codificada por colores como se indica en la leyenda debajo del gráfico.

Figura 54.

GUI App Scope Network Monitor

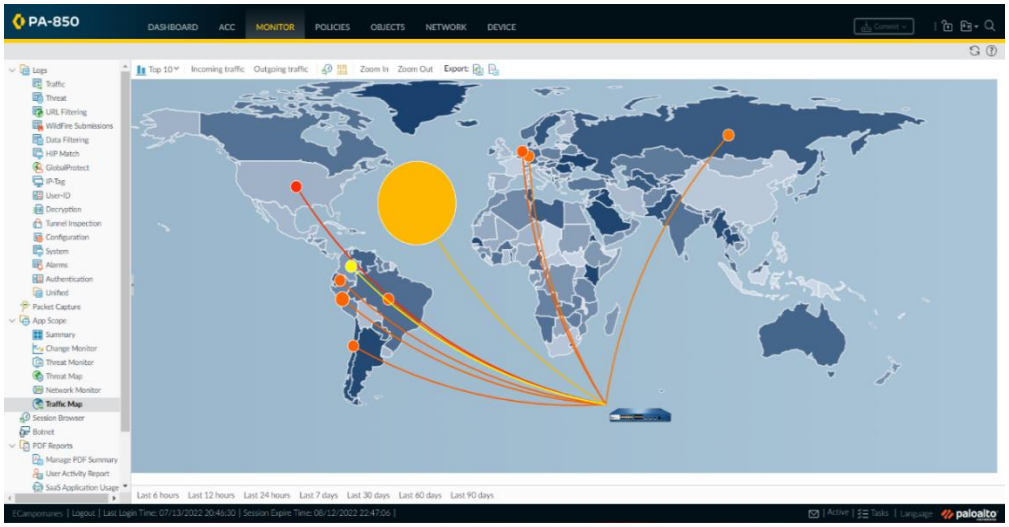


Fuente: Palo Alto Networks

Traffic Map: El informe traffic map muestra una vista geográfica de los flujos de tráfico según sesiones o flujos.

Figura 55.

GUI App Scope Traffic Map

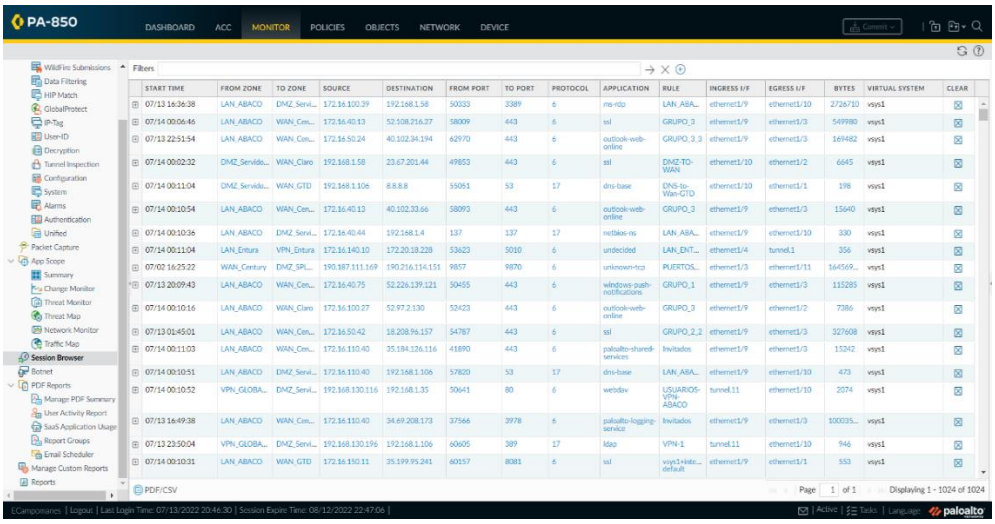


Fuente: Palo Alto Networks

Session Browser: Navegador de sesión permite examinar y filtrar las sesiones en ejecución actuales en el firewall, esto para obtener información sobre las opciones de filtrado de una determinada página.

Figura 56.

GUI Session Browser

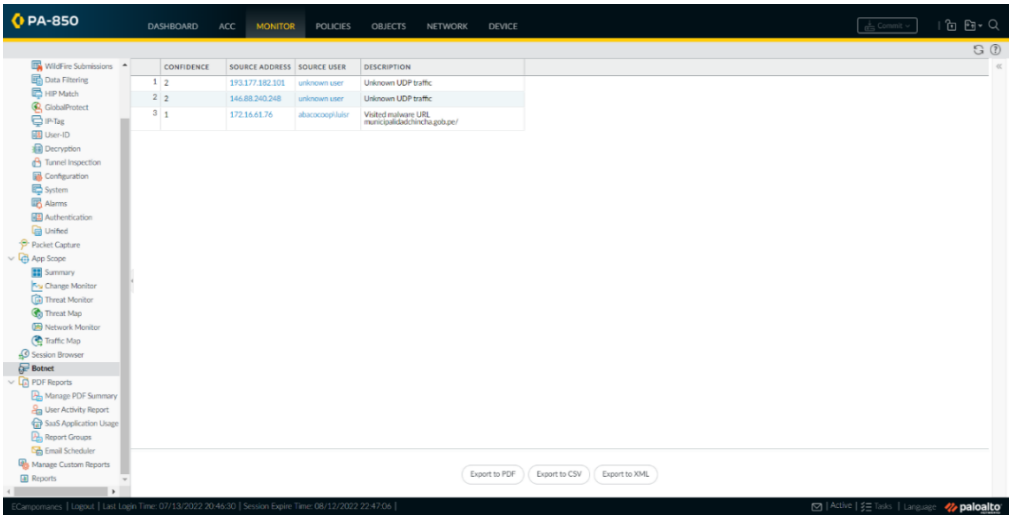


Fuente: Palo Alto Networks

Botnet: El informe de botnet permite utilizar mecanismos basados en el comportamiento para identificar posibles hosts infectados con malware y botnet en la red, el informe asigna a cada host una puntuación de confianza de 1 a 5 para indicar la probabilidad de infección por botnet, donde la puntuación más alta en este caso es 5 por lo tanto tiene mayor probabilidad de amenaza.

Figura 57.

GUI Botnet



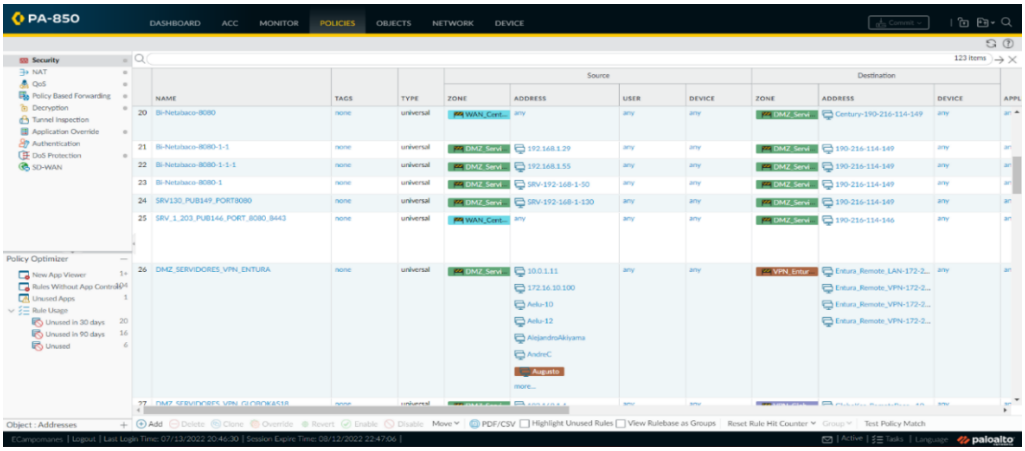
Fuente: Palo Alto Networks

- **POLICIES**

Security: Las reglas de la política de seguridad hacen referencia a las zonas de seguridad y le permiten permitir, restringir y rastrear el tráfico en la red según la aplicación, el usuario o grupo de usuarios y el servicio dependiendo del (puerto y protocolo).

Figura 58.

Policies Security

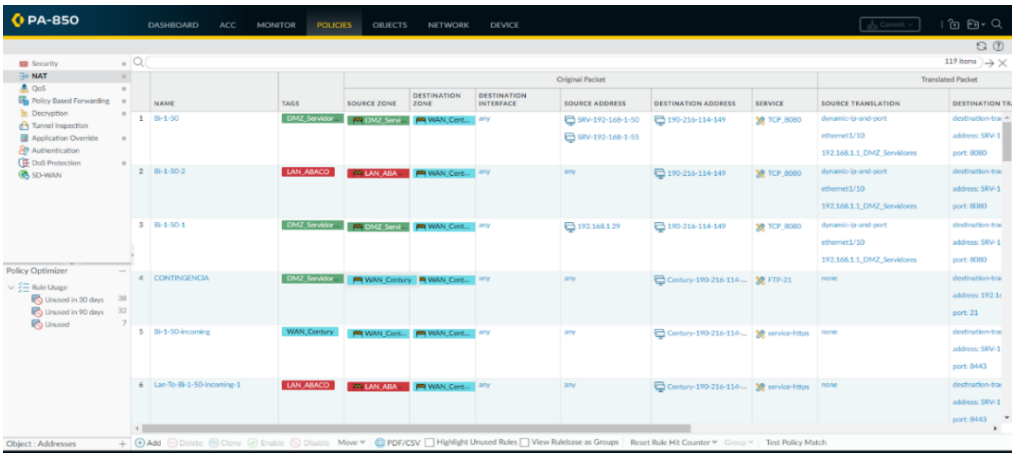


Fuente: Palo Alto Networks

NAT: Al definir las interfaces de capa 3 en el firewall se configura políticas de traducción de direcciones para especificar si las direcciones IP y los puertos de origen o de destino se convierten entre direcciones y puertos públicos y privados. Es así que en nuestro caso se encuentra traducido determinados servicios propios de la cooperativa Abaco para los accesos.

Figura 59.

Policies NAT

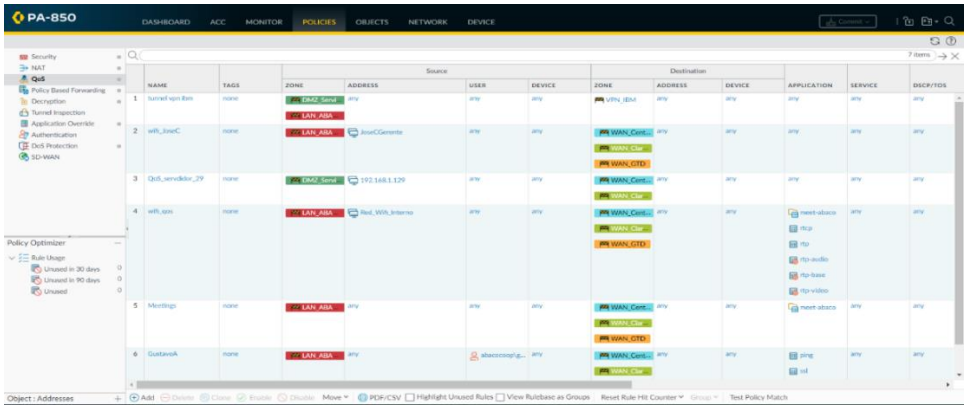


Fuente: Palo Alto Networks

QoS: La política de calidad de servicio sirve para definir el tráfico, en este caso recibe un tratamiento de QoS específico y asigna una clase de QoS para cada regla de política de QoS pues esta política se hace uso dependiendo del tipo de servicio asignado, en otras palabras, todo el tráfico que coincide con esta política será permitido con el valor agregado de calidad de servicio.

Figura 60.

Policies QoS

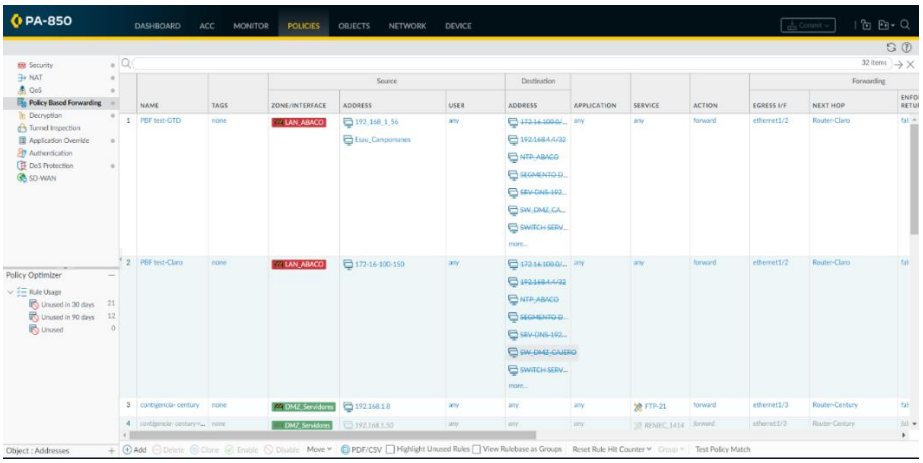


Fuente: Palo Alto Networks

Policy Based Forwarding: Cuando el tráfico ingresa, el enrutador virtual de la interfaz de ingreso dicta la ruta que determina la interfaz de salida y la zona de seguridad de destino según la dirección IP de destino. Al crear esta regla de reenvío basado en política (PBF) puede especificar otra información para determinar la interfaz de salida, incluida la zona de origen, la dirección de origen, el usuario de origen, la dirección de destino, la aplicación de destino y el servicio de destino.

Figura 61.

GUI POLICES PBF



Fuente: Palo Alto Networks

CAPITULO IV RESULTADOS

Luego de implementar el nuevo firewall Palo Alto se diferencia el cambio ya que anteriormente el firewall Fortinet tuvo caídas en la comunicación con los servidores afectando la sincronización de los usuarios finales para ingresar a las políticas definidos por grupos para el uso de los diversos servicios internos, así como la salida hacia internet.

- Antes de la implementación presentaba latencia en la red ocasionando demoras en las sesiones de los usuarios, así mismo el firewall Fortinet requería de un agente llamado FSSO (Fortinet Single Sign On) para que haya conexión con el controlador de dominio (DC) en el cual se encontraban grupos definidos para la autenticación de los usuarios y de esta manera consumir los recursos de la red.

A continuación, se visualiza la tabla de incidencias presentadas antes de la implementación:

Tabla 4.

Incidencias con Firewall Fortinet

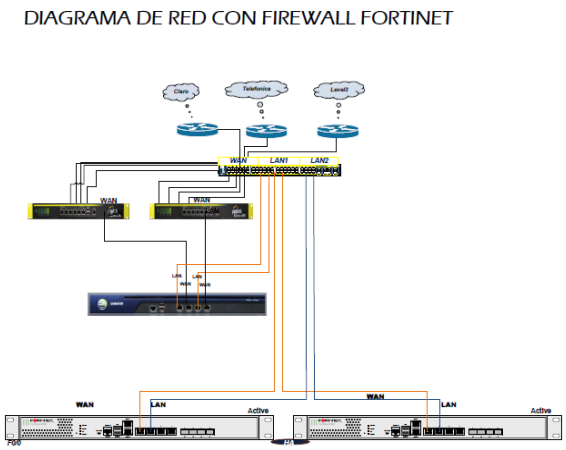
INCIDENCIAS CON FIREWALL FORTINET			
	2018	**2019**	**2020**
ENERO			
FEBRERO			**X**
MARZO	**X**		
ABRIL		**X**	
MAYO			**X**
JUNIO			
JULIO	**X**		
AGOSTO			
SETIEMBRE		**X**	
OCTUBRE	**X**		
NOVIEMBRE			
DICIEMBRE			

Fuente: Incidencias por el firewall Fortinet. Abaco

De la misma manera se optimizó esta solución inicial eliminando dos niveles de equipamiento entre ellos balanceadores de carga y firewall, como se muestra en la imagen:

Figura 62.

Diagrama de Red Firewall Fortinet



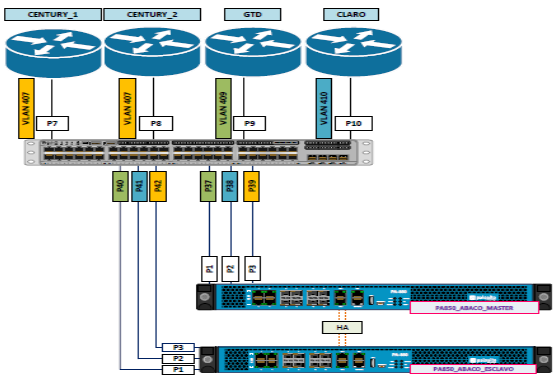
Fuente: Elaboración propia

- Después de realizar la implementación con el nuevo firewall palo alto se observa un cambio en la estabilidad de conexión con los servidores, así mismo la saturación de red mejoró en su totalidad brindando una mayor rapidez en el tráfico de red.

  Se muestra la imagen de la nueva implementación del Firewall Palo Alto:

Figura 63.

Diagrama de Firewall Palo Alto



Fuente: Elaboración Propia

A continuación, se muestra la tabla de incidencias ocurridas después de la implementación del Firewall Palo Alto.

Tabla 5.

Incidencias con firewall Palo Alto

INCIDENCIAS CON FIREWALL FORTINET			
	2020	**2021**	**2022**
ENERO			
FEBRERO			
MARZO			
ABRIL		**X**	
MAYO			**X**
JUNIO			
JULIO			
AGOSTO			
SETIEMBRE			
OCTUBRE			
NOVIEMBRE			
DICIEMBRE			

Fuente: Incidencias Firewall Palo Alto- Abaco

Finalmente, los resultados logrados posterior a la implementación del nuevo firewall palo alto.

Mapeo de los usuarios mediante **USER-ID**, el cual por medio de la identificación de los usuarios permite una visibilidad total de los procesos que se ejecutan y el contenido al que acceden, quién, cómo, cuándo y dónde, robusteciendo ampliamente la solución basada en el método confianza cero. Estos contenidos son inspeccionados a profundidad por mecanismos como **Content-ID**, el cual inspecciona todo el tráfico permitido usando múltiples técnicas de prevención de amenazas, con un control granular sobre las aplicaciones permitidas, reduciendo de esta manera la superficie de ataque en lo que corresponde a la red. Así mismo **APP-ID** identifica las aplicaciones al comparar las signaturas y las características transaccionales de cada aplicación contra la base de datos de palo alto.

BIBLIOGRAFÍA

Anon. (2015). Las pymes son más propensas a los ataques en la red En Colombia. Obtenido de http://www.colombia.com/tecnologia/actualidad/sdi/111715/las-pymesson-mas-propensas-a-los-ataques-en-la-red>).

Castillo Palomino, R. G. Domínguez Chavez, M. A. Sunca Galarza, C. I. (2017). Implementación de un firewall tmg forefront para la seguridad perimetral de la red de datos de la clínica aliada. [tesis para optar título, Universidad peruana de las américas]. Obtenido de http://repositorio.ulasamericas.edu.pe/handle/upa/322

Cabanillas Chávez, J. C. (2015). Propuesta de implementación de control de tráfico de la red con Linux para mejorar la calidad de servicio de la red LAN en una universidad privada de la ciudad de Cajamarca. [Tesis para optar maestría, Universidad Privada del Norte]

Cisco. (2020). What Is a Firewall. Recuperado por: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Cyberprimo. (2008). Obtenido de http://www.cyberprimo.com/2007/08/tipos-de-redes-informaticas.html

Debía Walkowski. (2019). CIA: los tres principios fundamentales de la seguridad de la información. Rev. Mundo contact. Obtenido de: https://mundocontact.com/cia-los-tres-principios-fundamentales-de-la-seguridad-de-la-informacion/

Duarte Martínez, R. F. Paredes Ríos, S. J. (2016). Análisis del uso que hacen los usuarios conectados a un punto de acceso inalámbrico, sin autenticación, con conexión a Internet, ubicado en el edificio CIDS de la Universidad Nacional Autónoma de Nicaragua (Unan-León), en el período comprendido entre el día 5 al día 23 del mes de octubre del año 2015. [para optar título, Universidad Nacional Autónoma de Nicaragua, UNAN – León]

Caballa Torres, E. Torres Flores, W., L. (2010). Implementación de una solución de seguridad informática bajo la plataforma de gestión unificada de amenazas. Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas e Informática. http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/15154/caballa_te.pdf?sequence=1&isAllowed=y

Guzmán, J.D. (2018). análisis y diseño de un modelo seguro con firewall three-part, para mitigar riesgos tecnológicos, en la red de voz y datos del fondo de empleados de vivienda y ahorro de alpina feval, en las ciudades de Bogotá y sopó. [para optar el título, Universidad cooperativa de Colombia]

Ibero (2020). La importancia de la seguridad de la información. AdminIberoBlogs obtenido de https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Joaquín Cajahuaringa, J. C. (2019). Implementación de firewall para el control de servicio de internet en la Filial Chanchamayo de la Universidad Peruana Los Andes. [para optar título, Universidad Peruana Los Andes] https://renati.sunedu.gob.pe/handle/sunedu/2889997

López Pablo. (2020). Que es un firewall y para qué sirve. Recuperado https://www.geeknetic.es/Firewall/que-es-y-para-que-sirve

Palo Alto networks. (2016). Firewall de nueva generación de Palo Alto networks. obtenido: https://www.paloaltonetworks.com.mx/apps/pan/public/downloadResource?pagePath=/content/pan/es_MX/resources/datasheets/descripcion-del-firewall

Palo alto networks. (2011). resumen de las funciones de firewall de nueva generación. obtenido: https://media.paloaltonetworks.com/documents/Firewall_Feature_Overview-spanish.pdf

Pacheco Meneses, J. Martínez Molina, K. (2009). Diseño e implementación de un servidor firewall en Linux. [para obtar el título, Universidad Tecnológica de Bolívar Cartagena de Indias]

Palo Alto. (2022). App-ID. Recuperado de https://www.paloaltonetworks.com/technologies/app-id

Martínez Molina K.J., Pacheco Meneses J., Zúñiga Salgado I. (2009). Firewall Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas). *Revista UIS Ingenierías*, vol. 8, núm. 2, pp. 155-165. https://www.redalyc.org/pdf/5537/553756879003.pdf