MODERNIZACION TECNOLÓGICA DE LA INFRAESTRUCTURA DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL PARA LA RED CORPORATIVA

PRESENTADO POR:
DAVID ALEJANDRO TORRES RONCANCIO
JOSE FELIPE ZAMBRANO PEREZ

ASESOR TÉCNICO DE PROYECTO:
INGENIERO ROBERT DARIO CASTRO GUTIERREZ

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
10/07/2020

Agradecimientos

Primero queremos agradecerle a Dios por bendecirnos la vida, por guiarnos a lo largo de esta etapa tan importante para nosotros, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Agradecemos a nuestros docentes de la Universidad El Bosque, por haber compartido sus conocimientos a lo largo de este año, de manera especial, al ingeniero Robert Darío Castro tutor de nuestro proyecto de investigación quien nos ha guiado durante el proceso de la elaboración del proyecto, también al ingeniero Oscar Arias quien nos apoyó con la asesoría y metodología.

Agradecemos a nuestros padres y familiares quienes nos brindaron su apoyo y motivación durante la ejecución de este proyecto.

Dedicatoria

El presente trabajo lo dedicamos principalmente a dios, quien nos guio durante el proceso bendiciéndonos y dándonos fuerzas para continuar con las metas propuestas. A nuestros padres que fueron el apoyo incondicional para nunca desfallecer bríndanos su amor y sabiduría para cerrar esta etapa tan importante para nuestra vida profesional.

A nuestros docentes de la universidad que hicieron parte de este proceso brindándonos su conocimiento y experiencia la cual nos permitió culminar esta etapa con la realización este proyecto.

RESUMEN

El proyecto consiste en la implementación de un dispositivo de seguridad perimetral con el fin de ofrecer una modernización de los servicios de seguridad que cumpla con los requerimientos determinados por la compañía. Se realizo un levantamiento de información inicial de la infraestructura de la organización para validar el estado inicial y flujos de conectividad. El diseño se propuso de acuerdo con las necesidades, requerimientos y limitaciones dadas por la compañía.

La implementación consta del despliegue de un firewall para proteger la integridad, confidencialidad y disponibilidad de la información de la organización, minimizando los accesos no autorizados; un dispositivo de autenticación el cual funcionará como administrador de acceso e inicio de sesión único, el cual nos permite tener conectividad con el directorio activo de la organización y el firewall para permitir crear políticas de acceso más efectivas y mitigar el acceso de red a usuarios no válidos. Finalmente, se implementará un dispositivo para el almacenamiento registro de eventos de los equipos implementados.

PALABRAS CLAVE

UTM, Firewall, IPS, Seguridad Perimetral, Seguridad informática, Registro de eventos, FSSO, Filtrado de contenido.

ABSTRACT

The project consists of the implementation of a perimeter security device to offer a modernization of security services that meets the requirements determined by the company. An initial information survey of the organization's infrastructure was carried out to validate the initial status and connectivity flows. The design was proposed according to the needs, requirements and limitations given by the company.

The implementation consists of the deployment of a firewall to protect the integrity, confidentiality and availability of the organization's information, minimizing unauthorized access; an authentication device which will function as access manager and single sign-on, which allows us to have connectivity with the organization's active directory and the firewall to allow creating more effective access policies and mitigating network access to non-users valid. Finally, a device will be implemented to store the event log of the implemented equipment.

KEYWORDS

UTM, Firewall, IPS, Perimeter Security, Computer Security, Event Log, FSSO, Content Filtering.

Tabla de contenido

Tabla de Ilustraciones

Lista de Tablas

1. Título

Modernización tecnológica de infraestructura de los servicios de seguridad perimetral de red corporativa.

2. Introducción

El desarrollo del proyecto consiste en la modernización tecnológica, optimización de accesos, recursos y la centralización de varios servicios para una empresa multinacional dedicada a la prestación de servicios de internet, telefonía y televisión por medio de un sistema de seguridad perimetral. La topología actual de la empresa cuenta con varios sistemas perimetrales los cuales no cuentan con un sistema de gestión de identidad para el acceso a sus servicios, generando retrasos para el acceso a clientes y operadores, además de eso se encuentra expuesto a fugas de información por no tener un control de estos accesos.

Debido a que la empresa se encuentra en un proceso de ampliación de servicios y clientes, se deben implementar unos dispositivos más robustos a nivel de hardware con el fin de soportar las nuevas solicitudes de los clientes mejorando así la disponibilidad, flexibilidad y escalabilidad de los servicios y así mismo adquirir nuevos consumidores para generar mayor rentabilidad a la organización.

Al momento la solución de seguridad perimetral presenta riesgos de ataques informáticos provenientes desde el interior de la compañía, como fuga y accesos no autorizados a la información; para mitigar estos riesgos se implementarán soluciones VPNs y gestión de identidad con unidades organizativas, incrementando de esta manera el nivel de seguridad de la información de la empresa.

Durante el proceso de diseño, la organización realizó un estudio basado en un análisis de tráfico, sesiones concurrentes, cantidad de usuarios, y requisitos de la organización para los requerimientos de hardware; independiente del modelo debe incluir dentro de sus funciones los servicios de firewall, IPS, control de navegación, VPN, antivirus.

3. Descripción general del proyecto

3.1 Definición del problema

Hoy por hoy la organización requiere la expansión de sus servicios de conectividad de red corporativa; haciendo uso de esta necesidad se aprovecha el mismo espacio y recursos para optimizar su seguridad perimetral ya que se encuentra muy accesible a nivel de redes, puertos y usuarios; permitiendo así que terceros o personas ajenas a la organización y servicios tengan acceso no restringido, actualmente no se ha presentado ningún incidente de seguridad, pero el riesgo es latente.

Para la red corporativa no se tiene un manejo de acceso por usuarios a las redes respectivas. La organización requiere realizar el seguimiento de eventos para los accesos a cada servicio y /o aplicativo.

La empresa hoy en día presta servicios de televisión, internet, telefonía local y móvil a nivel Latinoamérica, también presta servicios de almacenamiento en la nube y administración de equipos de IT para otras empresas.

La ejecución del proyecto puede aplicarse en otros tipos de organizaciones las cuales requieran brindar seguridad a sus servicios, optimizar accesos, centralizar plataformas de seguridad perimetral, implementar accesos remotos por medio de gestión de identidad.

Cuenta con más 29 millones suscriptores a nivel de telefonía y para los servicios de la red corporativa cuenta con más de 5 millones de usuarios que consumen los servicios de esta red a la cual se le realizara la modernización y optimización a nivel de seguridad perimetral.

Actualmente la organización se encuentra en proceso de modernización y optimización de su infraestructura, por lo tanto, ha contratado los servicios de proveedores, para implementar una solución que permita migrar los servicios de conectividad y seguridad de toda la red corporativa.

La organización cuenta un firewall centralizado con Dominios virtuales para los diferentes aplicativos basado en accesos a servidores y servicios con rutas estáticas, direccionamiento por interfaces, throughput máximo de 52 Gbps y un máximo de 11 millones de sesiones concurrentes. Los accesos a aplicativos, redes y servidores se

encuentran muy abiertos debido a la mala administración, errores humanos y a la necesidad de dejar operativo un servicio.

Las redes para cada servicio corporativo se encuentran divididas de acuerdo con su administración por áreas (Tecnologías de la Información, Red Alámbrica y Red móviles) generando complejidad en las conectividades, gestión de requerimientos y eventos.

El transcurso de tiempo en la implementación inicial de los servicios dio origen a obsolescencia tecnológica en los firewalls.

A nivel de limitación de hardware no se permite una ampliación de los servicios.

El crecimiento de red corporativa y de la organización en general hace necesario utilizar equipos más robustos a nivel de throughput, sesiones y hardware en general.

Debido a los diferentes operadores que administran la seguridad perimetral, la gestión de accesos, control de cambios e incidentes, es necesario controlar y monitorear el acceso a estos aplicativos y/o servicios.

Actualmente la red a nivel de acceso se encuentra expuesta; diferentes colaboradores tienen acceso a servicios que no están asignados a rol dentro de la compañía, pudiendo generar incidentes de seguridad e indisponibilidad del servicio.

Entre las causas del proyecto se encuentran:

- Indisponibilidad para nuevos servicios sobre la infraestructura corporativa.
- No se tendría soporte directo de fábrica en caso de un incidente.
- Riesgos de seguridad por la no actualización de parches para remediar las vulnerabilidades más recientes en los dispositivos de seguridad perimetral.
- Perdida de flujo de caja para nuevos servicios.
- Se extenderían las brechas de acceso ante posibles ataques a servidores y externos.
- No se tendría un control exhaustivo para el acceso a servicios críticos.
- Se restringiría el acceso a los aplicativos por la limitante de máximo de sesiones.
- Los colaboradores de la red corporativa tienen acceso a diferentes servicios los cuales no se encuentran asignados a su rol dentro de la organización.

3.2 Aspectos a solucionar

El crecimiento de red y de la organización en general hace necesario utilizar equipos más robustos a nivel de throughput, sesiones y hardware en general.

Debido a los diferentes operadores que administran la seguridad perimetral, la gestión de accesos, control de cambios e incidentes, es necesario controlar y monitorear el acceso a estos aplicativos y/o servicios.

Actualmente la red a nivel de acceso se encuentra expuesta; diferentes colaboradores tienen acceso a servicios que no están asignados a rol dentro de la compañía, esto generaría incidentes de seguridad e indisponibilidad del servicio.

3.3 Solución propuesta

Proponer un diseño e implementar una solución de seguridad informática en tecnología Fortinet, los cuales se tiene como Partner en la organización. La solución debe permitir migrar y centralizar los servicios configurados, implementar gestión de identidad por medio de hardware, aplicar un control de tráfico con un mayor throughput y un numero de sesiones más amplio y almacenar los registros de eventos de cada uno de los dispositivos.

4. Estado del arte

4.1 Marco de referencia teórico

Hoy en día el termino de seguridad perimetral se ha convertido en unos los principales requisitos de una organización ya que cada día se generan nuevos ataques informáticos y se encuentra en constante crecimiento.

Seguridad perimetral, proviene de términos militares, en la cuales tienen similitud algunas palabras. El perímetro consiste en una zona imaginaria que separa una empresa (sus computadoras, servidores, etc.) de otras redes (generalmente el internet).

Esta zona la separa un dispositivo que puede ofrecer la comunicación entre las redes, generalmente representada por un router, secuenciada de un dispositivo de seguridad, conocido como firewall, o trayendo a la terminología actual, firewall de última generación (NGFW).

El firewall se encarga de realizar la interconexión entre Internet y las redes internas de una organización. En él, es posible crear mecanismos de control para evitar ataques

bidireccionales, así como garantizar lo que realmente debe ser accedido, permitiendo un mejor uso del recurso de internet en la organización.

El perímetro se considera como la primera capa de defensa del mundo externo dentro de las estructuras organizativas en los últimos años, con la necesidad y el constante crecimiento, el posicionamiento de la seguridad perimetral ha cambiado de manera importante manejando un alcance de seguridad donde se contrala la Gestión de acceso e identidad, seguridad en redes y seguridad de aplicativos.

Anteriormente, la información se alojaba dentro de la organización, hasta que fuera posible alcanzarla remotamente por Internet; sin embargo, el almacenamiento aún continuaba en las empresas. En la mayoría de las organizaciones la parte de los sistemas estratégicos funcionaban en servidores propios ubicados dentro de la empresa, algunas de ellas sin acceso externo. La información en la nube se está convirtiendo en una realidad, actualmente muchas compañías tienen parte o mucho de su estructura en servicios remotos, accedidos por Internet. [1]

4.1.1 Amenazas que Neutralizan

En la seguridad perimetral los dispositivos se encargan de proteger amenazas externas procedentes desde cualquier red o redes a las que se esté conectado, este tipo de dispositivos neutraliza intentos de acceso no autorizados denegando las conexiones y generando visualización de todos los puertos de red.

Ocultan la dirección IP, puertos de los equipos e impidiendo que se conozca la estructura de nuestra red. Monitorean las comunicaciones entre redes impidiendo la saturación de servicios (ataques DoS y DDoS del inglés Denial of Service y Distributed Denial of Service respectivamente).

Protegen frente al uso malicioso y de riesgos externos procedentes de servicios web, también protegen los equipos de amenazas internas, por ejemplo, evitando el envío de información confidencial o la saturación de los recursos de comunicaciones. Sin embargo, estos dispositivos (hardware o software) no brindan protección de ataques cuyo tráfico no pase por ellos, de ataques de ingeniería social y de fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido o no esté siendo filtrado, ni auditado.

4.1.2 Firewall y VPN

Estos dispositivos se encargan de proteger equipos conectados a la red, la seguridad a nivel perimetral permite garantizar las conexiones seguras en la red externa y la red interna creando políticas de acceso y denegación para evitar ataques.

Permite gestionar y filtrar la totalidad de tráfico entrante y saliente que puede haber en diferentes redes. Si el tráfico entrante o saliente cumple con una serie de requisitos que se especifican de acuerdo con la exigencia de la organización, el tráfico podrá acceder o salir de la red u ordenador sin restricción alguna; en caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado.

En esta categoría se integra algunas herramientas que permite una conectividad extendida hacia sedes remotas, oficinas en diferentes ciudades, creando enlaces cifrados por medio de túneles para brindar mayor seguridad a la información al paso de esta por internet.

4.1.3 Gestión de identidad

Son dispositivos que permiten a la organización la administración de usuarios con el fin de identificar y asociar el rol que debe tener cada usuario y así mismo asignarle las políticas de seguridad correspondiente. Con estos dispositivos se tiene un mayor control para el acceso a los servicios que se tienen en la red.

4.2 Marco de referencia tecnológico

A continuación, se detallará el proceso de éxito de la solución de seguridad perimetral implementada para una entidad, donde se especifican los componentes y sus características, la topología de red, los flujos de tráfico y las conexiones físicas y lógicas de cada módulo implementado.

4.2.1 Dispositivos de la Implementación

Los componentes de la solución corresponden a firewalls, repositorio de logs, Centralización de equipos y dispositivos de gestión de identidad marca Fortinet.

El dispositivo 500E ofrece capacidades de firewall de próxima generación para medianas y grandes empresas. Incluye una tecnología de protección contra amenazas cibernéticas con un alto rendimiento de seguridad, eficacia y una gran visibilidad. Ofrece

hasta 8 millones sesiones recurrentes, 36 Gbps de tráfico de firewall, 7,9 Gbps de IPS y 4,7 Gbps de protección contra amenazas; incluye 8 interfaces RJ45, 2 interfaces RJ45 MGMT, 2 slots 10GE SFP+, 8 slots 1GE SFP, 1 interface RJ45 para consola y 2 puertos USB.

Ilustración 1. FortiGate-500E - Copyright ©2014 Fortinet, Inc [2]

El dispositivo 300E ofrece capacidades de firewall de próxima generación para medianas y grandes empresas. Incluye una tecnología de protección contra amenazas cibernéticas con un alto rendimiento de seguridad, eficacia y una gran visibilidad. Ofrece hasta 4 millones de sesiones recurrentes, 32 Gbps de tráfico de firewall, 5 Gbps de IPS y 3 Gbps de protección contra amenazas; incluye 16 interfaces RJ45, 2 interfaces RJ45 MGMT, 16 slots 1GE SFP, 1 interface RJ45 para consola y 2 puertos USB.

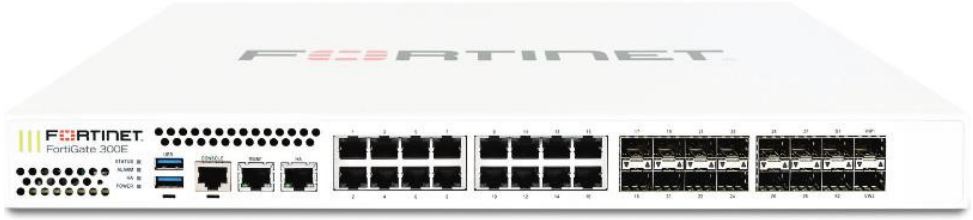


Ilustración 2. FortiGate-300E - Copyright ©2014 Fortinet, Inc [2]

El repositorio de logs proporciona información profunda sobre amenazas avanzadas a través de la Orquestación, Automatización y Respuesta de Panel Único para toda su superficie de ataque para reducir riesgos y mejorar la seguridad general de la organización.

Cuenta con capacidad de almacenamiento de 200GB de logs por día, y un total de 12TB (4x3TB) de almacenamiento.

Ilustración 3. FortiAnalyzer 400E - Copyright ©2014 Fortinet, Inc [2]

Los dispositivos de gestión de identidad de usuario fortalecen la seguridad empresarial al simplificar y centralizar la gestión y el almacenamiento de la información de identidad del usuario.

Ilustración 4. FortiAuthenticator VM - Copyright ©2014 Fortinet, Inc [2]

FortiManager VM proporciona la oportunidad de administrar todos los equipos de la marca Fortinet desde una misma consola, evitando el trabajo de autenticarse en cada uno de ellos directamente para hacer los cambios.

También reduce la complejidad del despliegue de cambios, y permite ejecutar scripts en la red de forma automatizada. Adicionalmente, al estar montado sobre la misma base del FortiAnalyzer, puede funcionar como uno de estos de una manera muy básica pero que cumple con lo solicitado en el entorno de seguridad. Al ser una plataforma virtual en la nube, su capacidad de almacenamiento depende del hardware y el hypervisor en el cual se monta.

Ilustración 5. FortiManager VM- Copyright ©2014 Fortinet, Inc [2]

4.2.2 Arquitectura

A continuación, se muestra la arquitectura general para la solución de seguridad perimetral de la entidad:

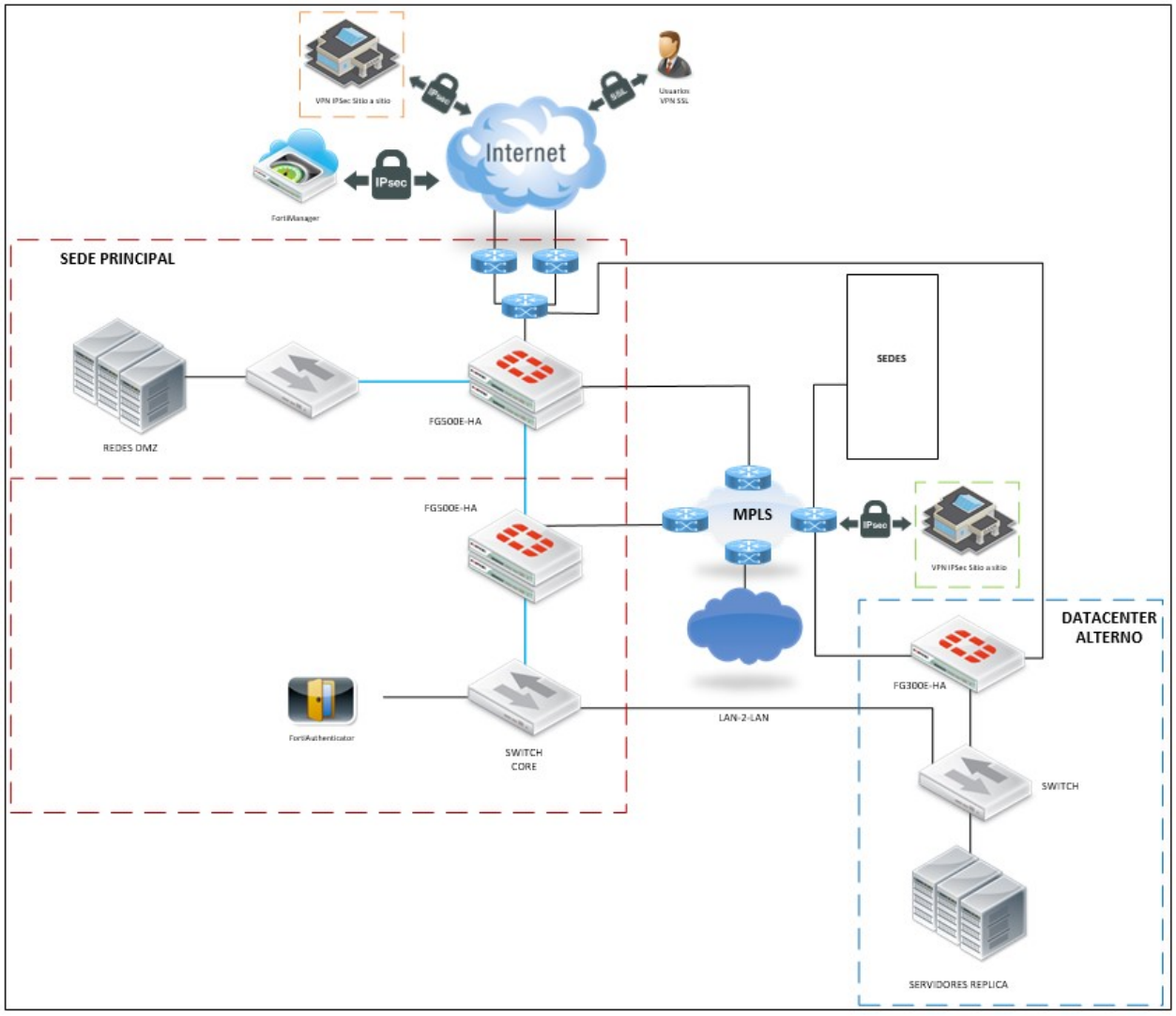


Ilustración 6. Arquitectura entidad – Kappa 10

En el diagrama anterior se muestra la solución de seguridad perimetral propuesta para la entidad, la cual cuenta con cuatro firewall en alta disponibilidad (HA), los cuales están encargados de realizar los NATs de las publicaciones de los servicios de Internet, y establecer las políticas de navegación de la red LAN con su respectivo filtrado de páginas web y aplicaciones, y por último de establecer las VPN SSL Client-to-Site e IPSec Site-to-

Site para los diferentes propósitos de la entidad.

4.2.3 Flujo de tráfico de navegación

A continuación, se muestra el flujo de tráfico de la navegación con sus respectivas convenciones:

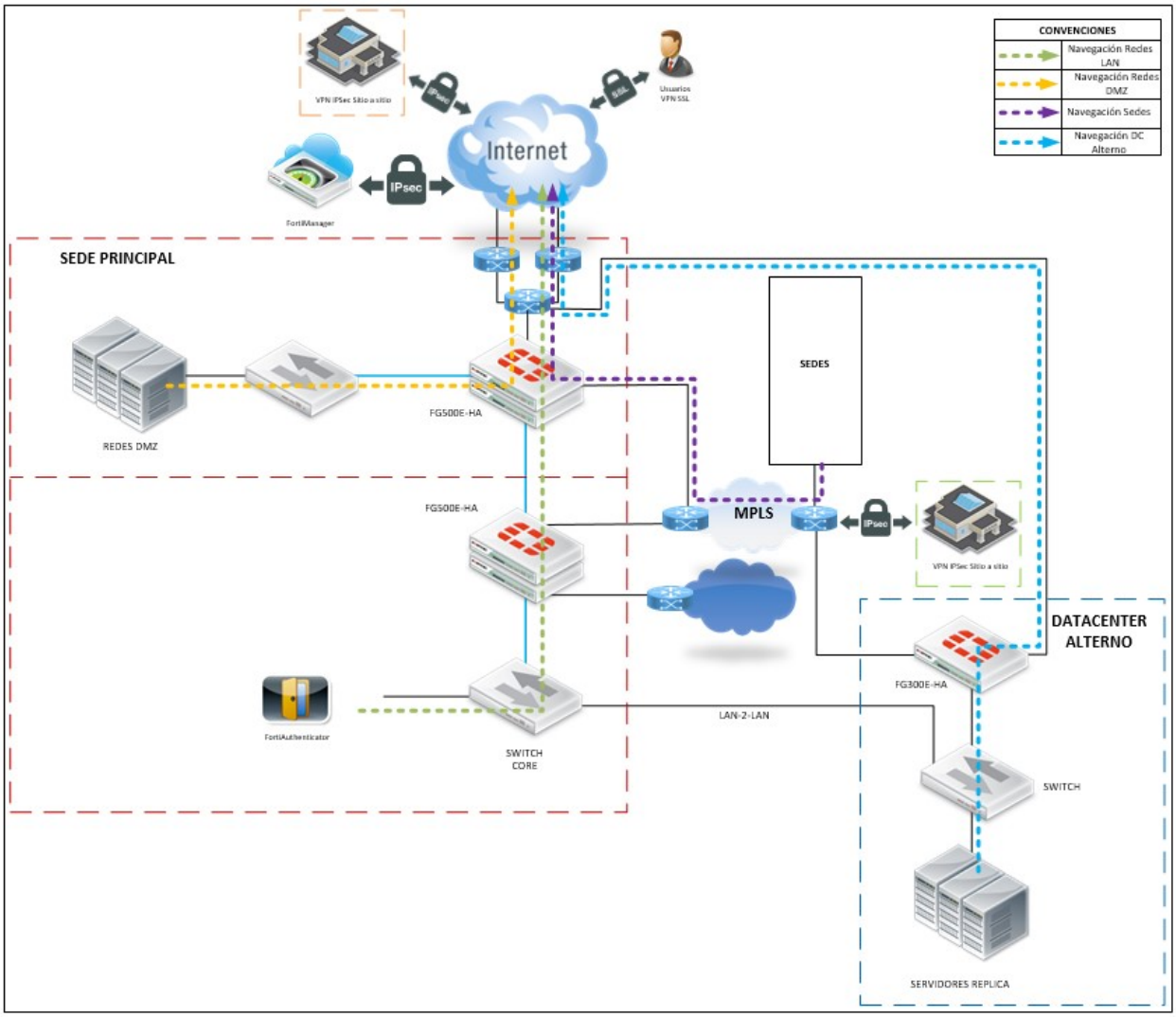


Ilustración 7. Flujo de tráfico de navegación - Kappa 10

En el diagrama anterior se muestra los flujos de navegación de la sede principal y el DC Alterno de la entidad. Cada sede cuenta con su canal de Internet Independiente soportado por diferentes proveedores de servicio, con lo cual se facilita y promueve el entorno contingente y el DRP.

4.2.4 Flujo de tráfico de navegación

A continuación, se muestran los flujos de tráfico entre las redes LAN y las redes DMZ con sus respectivas convenciones:

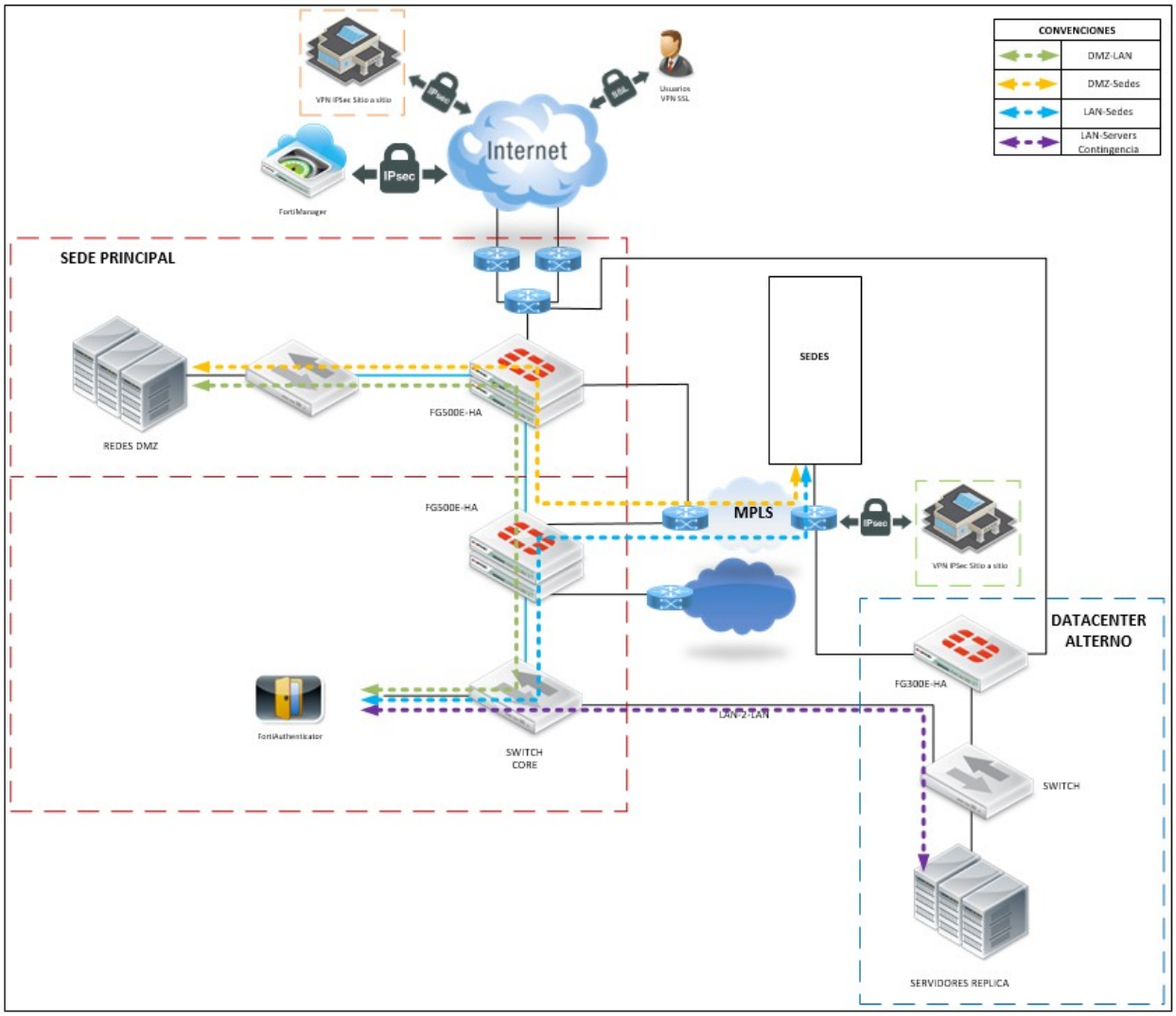


Ilustración 8. Flujo de tráfico de LAN a DMZ – Kappa10

En el diagrama anterior se muestra los flujos tráfico entre las diferentes redes LAN y las redes DMZ de la entidad. Entre los diferentes flujos están los que van desde la sede principal hacia las DMZ, desde la sede principal hacia el DC Alterno, de la sede principal hacia las oficinas y viceversa, y de las oficinas hacia las DMZ ubicadas en el DC principal.

4.2.5 Alta disponibilidad

Él HA está configurado en modo Active-Passive, esto significa que una máquina se encuentra activa (master) y la otra se encuentra como subordinada (backup).

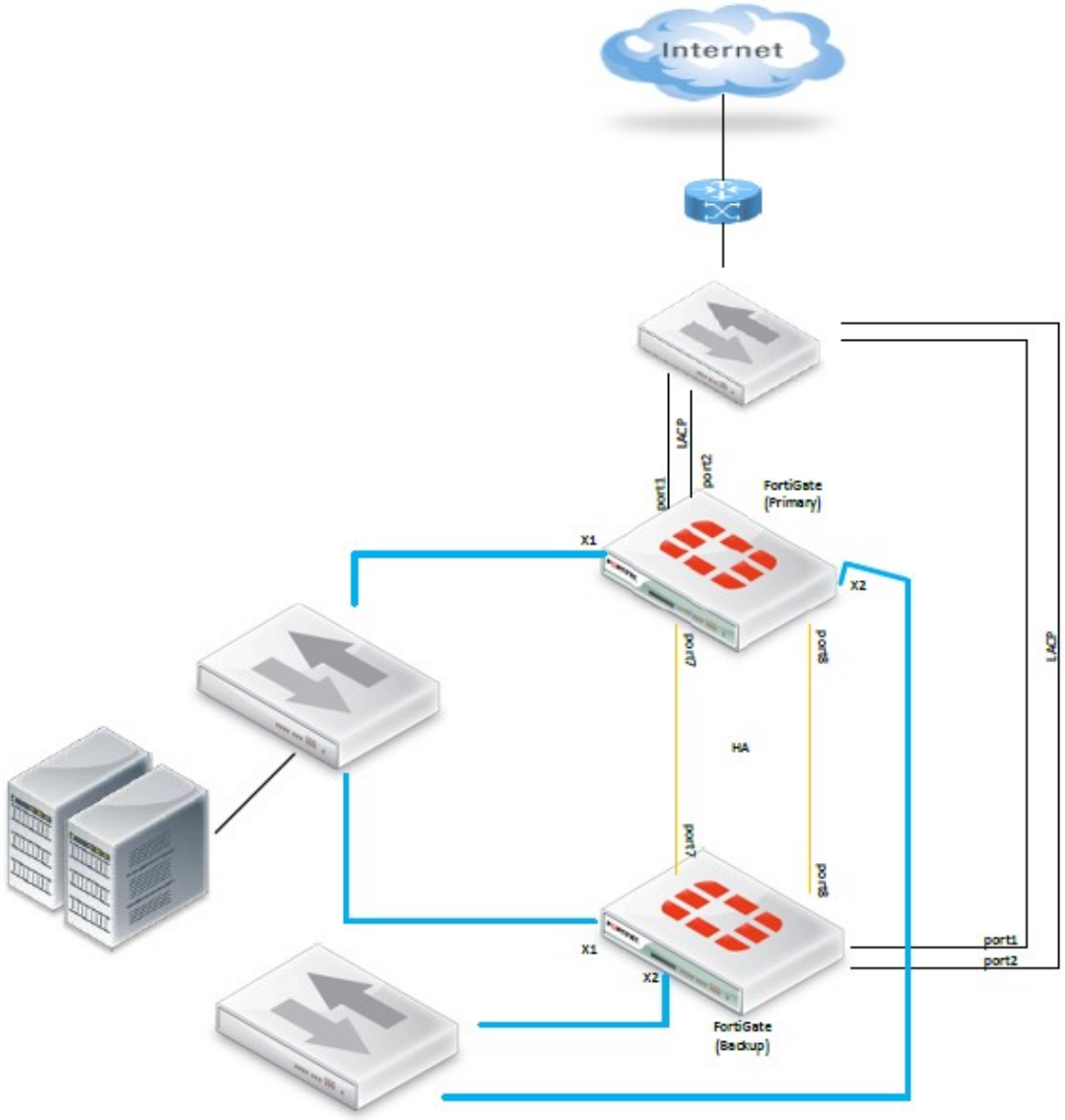


Ilustración 9. High Availability – Kappa 10

5. Glosario de términos

BGP: es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP. [3]

El protocolo ligero de acceso a directorios (LDAP): en inglés: El Lightweight Directory Access Protocol (LDAP) es un protocolo de servicio de directorio que se ejecuta en una capa por encima de la pila TCP / IP. Proporciona un mecanismo utilizado para conectarse, buscar y modificar directorios de Internet.

El servicio de directorio LDAP se basa en un modelo cliente-servidor. La función de LDAP es permitir el acceso a un directorio existente.

El modelo de datos (datos y espacio de nombres) de LDAP es similar al del servicio de directorio X.500 OSI, pero con menores requisitos de recursos. La API LDAP asociada simplifica la escritura de aplicaciones de servicio de directorio de Internet. [4]

Firewall: Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. [5]

IPS: Un sistema de prevención de intrusiones (IPS) es una tecnología de seguridad de red / prevención de amenazas que examina los flujos de tráfico de red para detectar y prevenir vulnerabilidades. Los exploits de vulnerabilidad generalmente se presentan en forma de entradas maliciosas a una aplicación o servicio objetivo que los atacantes usan para interrumpir y obtener el control de una aplicación o máquina. [6]

Nmap: es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales, La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la "tabla de puertos interesantes. [7]

Partner: En el ámbito de lo laboral o de la empresa, los partners son los propietarios de la entidad, socios o accionistas, es decir quienes tienen un negocio con otro. [8]

Single Sign On: conocido también como SSO por sus siglas en inglés permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes

sistemas y recursos. El SSO es de gran utilidad cuando existen diferentes sistemas a los que es posible acceder mediante una única contraseña y se desea evitar el ingreso repetitivo de estas cada vez que el usuario se desconecte del servicio. Para los usuarios supone una gran comodidad ya que identificándose solo una vez es posible mantener la sesión válida para el resto de las aplicaciones que hacen uso del SSO.

Throughput: La tasa de transferencia efectiva (en inglés throughput) es el volumen de trabajo o de información neto que fluye a través de un sistema, como puede ser una red de computadoras. [9]

VDOM: Los dominios virtuales (VDOM) se pueden usar para dividir una sola unidad FortiGate en dos o más instancias virtuales de FortiOS que funcionan como unidades FortiGate independientes [10]

Web filter: Un filtro web, comúnmente conocido como "software de control del contenido", es un software diseñado para restringir los sitios web que un usuario puede visitar en su equipo. Estos filtros pueden funcionar con una whitelist o una blacklist: las whitelists solo permiten el acceso a sitios elegidos específicamente por quien configura el filtro; las blacklists restringen el acceso a sitios no deseados según lo determinado por las normas instaladas en el filtro. Estos programas analizan la URL del sitio deseado y realizan búsquedas en el contenido del sitio en busca de palabras claves restringidas y, tras ello, deciden si bloquean o permiten la conexión. [11]

6. Justificación

Con la implementación del sistema de seguridad perimetral se busca tener un mayor control en el acceso a los sistemas informáticos de la organización con el fin de mitigar las fugas de información, controlar los accesos no autorizados, atenuar la interrupción de los servicios o afectación de su plataforma operativa. La organización se encuentra en un proceso de expansión de servicios y la plataforma actual se encuentra limitada a nivel físico y lógico impidiendo este crecimiento afectando así la entrada de nuevos clientes y mejorando la competitividad.

La implementación de la solución permitirá a la organización a través de la optimización y centralización, un control más eficiente de acceso que garantice la conectividad de clientes y operadores dentro de la organización por medio de unidades organizativas.

7. Objetivos

7.1. General

Actualización, optimización y centralización de la infraestructura de los servicios de seguridad perimetral para la red corporativa.

7.2. Específicos

- Proponer e implementar un firewall perimetral basado en dominios virtuales para mitigar los accesos no autorizados a cada servicio y garantizar la conectividad.
- Implementar un dispositivo de gestión de identidad para relacionarlo con el directorio activo de la organización para agilizar y controlar la conectividad de clientes y operadores a sus plataformas.
- Implementar sistemas de filtrado basado en usuarios con el objetivo de restringir, controlar la navegación y amenorar la descarga de software malicioso.
- Proponer y/o implementar un sistema de conexión cliente a sitio segura, mitigando la posibilidad de interceptación de información entre un empleado, proveedores remotos y la organización.

8. Requerimientos

8.1 Requerimientos funcionales

- Migrar y configurar VPNs Cliente sitio con el fin de restringir el intercambio de información entre cada una de los operadores remotos a través de Internet, contando con grupos de usuarios para cada servicio.
- Migrar y configurar unidades organizativas usando un hardware de administración de acceso e inicio de sesión único, con el fin de garantizar que solo la persona adecuada en el momento adecuado pueda acceder a sus redes y datos confidenciales mitigando el acceso no autorizado.
- Asegurar y configurar la recepción del enrutamiento dinámico (BGP) con objetivo de optimizar la interconexión de redes entre el Router y el Firewall.
- Realizar una correcta distinción entre las redes MZ, DMZ, VPNs y salida a internet por medio de una configuración de VDOM en el firewall para atenuar los accesos a cada segmento.

8.2 Requerimientos no funcionales

- Implementar la solución en esquema de alta disponibilidad en modo activo-pasivo.
- Conservar los logs de eventos históricos de cada una de las conexiones.
- Asegurar y configurar la conectividad con el servidor de autenticación para accesos de los usuarios administradores y operadores.

8.3. Requerimientos de restricción

- Implementar la solución propuesta basado en la línea del fabricante Fortinet ya que la empresa cuenta con servicio de disponibilidad preferencial con este fabricante.
- El proyecto se encuentra limitado a la información y disponibilidad de la compañía para su ejecución.

9. Metodología

El desarrollo del proyecto se divide en 4 etapas principales con el objetivo de abarcar los requerimientos tanto de información, ejecución y documentación.

9.1 Levantamiento de Información

En esta etapa se realiza el levantamiento de la información de la compañía, así como también la infraestructura que soporta la operación. Actualmente la organización ya cuenta con toda la información relevante respecto a usuarios y grupos de usuarios de directorio activo la cual es entregada al área de implementación. Adicionalmente se deben identificar los servicios y aplicaciones informáticas, su topología de red y valorar los controles de seguridad informática existentes.

9.2 Diseño

Con la información obtenida en la primera etapa, se deben seleccionar los componentes de seguridad que concuerden a los requerimientos delimitados por la organización teniendo en cuenta el presupuesto, se realizará una valoración de los modelos que ofrecen este tipo de recursos de seguridad perimetral para realizar una evaluación de recurso que ofrezca una mejor relación costo-beneficio.

Ya que la organización cuenta con contratos de exclusividad con el fabricante Fortinet se debe escoger un modelo de dicha marca. Los dispositivos para implementar se deben agregar dentro de la topología de red especificando la conectividad de cada uno de ellos dentro de la solución. Luego de que se asegure la correcta conexión entre los dispositivos de seguridad, se diseñará la distribución de cada uno de estos.

- Diseño de políticas de acceso para cada servicio.
- Diseño de conexiones VPN sitio a sitio y cliente sitio seguras.
- Diseño de estructura organizacional en caso de que no se tenga una ya definida por la empresa.
- Diseño del sistema de prevención de intrusiones.
- Diseño de grupos de acceso para cada servicio.

9.3 Implementación

Al ya estar definido el diseño del sistema de seguridad perimetral y de cada uno de sus componentes, se procede a realizar la respectiva configuración e implementación de cada uno de ellos como se relaciona a continuación:

- Instalar un equipo NGFW que permita todos los servicios de seguridad

perimetral para la solución propuesta.

- Configurar un Sistema de Prevención de Intrusos (IPS) para restringir las conexiones externas.
- Configurar el sistema DDoS para evitar las interrupciones de servicio.
- Agregar Las unidades organizativas de directorio activo con la solución del dispositivo de gestión de identidad.
- Configurar reglas de firewall de acuerdo con lo diseñado.
- Configurar VPNs cliente a sitio discriminadas por grupos de usuarios y VPNS sitio a sitios seguras entre las diferentes sedes de la empresa.

9.4 Pruebas

Durante la implementación se deben realizar pruebas de la solución de que garanticen el buen funcionamiento de cada uno de los dispositivos del sistema de seguridad perimetral.

- Pruebas de funcionamiento de las aplicaciones de la organización, garantizando la funcionalidad adecuada de estas.
- Pruebas de conectividad entre los diferentes segmentos de red de acuerdo con cada grupo de usuarios para evidenciar tráfico permitido y denegado.
- Pruebas de conectividad entre las sedes de la de la organización.
- Pruebas de conectividad de las VPNs configuradas.
- Realizar la valoración de las pruebas realizadas y aplicar las medidas correctivas y de mejora.

9.5 Documentación

Como una etapa colateral al desarrollo se cuenta con una fase de documentación en la cual se justificarán las actividades desarrolladas en cada una de las etapas y documentación del proyecto.

10. Desarrollo de la implementación

10.1 Levantamiento de información

El objetivo de la implementación es la centralización y optimización de servicios de seguridad perimetral de la organización. Actualmente en la empresa cuenta con algunos firewalls de diferentes marcas donde algunos de ellos centralizan servicios de la compañía. Para acceder a la red interna se deben realizar cambios estándar en cada uno de ellos para garantizar la conectividad del usuario hacia la red, también se debe realizar la configuración de enrutamiento estático en los diferentes firewalls, generando retrasos en los accesos y dificultad en la administración y la posibilidad de errores humanos aumentan a medida que aumentan los requerimientos ya que se pueden ocasionar afectaciones por manejo de los diferentes dispositivos de comunicación.

Se ilustra la topología actual de la compañía.

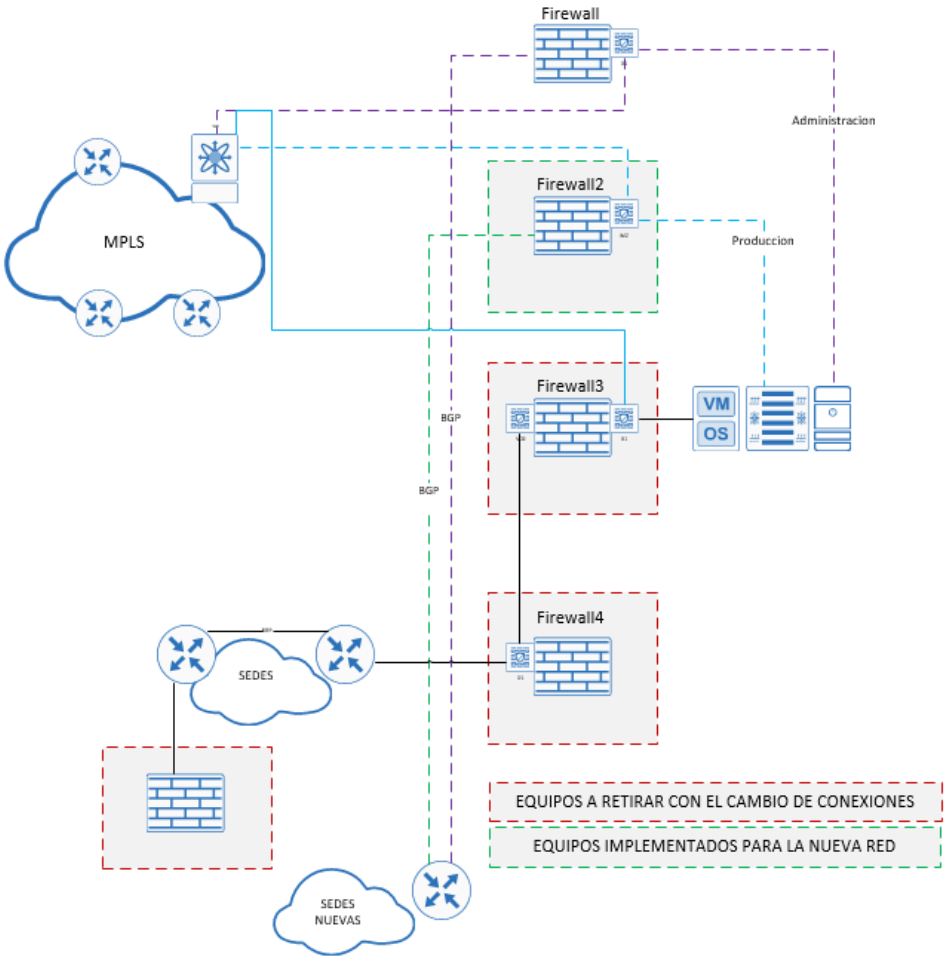


Ilustración 10. Topología actual de la compañía - Propia de los autores.

La conectividad a cada servicio se realiza a través de políticas de direccionamiento IP con lo cual cada persona que tenga acceso a la red tendrá el mismo acceso que tiene cualquier persona dentro de la organización, no existe una discriminación de accesos de acuerdo a roles dentro de la organización.

Actualmente los usuarios remotos se conectan a ciertos servicios mediante aplicaciones de escritorio remoto libres e inseguros como TeamViewer y AnyDesk, se requiere un control más efectivo para evitar consumo de ancho de banda más elevado por medio de roles.

El procedimiento para generar una solicitud de acceso a cualquier servidor de la red MZ tiene un tiempo de espera 12 días hábiles, 3 días por cada dispositivo de seguridad perimetral.

Para la migración de los servicios que se encuentran el Firewall inicial de cada uno de los VDOMs se realizó el respectivo levantamiento de información identificando el direccionamiento de cada una de sub interfaces.

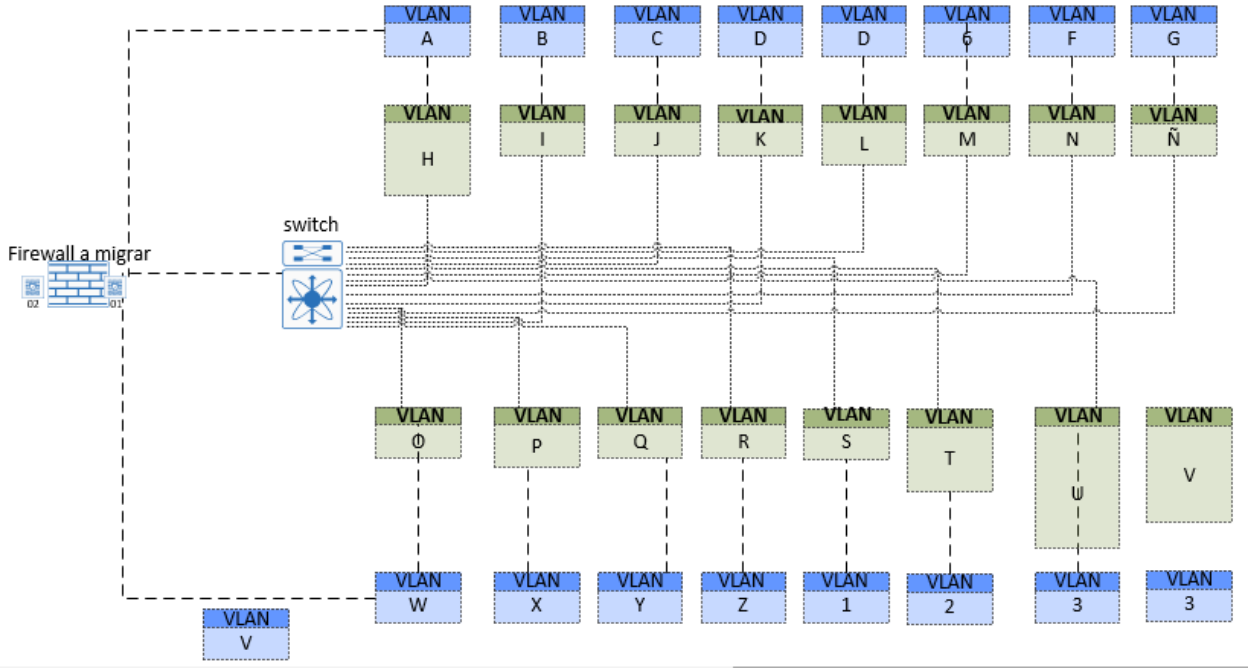


Ilustración 11. Interfaces FW a Migrar - Propia de los autores.

También se hizo una relación entre los nombres de las interfaces del firewall a migrar y el nuevo firewall que se implementara.

Nombre Interfaces firewall a migrar	Nombre Interfaces firewall a implementar
Red 1	Red Nueva 1
Red 2	Red Nueva 2
Red 3	Red Nueva 3
Red 4	Red Nueva 4
Red 5	Red Nueva 5

Tabla 1. Relación de interfaces actual y nueva. – Propia de autores

10.2 Diseño

10.2.1 Arquitectura general

A continuación, se detalla la topología y el diagrama de conexión de los dispositivos firewalls, gestión de identidad, repositorio de logs los cuales instalados en el Datacenter. Los equipos se interconectan entre sí, y con la nueva red mediante nueva conexión hacia los Switches.

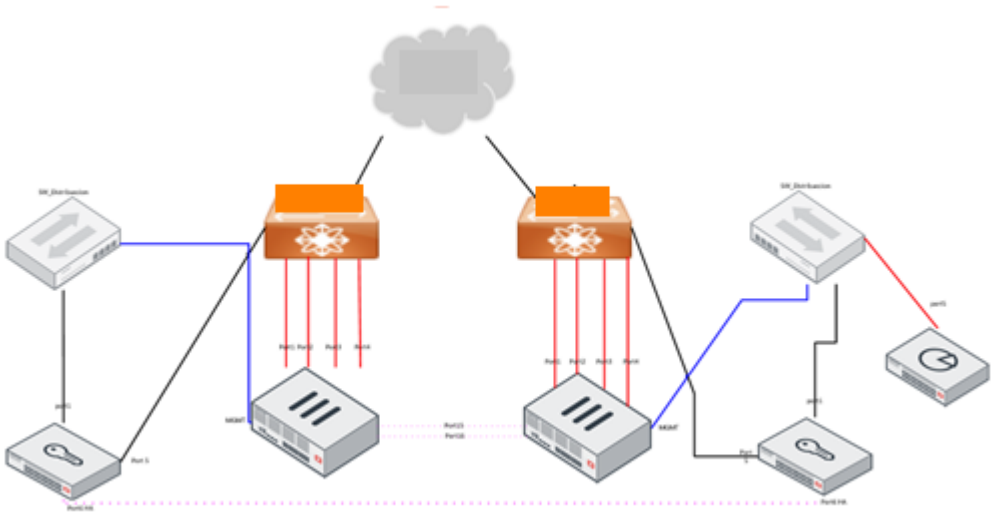


Ilustración 12. Diagrama Físico Datacenter. - Propia de los autores.

En el diagrama anterior se conectaron los firewalls de producción contra los Switch de servicios con puertos a 10GB, las conexiones de Alta disponibilidad se realizarán en fibra a 1GB y la conexión a gestión por el puerto MGMT en cobre.

El clúster de dispositivo de gestión de identidad también ira en Alta disponibilidad entre los módulos a 1GB y la otra interface de 1GB es para la producción, que se conectara a los Switch.

El repositorio de logs es un equipo de gestión que estarán conectados a la red de administración de la organización para que alcancen a los equipos de producción.

10.2.2 Diagrama Lógico

A continuación, se ilustra el diseño lógico el cual contiene una configuración redundante para el Clúster del firewall con 5 VDOM; todas las conexiones de cada VDOM que van hacia la red corporativa con enrutamiento dinámico (BGP), para una mejor administración de estas conexiones.

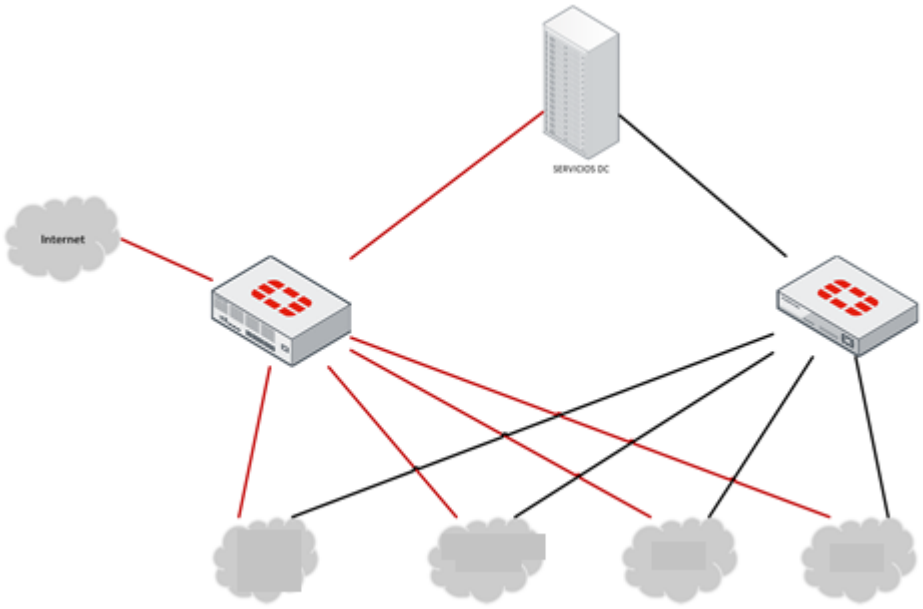


Ilustración 13. Diagrama global. - Propia de los autores.

Clúster Firewall

- VDOM INTERNET: Este VDOM tendrá una conexión directa a internet con el fin de tener salida de navegación a los usuarios de la red corporativa.
- VDOM DMZ: Este VDOM soporta las publicaciones de las DMZ, también tendrá una conexión directa hacia internet ya que manejará direccionamiento público de los servidores de la DMZ, y no tendrá una conexión directa contra ninguna de las redes.
- VDOM MZ: Por este VDOM se controlará el acceso de los usuarios de la red corporativa hacia los servidores de la MZ. Tendrá salida a Internet por medio de un VDOM link con el VDOM de internet. Adicionalmente contará con conexiones directas a las demás redes de la organización.

- VDOM VPN: Este VDOM contará con una conexión directa a Internet con el único fin de configurar las VPNs Sitio a Sitio o Cliente sitio que consultarán los servicios de la red de la compañía.

- VDOM ROOT: Este VDOM es para administración y gestión de los equipos, y necesita conexión a Internet por la IP de gestión, para la actualización y el registro contra los servidores de FortiGuard. Además, contará con conexión a la red de administración a la cual se conectarán los dispositivos como el repositorio de logs y el de gestión de identidad.

10.2.3 Arquitectura general de VDOMS

A continuación, se muestra el diagrama general de lo Vdoms para la implementación.

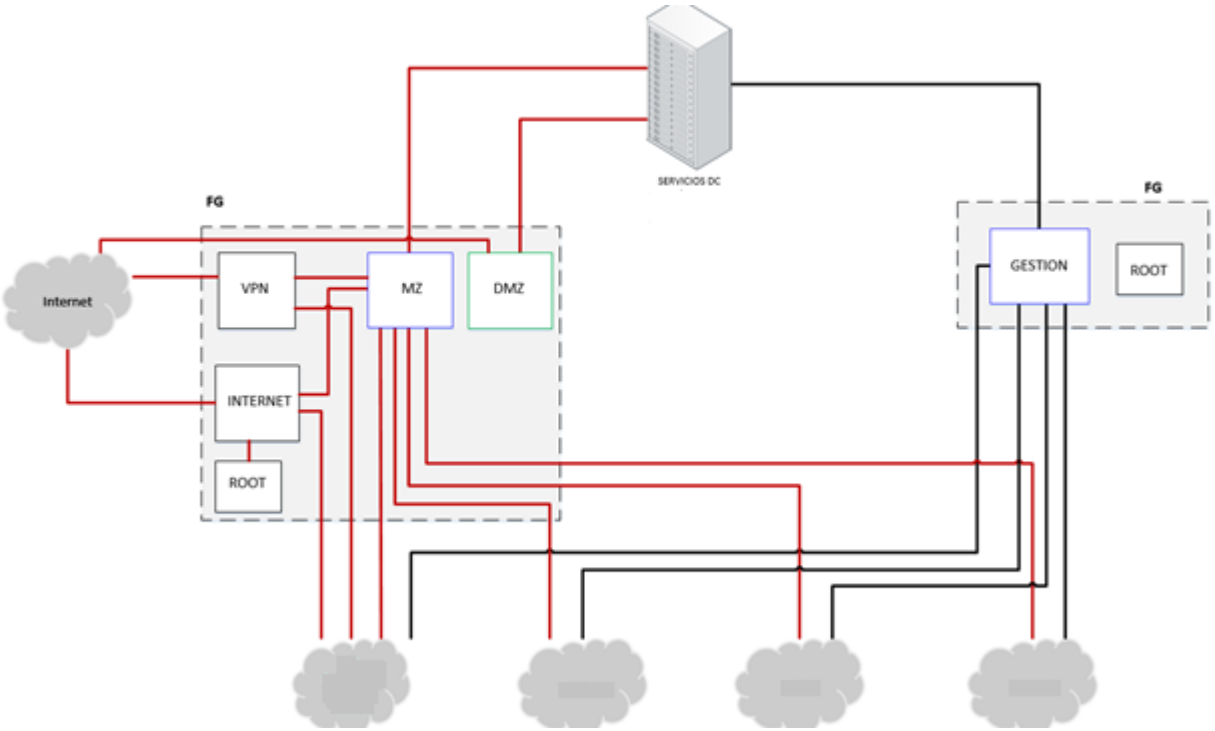


Ilustración 14.Diagrama general de Vdoms del Firewall. - Propia de los autores

En el diagrama anterior se muestra los vdoms relacionados en el Firewall que se configuraran para una mejor administración y distribución de tráfico.

10.2.4 Flujo de tráfico de la navegación de usuarios

El siguiente diagrama nos indica el flujo de salida a internet de los usuarios de la red de la organización. Los usuarios por medio de una conexión directa que tiene el VDOM MZ contra las demás redes, pasan por un VDOM Link hacia el VDOM internet el cual controla en tráfico mediante políticas de Firewall, filtrado de aplicaciones y navegación web.

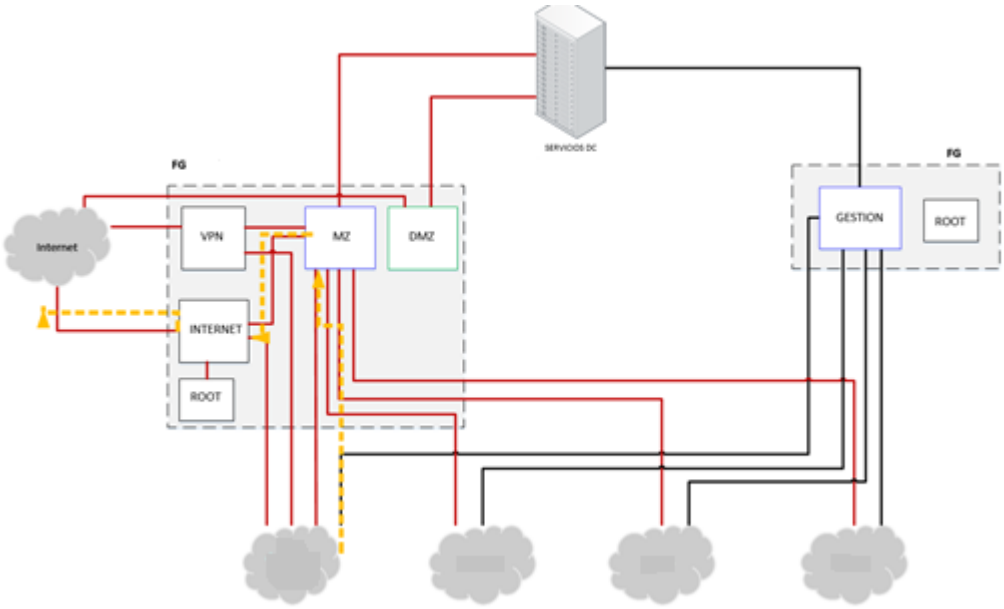


Ilustración 15. Diagrama navegación usuarios. - Propia de los autores

10.2.5 Flujo de tráfico de consultas MZ

En el diagrama siguiente, se observa el Flujo del tráfico para consultar los servidores de MZ desde las diferentes redes de la compañía.

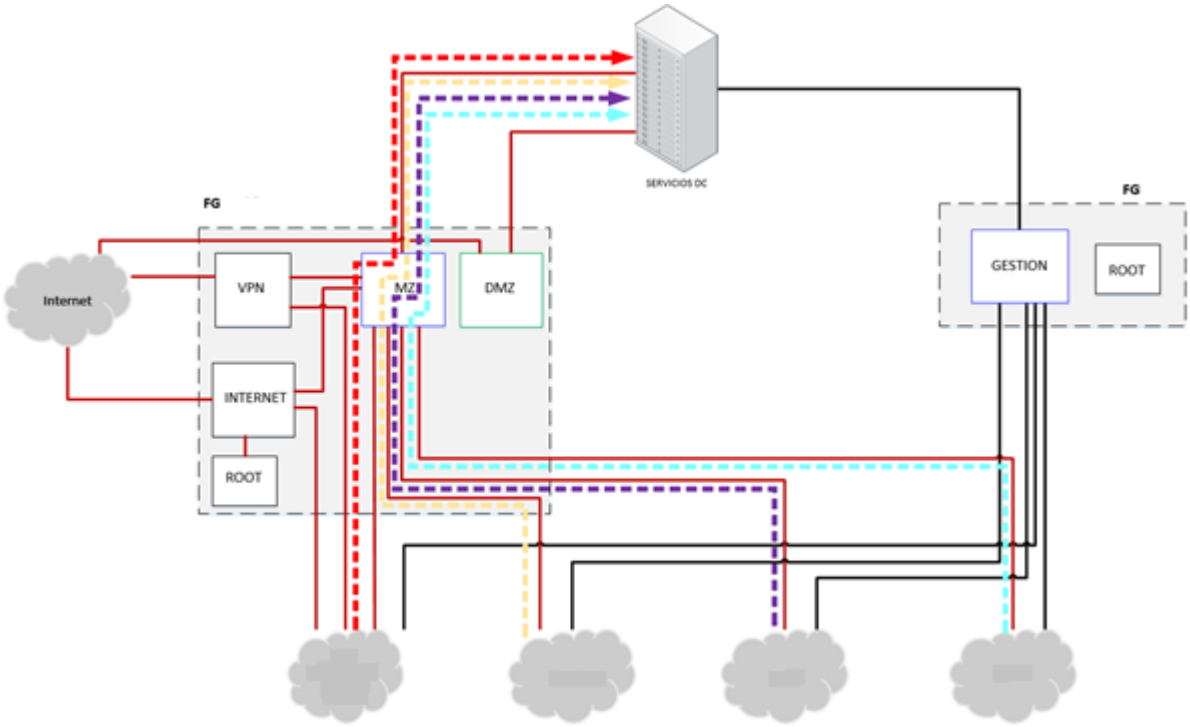


Ilustración 16. Diagrama consultas MZ- Propia de los autores.

10.2.6 Flujo de tráfico de consultas DMZ

En el siguiente diagrama, se evidencia la consulta a las publicaciones de la compañía desde internet, y para consultas de las demás redes, es necesario que los DNS internos resuelva la IP privada de los servicios de DMZ.

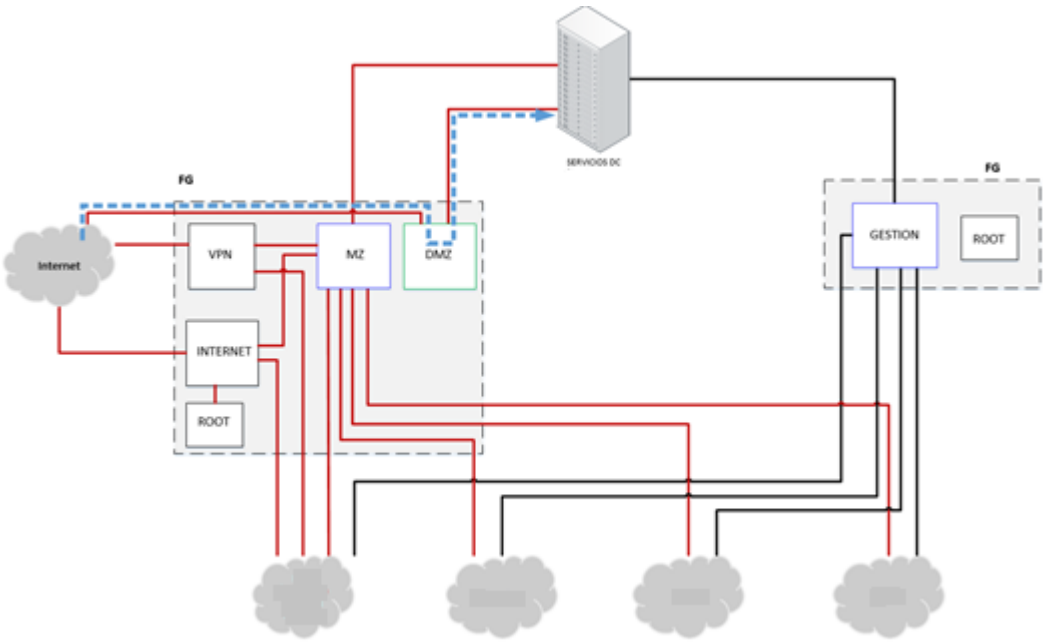


Ilustración 17. Diagrama consultas DMZ. - Propia de los autores

10.2.7 Diseño VPN

10.2.7.1 Conexión segura para colaboradores

Para la conexión de segura de los colaboradores y con el fin de velar por la integridad y confidencialidad de la información se configurará una VPN para garantizar la seguridad a través del túnel.

Propiedades de Túnel	**Sede Principal**	**Colaborador Remoto**
Fabricante de Firewall	FortiGate	FortiClient
IP Gateway "Peer"	201.X.X.X	Dialup
Tipo de VPN	CLIENT TO SITE	CLIENT TO SITE
Versión de Dispositivo de VPN	FortiOS V5	FortiClient V6.2
Dominio de Encriptación	10.X.X.X/X	20.X.X.X/X

FASE 1

Propiedades de Túnel	**Sede Principal**	**Colaborador Remoto**
Método de Autenticación	Llave Pre compartida Clave Definida por la	Llave Pre compartida Clave Definida por la

	organización	organización
Protocolo de VPN	IPSec	IPSec
Grupo de Diffie - Hellman	5	5
Algoritmo de Encripción	AES128	SHA1
Algoritmo de Integridad	SHA256	SHA256
Modo IKE	Aggressive Mode	Aggressive Mode
Tiempo de Renegociación	86400 segundos	86400 segundos

FASE 2

Propiedades de Túnel	**Sede Principal**	**Colaborador Remoto**
Encapsulación (ESP o AH)	ESP	ESP
Algoritmo de Encripción	AES128	SHA1
Algoritmo de Integridad	SHA256	SHA1
PFS (Perfect Forward Secrecy)	DH Group 5	DH Group 5
Tiempo de Renegociación	43200 segundos	43200 segundos

REGLAS

Origen	**Destino**	**Protocolo/puerto**
20.X.X.X/X	10.X.X.X/X	HTTPS TCP 443 PING - TRACEROUTE

Tabla 2. Configuración VPN colaboradores- Propia de autores

10.2.7.2 Flujo de trafico de conexiones VPN

En el siguiente diagrama se identifica el flujo de los usuarios de VPN cliente sitio, el terminador de estas VPN estará en le VDOM de VPN y desde ahí podrá consultar los diferentes servicios a los que tiene accesos los usuarios de VPN, que pueden ser servicios de MZ, o servicios que se encuentre por la red corporativa.

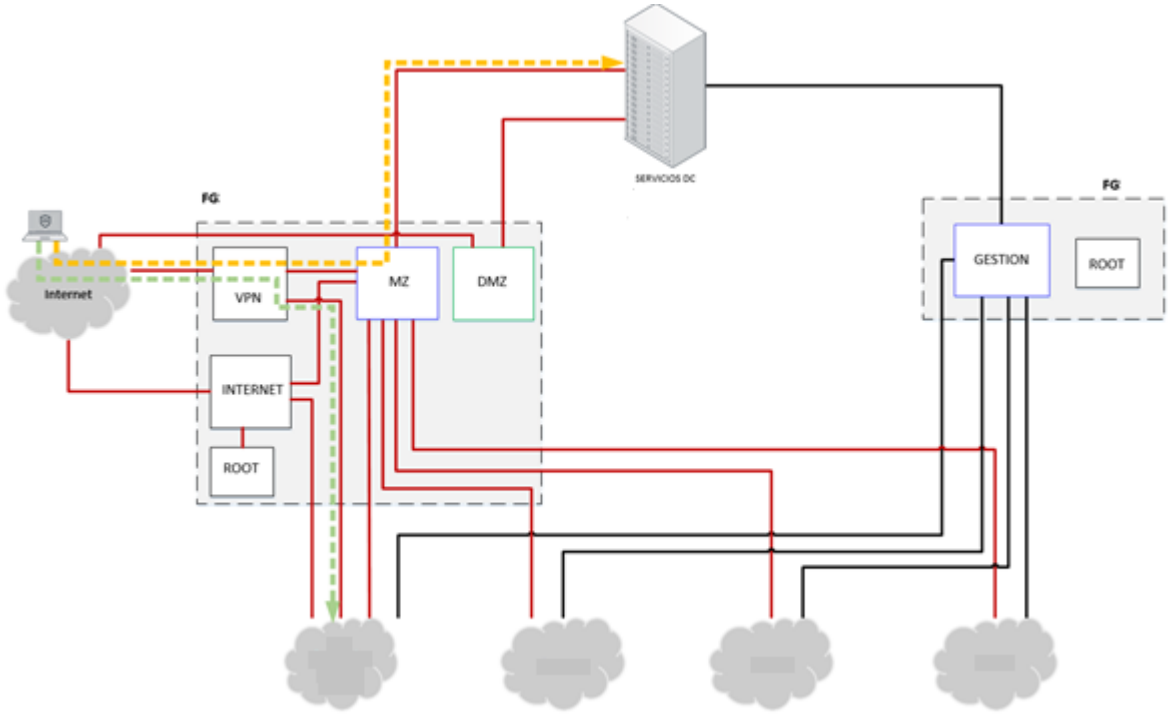


Ilustración 18. Diagrama VPN Cliente a sitio. - Propia de los autores.

10.2.8 Diseño de filtrado de contenido

FortiGuard Web Filtering es el servicio de filtrado web certificado por VBWeb mejor calificado en la industria para la efectividad de seguridad de Virus Bulletin. Bloqueó el 97.8% de las descargas directas de malware y detuvo el 98.6% del malware servido a través de todos los métodos probados en las pruebas de seguridad VBWeb 2017 de Virus Bulletin. [11]

Actualmente los dispositivos de Fortigate contienen integrado este servicio de filtrado de contenido a través de una licencia, cuenta con 87 categorías donde permite restringir el acceso a diferentes sitios web por medio de las políticas y perfilamiento de los usuarios. De acuerdo los requisitos de acceso a la navegación web se definieron los siguientes perfiles con el fin de permitir o bloquear sitios web.

La descripción de cada uno de las sub categorías se encuentra en el anexo A.

	Básico	Intermedio	VIP
Sub-Categoria	Perfil 1	Perfil 2	Perfil 3
	Allow / Deny	Allow / Deny	Allow / Deny
Drug Abuse	Deny	Deny	Deny
Hacking	Deny	Deny	Deny
Illegal or Unethical	Deny	Deny	Deny

	Básico	Intermedio	VIP
Discrimination	Deny	Deny	Deny
Explicit Violence	Deny	Deny	Deny
Extremist Groups	Deny	Deny	Deny
Proxy Avoidance	Deny	Deny	Deny
Plagiarism	Deny	Deny	Deny
Child Abuse	Deny	Deny	Deny
Alternative Beliefs	Allow	Allow	Allow
Abortion	Deny	Deny	Deny
Other Adult Materials	Deny	Allow	Allow
Advocacy Organizations	Deny	Deny	Deny
Gambling	Allow	Allow	Allow
Nudity and Risque	Deny	Deny	Deny
Pornography	Deny	Deny	Deny
Dating	Allow	Allow	Allow
Weapons (sales)	Deny	Deny	Deny
Marijuana	Allow	Allow	Allow
Sex Education	Allow	Allow	Allow
Alcohol	Allow	Allow	Allow
Tobacco	Allow	Allow	Allow
Lingerie and Swimsuit	Allow	Allow	Allow
Sports Hunting and War Games	Allow	Allow	Allow
Freeware and Software Downloads	Deny	Allow	Allow
File Sharing and Storage	Deny	Deny	Deny
Streaming Media and Download	Allow		
Peer-to-peer File Sharing	Deny	Deny	Deny
Internet Radio and TV	Allow	Allow	Allow
Internet Telephony	Allow	Allow	Allow
Malicious Websites	Deny	Deny	Deny
Phishing	Deny	Deny	Deny
Spam URLs	Deny	Deny	Deny
Advertising	Deny	Deny	Allow
Brokerage and Trading	Allow	Allow	Allow
Games	Allow	Allow	Allow
Web-based Email	Allow	Allow	Allow
Entertainment	Allow	Allow	Allow
Arts and Culture	Allow	Allow	Allow
Education	Allow	Allow	Allow
Health and Wellness	Allow	Allow	Allow
Job Search	Allow	Allow	Allow
Medicine	Allow	Allow	Allow
News and Media	Allow	Allow	Allow
Social Networking	Allow	Allow	Allow
Political Organizations	Allow	Allow	Allow

	Básico	Intermedio	VIP
Reference	Allow	Allow	Allow
Global Religion	Allow	Allow	Allow
Shopping and Auction	Deny	Deny	Deny
Society and Lifestyles	Allow	Allow	Allow
Sports	Allow	Allow	Allow
Travel	Allow	Allow	Allow
Personal Vehicles	Allow	Allow	Allow
Dynamic Content	Allow	Allow	Allow
Meaningless Content	Allow	Allow	Allow
Folklore	Allow	Allow	Allow
Web Chat	Allow	Allow	Allow
Instant Messaging	Allow	Allow	Allow
Newsgroups and Message Boards	Allow	Allow	Allow
Digital Postcards	Allow	Allow	Allow
Child Education	Allow	Allow	Allow
Real Estate	Allow	Allow	Allow
Restaurant and Dining	Allow	Allow	Allow
Personal Websites and Blogs	Deny	Deny	Deny
Content Servers	Allow	Allow	Allow
Domain Parking	Deny	Allow	Allow
Personal Privacy	Allow	Allow	Allow
Finance and Banking	Allow	Allow	Allow
Search Engines and Portals	Allow	Allow	Allow
General Organizations	Allow	Allow	Allow
Business	Allow	Allow	Allow
Information and Computer Security	Allow	Allow	Allow
Government and Legal Organizations	Allow	Allow	Allow
Information Technology	Allow	Allow	Allow
Armed Forces	Allow	Allow	Allow
Web Hosting	Allow	Allow	Allow
Secure Websites	Allow	Allow	Allow
Web-based Applications	Allow	Allow	Allow
Unrated	Allow	Allow	Allow

Tabla 3. Categorías por perfil de navegación - Propia de autores

10.2.9 Diseño de Sistema de prevención de Intrusos

Se implementará un sistema IPS (sistema de previsión de intrusos) en le VDOM de internet con el fin de brindar mayor seguridad a los servicios de la compañía mitigando ataques originados desde internet. Se realizará en dos fases la primera consiste en configurar los perfiles de seguridad IPS en detección y activarlos de manera beta en los servicios correspondientes con el fin de generar un reporte a las 24 horas para identificar

las firmas que son potencialmente peligrosas para la organización y lo que se encuentra expuesto si no se activa el perfil de seguridad IPS.

La segunda parte consiste en activar el perfil definido para que detecte y contenga ataques y anomalías de severidad critica, alta realizara la acción de bloquear y para media, baja e información realizara la acción que por defecto está estipulado por el fabricante que se encuentra contenida en la base de datos de Fortinet para sistemas operativos Linux y Windows.

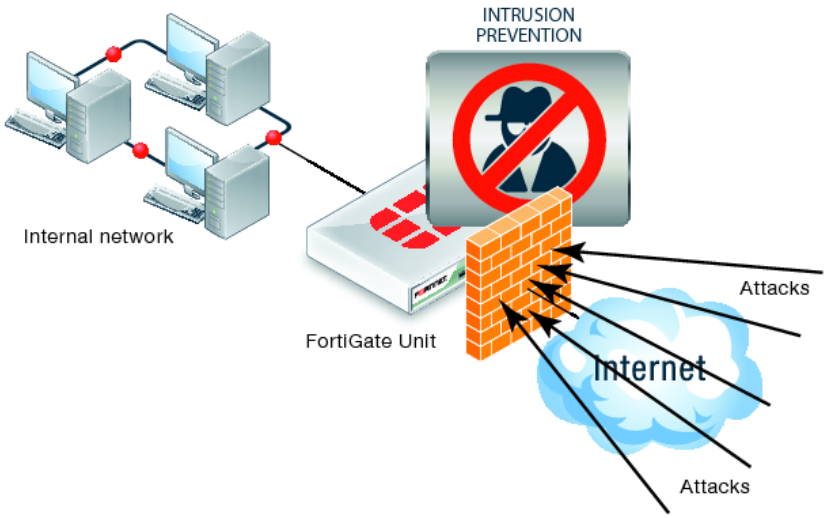


Ilustración 19. Funcionamiento IPS. – ncora.com. [12]

Para contener los ataques de denegación de servicio se cuenta con un módulo de políticas de DoS con anomalías de tcp_syn_flood, icmp_flood, upd_flood donde se define la cantidad de peticiones permitidas hacia los servicios y la acción que realizara después de sobre pasar las peticiones permitidas.

Interface Origen	IP Origen	Interface Destino	IP Destino	Servicios	Perfil IPS	Observaciones	Acción
Internet	ALL	Red Servidores	IP publica	HTTPS HTPP	IPS_Compañia	Publicación Servidor WEB	Permitir

Tabla 4. Política de firewall con perfil IPS. - Propia de los autores

10.2.10 Diseño de autenticador Fortinet

Es un dispositivo en appliance el cual ofrece una gestión de acceso que establece la identidad de la seguridad en una red, este dispositivo nos brinda diferentes alternativas que son vital a la hora de crear una política de seguridad efectiva, endureciendo la seguridad al garantizar que solo la persona adecuada en el momento adecuado pueda acceder a sus redes y datos confidenciales.

El diseño consiste en integrar el directorio activo de la organización hacia el FortiAuthenticathor con el fin de conocer las unidades organizaciones del directorio, así mismo se debe integrar el dispositivo hacia el Firewall para poder realizar la gestión de identidad a través de políticas de firewall.

Se definió integrar un dispositivo con el fin de evitar procesamiento al Firewall cuando se realicen las consultas a los grupos de la unidad organizacional del directorio activo.

Este procedimiento se realizará en 4 etapas:

- La primera etapa radica en un prerrequisito para poder realizar la integración del dispositivo de gestión de identidad con el directorio activo, la cual consta en realizar configuraciones en el servidor de directorio activo que lo debe realizar el administrador del servidor.

- La segunda etapa se realiza integración con el directorio Activo de la compañía que consiste en permitir que a través del dispositivo de gestión de identidad se visualice de las unidades organizacionales que contenga el directorio, para ello se debe realizar ciertas configuraciones en el directorio activo y en autenticador.

- La tercera etapa es la integración del autenticador con el firewall a través del FSSO, para esto se debe realizar configuración en los dos dispositivos.

- La cuarta etapa consiste en realizar filtros de unidades organizacionales en el dispositivo autenticador el con el fin de evitar procesamiento de recursos

del firewall en la consulta de estas unidades.

- La quinta etapa consiste en la configuración del firewall con la creación de las políticas de acceso incluyendo los grupos de navegación con el fin de controlar el acceso a los servidores.

A continuación, se relaciona el flujo de tráfico para consulta desde las diferentes redes hacia la red MZ.

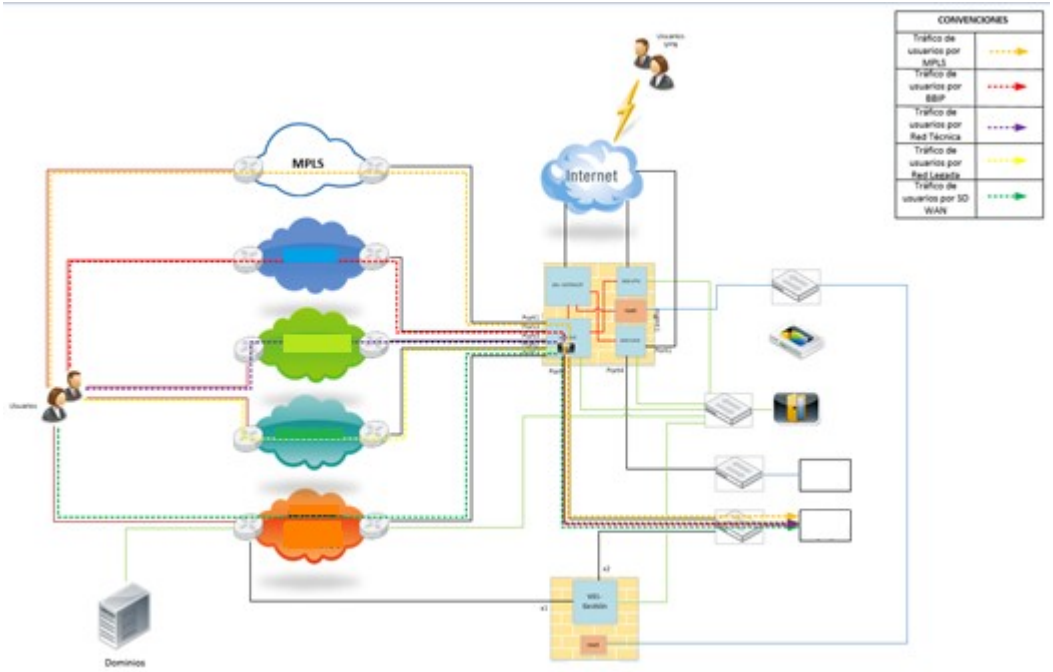


Ilustración 20. Flujo de tráfico consultas MZ. - Propia de los autores.

En la siguiente grafica se ilustra el flujo de tráfico para los usuarios de VPN client to site.

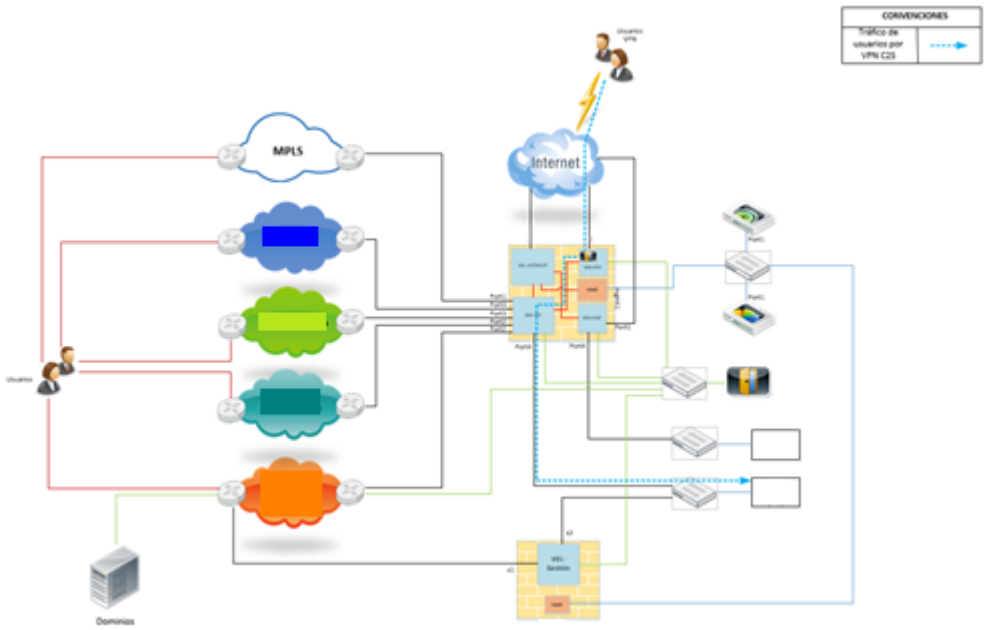


Ilustración 21. Flujo de tráfico consultas VPN cliente sitio. - Propia de los autores

10.3 Implementación

10.3.1 Configuración de firewall

A continuación, se detallará la configuración realizada en el firewall para la implementación.

Información general

HA Status: High Availability (Clúster)

Host Name: COMPAÑIA1 / COMPAÑIA2

Serial Number: FG39XXXXXX / FG39XXXXXX

Operation Mode: NAT

Firmware Versión: v5.X.X, build16XX (GA)

Puertos de gestión

Los puertos configurados en el firewall son los siguientes:

Servicio	Puerto
HTTP Port	80
HTTPS Port	10443

SSH Port	22
Telnet Port	23

Tabla 5. Listado de puertos de gestión - Propia de autores

DNS

Los DNS configurados en el firewall son los siguientes:

Primary DNS Server	208.X.X.X
Secondary DNS Server	208.X.X.X

Tabla 6. DNS configurados- Propia de autores

Distribución de Interfaces

Las interfaces del firewall están distribuidas de la siguiente manera:

Nombre	Dirección IP	Tipo	VLAN ID	VDOM
Loopback	100.X.X.X/X.X.X.X	Loopback Interface		V02-MZ
mgmt1	172.X.X.X/X.X.X.X	Physical Interface		root
mgmt2	192.X.X.X/X.X.X.X	Physical Interface		root
Red Nueva 3	0.0.0.0/0.0.0.0	Physical Interface		root
INTERNET	172.X.X.X/X.X.X.X	VLAN	A	V01-INTERNE
Red Nueva 3	100.X.X.X/X.X.X.X	VLAN	B	V02-MZ
Red Nueva 1	100.X.X.X/X.X.X.X	VLAN	C	V02-MZ
VPN	172.X.X.X/X.X.X.X	VLAN	D	V04-VPN
port2	0.0.0.0/0.0.0.0	Physical Interface		root
Red Nueva 4	100.X.X.X/X.X.X.X	VLAN	E	V02-MZ
Red Nueva 4	100.X.X.X/X.X.X.X	VLAN	F	V02-MZ

Nombre	Dirección IP	Tipo	VLAN ID	VDOM
Red Nueva 4	100.X.X.X/X.X.X.X	VLAN	G	V02-MZ
port3	0.0.0.0/0.0.0.0	Physical Interface		root
Red Nueva 2	100.X.X.X/X.X.X.X	VLAN	H	V02-MZ
Red Nueva 5	100.X.X.X/X.X.X.X	VLAN	I	V02-MZ
port4	0.0.0.0/0.0.0.0	Physical Interface		root
Red Nueva 3	0.0.0.0/0.0.0.0	VLAN	J	V02-MZ
Red Nueva 2	0.0.0.0/0.0.0.0	VLAN	K	V02-MZ
Red Nueva 5	0.0.0.0/0.0.0.0	VLAN	L	V02-MZ
Red Nueva 1	172.X.X.X/X.X.X.X	VLAN	M	V02-MZ
Red Nueva 2	172.X.X.X/X.X.X.X	VLAN	N	V02-MZ
Red Nueva 4	0.0.0.0/0.0.0.0	VLAN	Ñ	V02-MZ
Red Nueva 2	172.X.X.X/X.X.X.X	VLAN	O	V02-MZ
Red Nueva 5	172.X.X.X/X.X.X.X	VLAN	P	V02-MZ
Red Nueva 1	172.X.X.X/X.X.X.X	VLAN	Q	V01-INTERNE

Tabla 7. Distribución de Interfaces - Propia de autores

Enrutamiento estático:

El esquema de enrutamiento del firewall comprende tanto enrutamiento estático como dinámico.

Para la parte del enrutamiento estático se configuraron rutas en cada uno de los VDOMs, explicadas a continuación.

VDOM root:

Las siguientes rutas se configuraron para alcanzar las redes de gestión de la organización:

Destino	Gateway	Interfaz	Comentarios
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
192.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	
172.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	
10.X.X.X/X.X.X.X	172.X.X.X	mgmt	

Tabla 8. Rutas para acceso a gestión del firewall- Propia de autores

VDOM V01-INTERNE:

Las siguientes rutas se configuraron para alcanzar Internet y las redes alojadas en el VDOM V02-MZ:

Destino	Gateway	Interfaz	Comentarios
0.0.0.0/0	172.X.X.X	INTERNET	salida a internet
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	Redes MZ

Tabla 9. Rutas VDOM 01-Propia de autores

VDOM V02-MZ:

Las siguientes rutas corresponden a los servicios protegidos por el Firewall.

Destino	Gateway	Interfaz	Comentarios
100.X.X.X/X.X.X.X		BGP	Ruta prueba BGP
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 3	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 1	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 3	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 5	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 1	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 4	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 1	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 5	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 3	N/A

Destino	Gateway	Interfaz	Comentarios
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 4	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 5	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 1	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 4	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 5	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 4	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 3	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 5	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 1	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A

Destino	Gateway	Interfaz	Comentarios
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 5	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 2	N/A
172.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 5	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 3	N/A
0.0.0.0/0	172.X.X.X	Red Nueva 2	N/A
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 1	N/A

Tabla 10. Rutas VDOM 02-Propia de autores

VDOM V03-DMZ:

Las siguientes rutas corresponden a los servicios DMZ protegidos por el Firewall:

Destino	Gateway	Interfaz	Comentarios
100.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 3	
0.0.0.0/0	172.X.X.X	Red Nueva 2	
172.X.X.X/X.X.X.X	172.X.X.X	Red Nueva 1	

VDOM V04-VPN:

Las siguientes rutas corresponden a la navegación y servicios del VDOM VPN:

Destino	Gateway	Interfaz	Comentarios
0.0.0.0/0	172.X.X.X	Red Nueva 5	N/A

Enrutamiento dinámico:

El esquema de enrutamiento del firewall comprende tanto enrutamiento estático como dinámico.

Para la parte del enrutamiento dinámico se configuraron comunidades BGP (Border Gateway Protocol) en algunos de los VDOMs, como se puede ver a continuación.

VDOM root:

No contiene enrutamiento dinámico.

VDOM V01-INTERNE:

No contiene enrutamiento dinámico.

VDOM V02-MZ:

Para este VDOM se configuró el siguiente esquema de enrutamiento dinámico BGP:

AS Local: 8XXX

Router ID: 100.X:X:X

TABLA DE VECINOS BGP				
IP	**AS Remoto**	**Descripción**	**Routemap (Entrada)**	**Routemap (Salida)**
100.X.X.X/X.X.X.X	1	N/A	Red Nueva 1	Red Nueva 5
100.X.X.X/X.X.X.X	2	N/A	Red Nueva 3	Red Nueva 4
100.X.X.X/X.X.X.X	3	N/A	Red Nueva 2	Red Nueva 3
100.X.X.X/X.X.X.X	4	N/A	Red Nueva 4	Red Nueva 1
100.X.X.X/X.X.X.X	5	N/A	Red Nueva 3	Red Nueva 4
100.X.X.X/X.X.X.X	6	N/A	Red Nueva 3	Red Nueva 2
100.X.X.X/X.X.X.X	7	N/A	Red Nueva 2	Red Nueva 1
100.X.X.X/X.X.X.X	8	N/A	Red Nueva 4	Red Nueva 5
100.X.X.X/X.X.X.X	9	N/A	Red Nueva 3	Red Nueva 4
100.X.X.X/X.X.X.X	10	N/A	Red Nueva 2	Red Nueva 1
100.X.X.X/X.X.X.X	11	N/A	Red Nueva 4	Red Nueva 5

Tabla 11. Rutas VDOM 02-Propia de autores

Teniendo en cuenta la tabla anterior se deduce lo siguiente:

- El tráfico BGP se está filtrando de tal manera que el firewall no redistribuya ninguna ruta por defecto (0.0.0.0/0) a ninguno de sus vecinos.
- El firewall no aprende ninguna ruta por defecto mediante BGP.

- Las rutas aprendidas mediante los vecinos SDWAN solo se redistribuyen a los vecinos de las redes de la organización.
- Las rutas aprendidas mediante los vecinos de Red Corporativa y Red integrados solo se redistribuyen a la red SDWAN.
- Todas las rutas estáticas configuradas en el VDOM V02-MZ se redistribuyen automáticamente mediante el protocolo BGP a TODOS los vecinos configurados.

VDOM V03-DMZ:
No contiene enrutamiento dinámico.

VDOM V04-VPN:
No contiene enrutamiento dinámico.

Configuración de Logs

Para la implementación se realizó una integración en el VDOM global entre los dos dispositivos tanto FGT y FAZ el cual cumple la finalidad de recibir todos los logs que se envían desde el firewall con el fin de poder tener una auditoria de logs y poder generar reportes.

La integración consiste en activar en el firewall él envió de logs a otro dispositivo configurando la IP del dispositivo que recibirá los logs en tiempo real, una vez activada la configuración el firewall envía una petición de solicitud repositorio de logs.

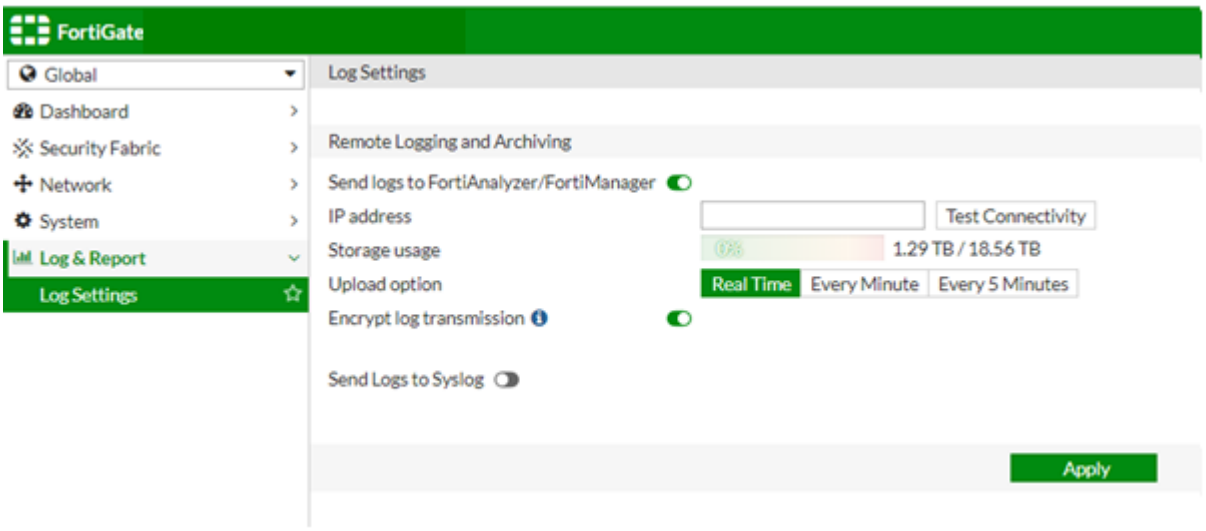


Ilustración 22. Configuración de logs Firewall. - Propia de los autores

Una vez enviada esta solicitud en el equipo FAZ esta petición se debe aceptar con la finalidad de que los logs del dispositivo se alojen en el repositorio de logs y así tener un control de estos mismos.

Administración y gestión

URL de administración por medio de Navegador WEB por medio de VPN cliente sitio y las redes internas de administración de la organización:

FortiGate Red Compañía: https://172.X.X.X

Para la administración por SSH se debe usar las mismas IP con el puerto indicado.

10.3.2 Configuración de Autenticador Fortinet

A continuación, se detallará la configuración realizada en el FortiAuthenticathor para la implementación.

Información general

HA Status: High Availability (Clúster)

Host Name: FAC-COMPAÑIA1 / FAC-COMAPÑIA2

Serial Number: FAC3XXXXXXXXX / FAC3XXXXXXXX

Firmware Version: v6.X.X, build5XXX (GA)

Puertos de gestión

Los puertos configurados en el equipo autenticador son los siguientes:

Servicio	Puerto
HTTP Port	80
HTTPS Port	10443
SSH Port	22
Telnet Port	23

Tabla 12. Gestión de autenticador Fortinet- Propia de autores.

DNS

Los DNS configurados en el equipo son los siguientes:

Primary DNS Server	208.X.X.X
Secondary DNS Server	208.X.X.X

Tabla 13. DNS autenticador Fortinet-Propio de autores.

Distribución de Interfaces

Las interfaces del FAC están distribuidas de la siguiente manera:

Nombre	Dirección IP	Tipo
Port 1	172.X.X.X/X.X.X.X	Physical Interface
Port 2	172.X.X.X/X.X.X.X	Physical Interface
Port 3	N/A	Physical Interface
Port 4	N/A	Physical Interface
Port 5	100.X.X.X/X.X.X.X	Physical Interface
Port 6	10.X.X.X/X.X.X.X	Physical Interface

Tabla 14. Distribución de puertos autenticador Fortinet-Propia de autores

Enrutamiento estático:

El esquema de enrutamiento del autenticador comprende solo enrutamiento estático que se divide en dos partes principales la primera corresponde a la interconexión con el firewall.

IP / Mascara	Gateway	Device
0.0.0.0/0	100.X.X.X/X.X.X.X	Port 5
10.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
10.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
10.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
10.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
10.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
172.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1
192.X.X.X/X.X.X.X	172.X.X.X/X.X.X.X	Port 1

Tabla 15. Rutas estáticas autenticador Fortinet-Propias de autor

Configuración de Logs

Para la implementación se realizó una integración entre los dos dispositivos tanto FAC y FAZ el cual cumple la finalidad de recibir todos los logs que se envían desde el autenticador con el fin de poder tener una auditoria de logs y poder generar reportes.

La integración consiste en activar en el autenticador él envió de logs a otro dispositivo configurando la IP del dispositivo que recibirá los logs, una vez activada la configuración el dispositivo FAC envía una petición de solicitud al FAZ.

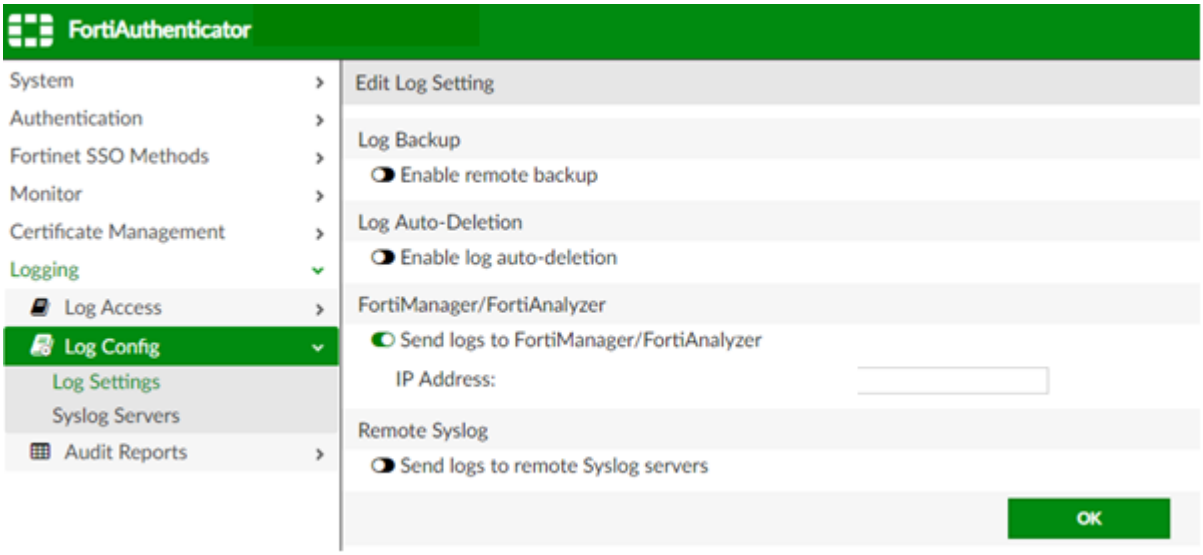


Ilustración 23. Configuración de logs FAC. - Propia de los autores.

Una vez enviada esta solicitud en el equipo FAZ esta petición se debe aceptar con la finalidad de que los logs del dispositivo se alojen en el FAZ y así tener un control de estos mismos.

Administración y gestión

URL de administración por medio de Navegador WEB por medio de VPN cliente sitio y las redes internas de administración de la organización:

FortiAuthenticator Red Compañia: https://172.X.X.X

Para la administración por SSH se debe usar las mismas IP con el puerto indicado.

10.3.3 Configuración de Analizador de logs de Fortinet (FortiAnalyzer)

A continuación, se detallará la configuración realizada en el dispositivo para la implementación.

Información general

Host Name: FAZ_Compañia.

Serial Number: FL-2XXXXXXXXXX

Firmware Version: v6.X.X-build029XXX (GA)

Puertos de gestión

Los puertos configurados en el equipo FAZ son los siguientes:

Servicio	Puerto
HTTP Port	80
HTTPS Port	10443
SSH Port	22
Telnet Port	23

Tabla 16. Gestión de FortiAnalyzer-Propia de autores

DNS

Los DNS configurados en el equipo FAZ son los siguientes:

Primary DNS Server	208.X.X.X
Secondary DNS Server	208.X.X.X

Tabla 17. DNS de FortiAnalyzer-Propia de autores

Distribución de Interfaces

Las interfaces del FAZ-2000E están distribuidas de la siguiente manera:

Nombre	Dirección IP	Tipo
Port 1	172.X.X.X/X.X.X.X	Physical Interface
Port 2	0.0.0.0/0.0.0.0	Physical Interface
Port 3	0.0.0.0/0.0.0.0	Physical Interface
Port 4	0.0.0.0/0.0.0.0	Physical Interface
Port 5	0.0.0.0/0.0.0.0	Physical Interface
Port 6	0.0.0.0/0.0.0.0	Physical Interface

Tabla 18. Distribución de interfaces FortiAnalyzer-Propia de autores.

Enrutamiento estático:

El esquema de enrutamiento del repositorio de logs comprende solo enrutamiento estático para la red de gestión que tiene la compañía corresponde al puerto 1 y con ello alcanzar el dispositivo desde las diferentes redes de la compañía.

IP / Mascara	Gateway	Device
10.X.X.X /X.X.X.X	172.X.X.X	Port 1
10.X.X.X /X.X.X.X	172.X.X.X	Port 1
10.X.X.X /X.X.X.X	172.X.X.X	Port 1
10.X.X.X /X.X.X.X	172.X.X.X	Port 1
10.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
172.X.X.X /X.X.X.X	172.X.X.X	Port 1
192.X.X.X /X.X.X.X	172.X.X.X	Port 1

Tabla 19. Rutas estáticas FortiAnalyzer-Propia de autores.

Configuración de logs

En el repositorio de logs se aceptó las solicitudes de integración recibidas de los dispositivos firewall y del autenticador, se configuro el tamaño de almacenamiento de cada dispositivo.

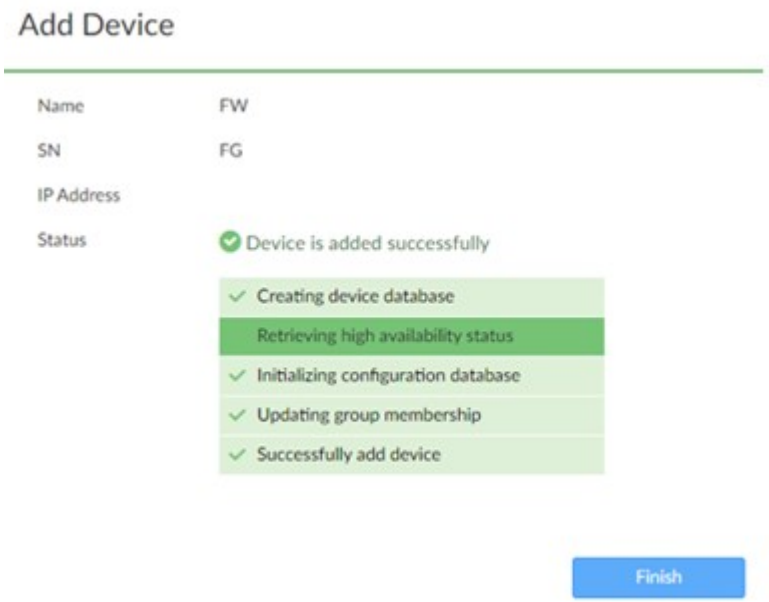


Ilustración 23. Creación ADOM FortiAnalyzer-Propia de autores.

Para el firewall se configuro 15 TB de almacenamiento de acuerdo a lo requerido por la compañía, cuenta con 2.15 TB y se generó alerta de aviso al 90% de utilización de este almacenamiento.

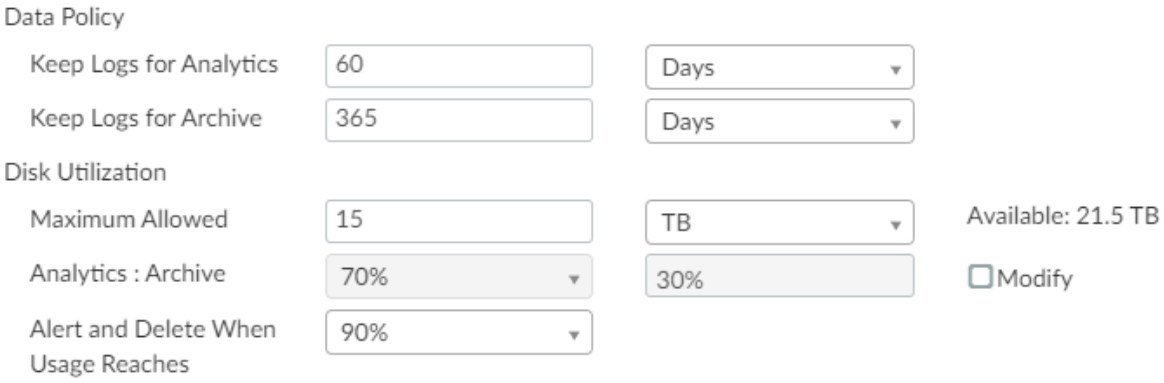


Ilustración 24. Configuración de almacenamiento al Firewall. - Propia de los autores

Al configurar el almacenamiento para el firewall en el ADOM root el cual se encarga de gestionar las configuraciones de los demás ADOMs.

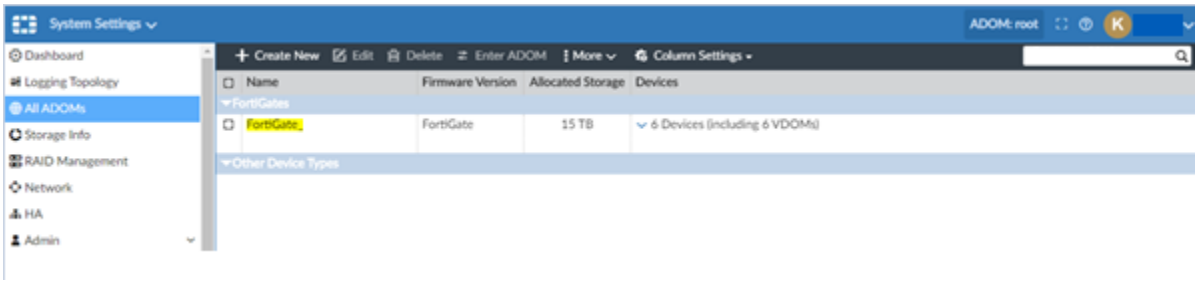


Ilustración 25. ADOM FGT. - Propia de los autores

Para el equipo autenticador se configuro 50 GB de almacenamiento de acuerdo con lo requerido por la compañía, cuenta con 6.5 TB disponibles y se generó alerta de aviso al 90% de utilización de este almacenamiento.

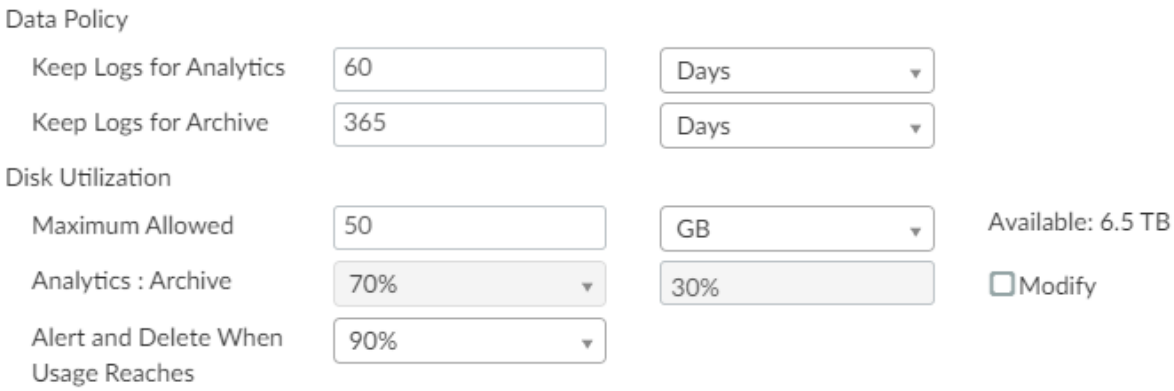


Ilustración 26. Configuración de almacenamiento al FAC. - Propia de los autores

Al configurar el almacenamiento para el equipo autenticador en el ADOM root se visualiza el total del almacenamiento configurado.

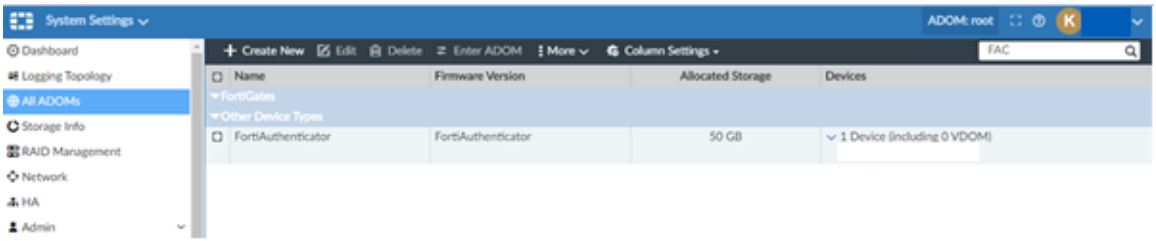


Ilustración 27. ADOM FAC. - Propia de los autores.

Creación ADOM

Para la implementación se configuro dos ADOMs, el primero para los logs provenientes de firewall y el segundo corresponde al dispositivo autenticador, se realizó esta configuración con el fin de maximizar la administración del dispositivo y se logre identificar los logs de manera más eficiente los logs de cada dispositivo y así mismo por auditoria de logs sea más fácil la generación de los reportes.

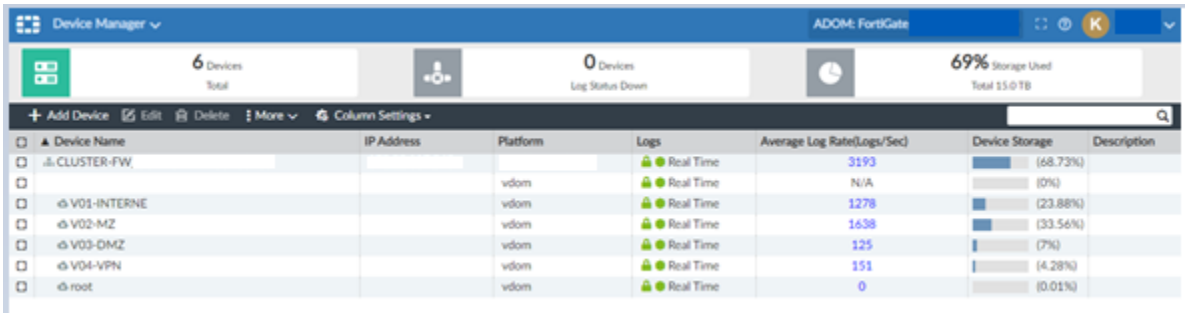


Ilustración 28. ADOM FGT-3960E. - Propia de los autores

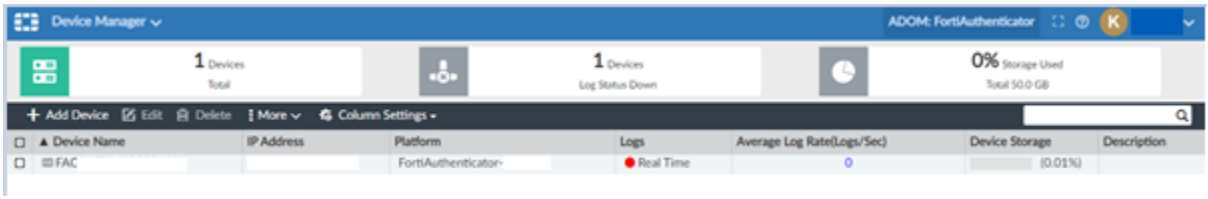


Ilustración 29. ADOM FAC-3K. - Propia de los autores

Administración y gestión

URL de administración por medio de Navegador WEB por medio de VPN SSL y las redes internas de administración de la compañía:

FortiAnalyzer Red Compañía: https://172.X.X.X

Para la administración por SSH se debe usar las mismas IP con el puerto indicado.

10.3.4 Implementación de módulos de seguridad.

10.3.4.1 Implementación de políticas de tráfico

En el firewall se configuraron al rededor 2900 políticas tanto el VDOM de internet como en el VDOM MZ, VPN, DMZ que son las que se muestran a continuación:

El VDOM MZ cuenta con 2185 políticas que se encuentran distribuidas de la siguiente manera:

El primer flujo corresponde a la interfaz llamada ASIS y su destino es INS DE que correspondía a red DC en el firewall anterior y cuenta con el siguiente direccionamiento

Tabla 20. Direccionamiento ASIS de autores.

Ilustración 30. Política firewall VDOM MZ ASIS a INS DE. - Propia de los autores.

El segundo flujo corresponde el origen a ASIS y el destino OR por donde se conoce los servidores de la red de servicios.

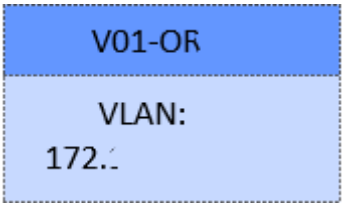


Tabla 21. Direccionamiento OR- Propia de autores

Ilustración 31. Política Firewall VDOM MZ ASIS a OR. - Propia de los autores.

El tercer flujo cuenta con 7 políticas que tienen un origen de ASIS hacia PRO que correspondía a la interfaz MPLS del VDOM 02 y MPLSPRO del VDOM 04 en el firewall anterior.

Ilustración 32. Política Firewall VDOM MZ ASIS a PRO. - Propia de los autores

El cuarto flujo contiene 3 políticas que corresponde de ASIS hacia RED el cual corresponde a los mismos nombres migrados de firewall anterior.

Ilustración 33. Política Firewall VDOM MZ ASIS a BB. - Propia de los autores

El quinto flujo corresponde al origen de ASIS con un destino llamado RED y RED L con 48 políticas que corresponde a la interfaz de red IT en el firewall anterior y para esta migración se dividió red IT llamada RED y RED L en el firewall de corporativo.

Ilustración 34. Política Firewall VDOM MZ ASIS a RED y RED L. - Propia de los autores

El sexto flujo tiene el origen ASIS y su destino RED-T con 10 políticas nombradas como se encontraba en el firewall anterior.

Ilustración 35. Política Firewall VDOM MZ ASIS a RED T Propia de autores.

El séptimo flujo corresponde a un origen de ASIS con un destino de TV con 4 políticas las cuales en firewall de anterior se conocía con el nombre de sub en los vdom

02 y 04.

Ilustración 36. Política Firewall VDOM MZ. ASIS a TV- Propia de autores.

El octavo flujo corresponde a un origen de ASIS destino V que es la interfaz del vlink de conexión con el vdom de internet.

Ilustración 37. Política Firewall VDOM MZ. ASIS a V- Propia de autores.

El noveno flujo cuenta con 30 políticas con un origen llamado EC hacia los destinos RED y RED L que correspondían a la interfaz llamada RED T en el firewall anterior.

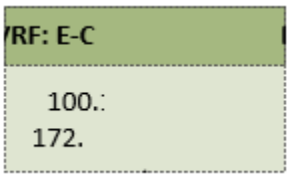


Tabla 22. Direccionamiento EC- Propia de autores

Ilustración 38. Política Firewall VDOM MZ. EC a RED y RED L- Propia de autores.

El décimo flujo contiene con 1 política desde EC con un destino TV que correspondía en los vdom 02 y 04 del firewall anterior.

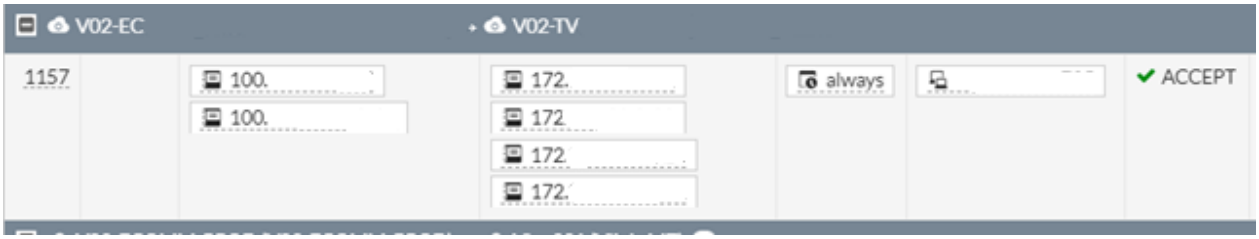


Ilustración 39. Política Firewall VDOM MZ. EC a TV- Propia de autores.

El undécimo flujo con 1 política desde EC hacia V que es la interfaz del vlink de conexión con el vdom de internet.

Ilustración 40. Política Firewall VDOM MZ. EC a V- Propia de autores

El duodécimo flujo contiene una política que su origen corresponde a GE con el direccionamiento mencionado en la imagen hacia un destino EC.

V01-GE
VLAN: 172.

Tabla 23. Direccionamiento GE- Propia de autores

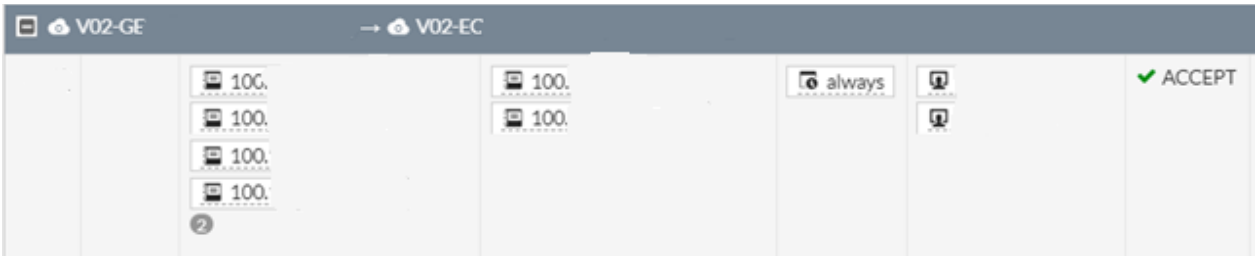


Ilustración 41. Política Firewall VDOM MZ. GE a EC- Propia de los autores.

El décimo tercer flujo con 2 políticas va desde GES hacia IN que se conocía en el firewall anterior como RED D.

Ilustración 42. Política Firewall VDOM MZ. GE a IN- Propia de los autores

El décimo cuarto flujo con lleva 3 políticas con origen GE hacia INS que se conocía en el firewall anterior como RED D.

Ilustración 43. Política Firewall VDOM MZ. GE a INS- Propia de los autores

El décimo quinto flujo corresponde a GE hacia RED B que se conocen con el mismo nombre en los dos firewalls tanto el migrado como otro de los que se piensa centralizar en el nuevo dispositivo implementado.

Ilustración 44. Política Firewall VDOM MZ. GE a RED B- Propia de los autores

El décimo sexto flujo contiene 4 políticas que su origen es a GE y su destino es RED y RED L que se conocía en el firewall anterior como red IT.

Ilustración 45. Política Firewall VDOM MZ. GE a RED y RED L- Propia de los autores

El décimo séptimo flujo tiene un origen de GE hacia la interfaz V que corresponde a la comunicación entre vdom de MZ y vdom de internet.

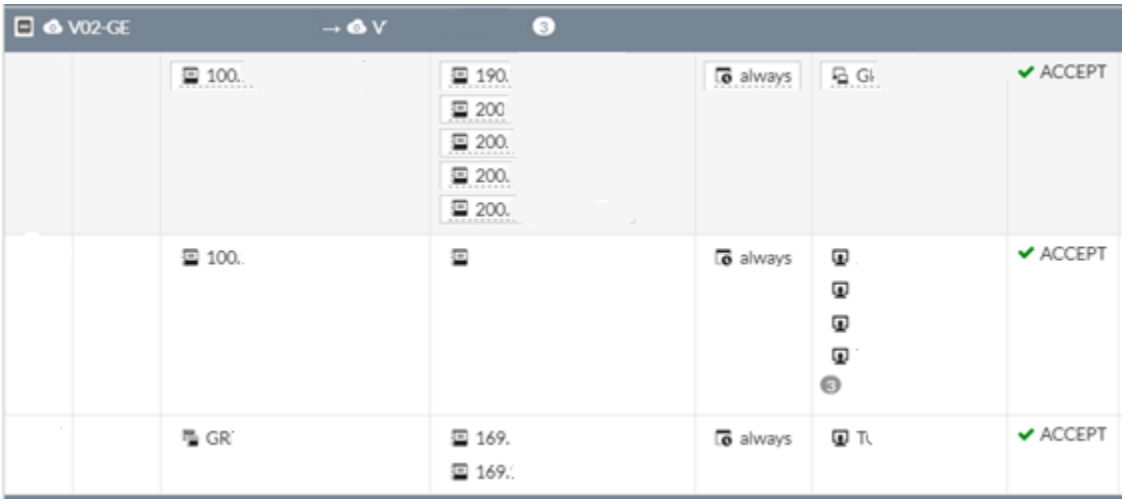


Ilustración 46. GE a Internet- Propia de los autores

El décimo octavo flujo a INS que se conocía como RED D en el firewall migrado y su destino es ASIS con 6 políticas.

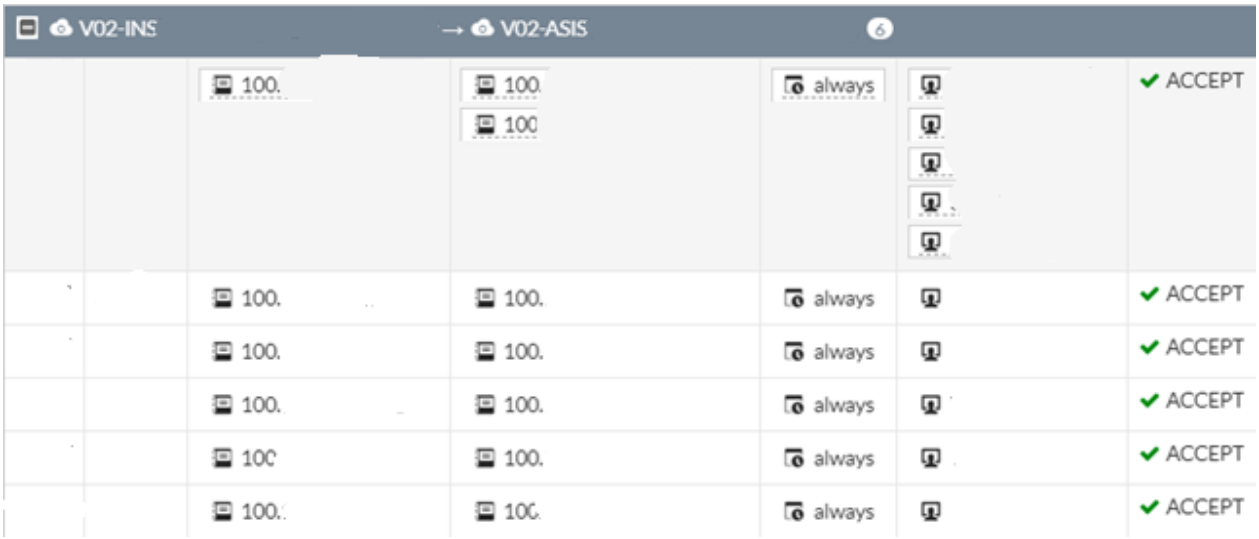


Ilustración 47. Política Firewall VDOM MZ. INS a ASIS. - Propia de los autores.

El décimo noveno flujo corresponde a INS hacia IN esto es un flujo de comunicación entre el aplicativo de INS que en el firewall migrado no se tenía ya que esas políticas ya que se conocía por una misma interfaz llamada RED.

Ilustración 48. Política Firewall VDOM MZ. INS a IN. - Propia de los autores

El vigésimo flujo contiene 18 políticas de DESARROLLO hacia PR que como se mencionó anteriormente esa interfaz de destino correspondía a las interfaces llamadas sub para vdom 02 y 04 del firewall migrado.

Ilustración 49. Política Firewall VDOM MZ. DESARROLLO a PR. - Propia de los autores

El vigésimo primer flujo cuenta con 13 políticas de DESARROLLO hacia la interface RED B.

Ilustración 50. Política Firewall VDOM MZ. DESARROLLO a RED B. - Propia de los autores

El vigésimo segundo flujo consiste en 374 políticas que su objetivo es alcanzar las redes que se encuentran en las interfaces de RED y RED L desde la interface de DESARROLLO.

Ilustración 51. Política Firewall VDOM MZ. DESARROLLO a RED y RED L. - Propia de los autores

El vigésimo tercer flujo funciona desde DESARROLLO hacia la interface RED T con 24 políticas.

Ilustración 52. Política Firewall VDOM MZ. DESARROLLO a RED T. - Propia de los autores

El vigésimo cuarto flujo corresponde a la conexión desde DESARROLLO hacia vdom link de internet con 40 políticas.

Ilustración 53. Política Firewall VDOM MZ. DESARROLLO a Internet. - Propia de los autores

El vigésimo quinto flujo contiene 2 políticas de INS hacia ASIS.

Ilustración 54. Política Firewall VDOM MZ. INS a ASIS. - Propia de los autores

El vigésimo sexto flujo es INS hacia DESARROLLO es una comunicación entre el aplicativo de INS son reglas nuevas ya que INS en el firewall anterior se conocía como RED.

Ilustración 55. Política Firewall VDOM MZ. INS a DESARROLLO. - Propia de los autores

El vigésimo séptimo flujo con un origen la interface INS hacia la interface destino correspondiente a PR que contendrá a las interfaces llamadas MPLS Y MPLSPRO en el firewall anterior.

Ilustración 56. Política Firewall VDOM MZ. INS a PR. - Propia de los autores

El vigésimo octavo flujo contiene 17 políticas desde la interface INS hacia la interface RED B.

Ilustración 57. Política Firewall VDOM MZ. INS a RED B. - Propia de los autores

El vigésimo noveno flujo con 166 políticas de INS consultando las redes de IT conocidas en el firewall migrado como RED y RED L.

Ilustración 58. Política Firewall VDOM MZ. INS a RED y RED L. - Propia de los autores.

El trigésimo flujo corresponde a accesos desde INS hacia la interface RED T con 21 políticas.

Ilustración 59. Política Firewall VDOM MZ. INS a RED T. - Propia de los autores.

El trigésimo primero flujo corresponde a la conectividad de INS con el vdom de internet.

Ilustración 60. Política Firewall VDOM MZ. INS a Internet. - Propia de los autores.

El trigésimo segundo flujo corresponde a unos accesos desde PRO que se conocía con el nombre de sub en firewall migrado hacia DESARROLLO y PRODUCCION que correspondía a la interfaz llamada RED en el firewall anterior.

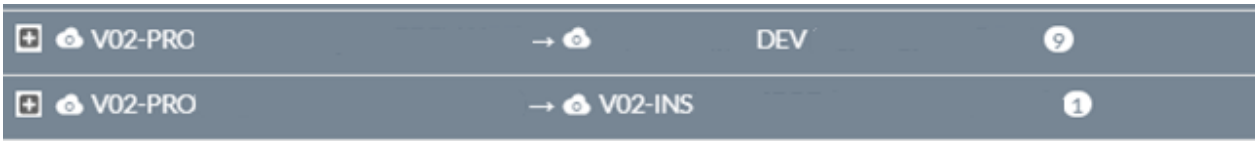


Ilustración 61. Política Firewall VDOM MZ. PRO a INS y DESARROLLO. - Propia de los autores.

El trigésimo tercer flujo contiene 4 políticas con un origen PRO hacia la red conocía como RED en el firewall migrado y en el nuevo corresponde a la interface RED e interface RED L.

Ilustración 62. Política Firewall VDOM MZ. PRO a RED y RED L. - Propia de los autores.

El trigésimo cuarto flujo contiene 2 políticas con un origen desde RED B y su destino es ASIS.

Ilustración 63. Política Firewall VDOM MZ. RED B a ASIS - Propia de los autores.

El trigésimo quinto flujo contiene 1 política con un origen desde RED B y su destino es GE.

Ilustración 64. Política Firewall VDOM MZ. RED B a GE. - Propia de los autores.

El trigésimo sexto flujo contiene 11 políticas con un origen desde RED B y su destino es DESARROLLO.

Ilustración 65. Política Firewall VDOM MZ. RED B a DESARROLLO. - Propia de los autores.

El trigésimo séptimo flujo contiene 2 políticas con un origen desde RED B y su destino es RED Y RED L.

Ilustración 66. Política Firewall VDOM MZ. RED B a RED y RED L. - Propia de los autores

El trigésimo octavo flujo corresponde a la conexión de una interfaz virtual desde RED y RED L hacia la loopback de vdom MZ.

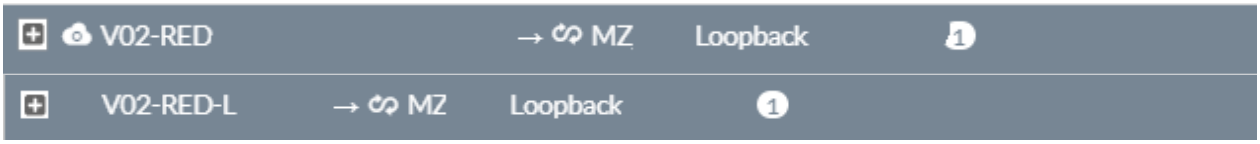


Ilustración 67. Política Firewall VDOM MZ RED y RED L a interfaz Virtual. - Propia de los autores

El trigésimo noveno flujo corresponde desde la RED y RED L que correspondía a la interfaz llamada Red en el firewall de anterior hacia ASIS.

Ilustración 68. Política Firewall VDOM MZ RED y RED L a ASIS. - Propia de los autores

El cuadragésimo flujo corresponde desde RED y RED L que correspondía a la interfaz llamada RED en el firewall anterior hacia EC.

Ilustración 69. Política Firewall VDOM MZ. RED y RED L a EC. - Propia de los autores

El cuadragésimo primero flujo corresponde desde la RED y RED L que correspondía a la interfaz llamada RED en el firewall anterior hacia GE.

Ilustración 70. Política Firewall VDOM MZ. RED y RED L a GE. - Propia de los autores

El cuadragésimo segundo flujo corresponde desde la RED y RED L que correspondía

a la interfaz llamada RED en el firewall anterior hacia la interface DESARROLLO e interface INS.

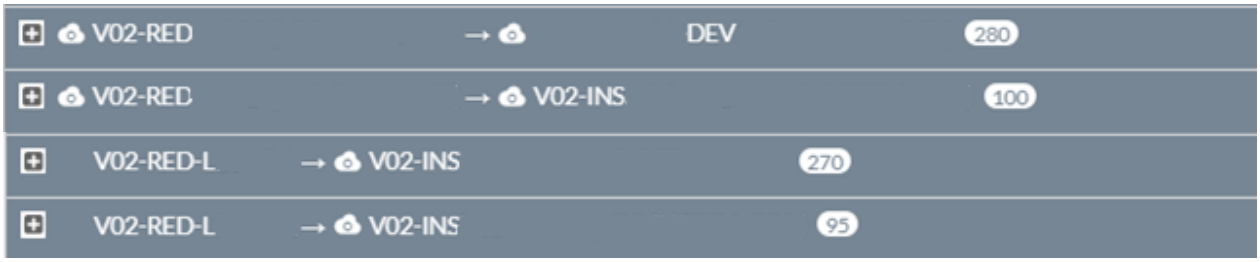


Ilustración 71. Política Firewall VDOM MZ. RED y RED L a INS y Desarrollo. - Propia de los autores

El cuadragésimo tercero flujo corresponde desde la RED y RED L que correspondía a la interfaz llamada RED en el firewall anterior hacia OR.

Ilustración 72. Política Firewall VDOM MZ. RED y RED L a OR. - Propia de los autores

El cuadragésimo cuarto flujo corresponde desde la RED y RED L que correspondía a la interfaz llamada RED en el firewall anterior hacia la interface implementada con el nombre PR.

Ilustración 73. Política Firewall VDOM MZ. RED y RED L a PR. - Propia de los autores

El cuadragésimo quito flujo corresponde desde la RED que es la red que se conoce por el sdwan hacia los servicios de RED L que se conoce como las sedes con 159 políticas y 6 bidireccionales.

Ilustración 74. Política Firewall VDOM MZ. RED y RED L. - Propia de los autores

El cuadragésimo sexto flujo corresponde desde la RED y RED L que correspondía a la interfaz llamada RED en el firewall anterior hacia RED T.

Ilustración 75. Política Firewall VDOM MZ. RED y RED L. - Propia de los autores

El cuadragésimo séptimo flujo corresponde desde la RED L y RED hacia la conexión del vdom de internet.

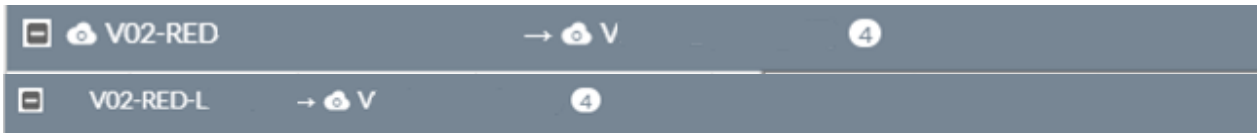


Ilustración 76. Política Firewall VDOM MZ. RED y RED L a Internet. - Propia de los autores

El cuadragésimo octavo flujo corresponde a una interfaz virtual entre RED T hacia MZ.

Ilustración 77. Política FTG 3960E VDOM MZ. RED T a MZ - Propia de los autores.

Los siguientes flujos corresponden desde el origen de RED T hacia la red de servicios como es ASIS, DESARROLLO, INS y la RED conocida en este firewall como RED y RED L.

Ilustración 78. Política FTG 3960E VDOM MZ. RED T - Propia de los autores

El quinta cuadragésimo flujo corresponde a un acceso hacia la RED L desde la interfaz TET.

Ilustración 79. Política Firewall VDOM MZ. TET a RED L. - Propia de los autores.

Los siguientes dos flujos corresponden al acceso hacia los servicios de ASIS y EC desde TV que anteriormente se mencionó a que interfaz correspondía en el firewall anterior.

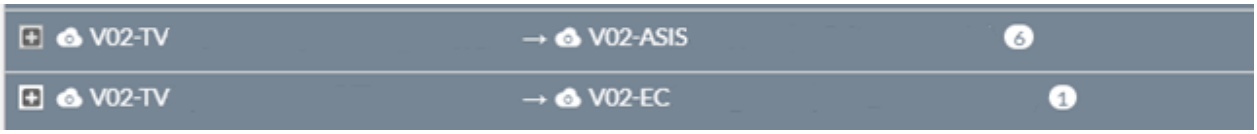


Ilustración 80. Política Firewall VDOM MZ. TV a EC y ASIS - Propia de los autores.

Los siguientes flujos correspondiente a publicaciones que se están consultando desde internet hacia los servidores y llegan por el vdom link desde el dominio virtual vdom internet.

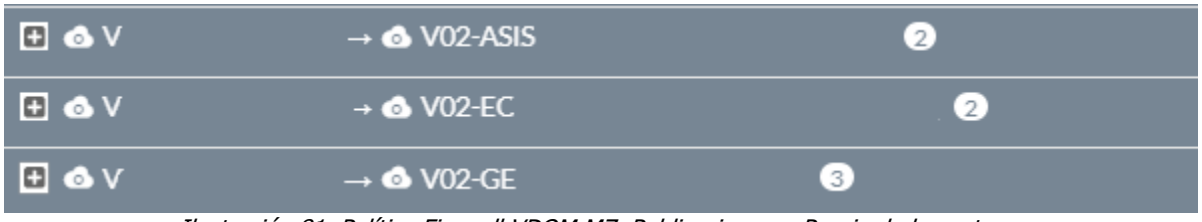


Ilustración 81. Política Firewall VDOM MZ. Publicaciones. - Propia de los autores

Los siguientes flujos consisten en los accesos de una VPN ssl con el fin de alcanzar los servicios de este aplicativo y de la RED y RED L. Se conocen a través del vdom link que interconecta MZ e Internet.

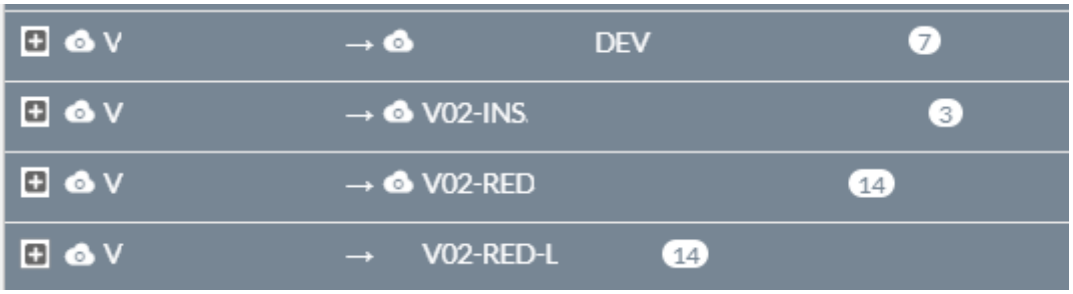


Ilustración 82. Política Firewall VDOM MZ. Conexiones de VPN. - Propia de los autores

Los siguientes flujos consisten en los accesos de una VPN ssl llamada TET de proveedor con el fin de alcanzar los servicios de este aplicativo. Se conocen atreves del vdom link de interconexión entre MZ e Internet.

Ilustración 83. Ilustración 82. Política Firewall VDOM MZ. Conexiones de VPN CISCO. - Propia de los autores

VDOM Internet

El VDOM de internet cuenta con Los siguientes flujos:

El primer flujo corresponde a las publicaciones que tiene la compañía y llega desde internet direccionado hacia el VDOM MZ por medio de VDOM Link Internet.

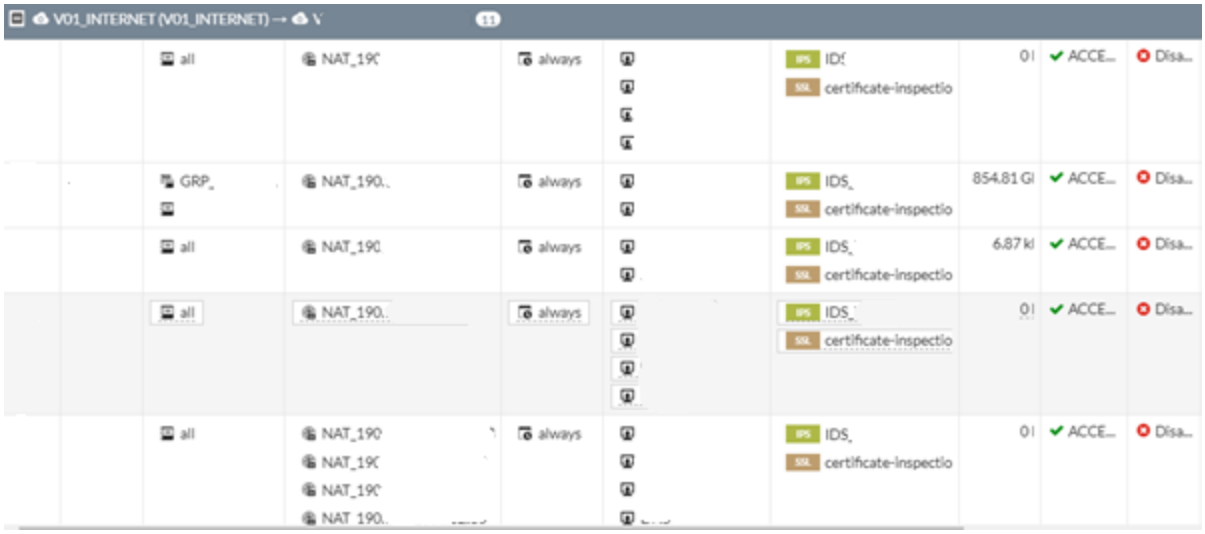


Ilustración 84. Política Firewall VDOM INTERNET a MZ. - Propia de los autores

El segundo flujo corresponde a las publicaciones que tiene la compañía y llega desde internet direccionado hacia el VDOM DMZ por medio de VDOM Link Internet.

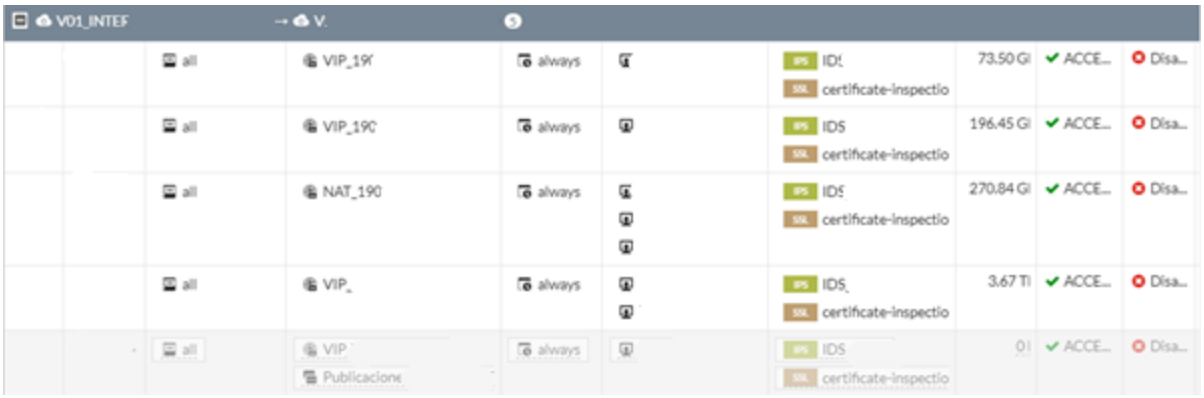


Ilustración 85. Ilustración 84. Política Firewall VDOM INTERNET a DMZ. - Propia de los autores

El tercer flujo corresponde a los servicios que tienen salida de navegación desde VDMO MZ hacia el VDOM Internet.

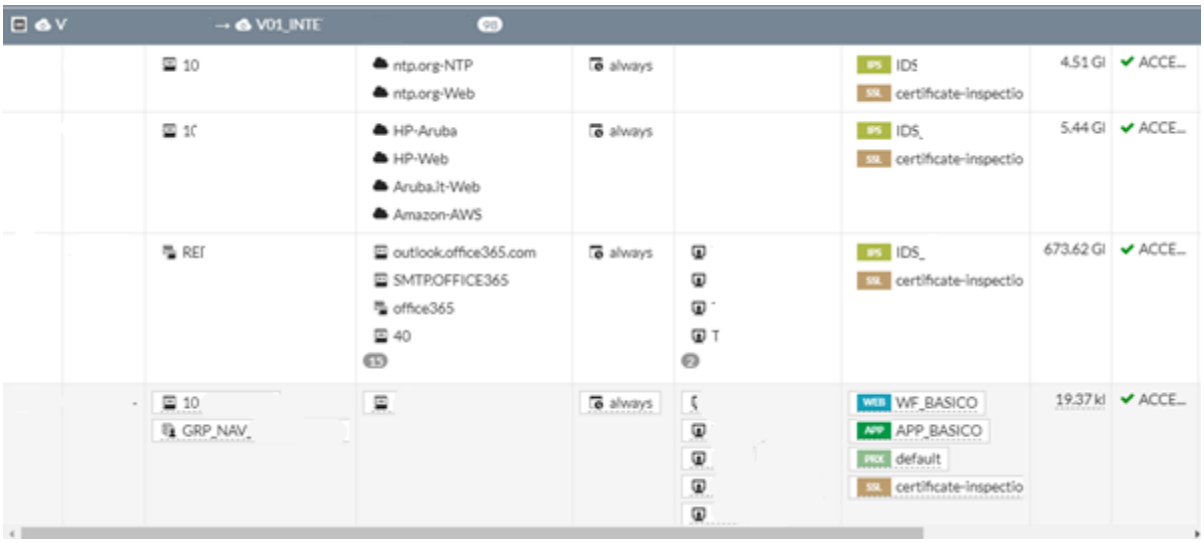


Ilustración 86. Política Firewall VDOM INTERNET MZ a Internet. - Propia de los autores

VDOM DMZ

El VDOM DMZ cuenta con algunas publicaciones de la compañía y tiene 6 políticas con el siguiente flujo:

El tráfico hacia las publicaciones que tiene la compañía, llega desde internet direccionado hacia el VDOM DMZ por medio de VDOM Link DMZ Internet.

Ilustración 87. Política Firewall VDOM DMZ Publicaciones. - Propia de los autores

VDOM VPN

El VDOM VPN cuenta con todos los accesos remotos de la compañía (VPNs) tiene 104 políticas con el siguiente flujo que permite a los usuarios remotos llegar a los servicios destinados en el VDOM MZ.

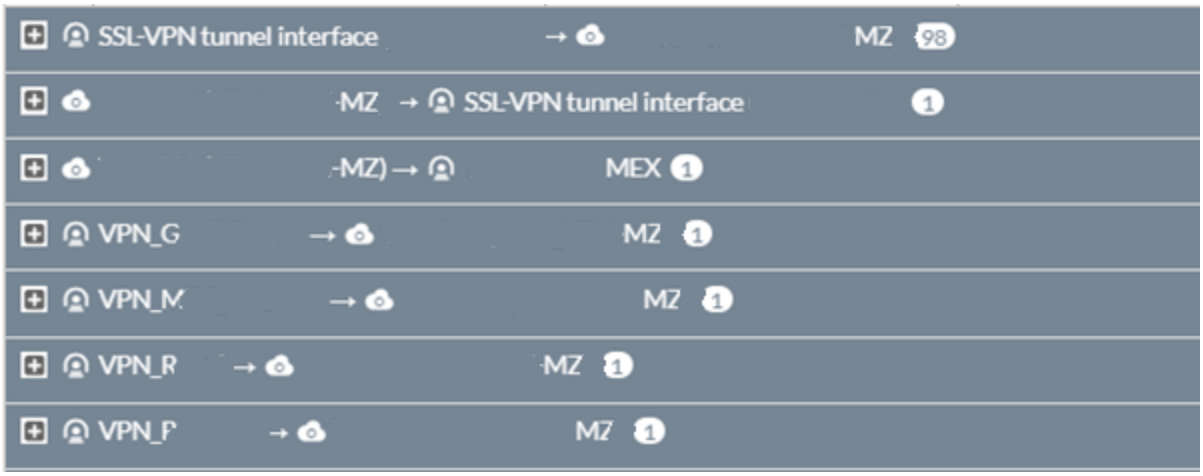


Ilustración 88. Política Firewall VPN. - Propia de los autores

10.3.4.2 Implementación de VPN

Se implemento una VPN cliente sitio para las conexiones de teletrabajo de lo colaboradores con los siguientes parámetros de configuración.

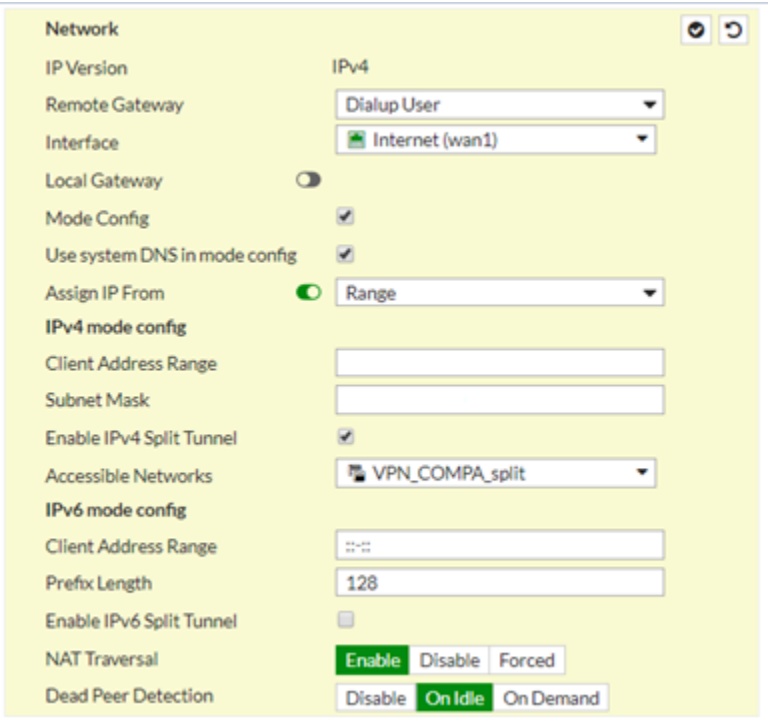


Ilustración 89. Configuración VPN Tunel y rango-Propia de autores.

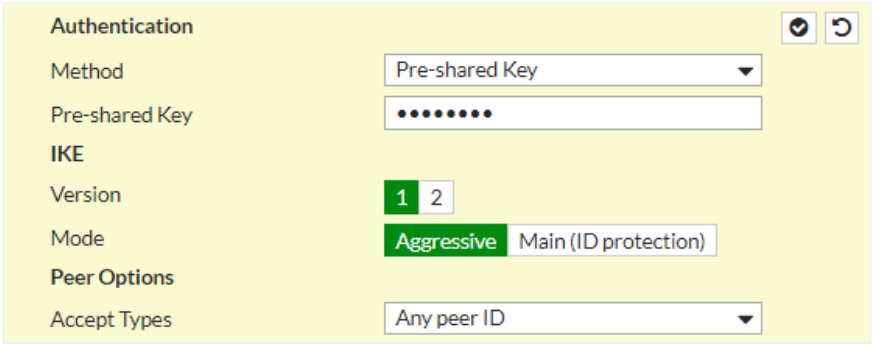


Ilustración 90. VPN método de autenticación-Propia de autores.

Para la fase 1 de la VPN se configuro los siguientes algoritmos de encriptación:

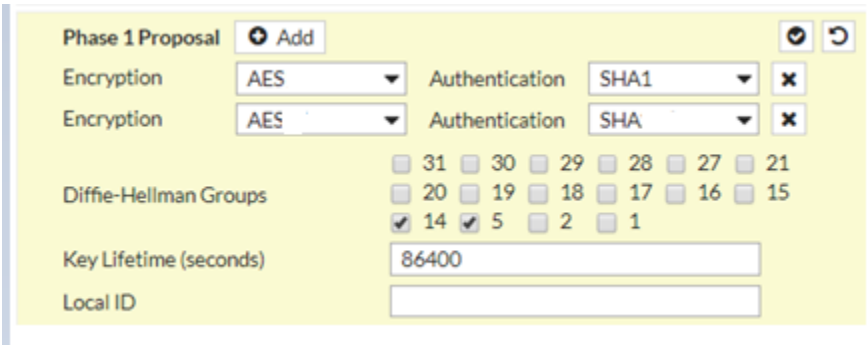


Ilustración 91. VPN métodos de encriptación Fase 1-Propia de autores.

Para fase 2 se configuro lo que se evidencia en la siguiente imagen.

Ilustración 92. VPN métodos de encriptación Fase 2-Propia de autores.

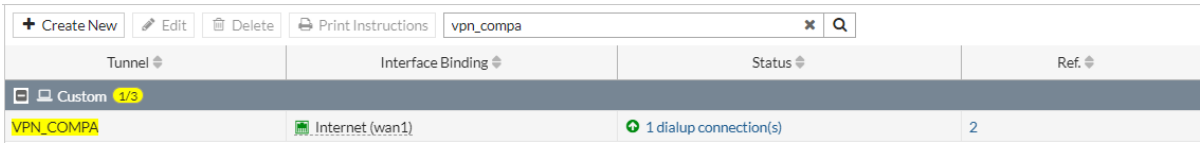


Ilustración 93. Estado de conexiones VPN-Propia de autores.

Se configuro la regla de acceso con el origen de la VPN creada hacia el destino que corresponde a la Red DMZ con el fin de que lo colaboradores tengan alcance hacia los servidores desde sitio remoto seguro.

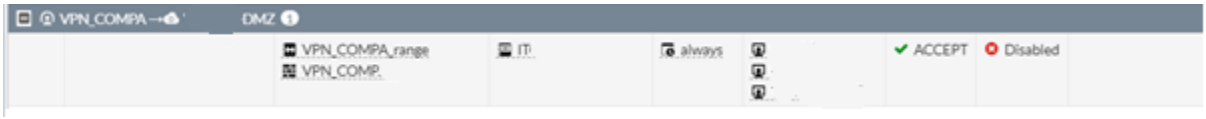


Ilustración 94. Accesos de VPN-Propia de autores.

10.3.4.3 Implementación de Filtrado de Contenido

En la configuración del módulo de seguridad para el filtrado de navegación el cual se realizó en el domino virtual de internet el cual se dividió en tres perfiles de seguridad (VIP, Intermedio, Básico) los cuales son grupos creados en el directorio activo e integrados al Autenticador mediante un LDAP y conectado al Firewall mediante Single Sing-ON, esto con la finalidad de tener la administración de los usuarios por el directorio activo lo cual facilita la administración y garantiza un mayor control con una granularidad al servicio de navegación que está accediendo cada colaborador de la compañía.

A continuación, se detallará la configuración realizada para los tres perfiles de seguridad para la navegación de los usuarios.

Perfil de navegación Básico

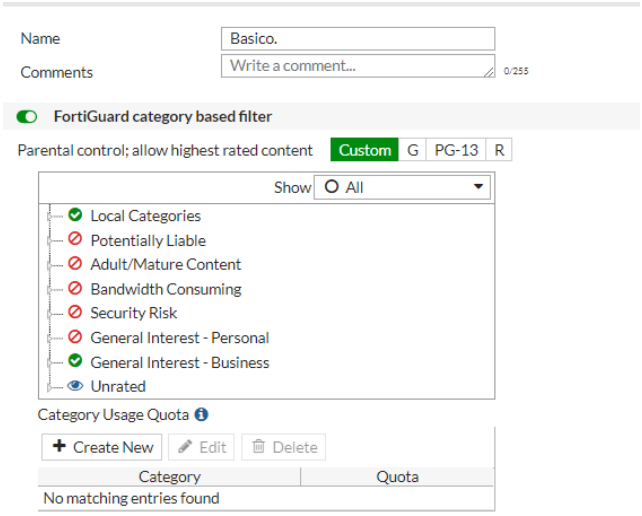


Ilustración 95. Perfil de Navegación Básico-Propia de autores.

Perfil de navegación Intermedio

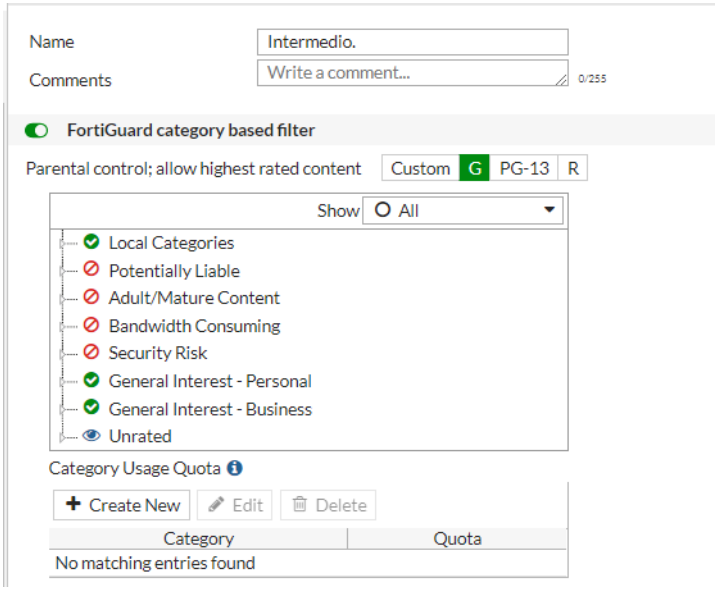


Ilustración 96. Perfil de navegación Intermedio-Propia de autores.

Perfil de navegación VIP

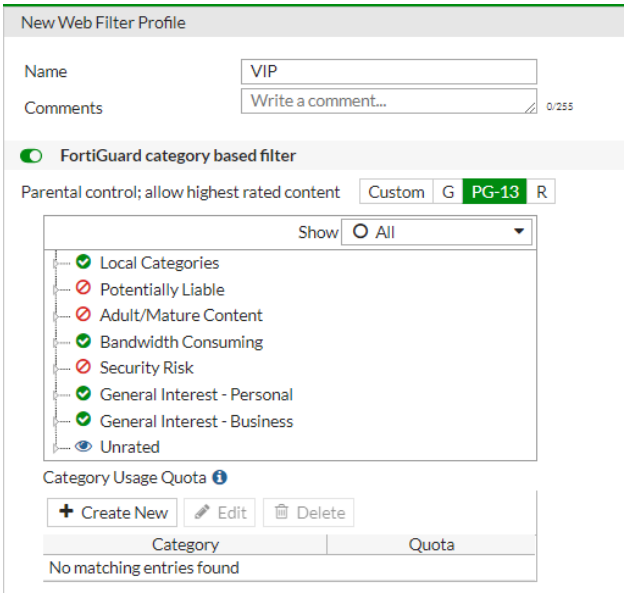


Ilustración 97. Perfil de navegación VIP-Propia de autores.

10.3.4.4 Implementación de Perfiles IPS

Según lo propuesto en diseño se configuro dos perfiles de seguridad de IPS uno en detección llamado IDS_Beta que se configuro de la siguiente manera:

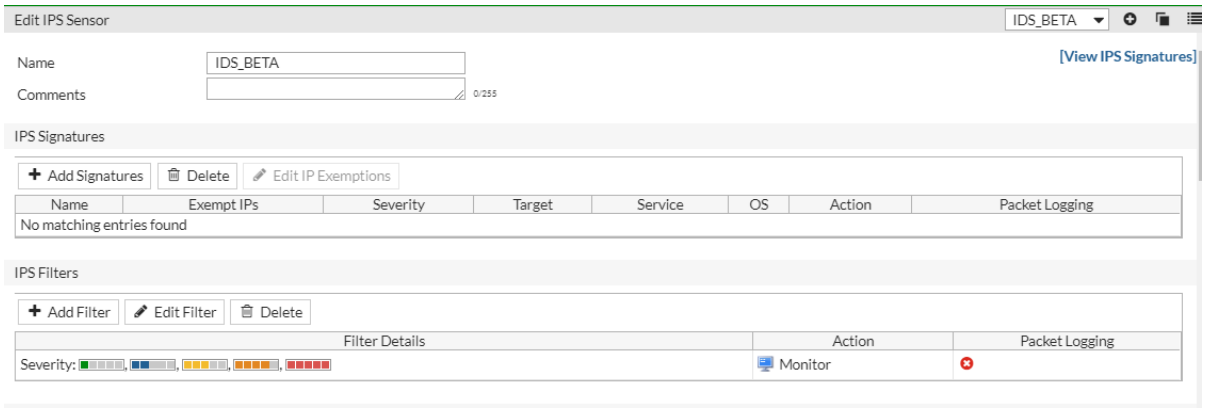


Ilustración 98. Perfil IPS modo monitoreo-Propia de autores.

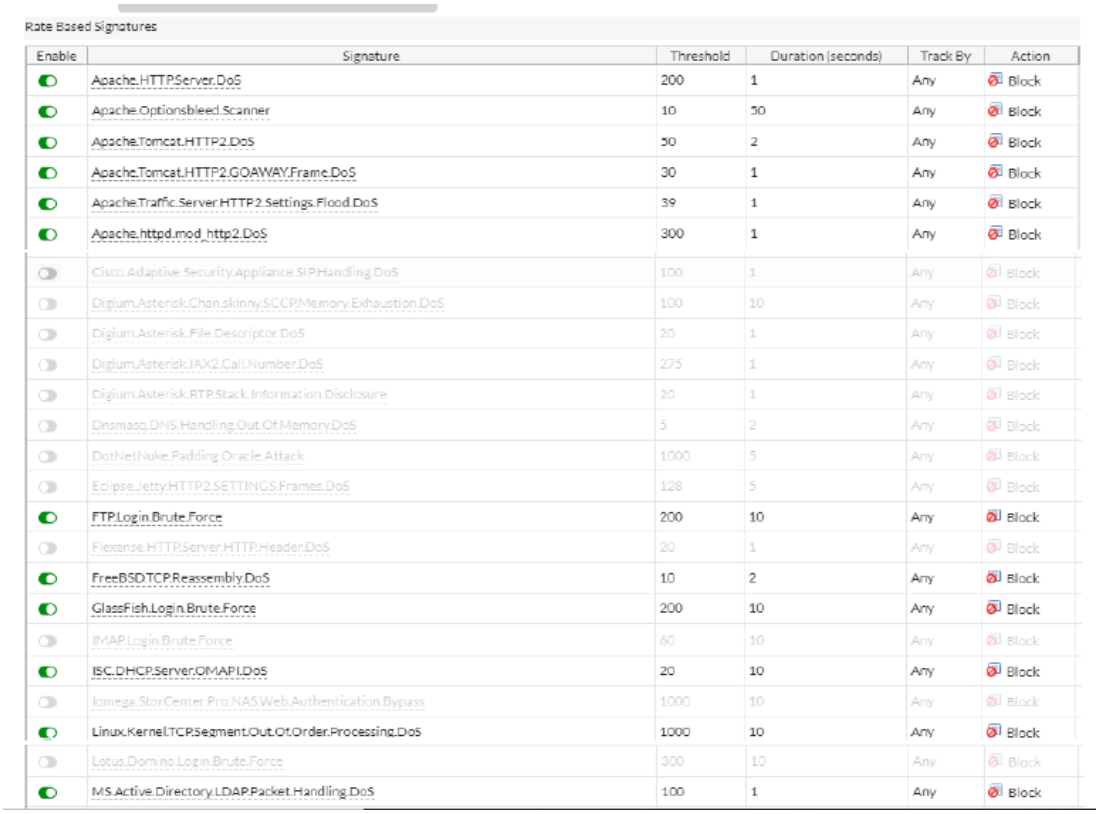
En el perfil de IDS_Beta se aplican alrededor de 13362 firmas para el análisis con la acción activada de monitor la cual permite detectar que firmas son altamente peligrosas para los servidores.

Name	Severity	Target	OS
2Wire.Wireless.Router.XSRF.Password.Reset		Server, Client	Linux
3Com.3CDaemon.FTP.Server.Buffer.Overflow		Server	Windows
3Com.3CDaemon.FTP.Server.Information.Disclosure		Client	Windows
3Com.Intelligent.Management.Center.Information.Disclosure		Server	Windows
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		Server	Linux
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		Server	Linux
3CX.Phone.System.VAD_Deploy.Arbitrary.File.Upload		Server	Windows
3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow		Client	Windows
3ivx.MPEG4.File.Processing.Buffer.Overflow		Client	Windows
3S-Pocketnet.VMS.ActiveX.Control.Buffer.Overflow		Client	Windows
4D.WebStar.FTP.Command.Buffer.Overflow		Server	Windows
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow		Server	Windows
7-Zip.RAR.Solid.Compression.Remote.Code.Execution		Server, Client	Windows
74CMS.Config.Controller.Remote.Code.Execution		Server	Windows, Linux, BSD, Solaris, MacOS
427BB.Cookie.Based.Authentication.Bypass		Server	Other
427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection		Server	Other
1024CMS.Standard.PHP.File.Inclusion		Server	Windows, Linux, BSD, Solaris, MacOS
A32S.Botnet		Server, Client	All
AAEH.Botnet		Server	All

« ‹ 1 /268 › » [Total: 13362]

Ilustración 99. Firmas IPS-Propia de autores.

Se agregan las firmas rate-based para bloquear el tráfico específico cuando se excede el umbral durante el período de tiempo configurado.



Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action
●	Apache.HTTP.Server.DoS	200	1	Any	Block
●	Apache.Optionsbleed.Scanner	10	30	Any	Block
●	Apache.Tomcat.HTTP2.DoS	50	2	Any	Block
●	Apache.Tomcat.HTTP2.GOAWAY.Frame.DoS	30	1	Any	Block
●	Apache.Traffic.Server.HTTP.2.Settings.Flood.DoS	39	1	Any	Block
●	Apache.httpd.mod_http2.DoS	300	1	Any	Block
○	Cisco.Adaptive.Security.Appliance.SIP.Handling.DoS	100	1	Any	Block
○	Digium.Asterisk.Chan.skinny.SCCP.Memory.Exhaustion.DoS	100	10	Any	Block
○	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block
○	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block
○	Digium.Asterisk.RTP.Stack.Information.Disclosure	20	1	Any	Block
○	Dnsmasq.DNS.Handling.Out.Of.Memory.DoS	5	2	Any	Block
○	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block
○	Eclipse.Jetty.HTTP2.SETTINGS.Frames.DoS	128	5	Any	Block
●	FTP.Login.Brute.Force	200	10	Any	Block
○	Flexense.HTTP.Server.HTTP.Header.DoS	20	1	Any	Block
●	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block
●	GlassFish.Login.Brute.Force	200	10	Any	Block
○	IMAP.Login.Brute.Force	60	10	Any	Block
●	ISC.DHCP.Server.OMAPI.DoS	20	10	Any	Block
○	Iomega.StorCenter.Pro.NAS.Web.Authentication.Bypass	1000	10	Any	Block
●	Linux.Kernel.TCP.Segment.Out.Of.Order.Processing.DoS	1000	10	Any	Block
○	Lotus.Domino.Login.Brute.Force	300	10	Any	Block
●	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	Block

Ilustración 100. Firmas basadas en umbral 1-Propia de autores.

MS.Windows.HTTP2.Resource.Loop.DoS	6	1	Any	Block
MS.Windows.Server.DNS.Response.Caching.Code.Execution	100	1	Any	Block
MS.Windows.UDP.Remote.Code.Execution	100	10	Any	Block
MS.Windows.WPAD.Proxy.Discovery.Privilege.Elevation	5	1	Any	Block
MS.Windows.WPAD.Proxy.Discovery.Response.Privilege.Elevation	2000	1	Any	Block
MS.XML.Core.Services.Memory.Corruption	5	10	Any	Block
McAfee.VirusScan.ENT.Linux.Auth.Token.Information.Disclosure	5	20	Any	Block
Memcached.UDP.Amplification.Detection	50	1	Any	Block
MySQL.Login.Brute.Force	60	60	Any	Block
NTLM.Authentication.Brute.Force	200	10	Any	Block
Nginx.0-Length.Headers.Leak.DoS	100	1	Any	Block
Novell.Open.Enterprise.Server.HTTPSTK.SSL.Free.DoS	10	1	Any	Block
Novell.eDirectory.SOAP.Request.Parsing.DoS	4	2	Any	Block
OpenSSH.sshd.Kex.Input.Kexinit.DoS	5	1	Any	Block
OpenSSL.Private.DH.exponent.Disclosure	35	10	Any	Block
OpenSSL.Undefined.Warnings.DoS	20	1	Any	Block
Oracle.Application.Server.SID.Brute.Force	300	10	Any	Block
Oracle.MySQL.Server.InnoDB.Memcached.Plugin.DoS	60	1	Any	Block
Oracle.XML.DB.SID.Brute.Force	300	10	Any	Block
POP3.Login.Brute.Force	200	10	Any	Block
PowerDNS.Authoritative.Server.Dot.Character.DoS	100	5	Any	Block
PowerDNS.Authoritative.Server.Long.qname.Handling.DoS	100	5	Any	Block
Red.Hat.389.Directory.Server.TLS.DoS	30	1	Any	Block
Red.Hat.389.Directory.Server.vslapd_log_emergency_error.DoS	20	3	Any	Block
SAP.BusinessObjects.User.Brute.Force	200	10	Any	Block
SAP.Management.Console.Username.Brute.Force	200	10	Any	Block
SIP.Register.Brute.Force	500	1	Any	Block

Ilustración 101. Firmas basadas en umbral 2-Propia de autores.

Se aplico el perfil de seguridad IPS tanto en las políticas de salida como de entrada de navegación para identificar los riesgos a los que se está expuesto si no se activa no se implementa un IPS.

Ilustración 102. Prevención de intrusiones outside-Propia de autores.

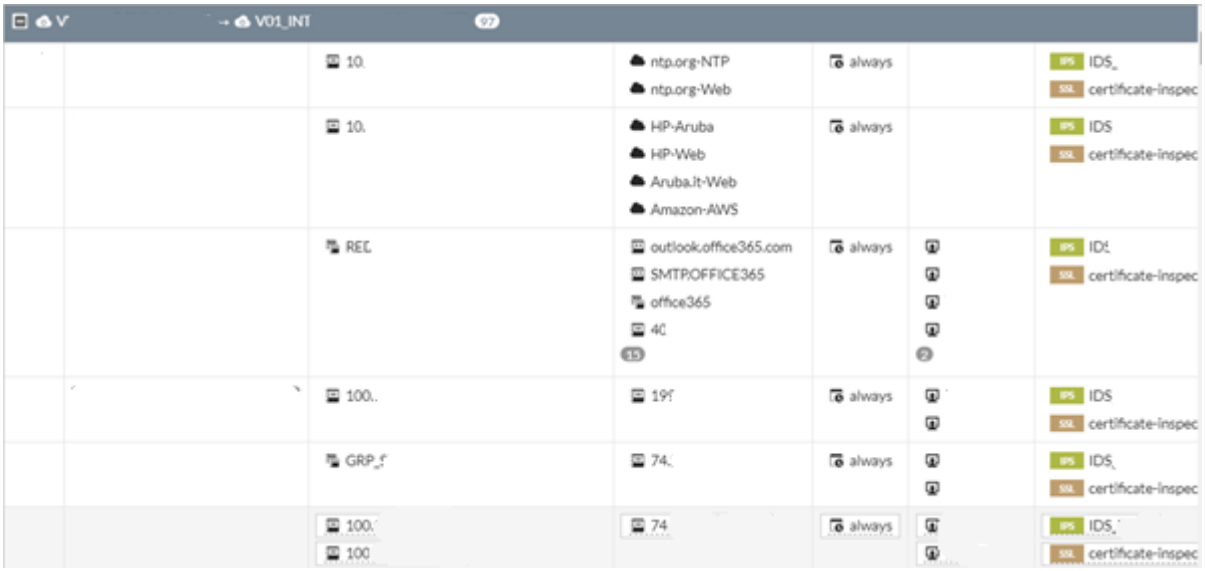


Ilustración 103. Prevención de intrusiones Inside-Propia de autores.

Por medio del dispositivo FAZ-2000 se generó un reporte de las últimas 24 horas después de activar el perfil de IPS en la función de detección. El reporte completo se encuentra en Anexo B.

Se detectó una firma con más de 20000 eventos de Backdoor.DoublePulsar es compatible con los protocolos SMB y RDP. Además de la comunicación de puerta trasera, la firma detecta el intento de escaneo a través del protocolo RDP. Por lo tanto, el desencadenante de esta firma no significa necesariamente una infección, pero si la

detección está en el protocolo RDP (puerto 3389)

Intrusions Monitored

#	Intrusion Name	Intrusion Type	Severity	Counts
1	Backdoor.DoublePulsar	Malware	Critical	20,843
2	tcp_dst_session	Anomaly	Critical	2,896
3	ip_dst_session	Anomaly	Critical	2,883
4	H-worm.Botnet		Critical	207
5	tcp_syn_flood	Anomaly	Critical	27
6	Apache.Commons.Collection.InvokerTransformer.Code.Execution	OS Command Injection	Critical	13
7	Linear.eMerge.card_scan_decoder.php.Command.Injection		Critical	3
8	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution		Critical	1
9	Mirai.Botnet		High	7
10	MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	Information Disclosure	Medium	214
11	TCP.Out.Of.Range.Timestamp	DoS	Low	3,258,711
12	TCP.Overlapping.Fragments	Buffer Errors	Low	8,235
13	HTTP.Request.Smuggling	Permission/Priviledge/Access Control	Low	5,165
14	NBSS.Invalid.Fragment	Anomaly	Low	62
15	TCP.Bad.Option.Length	Anomaly	Low	30
16	TCP.Window.Size.Zero.DoS	DoS	Low	8

Ilustración 104. Fragmento de reporte de alertas IPS-Propia de autores.

Después de identificar los riesgos y las firmas potenciales se configura el perfil de seguridad IPS que funciona como detección y contención de ataques, se configuro dos políticas una bloqueando todas las firmas catalogadas como altas y críticas y la otra tomando la acción por default que indica el fabricante Fortinet para las firmas bajas, medias e informativas con el fin de brindar mayor seguridad a la red de la organización.

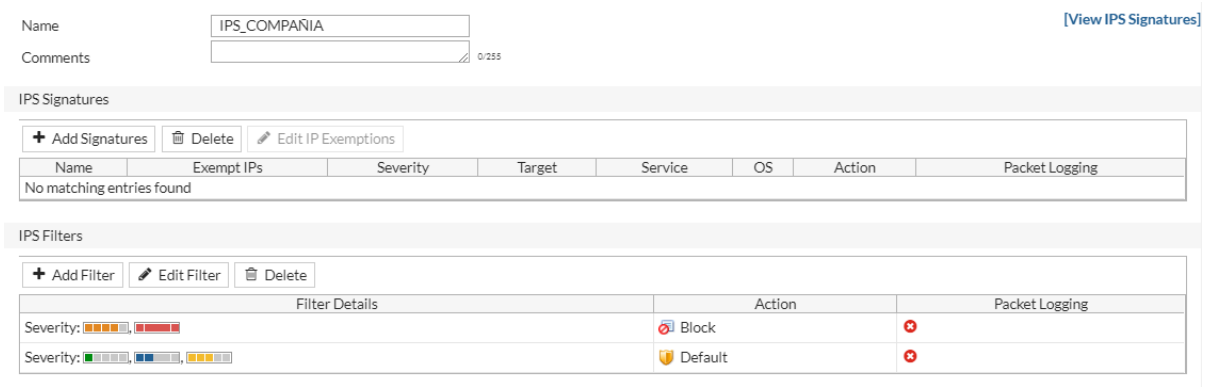


Ilustración 105. Perfil IPS en modo bloqueo-Propia de autores.

Así mismo este perfil analizara 13362 firmas que pertenece a la base de datos que tiene el firewall y que se actualiza con FortiGuard.

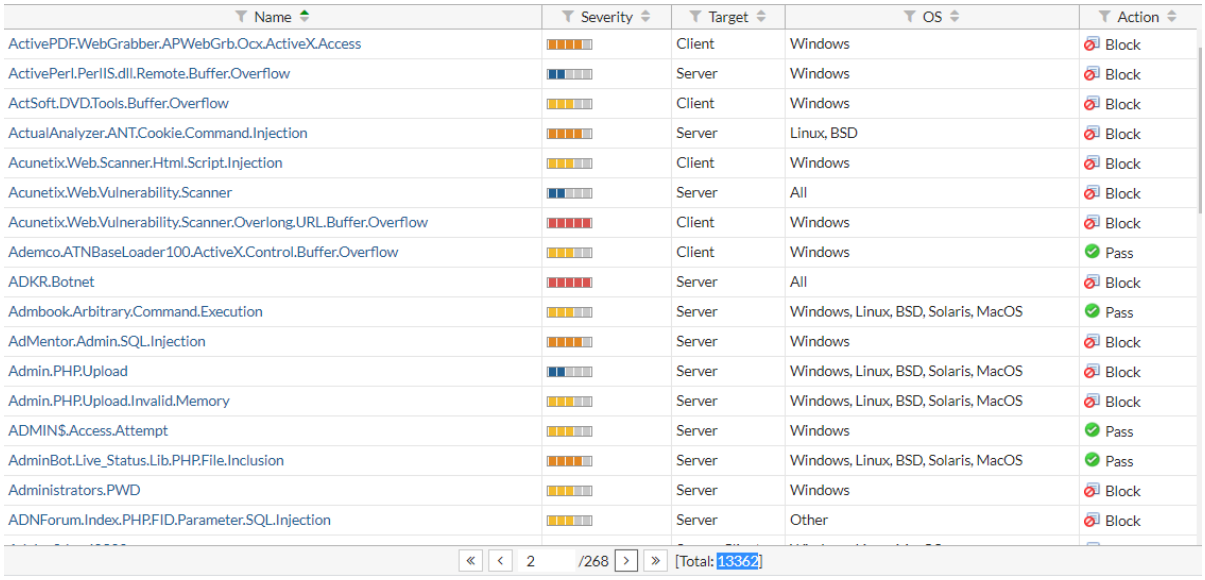


Ilustración 106. Firmas bloqueadas y permitidas-Propia de autores.

10.3.5 Implementación Autenticador FortiAuthenticathor

Para la implementación del dispositivo se llevó acabo las siguientes configuraciones con el fin de realizar la integración entre el directorio activo y el Firewall.

A continuación, se detalla el funcionamiento de dispositivo Autenticador en la organización, el cual su función principal es la gestión y control de usuarios.

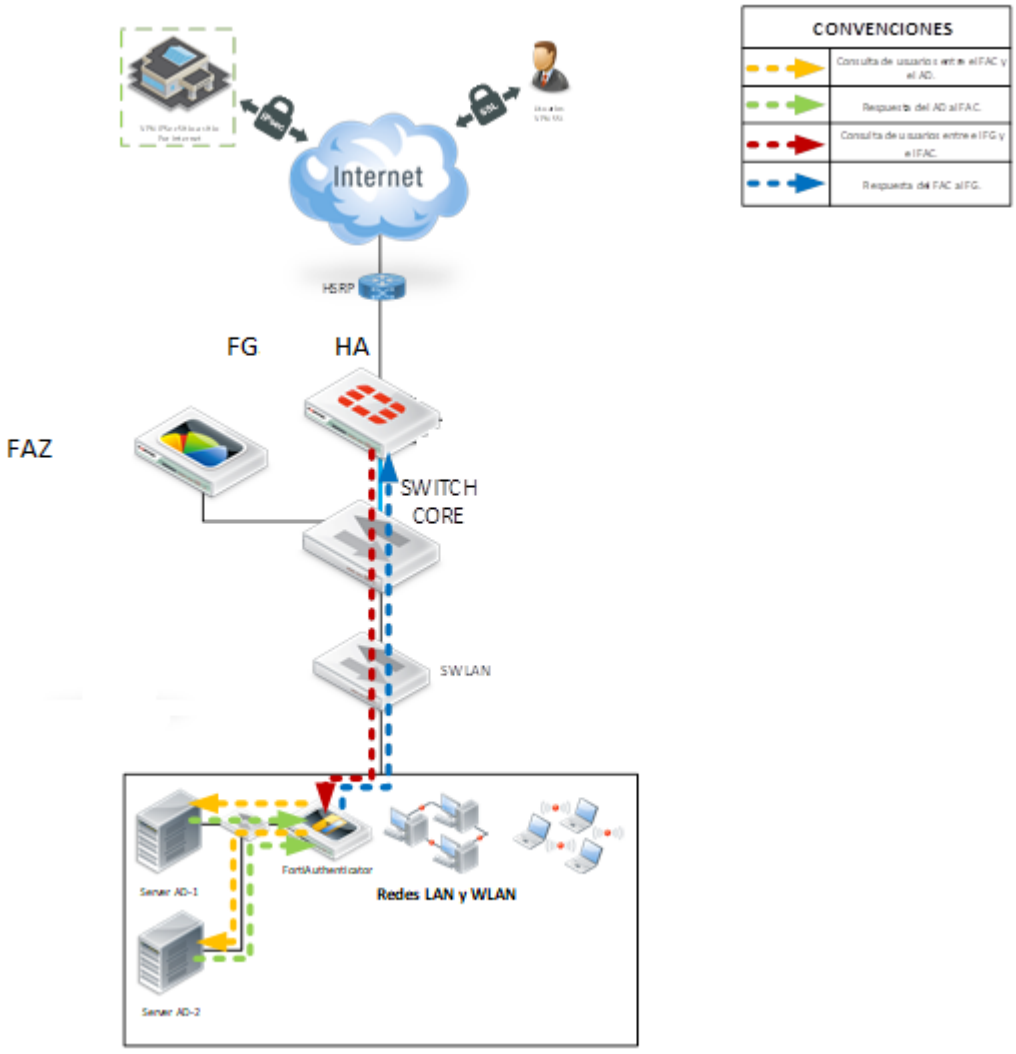


Ilustración 107. Flujo de funcionamiento autenticador Fortinet-Propia de autores.

En la imagen anterior se evidencia que el Autenticador el cual se instala en el medio de los directorios activos y el firewall.

Para conexión al directorio activo el Autenticador lo maneja a través del LDAP y así podrá visualizar las unidades organizaciones, y para la integración del Firewall con el Autenticador se realizó a través del FSSO para la navegación de los usuarios, con estas configuraciones evitamos el procesamiento del firewall y mitigar fugas de información controlándolo con los usuarios del AD.

Para la integración del directorio activo y el firewall, es necesario lo siguiente:

Crear un usuario con privilegios de lectura del árbol completo del directorio activo, para que el Autenticador sea capaz de leer los eventos de logon que lleguen al servidor. Suministrar a los ingenieros el usuario, la clave y la dirección IP del Directorio activo, así como su nombre de NetBios.

El servicio de DHCP se debe tener completamente sincronizado con el de DNS, de manera tal que, si un equipo cambia de IP a otra, el DNS actualice en forma inmediata el registro con los datos de hostname y nueva IP entregada por el DHCP.

Todos los equipos de la red deben tener habilitado el servicio "Registro Remoto", se recomienda crear una GPO en el dominio para que se asegure que todos los equipos del dominio tengan el servicio activo e iniciando de forma automática.

El tiempo de replicación entre servidores Domain Controller debe ser inmediato (se recomienda no más de 1 segundo), dado que todos los eventos que se registren en cada DC deben poder verse desde el DC principal donde se instale el agente FSSO.

Se debe asegurar conectividad Full entre el servidor Domain Controller donde se instale el agente y todos los hosts de la red mediante los puertos de NetBios.

Adicionalmente, en el servidor se debe garantizar que la configuración del firewall de Windows y del software antivirus se puedan agregar excepciones sobre los siguientes puertos:

TCP/3268 - LDAP group membership lookup (Global Catalog)

TCP/389 - LDAP domain controller discovery and group membership lookup

UDP/8002 – DC Agent keepalive and push logon info to CA

TCP/8000 – CA keepalive and push logon info to Fortigate

TCP/8000 - NTLM

UDP/53 – CA DNS

TCP/445 – Workstation check, polling mode (preferred method)

TCP/135, TCP/139, UDP 137 – Workstation check, polling mode (fallback method)

TCP/445 – Remote access to logon events

TCP/389 – group lookup using LDAP

TCP/3268 – group lookup using LDAP with global catalog

TCP/636 - Group lookup using LDAPS

UDP/53 – Resolve FSSO server name

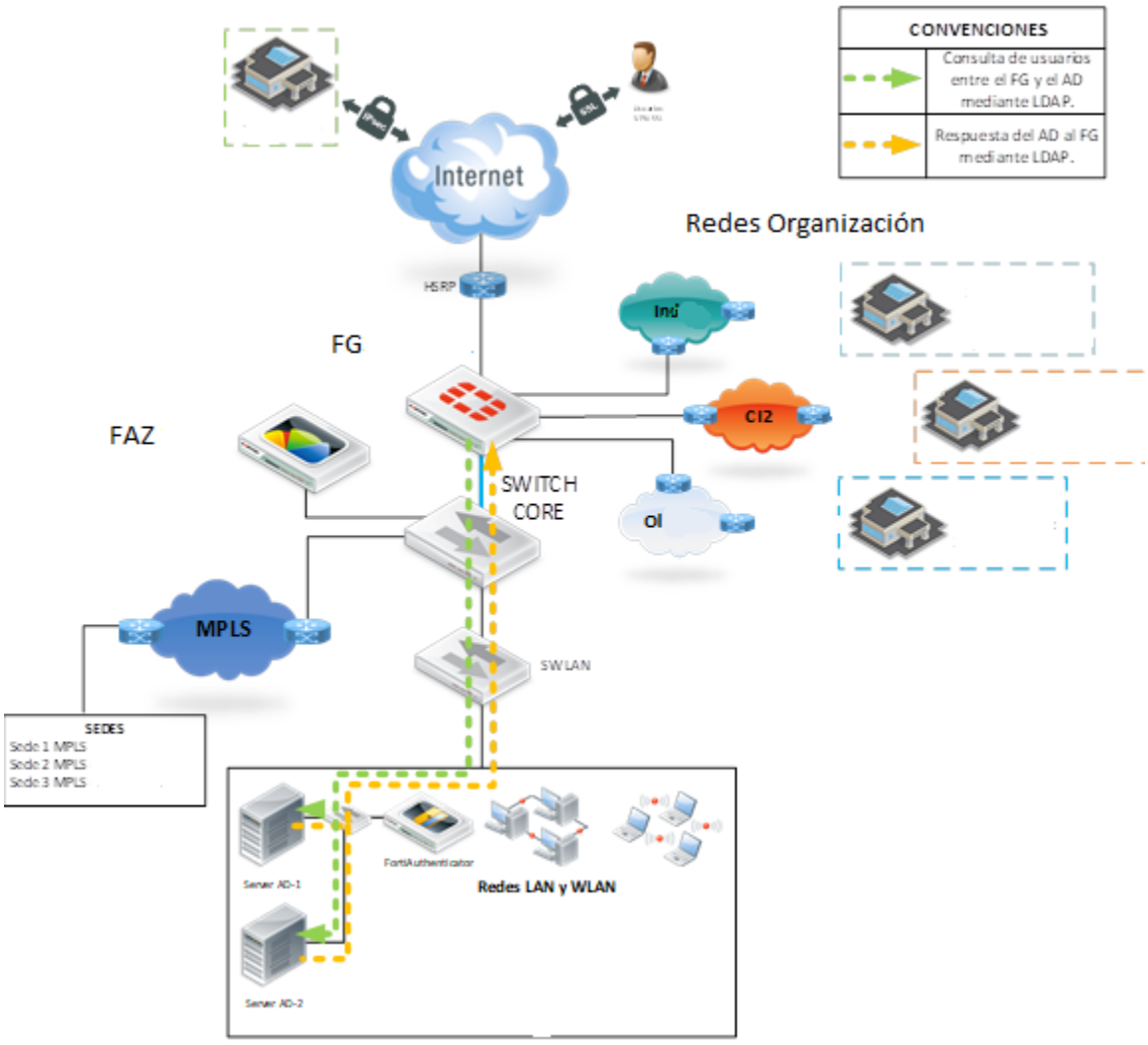


Ilustración 108. Flujo de conectividad unidades organizativas-Propia de autores.

En el autenticador se realizó la configuración a través de conexión LDAP para lograr la integración del directorio activo y poder visualizar su unidad organizativa.

Se configura un servidor LDAP apuntando al directorio activo de la organización con el usuario y contraseña de lectura.

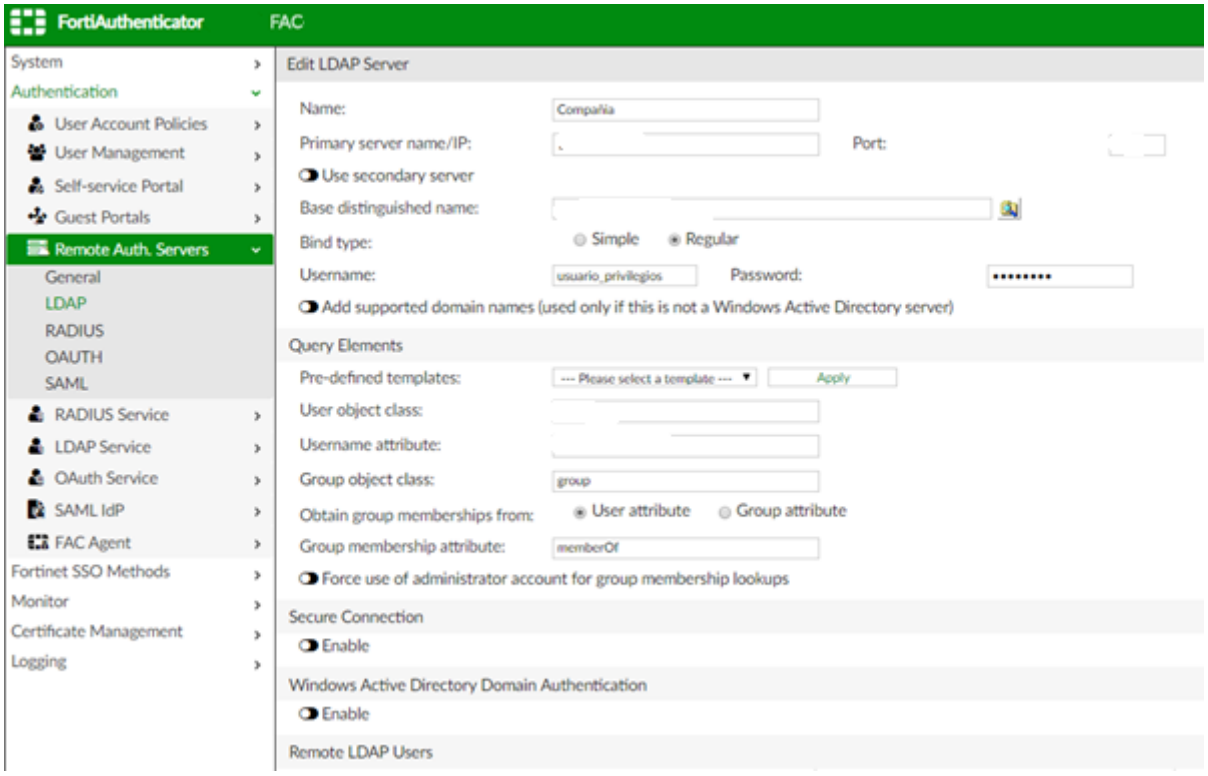


Ilustración 109. Configuración de servidor LDAP-Propia de autores.

Para la integración del Autenticador con el Firewall se realizado a través de Single Sign-On (FSSO) con el fin de consultar los grupos creados en el directorio activo para la salida de navegación de la compañía, para esto se requiere que el firewall tenga conectividad al autenticador a través de los puertos TCP 8000 y 8002 UDP, (estos puertos están por defecto, pero se pueden modificar) y una contraseña.

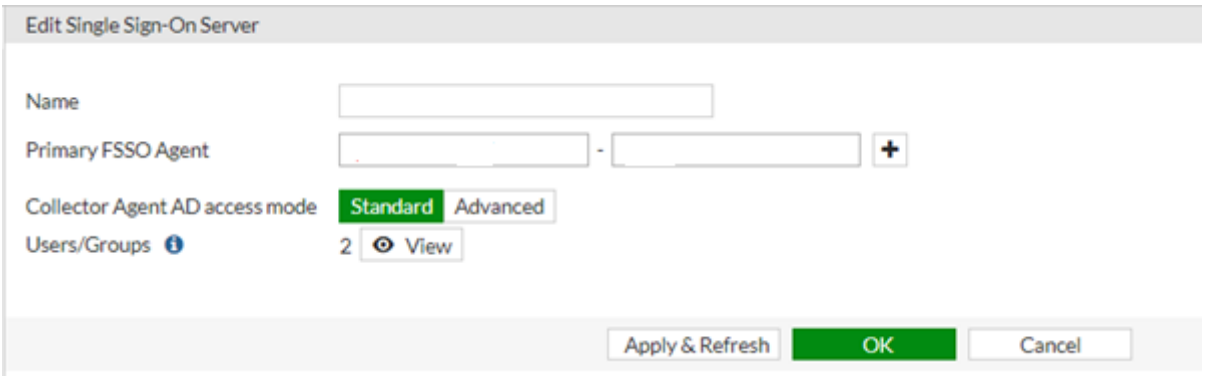


Ilustración 110. Configuración Firewall FSSO para la integración FAC-Propia de autores.

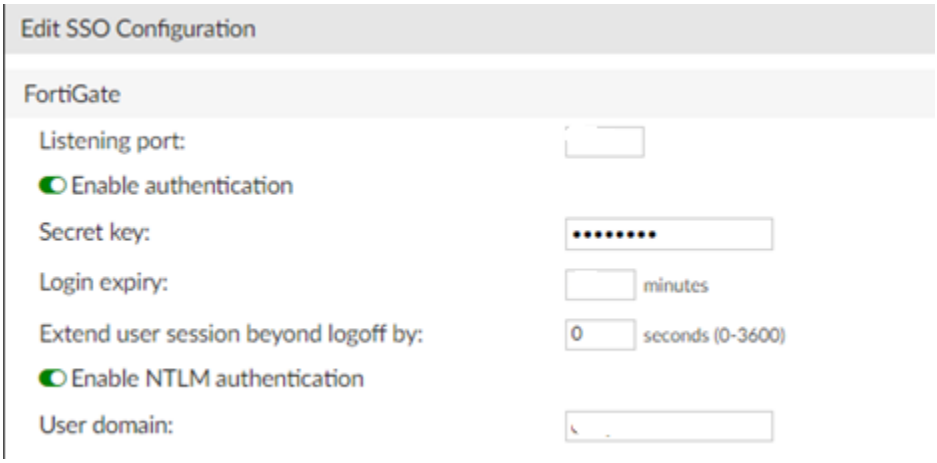


Ilustración 111. Configuración FAC para integración con firewall-Propia de autores.

Se configuró las fuentes autorizadoras para que los eventos de logon y logoff

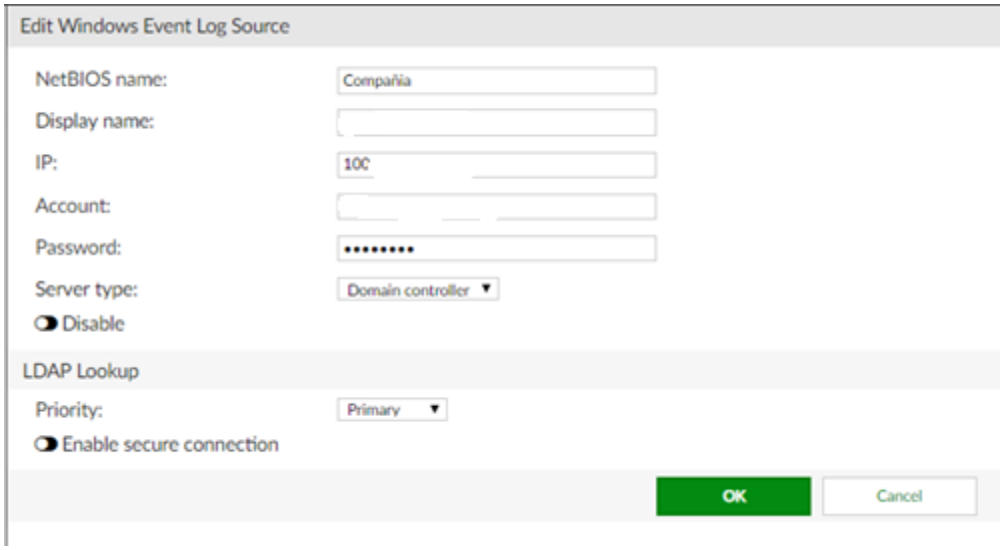


Ilustración 112.Configuracion FAC para tomar NETBIOS-Propia de autores.

Se crearon los filtros para los grupos de navegación con el fin que el Firewall no consulte todo el árbol del directorio activo evitando que se genere alto consumo de CPU y memoria del dispositivo.

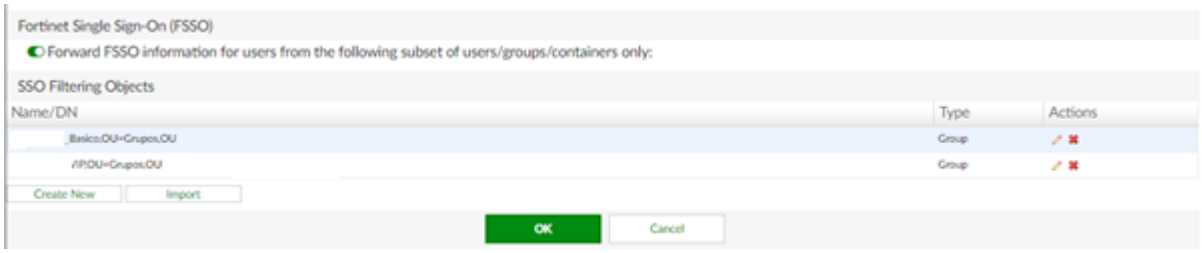


Ilustración 113.Filtrado de unidades organizativas-Propia de Autores.

10.4 Pruebas

10.4.1 Pruebas VPN

Para las pruebas de la VPN Client to Site se realizaron por medio de una conexión de internet a través de la aplicación forticlient. Se verifica que se establezca la conexión de manera exitosa y adicionalmente se realizaran pruebas de ping y traceroute y para garantizar los accesos requeridos.

Se toman capturas en el firewall evidenciando el paso del tráfico correcto y verificando la conexión desde el cliente VPN que se realiza a través del puerto UDP 500 que corresponde al IKE el cual garantiza el tráfico de la comunicación por medio de internet vaya cifrado.

Se realiza la configuración de los parámetros en el cliente VPN con el fin de realizar la conexión remota a la red e la organización.

Ilustración 114. VPN cliente sitio forticlient-Propia de autores.

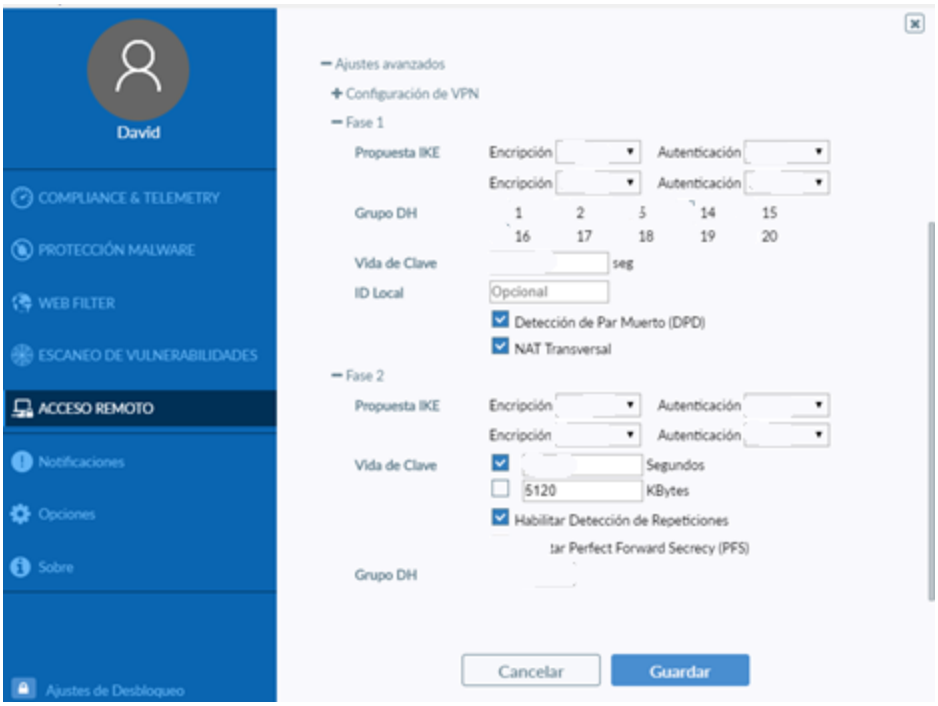


Ilustración 115. Fase 1 y Fase 2 forticlient-Propia de autores.

Se realiza la respectiva conexión con el usuario correspondiente creado desde el directorio activo.

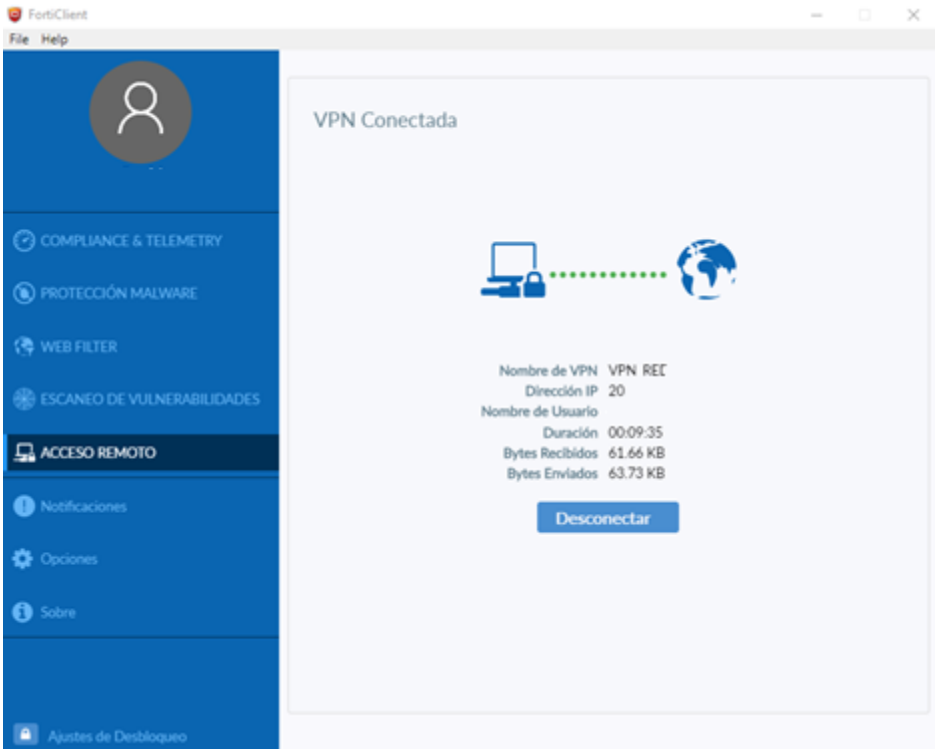


Ilustración 116. Conexión exitosa forticlient-Propia de autores.

En el Firewall se evidencia el tunnel creado para la VPN de la compañía, el cual se encuentra establecido y en estado UP y con data de entrada y de salida.

Ilustración 117. Estado de conexión VPN en firewall-Propia de autores.

Se verifica conectividad a los servicios configurados desde el equipo cliente hacia red de la organización.

```
C:\Users\David>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet 2:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::555d:d286:8888:35d8%11
   Dirección IPv4. . . . . . . . . . . . : 20.
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
```

Ilustración 118. Direccionamiento asignado al PC por la VPN-Propia de autores.

```
C:\Users\     >ping 10.

Haciendo ping a 10.      con 32 bytes de datos:
Respuesta desde 10.      : bytes=32 tiempo=82ms TTL=127
Respuesta desde 10.      : bytes=32 tiempo=53ms TTL=127
Respuesta desde 10.      : bytes=32 tiempo=58ms TTL=127
Respuesta desde 10.      : bytes=32 tiempo=106ms TTL=127

Estadísticas de ping para 10.      :
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 53ms, Máximo = 106ms, Media = 74ms

C:\Users\     >
```

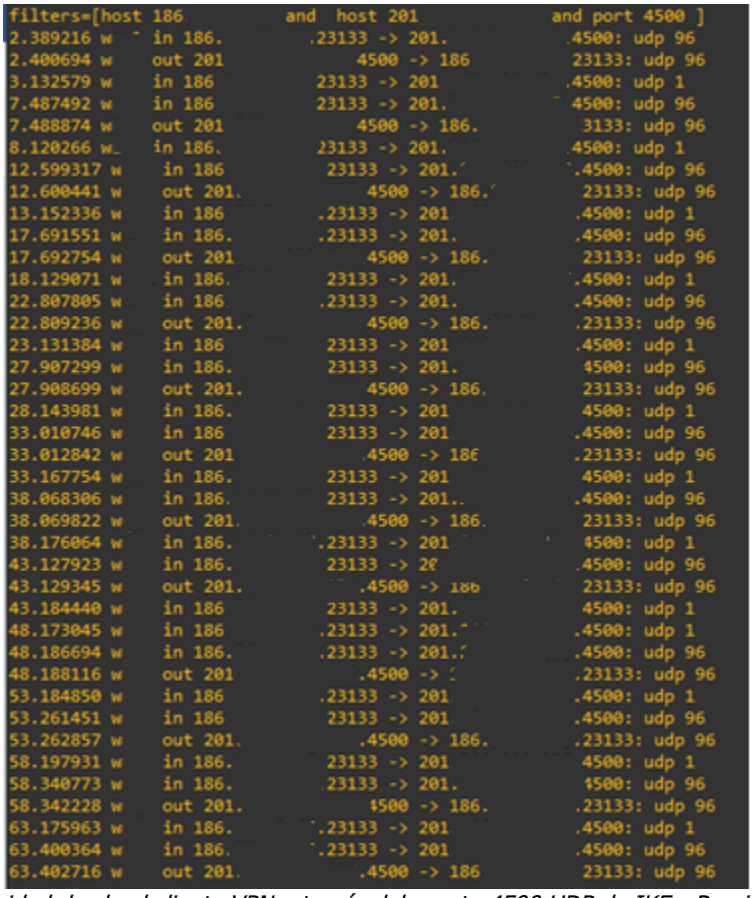
Ilustración 119. Prueba de conectividad a un servicio por VPN-Propia de autores.

```
C:\Users\.      tracert -d 10.

Traza a 10.       sobre caminos de 30 saltos como máximo.

  1    83 ms    59 ms    76 ms  169.
  2   932 ms    68 ms    61 ms  10.

Traza completa.
```

Ilustración 120. Saltos realizados de la VPN al destino-Propia de autores.

```
filters=[host 20.        and  host 10.      ]
31.599002 VPN_CO  in 20.        -> 10        icmp: echo request
31.599200 Vl       out 20.        -> 10        icmp: echo request
31.599244 i       out 20.        -> 10.       icmp: echo request
31.599444 V        in 10..      -> 20.        icmp: echo reply
31.599561 VPN_CO  out 10.      -> 20.        icmp: echo reply
32.667290 VPN_CC  in 20.        -> 10.       icmp: echo request
32.667479 \        out 20.        -> 10.      : icmp: echo request
32.667518 i.      out 20.        -> 10.      : icmp: echo request
32.667767 V        in 10.       -> 20.        icmp: echo reply
32.667906 VPN_CC  out 10.      -> 20.       : icmp: echo reply
33.643009 VPN_CO  in 20..       -> 10.       icmp: echo request
33.643196 V        out 20.        -> 10.       icmp: echo request
33.643235 i       out 20.        -> 10.       icmp: echo request
```

Ilustración 121. Captura de tráfico desde el firewall de la conexión VPN-Propia de autores.



Conectividad desde el cliente VPN a través del puerto 4500 UDP de IKE - Propia de los autores.

Conectividad del usuario a la VPN desde el Firewall.

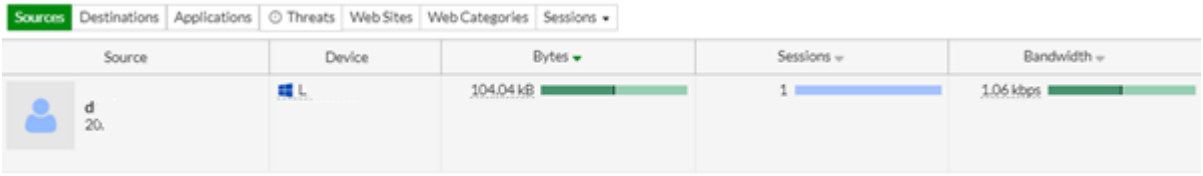


Ilustración 122. Evidencias de tráfico consumido por el usuario-Propia de autores.

10.4.2 Pruebas de filtrado de contenido

Se realizaron pruebas de navegación de los perfiles de filtrados de contenido configurados a través de conexión de la VPN:

Se realiza la conexión a la VPN donde se habilito que el usuario navegara a través de la red de la organización.

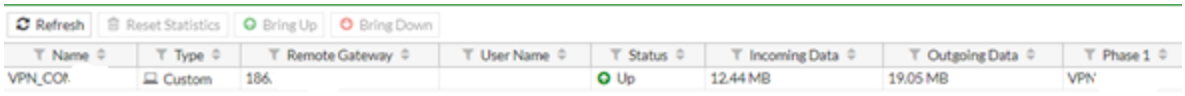


Ilustración 123. VPN para test filtrado de contenido-Propia de autores.

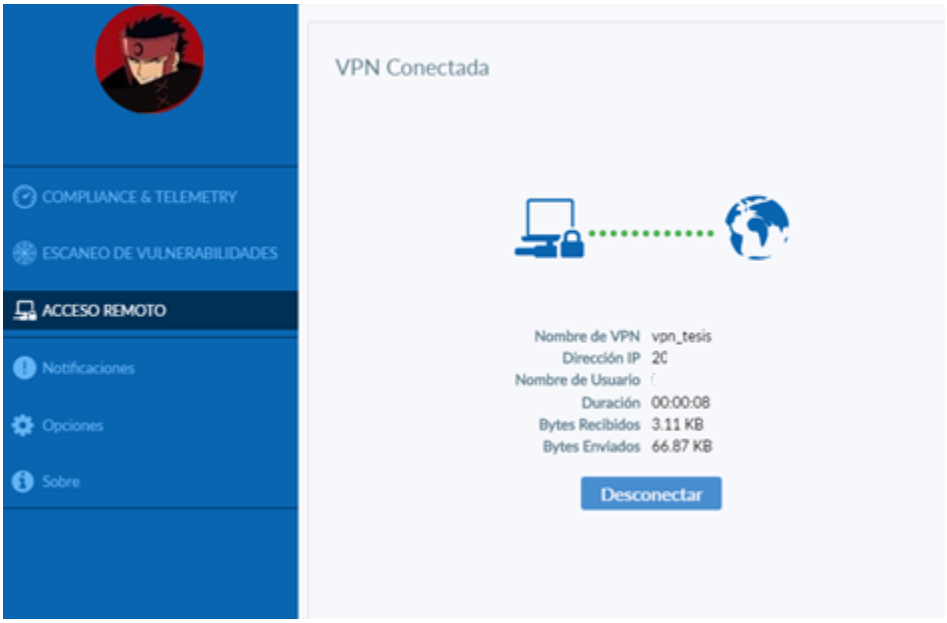


Ilustración 124. Conexión de cliente VPN al firewall-Propia de autores.

Se intenta acceder a sitios pornográficos lo cual la compañía lo tiene restringido.

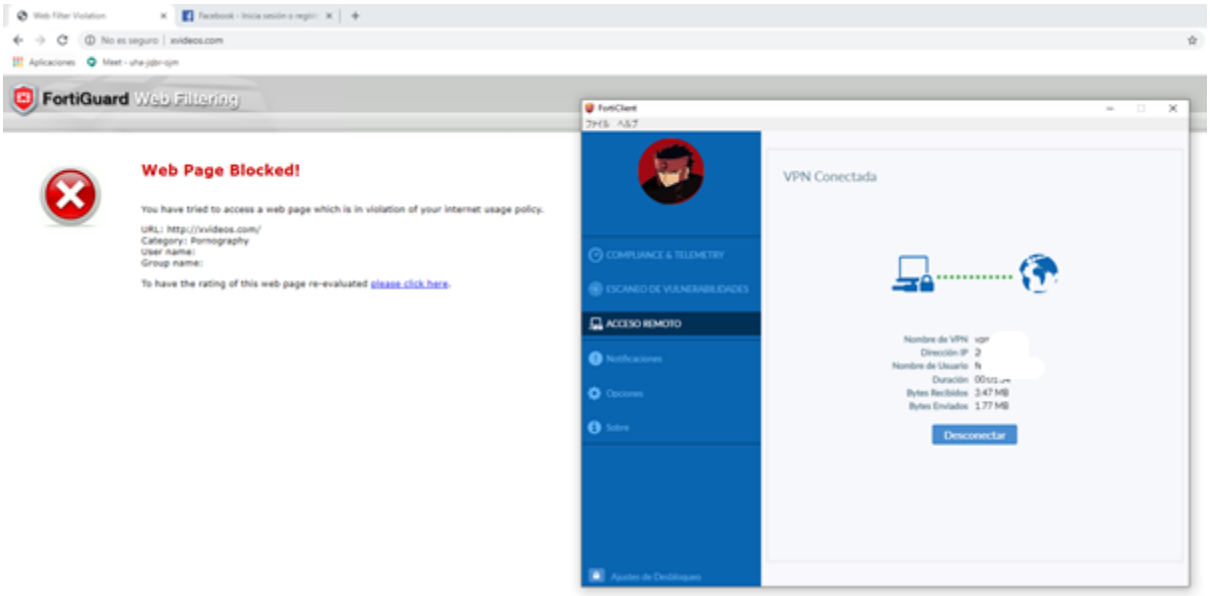


Ilustración 125. Prueba de filtrado de contenido categoría adultos-Propia de autores.

También se registra intentos de conexión a tiendas online en este caso Amazon la cual la empresa tiene restringido el acceso.

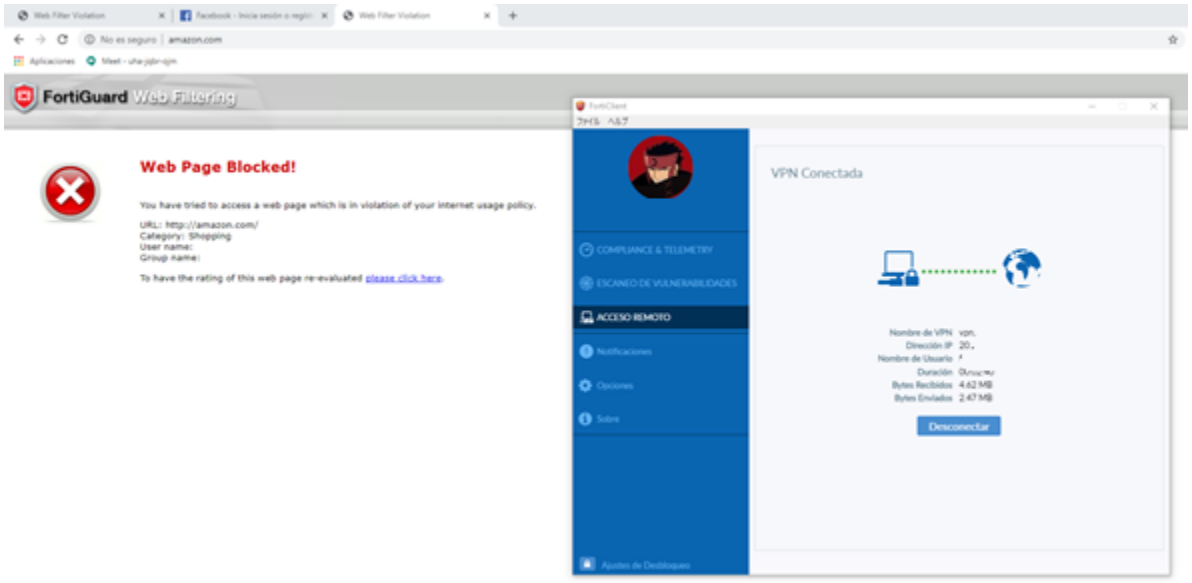


Ilustración 126. Prueba de filtrado de contenido categoría compras-Propia de autores.

Para el perfil de VIP tiene la categoría de redes sociales sin restricción.

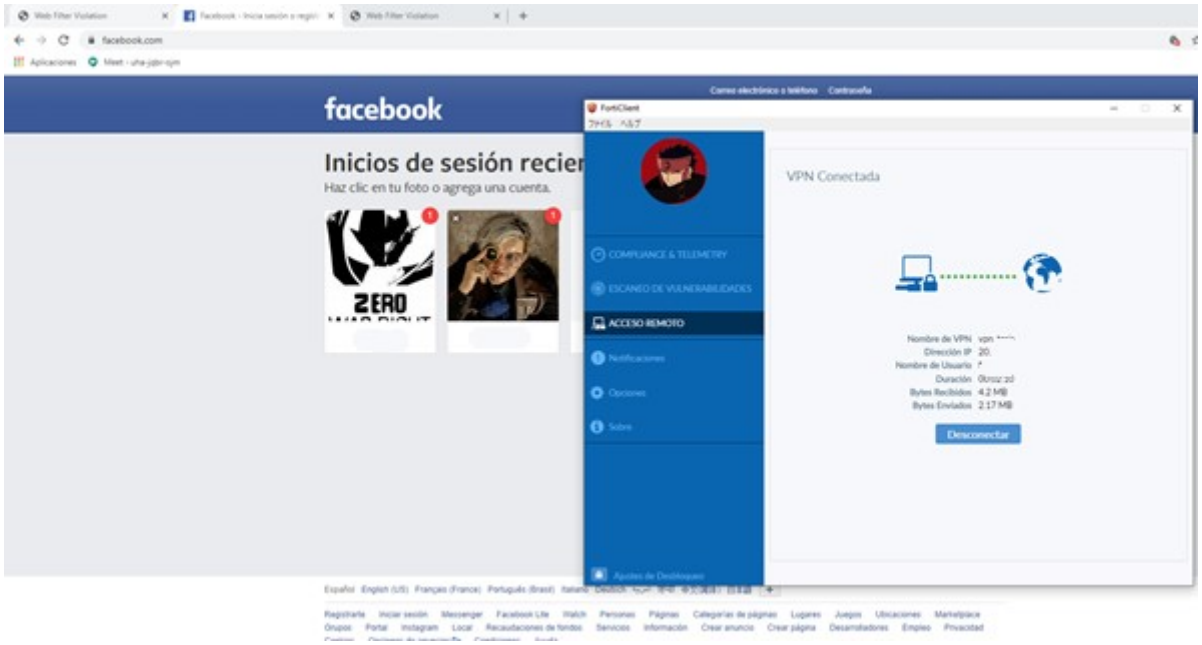


Ilustración 127. Prueba de filtrado de contenido categoría redes sociales-Propia de autores.

En el firewall muestra los eventos de la política creada para conceder el permiso del usuario con el fin de navegar por el internet de la compañía.

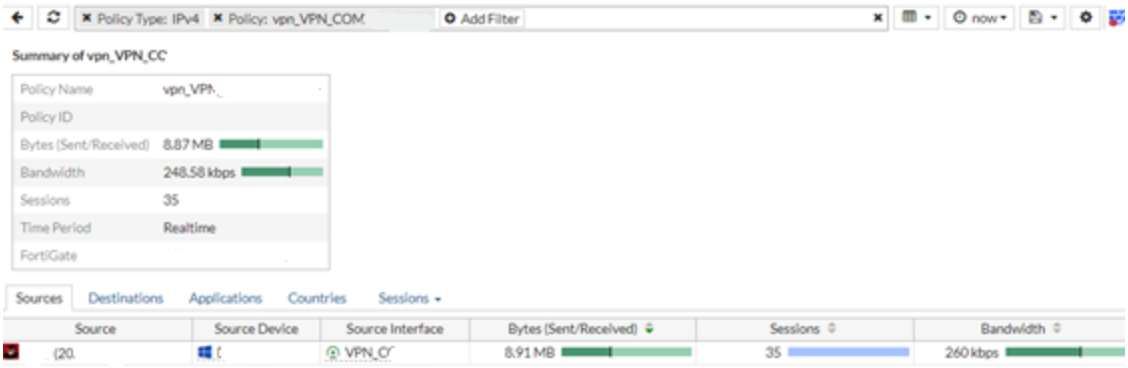


Ilustración 128. Eventos de VPN a política de filtrado-Propia de autores.

Se evidencio el tráfico de navegación que genero el usuario en repositorio de logs (FortiAnalyzer) como se muestra a continuación.

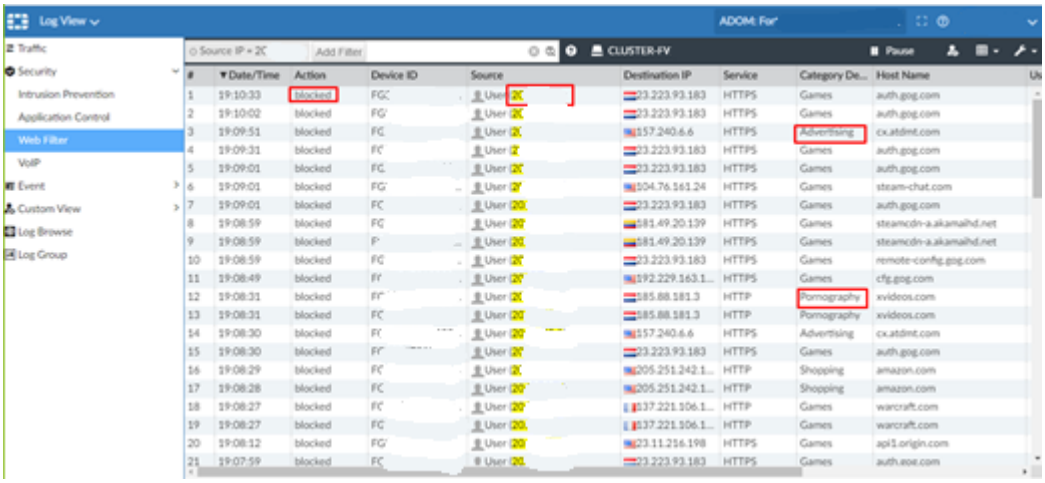


Ilustración 129. Identificación de bloqueo por categorías en Analizador de logs-Propia de autores.

10.4.3 Pruebas de perfil de seguridad IPS

Se realizaron las siguientes pruebas de los perfiles IPS en el equipo firewall:

- Ataques tipo SQL injection sobre las ip 190.xxx.xxx.xxx de los ambientes LIFE RAY.
- Escaneo de servicios sobre las ip 190.xxx.xxx.xxx de los ambientes L-XY.

Las pruebas se llevaron a cabo sobre las publicaciones de L-XY

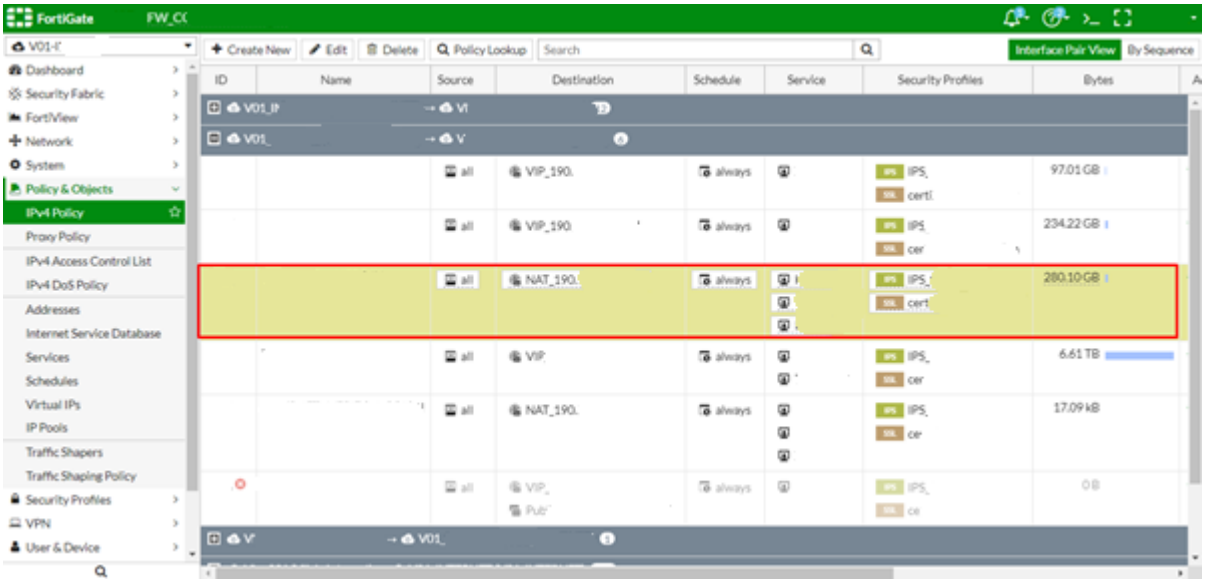


Ilustración 130. Política de IPS a validar-Propia de autores.

Pruebas generadas desde la IP

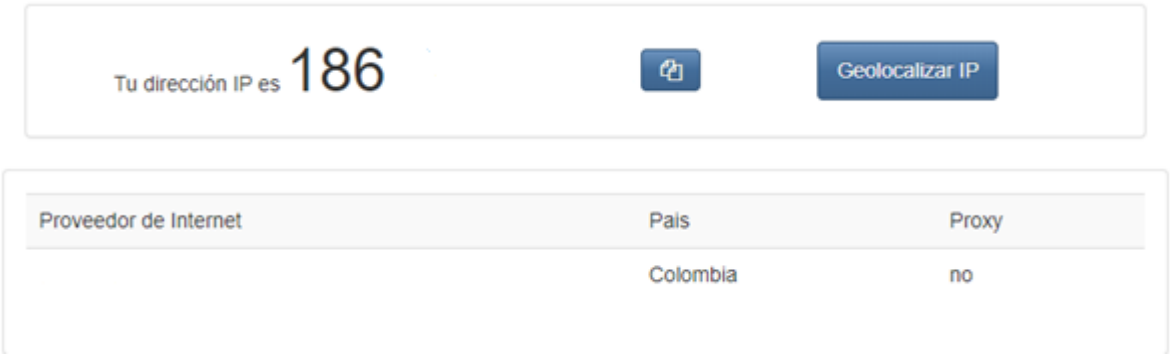


Ilustración 131. IP publica personal de origen de prueba-Propia de autores.

Para las pruebas se utilizó la herramienta Kali Linux.

- NMAP
- SQLMAP

Pruebas realizadas con NMAP

Destino: 190.xxx.xxx.xxx

```
root@kali:~# nmap -T4 -A -v 190.
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-11 21:22 -05
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:22
Completed NSE at 21:22, 0.00s elapsed
Initiating NSE at 21:22
Completed NSE at 21:22, 0.00s elapsed
Initiating Ping Scan at 21:22
Scanning 190.            [4 ports]
Completed Ping Scan at 21:22, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:22
Completed Parallel DNS resolution of 1 host. at 21:22, 0.18s elapsed
Initiating SYN Stealth Scan at 21:22
Scanning 190.            [1000 ports]
Discovered open port 443/tcp on 190.
Discovered open port 80/tcp on 190.
Completed SYN Stealth Scan at 21:22, 4.37s elapsed (1000 total ports)
Initiating Service scan at 21:22
Scanning 2 services on 190.
Completed Service scan at 21:25, 139.36s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 190.
Initiating Traceroute at 21:25
Completed Traceroute at 21:25, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 21:25
Completed Parallel DNS resolution of 2 hosts. at 21:25, 0.10s elapsed
```

Ilustración 132. Pruebas NMAP-Propia de autores.

```
SF:1\.co");
Warning: OSScan results may be unreliable because we could not find at least 1 open and
 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Device: load balancer

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.45 ms 10.
2   0.54 ms 190.

NSE: Script Post-scanning.
Initiating NSE at 21:26
Completed NSE at 21:26, 0.00s elapsed
Initiating NSE at 21:26
Completed NSE at 21:26, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 213.42 seconds
           Raw packets sent: 2043 (92.144KB) | Rcvd: 31 (1.292KB)
```

Ilustración 133. Resultado de pruebas NMAP-Propia de autores.

Registro FortiGate: Log&Report

Acción Dropped

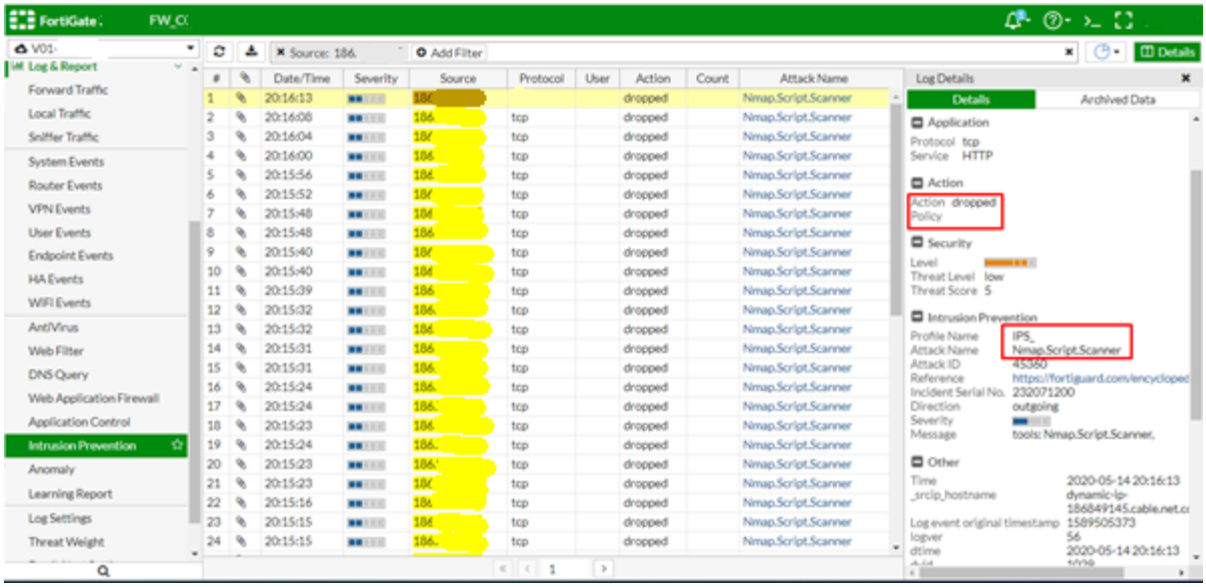


Ilustración 134. Resultado de eventos de IPS en firewall-Propia de autores.

Registro Ataques generados:

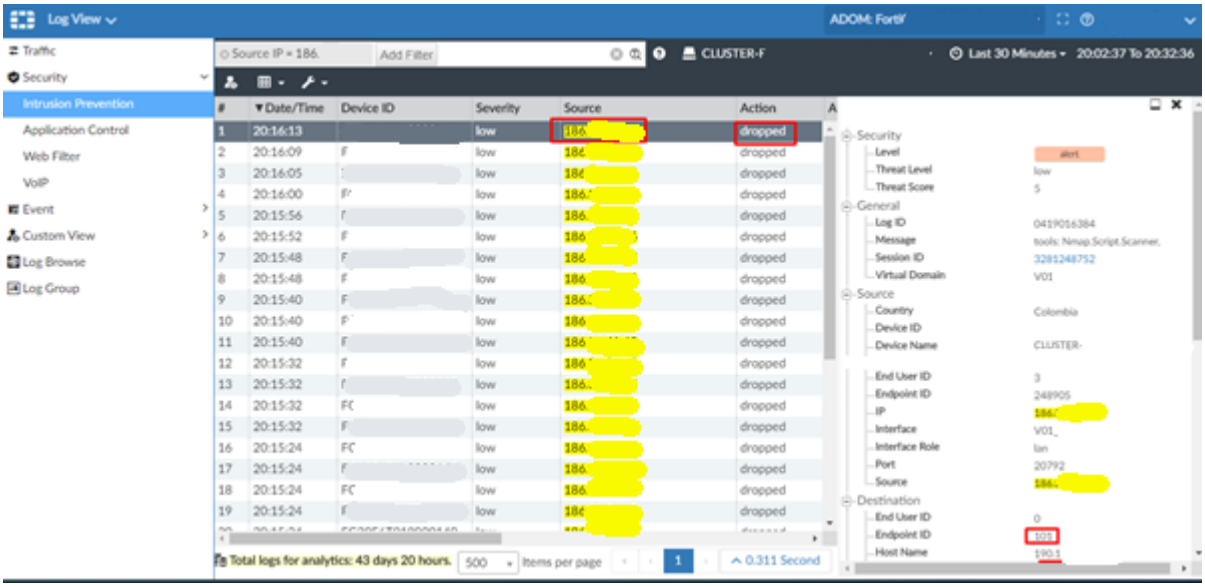


Ilustración 135. Registro de NMAP en analizador de LOGS-Propia de autores.

Tipo de Ataque detectado

- Nmap.Script.Scanner

Esto indica la detección de un intento de escaneo desde el escáner del motor de scripts Nmap. El motor de scripts Nmap se usa para sondear redes de computadoras para ver qué puertos o servicios están disponibles. Un atacante puede utilizar el motor de secuencias de comandos Nmap para identificar qué servicios está ejecutando el sistema de destino y realizar más ataques en función de sus hallazgos.

Pruebas SQLMAP

IP Destino 190.xxx.xxx.xxx

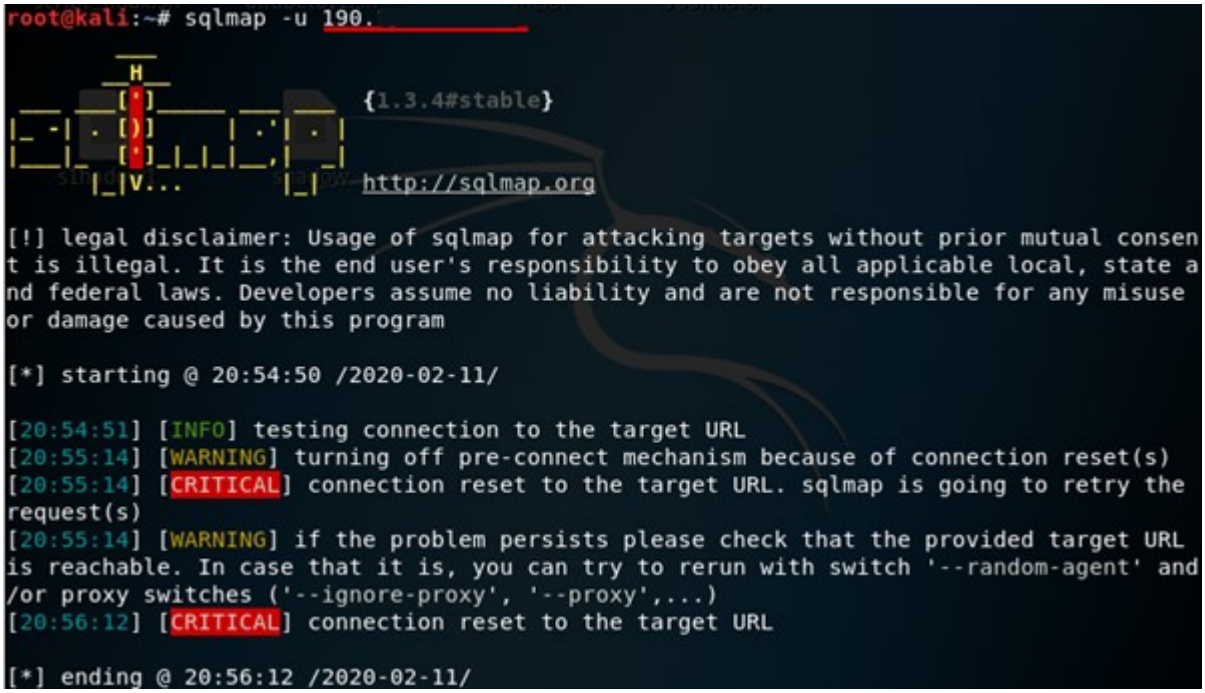


Ilustración 136. Pruebas SQLMAP a política IPS-Propia de autores.

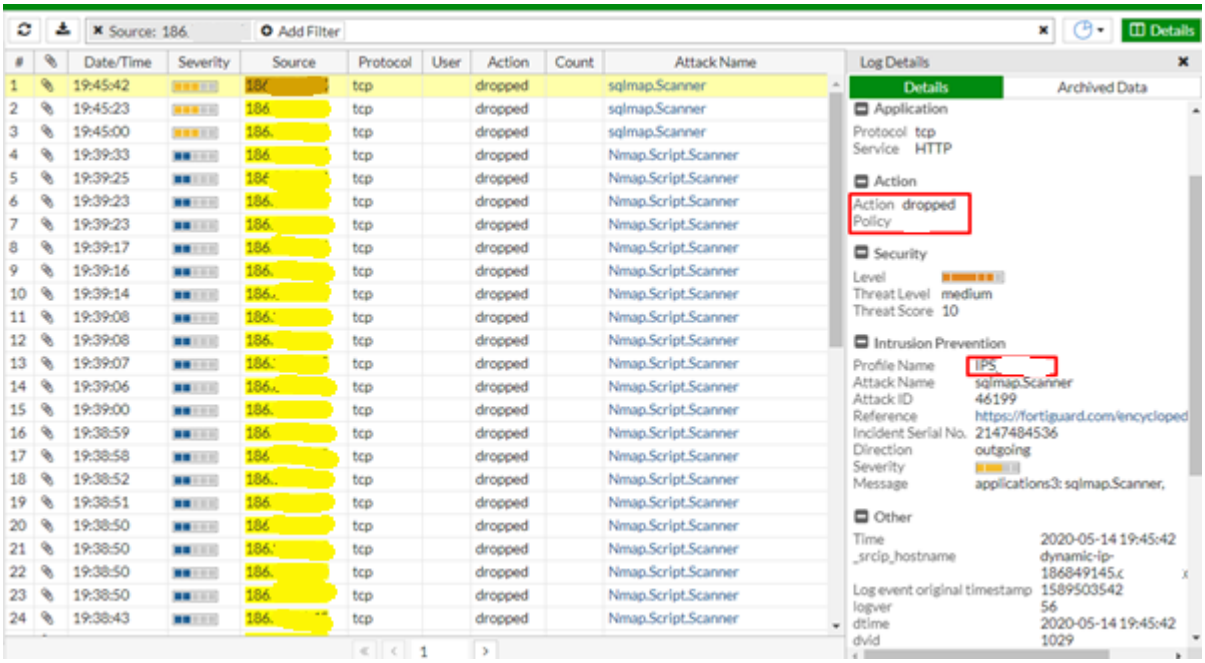


Ilustración 137. Resultado de eventos SQLMAP de IPS en firewall-Propia de autores

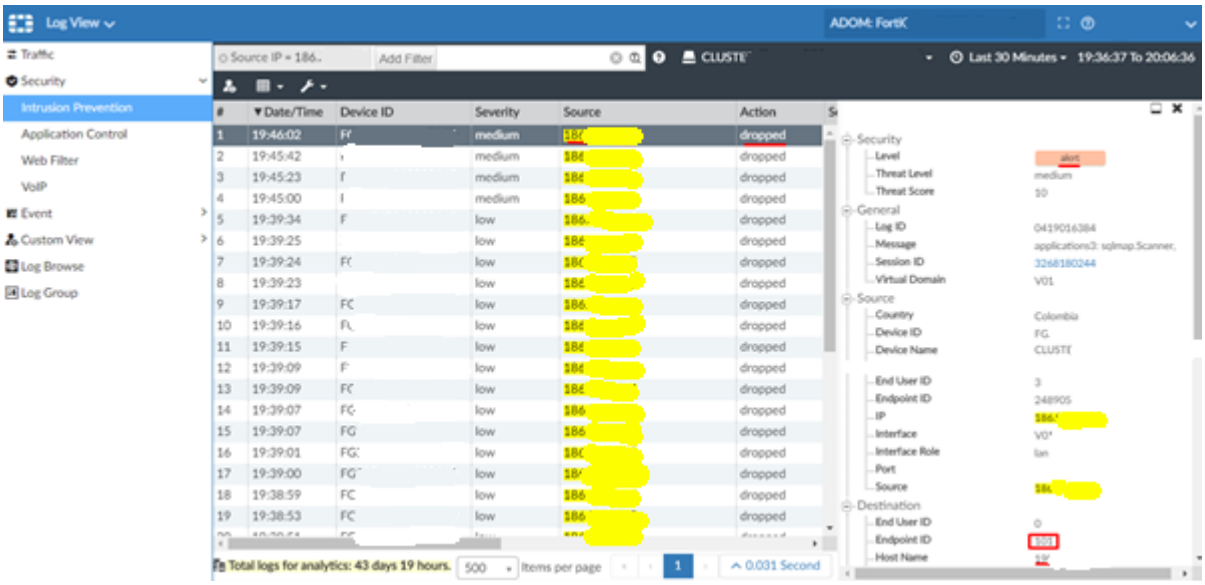


Ilustración 138. Registro de SQLMAP en analizador de LOGS-Propia de autores

Tipo de Ataques detectado

- sqlmap.Scanner

Esto indica la detección de un intento de escaneo de inyección SQL en un servidor por sqlmap Scanner.sqlmap Scanner se usa para sondear servidores web con bases de datos para ver qué sistemas son vulnerables a los ataques de inyección SQL. Un atacante puede usar el escáner para identificar que su sistema es vulnerable y realizar más ataques

en función de sus hallazgos.

10.4.4 Pruebas de servicios autenticador FortiAuthenticathor

Para las pruebas de conectividad correspondiente a la integración entre el Autenticador con el directorio activo se comprueba visualización de las unidades organizativas de los directorios activos integrados.

A continuación, se detalla los directorios activos configurados y el árbol de los directorios activos en la compañía.

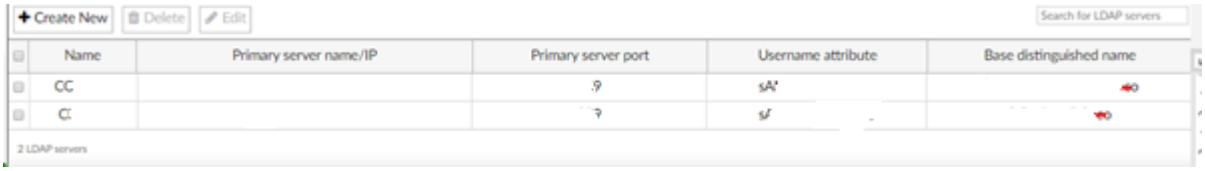


Ilustración 139. Listado de dominios- Propia de autores.

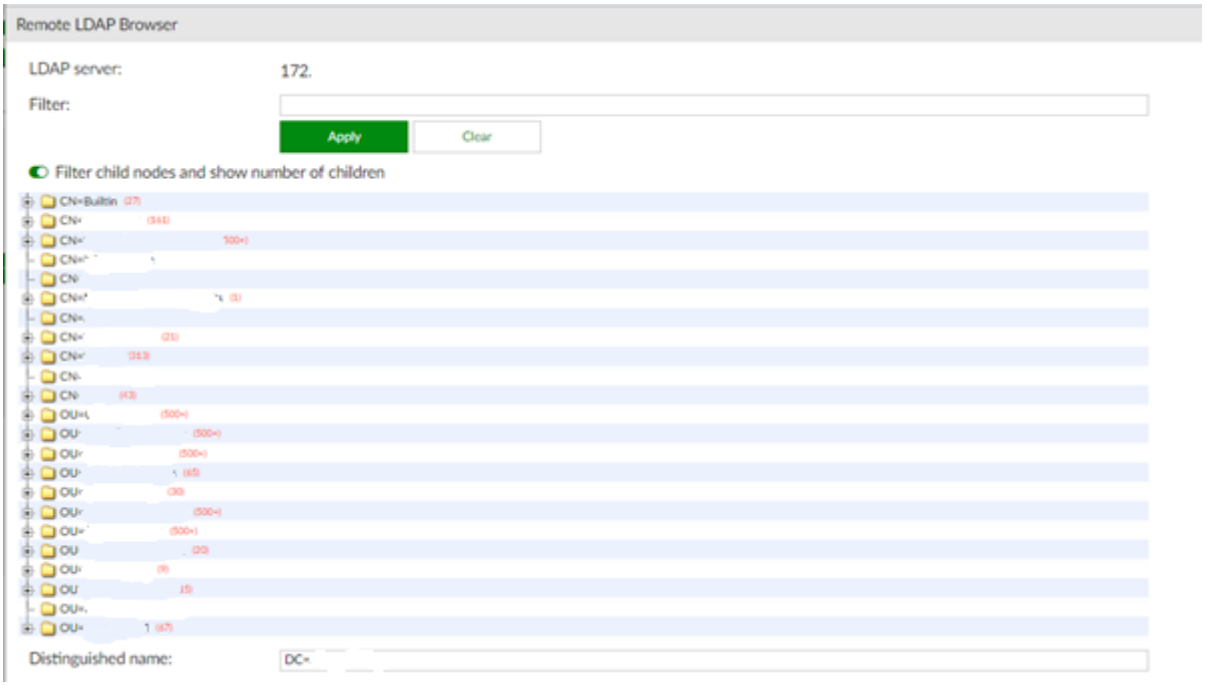


Ilustración 140. Unidades organizativas LDAP1-Propia de autores.

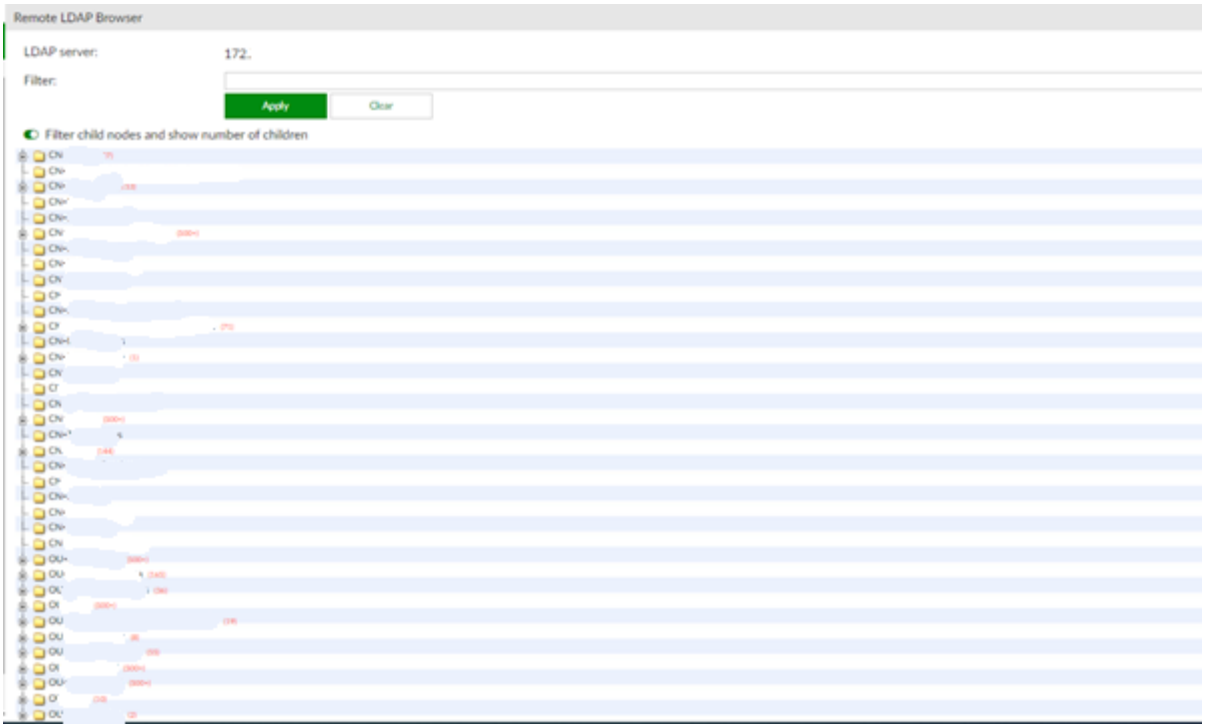


Ilustración 141,Unidades organizativas LDAP2-Propia de autores.

En la configuración correspondiente al FSSO con la integración del Firewall se visualiza el estado de las configuraciones exitosas en el firewall como se muestra a continuación.

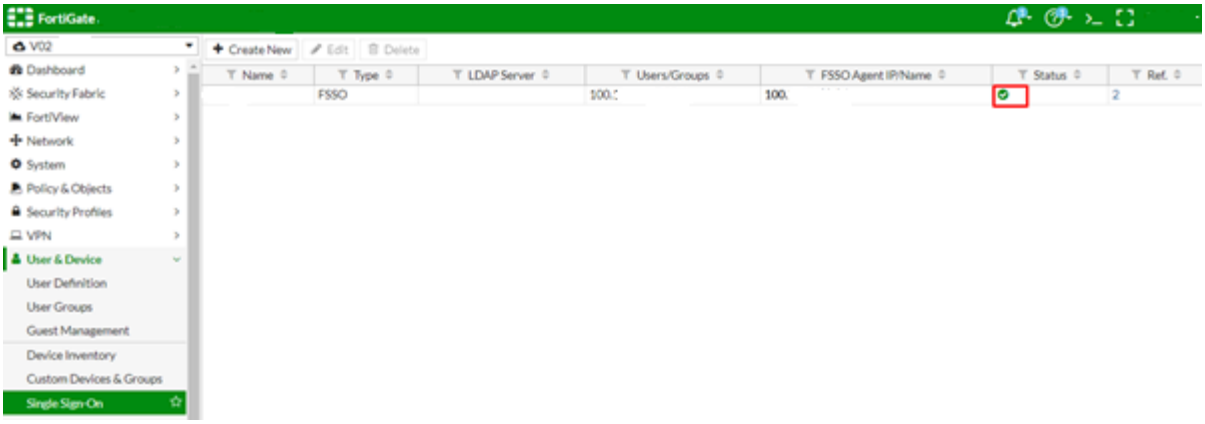


Ilustración 142. Conectividad FSSO firewall a autenticador-Propia de autores.

El en dispositivo Autenticador se visualizan los dominios conectados al directorio activo como se muestra en la siguiente imagen.

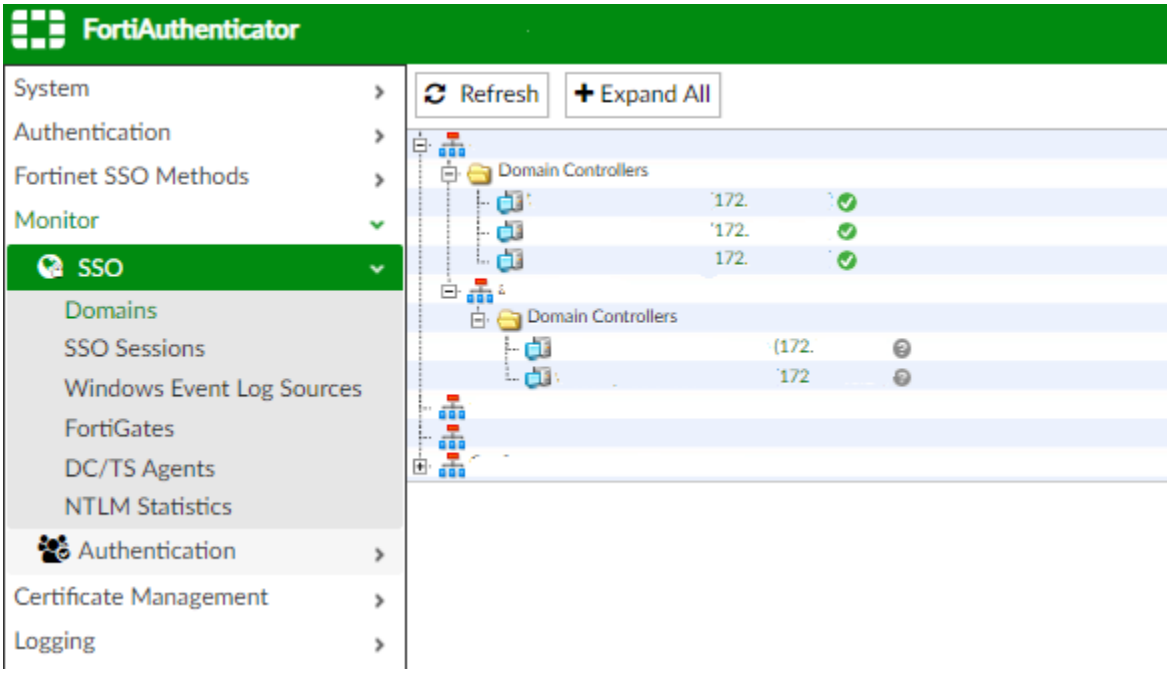


Ilustración 143. Controladores de dominio por dominios-Propia de autores

En la configuración se realizó un filtro de grupos en el autenticador con el fin de evitar procesamiento a nivel de CPU el equipo Firewall cuando se realice la consulta de los grupos del directorio activo.

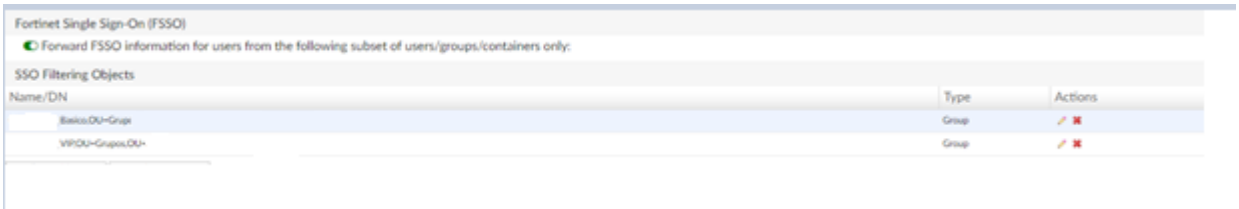


Ilustración 144. Filtrado de unidades organizativas-Propia de autores.

En el FortiGate no se debe visualizar todo el árbol del directorio activo ya que configuro el filtro solo se visualiza los grupos filtrados como se evidencia a continuación.

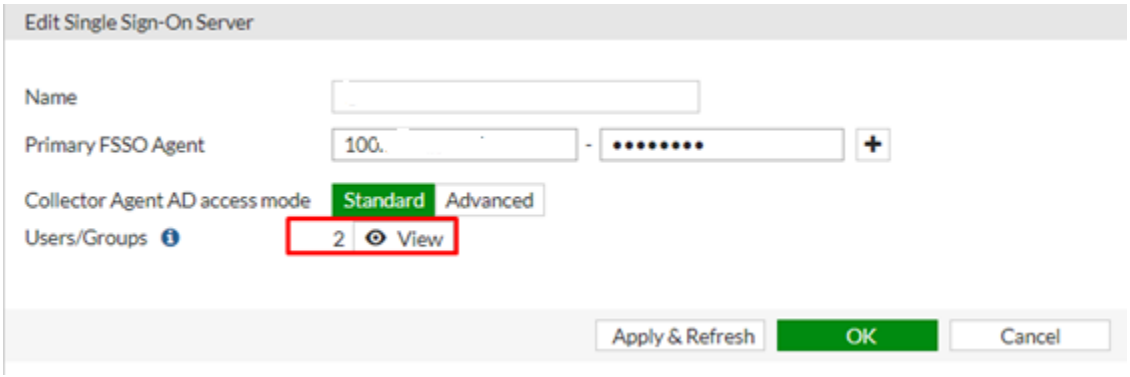


Ilustración 145. Unidades organizativas detectadas-Propia de autores.

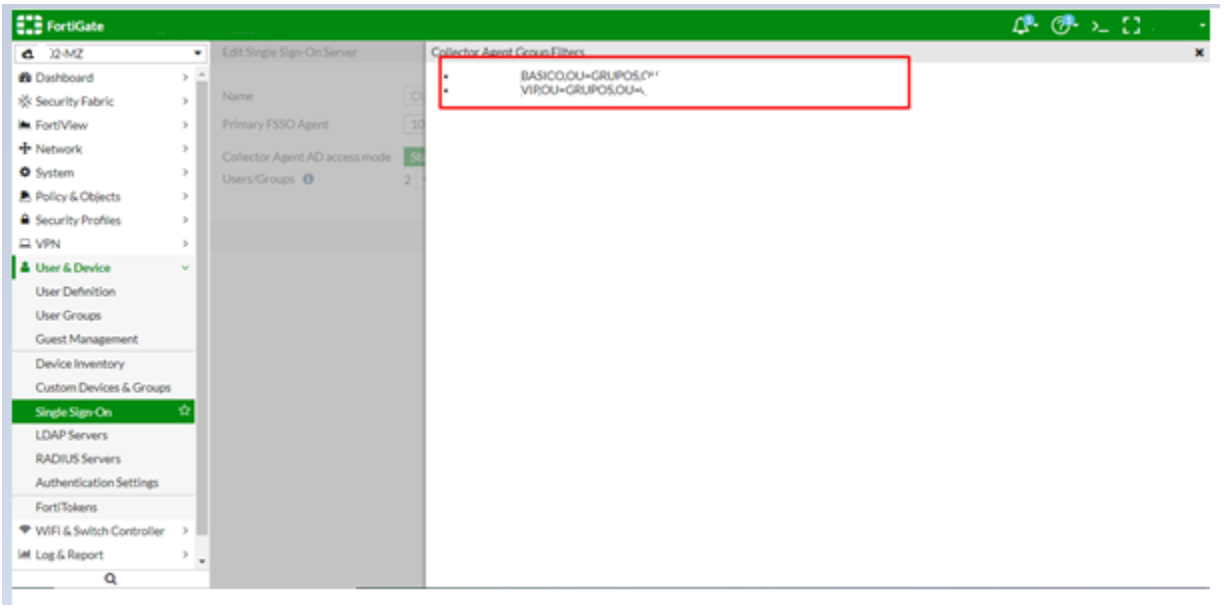


Ilustración 146. Unidades organizativas filtradas del autenticador al firewall-Propia de autores.

11. Resultados

Por medio de la implementación de dominios virtuales, se logra aislar cada uno de los servicios de la organización. Cada uno de los dominios virtuales funciona como un firewall virtual. No se presentaron inconvenientes durante la creación de cada uno de los dominios virtuales; sin embargo, el proyecto a nivel de organización sigue en proceso de implementación ya que aún se encuentran en validación y depuración de servicios y dispositivos de seguridad anteriores para la ejecución de políticas y accesos de acuerdo con la necesidad de la organización.

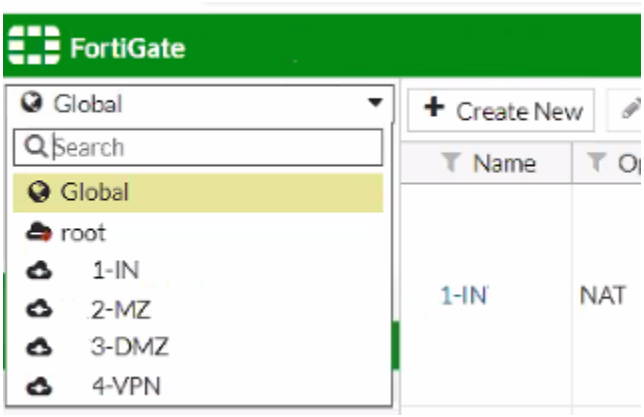


Ilustración 147. Dominios Virtuales creados-Propia de autores.

Para que el firewall cumpla con su propósito de limitar el acceso, se crearon varias políticas de acceso para cada subinterfaz. Las políticas creadas se validaron de manera satisfactoria a través de los eventos enviados al analizador de eventos implementado FortiAnalyzer por medio de los logs del firewall.

Ilustración 148. Validación de política de acceso-Propia de autores.

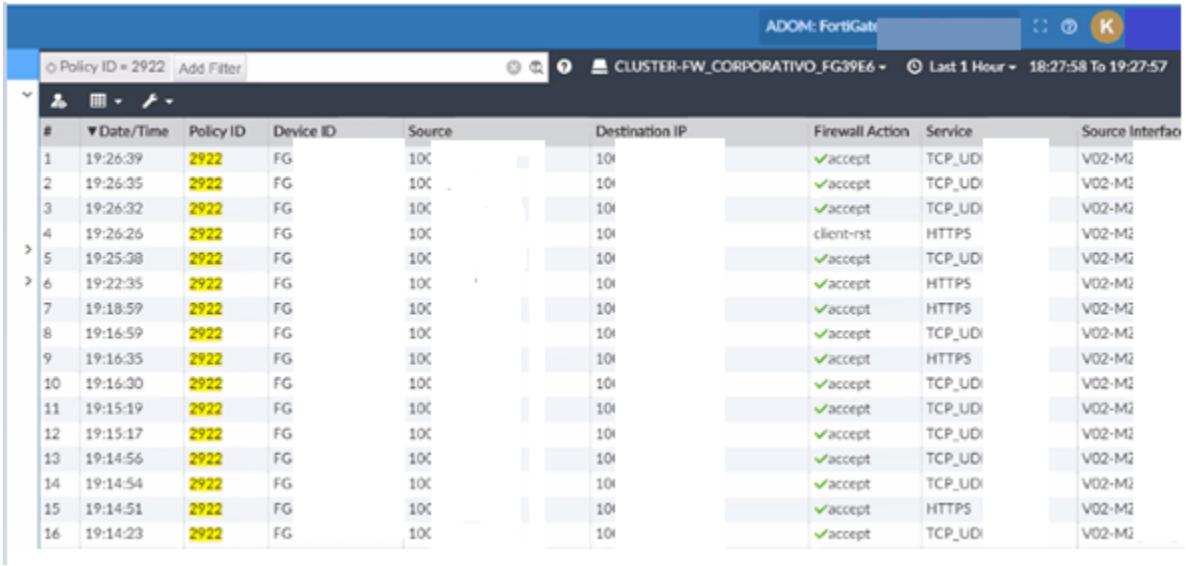


Ilustración 149. Validaciones de políticas-Propia de autores.

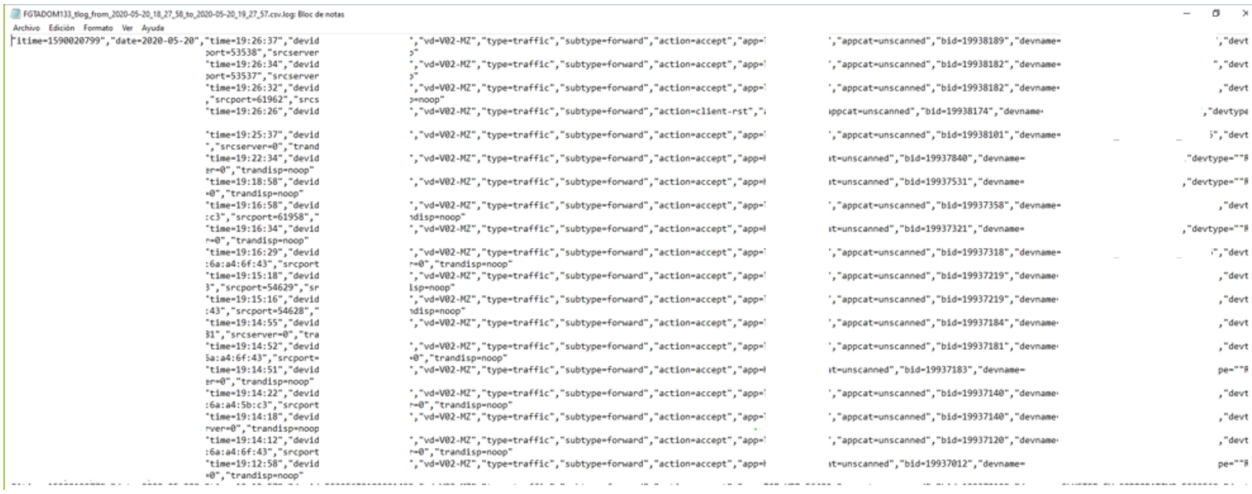


Ilustración 150. Log de eventos crudos-Propia de autores

	A	B	C	D	E	F	G	H	I
1	itime=1590020799	date=2020-05-20	time=19:26:37	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=accept	app=TCP_UI
2	itime=1590020795	date=2020-05-20	time=19:26:34	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=accept	app=TCP_UI
3	itime=1590020792	date=2020-05-20	time=19:26:32	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=accept	app=TCP_UI
4	itime=1590020786	date=2020-05-20	time=19:26:26	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=client-rst	app=HTTPS
5	itime=1590020738	date=2020-05-20	time=19:25:37	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=accept	app=TCP_UI
6	itime=1590020555	date=2020-05-20	time=19:22:34	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=accept	app=HTTPS
7	itime=1590020339	date=2020-05-20	time=19:18:58	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=accept	app=HTTPS
8	itime=1590020219	date=2020-05-20	time=19:16:58	devid=FG	vd=V02-MZ	type=traffic	subtype=forward	action=accept	app=TCP_UI

Ilustración 151. Organización de logs en Excel-Propia de autores.

Se logró implementar el hardware de autenticación FortiAuthenticathor de manera correcta, es de recalcar que el propósito de este dispositivo es llevar la carga de la lectura de grupos y usuarios del directorio activo de la organización y depurarlos para que se envíen al firewall, la organización cuenta con más de 500 grupos en más de 200 unidades organizativas.

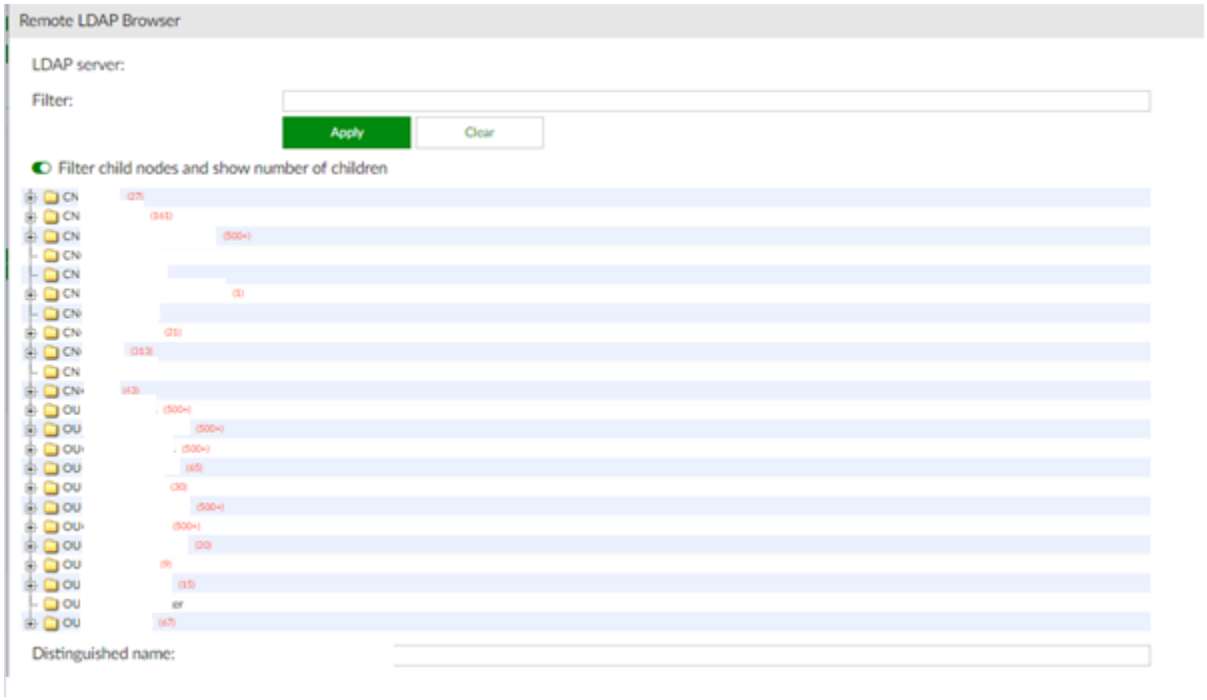


Ilustración 152. Unidades organizativas detectadas en autenticador-Propia de autores.

Se realiza una correcta implementación de un sistema de filtrado de contenido por medio de categorías para la necesidad de la organización. El filtrado y categorización se actualiza diariamente por medio de FortiGuard el cual es el servicio de actualizaciones y licenciamiento de Fortinet.

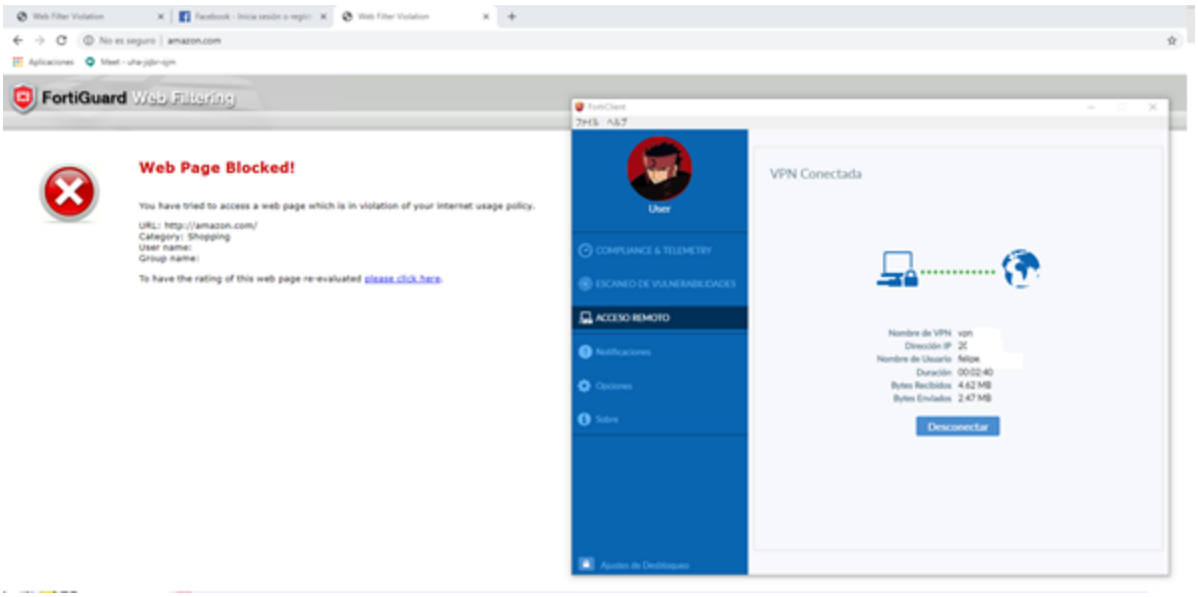


Ilustración 153. Resultado de pruebas filtrados de contenido-Propia de autores.

Se realizaron algunos manuales de acuerdo con nuestra experiencia y conocimientos suministrados por proveedor para la implementación de dominios virtuales

y la creación de una política de seguridad IPS efectiva, anexos C y D respectivamente.

12. Discusión

Para la implementación de seguridad perimetral no se controla el tiempo de la implementación de terceros, como en nuestro caso la implementación del cableado, propagación de direccionamiento, configuración de router y Switch.

Para la migración de cada servicio a nivel de políticas de acceso el proceso fue bastante largo ya que primero había que asegurar la conectividad a los destinos configurados y muchas veces por falta de información o desconocimiento de servicios y plataformas la conexión no resultaba exitosa, con lo cual se perdía mucho tiempo en depuración y resolución de problemas.

Para la VPN cliente sitio una forma de aumentar todavía más el nivel de seguridad es por medio de un certificado digital para cada destino el cual se puede cargar en las configuraciones de la VPN.

Para la configuración de la VPN cliente sitio fue necesario el uso del aplicativo FortiClient lo cual representa una desventaja ya que se debe instalar el aplicativo para su funcionamiento.

El uso de filtrado de contenido limita ampliamente el tráfico a través del dispositivo sin embargo por requerimientos de la organización esta característica es necesaria.

Firewall	IPS	NGFW	Threat Protection
240 Gbps	55 Gbps	40 Gbps	30 Gbps

Ilustración 154. Limitaciones técnicas de dispositivo- [2]

Durante la ejecución del proyecto se implementaron VPN IPSEC; sin embargo, la compañía aun hace uso de conexiones VPN ssl ya que por su simplicidad es más práctico para el usuario cliente promedio pueda hacer uso de ella, aun así, se recomienda que se migren a IPSEC.

Debido al tamaño de la organización este proyecto aún se encuentra en implementación por lo que se recomienda que al ya tener un sistema de autentificación efectivo como lo es un autenticador, es posible agregar parámetros adicionales de seguridad adicional para el acceso a dominios y políticas como es el caso de un doble factor de autenticación. Fortinet da la posibilidad de realizar esto por medio de FortiToken

la cual es una aplicación móvil que genera una llave adicional, esta característica tiene un costo adicional, pero proporciona una mayor seguridad.

Cabe resaltar que el proyecto está desarrollado en la plataforma del fabricante Fortinet y muchos de las funcionabilidades que presentan estos dispositivos pueden presentarse en diferentes fabricantes como Cisco, CheckPoint, palo alto y entre otros que cumplan las especificaciones requeridas por el proyecto.

13. Conclusiones

- Los dispositivos de seguridad utilizados de la marca Fortinet, además de cumplir con los requerimientos de restricción asignados por la organización, cumplieron correctamente para lograr los objetivos propuestos para la ejecución de este proyecto.
- Se logro realizar la implementación de dominios virtuales con el objetivo de aislar el tráfico entre servicios. Es importante recalcar que hay que ser muy estrictos al momento de permitir tráfico entre dominios virtuales ya que son puertas de conectividad y hay que evitar en lo mayor posible la mezcla.
- De acuerdo con el diseño y a pesar de que se logró abarcar gran parte de la actualización tecnológica de la organización, aún falta mucho más que puede ser realizado en una segunda etapa como lo que son migrar otros servicios de la compañía, la integración total de todos los usuarios de la organización en el autenticador y ya finalmente retirar los equipos anteriores.
- Muchas de las reglas migradas de los dispositivos anteriores son muy laxas y deben ser depuradas ya que la organización desconoce el objetivo y puertos a permitir de muchas de las políticas de seguridad, en varias ventanas de mantenimiento se depuraron algunas de ellas.
- Se logro implementar correctamente el sistema de filtrado web con autenticación de usuarios utilizando como intermediario entre el firewall y el directorio activo el dispositivo FortiAuthenticathor.
- Se logro realizar la implementación de VPNs cliente a sitio seguras tipo IPSEC; es importante anunciar que a nivel de seguridad este tipo de VPN es más confiable; sin embargo, debido al nivel funcional y técnico del

usuario promedio, la organización aun utiliza VPNs SSL ya que se requieren menos parámetros de configuración.

- Se lograron realizar pruebas más efectivas del IPS utilizando los conocimientos adquiridos en la especialización como lo es el uso de herramientas como Kali Linux, nmap etc.

14. Documentación de Referencia

Bibliografía

[1] C. Brodbeck, «Seguridad Digital de Resultados,» [En línea]. Available: https://ostec.blog/es/seguridad-perimetral/seguridad-perimetral-conceptos.

[2] Fortinet, «Fortinet,» 07 01 2018. [En línea]. Available: www.fortinet.com/. [Último acceso: 2019].

[3] A. S. Tanenbaum, Redes de Computadoras, Pearson Educación, 2003.

[4] Microsoft, «Microsoft,» 31 05 2018. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ldap/lightweight-directory-access-protocol-ldap-api. [Último acceso: 06 07 2020].

[5] Cisco, «Cisco,» [En línea]. Available: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html.

[6] P. Alto, «PaloAlto Networks,» [En línea]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips. [Último acceso: 06 07 2020].

[7] Nmap, «Nmap.org,» [En línea]. Available: https://nmap.org/man/es/index.html. [Último acceso: 06 07 2020].

[8] M. Porporatto, «Que Significado,» 25 11 2016. [En línea]. Available: https://quesignificado.com/partners/.

[9] R. A. D. I. d. España, «Diccionario Español De Ingeniería,» 29 08 2014. [En línea]. Available: http://diccionario.raing.es/es/lema/throughput.

[10] Fortinet Technical Documentation, «cookbook fortinet,» 06 01 2015. [En línea]. Available: https://cookbook.fortinet.com/vdom-configuration/.

[11] K. Lab., «latam kaspersky,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/web-filter.

[12] Staff High Tech Editores, «Info Channel,» 08 03 2016. [En línea]. Available: https://www.infochannel.info/fortinet-fue-certificada-por-su-efectividad-en-proteccion-web. [Último acceso: 2019].

[13] E. Ros, «ncora,» 17 Abril 2020. [En línea]. Available: ncora.com.

[14] Microsoft, «Microsoft,» 31 05 2018. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ldap/lightweight-directory-access-protocol-ldap-api. [Último acceso: 06 07 2020].

15. Anexos

- Anexo A: Descripción de categorías FortiGate.
- Anexo B: Informe FortiAnalyzer firmas IPS.
- Anexo C: Manual de configuración de VDOMS.
- Anexo D: Manual de configuración de IPS.