UACM

Universidad Autónoma
de la Ciudad de México

NADA HUMANO ME ES AJENO

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS
Y DE TELECOMUNICACIONES

Acceso de control utilizando un Firewall

T E S I S

QUE PARA OPTAR POR EL TÍTULO DE

**LICENCIADO EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS
Y DE TELECOMUNICACIONES**

P R E S E N T A

CRISTIAN ARMANDO CAMERO LOAIZA

D I R E C T O R

M. EN I. LUIS ENRIQUE ARANDA MELO

Ciudad de México, agosto de 2025.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Director de tesis:

Luis enrique Aranda Melo

Lectores:

1er. Lector:

Jorge Mendoza Zavala

2do. Lector:

David Estrada Espinosa

3er. Lector:

Victor Manuel Macías Medrano

Plantel de adscripción:

Casa Libertad

AGRADECIMIENTOS

A nuestra Alma Mater, la Universidad Autónoma de la Ciudad de México (UACM), por darnos la oportunidad de cumplir con nuestro sueño y metas, por no exigirnos nada y darnos mucho, ya que en nuestro país se requiere más Centros de Estudios como este, con su modelo educativo, porque todos tenemos el derecho de recibir al menos una oportunidad para demostrar de lo que somos capaces de realizar y hasta donde podemos llegar como persona.

Le agradezco a Dios por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Les agradezco a mis padres por apoyarme en todo momento y circunstancia, por los valores que me han inculcado y por haberme dado la oportunidad de tener una excelente educación en el transcurso de mi vida. Sobre todo, por ser un excelente ejemplo de vida a seguir.

A mis hermanos por ser parte importante de mi vida y representar la unidad familiar, por ser un ejemplo de desarrollo a seguir y llenar mi vida de alegría y amor cuando lo he necesitado.

A mi tutor de Tesis, le agradezco la confianza, apoyo y dedicación de tiempo para impulsarme a continuar el trabajo de investigación y hacerme más fácil el proceso administrativo para no tener problemas por esa vía, por haber compartido conmigo sus conocimientos y sobre todo su amistad.

A mi esposa por ser una parte muy importante de mi vida, por apoyarme en las buenas y en las malas, sobre todo por tú paciencia y amor incondicional en conjunto con mis hijos.

A mis amigos por confiar y creer en mí y haber hecho de mi etapa universitaria un trayecto de vivencias que nunca olvidare.

INDICE

INTRODUCCIÓN

Desde el comienzo de mi actividad laboral he obtenido experiencia profesional, al llevar a la práctica los conocimientos adquiridos a lo largo de mi formación, como realizar propuestas de administración en equipos de seguridad lógica y colocar estratégicamente equipos de seguridad, comprendiendo el mecanismo de funcionamiento de la infraestructura de una red LAN a WAN, conocimiento adquirido en los cursos de “Concentradores, witches y ruteadores”, “Estándares de área y amplia TCP/IP e informática en las telecomunicaciones”. Herramientas para brindar protección a los problemas de seguridad Lógica.

Desde hace mucho tiempo se ha venido hablando de seguridad informática, pero que tiene de cierto donde y en qué año nace esta palabra o frase de Seguridad Informática y sobre todo este concepto, si nos vamos un poco a el origen de esta historia en el año de 1980 apareció la primera manifestación sobre seguridad informática (SI), James P Anderson describe el documento Computer Segurity ThreatMonitoring and Surveillance (Seguridad en Computadores y Monitoreo de Amenazas y Vigilancia)

En la actualidad, toda empresa se basa en la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos. Dada la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para el resguardo y buen uso de la información y de los activos en general.

Se apoyará este trabajo de los Servicios de seguridad.

“El desarrollo del tema de tesis se formuló bajo las directrices que se especifican en la Recomendación X.800 para la gestión de seguridad de la información, teniendo el objetivo de disminuir el riesgo identificado, mediante procedimientos establecidos sistemáticamente de una empresa.” (Recomendación X.800. [2].

Este proyecto consiste en la construcción, documentación y configuración de una herramienta llamada firewall que permitirá crear controles de acceso de seguridad perimetral y administración de la red, abarcando dentro de esta solución el diseño de la herramienta, métodos y técnicas a, para finalmente conformar una propuesta que apoyara a la gestión de seguridad de la información con el fin de mitigar los riesgos.

El presente trabajo también se hablará de la importancia del equipo de seguridad Firewall y sus ventajas para la seguridad perimetral.

CAPÍTULO I

Marco teórico.

LA RECOMENDACIÓN X.800

La Recomendación X.800 ha sido preparada por la Comisión de Estudio VII y fue aprobada por el procedimiento de la Resolución No 2 el 22 de marzo de 1991. Recomendación X.800. [2]

En esta Recomendación, para la administración se utiliza para designar, en forma abreviada, tanto una Administración de telecomunicaciones como una empresa privada de explotación de telecomunicaciones reconocida.

La Recomendación X.200 del CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) describe el modelo de referencia básico para la interconexión de sistemas abiertos (ISA). Dicha Recomendación establece un marco para coordinar el desarrollo de Recomendaciones existentes y futuras para la interconexión de sistemas. Recomendación X.200. [3]

El objetivo de la ISA es permitir la interconexión de sistemas de computador heterogéneos de modo que puedan lograrse comunicaciones útiles entre procesos de aplicación. En distintos momentos, deben establecerse controles de seguridad para proteger la información intercambiada entre los procesos de aplicación. Recomendación X.800. [2].

Estos controles deben hacer que el costo de obtener o modificar los datos de una manera indebida sea mayor que el valor potencial de esta acción, o hacer que el tiempo requerido para obtener los datos de una manera indebida sea tan largo que pierdan su valor.

Esta Recomendación define los elementos arquitecturales generales relacionados con la seguridad que pueden aplicarse adecuadamente en las circunstancias en que se requiere la protección de la comunicación entre sistemas abiertos. Establece, en el marco del modelo de referencia, directrices y restricciones para mejorar las Recomendaciones existentes o formular nuevas Recomendaciones en el contexto de ISA con el fin de permitir comunicaciones seguras y proporcionar así un enfoque de la seguridad en la ISA.

Para comprender la presente Recomendación será útil una información básica sobre seguridad. Por tanto, se aconseja a los lectores que no estén muy

familiarizados con la seguridad que lean primero el anexo A. La presente Recomendación amplía el modelo de referencia Recomendación X.200. [2] para abarcar los aspectos de seguridad que son elementos arquitecturales generales de protocolos de comunicación, pero que no se examinan en el modelo de referencia.

1.2 servicios de seguridad

En la seguridad informática otro aspecto importante corresponde con los servicios de seguridad, ya que mejoran en un buen porcentaje la seguridad de un sistema y el flujo de información de una organización, estos servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

1.2.1 ¿Cuáles servicios?

Disponibilidad, autenticación, integridad, no repudio, control de acceso y disponibilidad.

Disponibilidad**:**

Es la encargada de asegurar el acceso de algún tipo de información a las personas autorizadas para mantenerla secreta y proteger los recursos de una información contra el descubrimiento internacional o accidental por personas no autorizadas a el sistema de información, es decir, protección de datos transmitidos de ataques pasivos por cualquier medio de fusión.

También se encarga de asegurar que nadie pueda Leer, Copiar, Descubrir o Modificar la información sin autorización y por consiguiente que ninguna persona pueda interceptar las comunicaciones o los mensajes entre entidades de diferentes organizaciones mundiales. Recomendación X.800. [2].

Autenticación**:**

Esto servicio de autentificación se encarga de verificar la identidad de algo o alguien, como puede ser la autentificación individual como la firma o si lo preferimos la contraseña.

La autenticación es utilizada para proporcionar la prueba a un sistema en realidad es la identidad de quien se pretende ser, y así mismo verificar la autenticación de la misma y acceder a dicha información, como medida principal a través de algo que se sabe (una contraseña o un numero personal de identificación, algo que se sabe, verifica la copia que está en el sistema de almacenamiento y determina si la autentificación es exitosa o no). algo que se tiene (una tarjeta o un pasaporte, es algo que se tiene y también el sistema verifica su autentificación); y algo que se es

(la voz, la retina, la huella digital o la imagen del rostro, que pueden identificar de quien se trata y la veracidad de la información en cuanto a lo que se trata de autentificación. Recomendación X.800. [2].

Integridad:

Este servicio verifica y garantiza, que la información trasmitida por cualquier medio no sufra cambios o modificaciones de forma no autorizada. [2].

No repudio:

Previene tanto al emisor como al receptor de negar un mensaje transmitido, el receptor del mensaje prueba la veracidad del mensaje que fue enviado por el presunto emisor y viceversa y confirma el recibido del receptor, el no repudio ofrece protección a un usuario frente a otro que niegue el mensaje y posteriormente la comunicación o recepción del mensaje enviado, por ejemplo, la firma digital.

Control de acceso:

Controla el acceso de los sistemas y aplicaciones mediante los medios de comunicación, el cual, al tratar de ganar acceso, debe identificarse primero o autenticarse, con el fin que un usuario sea identificado y autenticado de manera exitosa y permitir el acceso a la información relacionada.

La lista de control de acceso LCA (Lista de Control de Acceso) permite los permisos que determina quién puede tener acceso a los recursos de la red, esta lista le permite al propietario que dé acceso o deniegue el ingreso a los recursos a una entidad o un grupo de entidades. Recomendación X.800. [2].

Disponibilidad:

Este último servicio verifica que las personas autorizadas accedan a la información deseada cuando lo requieran y tantas veces como sea necesario, esto no significa que siempre se va tener este acceso, sino cuando sea requerido o necesario. Recomendación X.800. [2].

1.3 ¿Qué es ciberseguridad?

Se refiere a la protección de sistemas, redes y programas de ataques o amenazas digitales.
La ciberseguridad tiene múltiples capas de protección repartidas en las computadoras, redes, programas o datos que uno pretende mantener a salvo. En una organización, las personas, los procesos y la tecnología deben complementarse

para crear una defensa eficaz contra los ciberataques. Un sistema unificado de gestión de amenazas puede automatizar las integraciones entre productos selectos de seguridad y acelerar las funciones de operaciones de seguridad claves: detección, investigación y corrección. [4].

Historia de la ciberseguridad

La historia de los ciberataques refleja la historia misma de internet. El primer virus informático se creó a principios de la década de 1970 y fue descubierto en ARPANET, el predecesor del internet actual. Proofpoint. [9].

Ciberataques de alto perfil

Entre los casos más conocidos de una compañía tecnológica que ha sido víctima de un ciberataque, figura la gran filtración que sufrió Yahoo! entre 2013 y 2014, que puso en riesgo la información personal de los 3.000 millones de usuarios de Yahoo!, incluyendo sus nombres, contraseñas y otros datos. Yahoo! no reveló la existencia de la ex filtración de datos hasta el 2016, lo que les valió una multa de 35 millones de USD. Proofpoint. [4].

Edward Snowden se convirtió en un nombre totalmente familiar en los EE. UU. en 2015, cuando este exagente de la CIA y contratista gubernamental copió y filtró información clasificada de la Agencia de Seguridad Nacional. (Proofpoint,9).

El incidente WannaCry de 2017 se considera el primer ataque de ransomware. Este criptogusano atacó a 230.000 ordenadores con Windows en 150 países, exigiendo el pago de un rescate en bitcóin para desbloquear los equipos. Poco después, “NotPetya” atacó a otros 12.500 ordenadores con Windows utilizados por compañías energéticas, bancos y funcionarios del gobierno. Al principio, NotPetya daba la impresión de ser ransomware, pero hoy en día muchos sospechan que fue un ataque patrocinado por un estado cuyo objetivo era dañar infraestructuras críticas. Proofpoint. [9].

La filtración de 2017 de Equifax, una agencia crediticia, comprometió los datos de alrededor de 143 millones de ciudadanos americanos, titulares de 209.000 tarjetas de crédito. Proofpoint. [9].

Estos son apenas algunos de los mayores ciberataques conocidos. Una miríada de otros ataques ha desviado fondos, robado datos valiosos, dañado sistemas críticos y estafado víctimas, y eso sin contar los que no llegan a ser comunicados. Proofpoint. [9].

Durante décadas, la seguridad en la red se ha basado en detener estos ataques, con diversos niveles de éxito. Como disciplina, la ciberseguridad se puede dividir en tres períodos específicos: la Era del Control de Acceso, la Era de la Detección y la era actual: la Era de las Personas. Proofpoint. [9]

La era del control de acceso en la ciberseguridad

En los comienzos de la digitalización, la mayoría de los activos digitales, desde la informática y la información, hasta los fondos electrónicos, eran más fáciles de proteger. Era posible simplemente cerrar una puerta, y listo. Esta puede considerarse la “Era del Control de Acceso”. Proofpoint. [9].

Pero después, conectamos todo a las redes. Y todo lo que estaba en la red terminó por estar conectado a internet. Bloquear el acceso ya no era factible, ni tampoco deseable. Había que ir más allá de simplemente cerrar puertas. Había llegado la “Era de la Detección”.

La era de la detección en la ciberseguridad

Esta Era de la Detección se enfocó en encontrar virus, gusanos, cosas que se podían capturar con una herramienta antivirus o sistemas de detección o prevención de intrusiones (IDS/IPS). Y descubrimos problemas de cumplimiento en los registros de actividades, con herramientas tales como las de prevención de pérdida de datos (DLP, del inglés “data loss prevention”). Esto creó un nuevo conjunto de dificultades para la seguridad en la red, como la fatiga ante las alertas y los costes de cumplimiento. Proofpoint. [9].

Esta era estuvo enfocada en solidificar las infraestructuras empresariales: parchear vulnerabilidades en los sistemas informáticos, reforzar los perímetros, gestionar los puntos de contacto, etc. Proofpoint. [9].

1.4 Seguridad de la Red:

Conjunto de herramientas diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos, incluidas tanto las conexiones por cable como inalámbricas. La seguridad de red combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad. CISCO. [5].

1.5 Seguridad Perimetral:

Es la primera línea de defensa. El perímetro es donde se aplica y se valida la política, sin limitar su capacidad de acceder a lo que necesita. Si el acceso no se gestiona correctamente, una empresa puede ser susceptible a la infiltración o a la proliferación de amenazas, y la gravedad aumenta a medida que el panorama de amenazas crece. Por último, el perímetro de la red tiene un papel fundamental y

tiene el conjunto de responsabilidades más amplio en comparación con las redes principales y las redes centrales de datos. CISCO. [6].

1.6 Seguridad Lógica:

La seguridad lógica se refiere a la seguridad en el uso del software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios. La seguridad lógica involucra todas aquellas medidas establecidas por la administración para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.

Los principales objetivos de la seguridad lógica:

Restringir el acceso a los programas y archivos. Asegurar que estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto. Repositorio. [7].

1.7 Seguridad informática:

La seguridad informática es la disciplina que se encarga de proteger la integridad y la privacidad de la información, esta disciplina se ocupa de diseñar las normas, procedimientos métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Cuando hablamos de seguridad, este concepto se asocia a la certeza, falta de riesgo o contingencia. No es posible la certeza absoluta, si el elemento de riesgo siempre está presente, independientemente de las medidas que se tomen, significa tenerlo presente para seguimiento y evaluación de niveles de seguridad. También se entiende la seguridad informática como un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos, lo que se requiere también un nivel organizativo. (Libro Inicio y Evolución de la Seguridad Informática en el Mundo. [9].

La seguridad informática tiene un conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información. La seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Libro Inicio y Evolución de la Seguridad Informática en el Mundo. [9].

Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática

minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

Las amenazas a los sistemas de información pueden ser causadas por:

- Los usuarios: Son causa del mayor problema de seguridad informática, normalmente por un sobre dimensionamiento de permisos y restricciones.

- Programas maliciosos: Estos programas están destinados a afectar o hacer mal uso de los recursos de los sistemas. Muchas veces abren las puertas a intrusos y otras modifican directamente la información.

- Errores de Programación: Estos errores muchas veces son utilizados como exploits (es un software, fragmento de datos o secuencia de comandos que aprovecha una vulnerabilidad en un sistema o aplicación para provocar un comportamiento involuntario o imprevisto.) por los hackers.

- Intrusos: Son personas que consiguen acceder a la información o a programas a los cuales no están autorizadas.

- Siniestros: Los siniestros pueden resultar en la pérdida del material, archivos o de la información.

- Personal Técnico Interno: Algunas veces el personal interno por motivos de disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, entre otros, afectan o roban la información.

- Fallos Electrónicos o Lógicos.

¿Qué es un firewall?

Un firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, tales como la red LAN privada e Internet, que es una red pública y vulnerable. El firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un firewall puede considerarse como: un mecanismo para bloquear el tráfico y otro para permitirlo. Un firewall constituye más que una puerta cerrada con llave al frente de la red. Es un servicio de seguridad particular. 3Com Corporation, Seguridad de Redes. [10].

Los firewalls son también importantes porque proporcionan un único punto de restricción, donde se pueden aplicar políticas de seguridad y auditoría. Un firewall proporciona al administrador de la red, datos, información acerca del tipo y cantidad de tráfico que ha fluido a través del mismo y cuántas veces se ha intentado violar la seguridad. De manera similar a un sistema de circuito cerrado de TV, un firewall no

sólo bloquea el acceso, sino también monitorea a aquellos que están merodeando y ayuda a identificar los usuarios que han intentado violar su seguridad. 3Com Corporation, Seguridad de Redes. [10].

Funcionalidades básicas de los Firewalls

Dentro de sus funcionalidades se destacan las siguientes:

- Bloqueo de paquetes que se originan en un determinado rango de IP, puertos, dominios, direcciones de correo, etc.
- Bloqueo de paquetes formados por determinados protocolos o aplicaciones.
- Bloqueo de paquetes que sean reconocidos como firmas de ataques a sistemas o redes.
- Herramienta de análisis del comportamiento de sistemas y de red.
- Herramienta de análisis forense.
- Sistemas de defensa contra virus, gusanos y spam.
- Bloqueo de virus, gusanos, Troyanos y malware (software malicioso que se instala en un dispositivo sin el conocimiento del propietario para dañarlo o explotarlo).
- Bloqueo del uso de la red que protegen como origen de ataques.

Características de los Firewalls.

Para llevar a cabo un buen diseño hay que tener en cuenta las siguientes características:

- Control de Servicios: Determina el tipo de servicios de Internet que pueden ser permitidos hacia adentro o hacia afuera.
- Control de dirección: Determina en qué dirección cada servicio en particular se le permite circular.
- Control de Usuarios: Se implementan controles de acceso a un servicio de acuerdo al usuario que está tratando de acceder.
- Control de comportamiento: Controla como son utilizados cada servicio en particular (ejemplo: filtrado de correo electrónico)

Clasificación Firewalls

El firewall se puede clasificar en virtud de diferentes características como:

Modelo de arquitectura

Dependiendo del lugar donde se coloquen en la red pueden tener distintas funciones. Cuando hay dos o más firewalls implementados en una red, estos se

comunican con Internet u otras redes recibiendo el nombre de firewall de contención, en cambio el que se encuentra situado internamente y protege redes internas se le denomina firewall bastión. 3Com Corporation, Seguridad de Redes. [10].

Firewalls de software y hardware

Firewalls Software

- Soportados por varios Sistemas Operativos.
- Soportados en varias plataformas.
- Productos Mixtos.

Firewalls Hardware

- Hardware de aplicación más Sofware preinstalado.
- Sistemas operativos Fabricantes
- Funcionalidades añadidas como VPN, cache.
- Disco duros

Firewall de host y Firewalls de red

El firewall de host protege los sistemas donde están instalados, y los de Red protegen el entorno de la red o redes donde se han implementados.

Firewall red

- Protegen redes enteras
- Sistemas dedicados a la función de Firewall
- Módulos adicionales como IDS/IPS (sistema de detección de intrusiones/ sistema de prevención de intrusiones), antivirus

Firewall hosts

- Firewalls personales.
- Embebidos en Sistemas operativos.
- Sistemas de conexión externa a través de VPN (una red privada virtual)
- Baratos.

Tipos de filtrado en Firewalls

Hay tres tipos principales de filtrados basados en la capa del modelo OSI en la que los firewalls realizan el filtrado. Picouto Fernando, Lorente Iñaki. [11].

Filtrado a nivel de paquete

Se realiza a nivel de la capa de Red, examinando la cabecera del paquete. En los cuales se hace una verificación de la cabecera de los paquetes que contienen las direcciones IP y sus opciones, permitiendo o denegando su paso a las redes que

protegían. Se puede encontrar en los sistemas operativos, software, routers (acl) o firewall de hardware. Libro, ARROYO José. Linux Máxima Seguridad edición especial México. [12].

La utilización de un firewall a nivel de red, puede dar o negar acceso a un sitio basándose en variables, como:

- Dirección de fuente
- Protocolo
- Numero de puerto
- Contenido

Firewall de filtrado de circuito

Trabaja en las capas de transporte y sesión del modelo OSI (El modelo de interconexión de sistemas abiertos), su función principal es examinar la información TCP que se envían entre sistemas para verificar que la petición sea legítima.
Los filtros de circuito restringen los accesos que se encuentran en las cabeceras TCP y UDP (son protocolos de transmisión de datos que se utilizan para enviar información entre dispositivos).

Filtrado a nivel de aplicación (proxy)

Los servidores proxy se ejecutan en unos pocos programas que pueden ser seguros y confiables, estos programas son servicios específicos teniendo en cuenta que cada protocolo soporta su propio servicio proxy y gestionado por un proxy genérico.

La función principal es realizar conexiones punto a punto desde el cliente al proxy y desde este al servicio de red requerido.

- El usuario realiza la petición de un servicio de internet, como es HTTP, FTP, Telnet entre otras.

- El software instalado en el sistema del cliente lanza la petición de acuerdo con la política de seguridad a utilizar para el servicio de internet requerido.

- Proxy provee conexión actuando como Gateway del servicio remoto.

- Proxy realiza las comunicaciones necesarias para establecer la conexión con los sistemas extremos, mientras protegen los sistemas que están detrás del equipo.
- Todo el tráfico se enruta entre el usuario interno y el sistema externo a través del Proxy Gateway.

- El sistema Proxy debe ser implementado para ser usado por un solo servicio, sin configurar cuentas de usuarios, ni programas innecesarios.

Políticas de seguridad de los Firewalls

Una política de seguridad es una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información. Puede ser tan simple como una política de uso aceptable o contener muchas páginas y detallar cada aspecto de conectividad de los usuarios, así como los procedimientos de uso de redes. La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red. Libro, CISCO SYSTEMS. [13].

Los procedimientos de seguridad implementan políticas de seguridad que definen la configuración, el inicio de sesión, la auditoría y los procesos de mantenimiento de los hosts y dispositivos de red.

Una buena política de seguridad es la que nos permite definir las funciones que debe cumplir el Firewall y también informar al usuario que está permitido o denegado. Libro, CISCO SYSTEMS. [13].

Existen diferentes políticas de seguridad en la cuales tenemos**:**

1. Políticas de identificación y autenticación: especifica las personas autorizadas que pueden tener acceso a los recursos de la red.

2. Políticas de contraseña: garantiza que la contraseña de los usuarios cumpla con los requisitos mínimos y se cambien periódicamente.

3. Políticas de usos aceptables: Identifican aplicaciones y usos de red que son aceptables.

4. Políticas de acceso remoto: Define como los usuarios remotos pueden obtener acceso a la red y a que elementos disponibles.

Ventajas y desventajas de un Firewall

Ventajas:

• Permite al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados como son: hackers, espías y los mismos usuarios de la red privada negándole la entrada o salida de datos.

• Ofrece la posibilidad de monitorear la seguridad y si aparece alguna actividad sospechosa, generará una alarma ante la posibilidad que ocurra un ataque.

• Crea un archivo en donde se registra el tráfico que pasa a través del firewall.

• Controla los accesos provenientes de la red privada hacia el Internet.

• Controla los accesos provenientes de Internet hacia la red privada.

• Ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad auditando el uso del Internet, localizando con precisión los altos tráficos de consumo de ancho de banda.

Desventajas:

• No puede proteger contra los ataques de la Ingeniería Social.

• No puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación.

• No puede prohibir que se copien datos corporativos en disquetes o memorias portátiles.

• No puede ofrecer protección cuando el atacante lo traspasa.

• No cuenta con un sistema de escaneo para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él, ya que el Firewall no es un antivirus sino un escudo de protección.

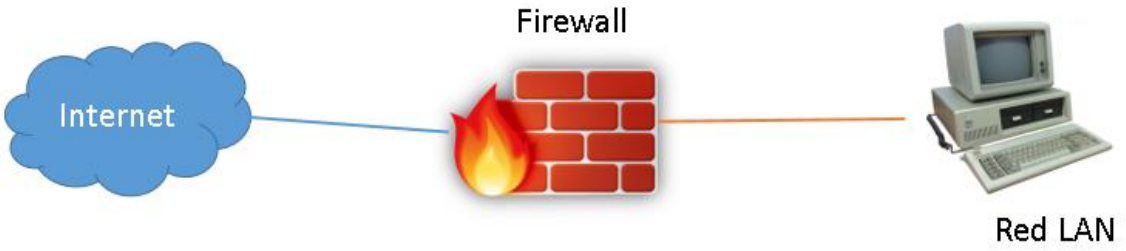


Figura 1.1 Diagrama de internet a una red.

A partir de la figura 1.1

Los firewalls suelen utilizar dos o más de los siguientes métodos:

- El filtrado de paquetes: método que permite permitir o denegar la entrada o salida de paquetes de datos de una red haciendo uso de un conjunto predefinido de reglas de filtrado.

- Application Gateway: La técnica de aplicación de pasarela emplea métodos de seguridad que se aplican a ciertas aplicaciones, tales como Telnet y servidores de transferencia de archivos.

- Circuito a nivel de gateway: Una puerta de enlace a nivel de circuito aplica estos métodos cuando se establece una conexión como el Protocolo de Control de Transmisión y paquetes comienzan a moverse.

- Servidores Proxy: Los servidores proxy pueden enmascarar direcciones de red reales e interceptar todos los mensajes que entran o salen de una red.

- Inspección de estado o filtrado de paquetes dinámico: Este método compara no sólo la información del encabezado, sino también partes más importantes de datos entrantes y salientes de un paquete. Estos se comparan con una base de datos de información de confianza para los partidos característicos. Esto determina si la información está autorizada

1.9 ¿Por qué la importancia de un Firewall?

Este mecanismo de seguridad continúa siendo altamente utilizado en el entorno corporativo. Según un estudio de seguridad informática en Latinoamérica, el 76% de los ejecutivos de 14 países de esta región cuentan con una solución de este tipo; lo que ubica al firewall en el segundo lugar de los controles de seguridad más utilizados, después de los antivirus.

1.10 Tipos de firewalls

1.10.1 Firewall proxy

Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red. Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir. CISCO. (2021). [1].

1.10.2 Firewall de inspección activa

Un firewall de inspección activa, que ahora se considera un firewall “tradicional”, permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Monitorea toda la actividad desde la apertura hasta el cierre de una conexión. Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión. CISCO. (2021). [1].

1.10.3 Firewall de administración unificada de amenazas (UTM)

Un dispositivo UTM (Unified Threat Management O Gestión Unificada de Amenazas) suele combinar de forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso para su administración.

Un UTM puede ser identificado fácilmente como un activo de software y hardware, o una combinación entre los dos, que centraliza en plataforma única características de filtrado stateful, VPN, proxy web, antivirus, IDS/IPS, inspección profunda de paquete (DPI). CISCO. (2021). [1].

1.10.4 Firewall de próxima generación (NGFW)

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir lo siguiente:

- Capacidades de firewall estándar, como la inspección activa
- Prevención de intrusiones integrada
- Control y reconocimiento de aplicaciones para ver y bloquear aplicaciones riesgosas
- Rutas de actualización para incluir futuras fuentes de información
- Técnicas para afrontar amenazas de seguridad en constante evolución
- Si bien estas funcionalidades se están convirtiendo cada vez más en el estándar para la mayoría de las empresas, los NGFW pueden hacer más. CISCO. (2021). [1].

1.11 Ventajas que se obtienen al implementar un firewall son**:**

Reducir riesgos, el camino para el intruso se vuelve complicado, aumentando con ello el grado de seguridad de la red.

Esta herramienta se relaciona con los beneficios que proporciona dicho dispositivo en cuanto a la protección, debido al proceso de filtración de conexiones exteriores que suelen realizar algunos tipos de software maliciosos como gusanos, virus o botnets (red zombi es un grupo de ordenadores o dispositivos que están bajo el control de un atacante). De igual manera, los firewalls bloquean las conexiones de posibles intrusos en la red como medida de seguridad para el control de conexiones al exterior.

Control de acceso

Esta política dirigida al control, privilegios, autorización y permisos que un usuario tiene para acceder a los recursos de red, debe de iniciar por un flujo de creación y registro de usuario, asignación de privilegios hasta la cancelación y retiro del usuario de la red.

Al implementar la seguridad en las operaciones**.**

Para este paso garantizar que los procesos y procedimientos se encuentren actualizados, esto garantiza resolver en un menor tiempo los incidentes y eventos de seguridad; Identificación de la información crítica, es la que permite el funcionamiento, y cumplir la misión de la organización; Gestión de riesgo, permite identificar la criticidad y reducir el impacto en la integridad y disponibilidad de la información; Vulnerabilidades y riesgos cibernéticos, mantenerse actualizado de las nuevas vulnerabilidades y riesgos que afectan la seguridad, en páginas del proveedor de la infraestructura y software; Copias de seguridad, es el respaldo ante posibles eventos, asegurando la disponibilidad e integridad de la información mediante políticas (incrementales, diferenciales y total) de copias de seguridad, recordar que se deben realizar pruebas de restauración periódicas para verificar la disponibilidad.**(**PROPUESTA BASADA EN LA SEGURIDAD LÓGICA PERIMETRAL EN LAS PYMES*,* COMO ESTRATEGIA PARA LA PROTECCIÓN CONTRA CIBERATAQUES**)**

CAPITULO 2
2. Implementación

Para dar inicio al desarrollo de la implementación de este proceso, las importancias de un Firewall para mí son: restringir el acceso a páginas prohibidas, aplicaciones maliciosas, etc., separar la red LAN de servidores de producción y analizar el tráfico de entrada y salida.

Para esta tesis en particular es mostrar la implementación de un Firewall NGFW que se pretende configurar, probar y mostrar la funcionalidad del control de acceso de una red LAN a internet. Para ello se va a crear un entorno como se simulo en una topología de red que podemos encontrar en variedad de empresas y centros de datos, esto simula la topología de una empresa que dispone de una red LAN interna para que los usuarios se comuniquen y que además tengan acceso a Internet a través de un Firewall que se basa sobre la plataforma de checkpoint, la cual, brindara seguridad mediante reglas de acceso, con esto el tráfico se vuelve más eficiente y seguro tanto de entrada como salida, dado que a medida que fluye por los medios de comunicación.

También en esta implementación, el principal instrumento de control de acceso es el firewall, cuyo dispositivo montado sobre appliance dedicado de Checkpoin conectado aun laptop, tiene como objetivo principal el acceso a todo el trafico entrante y saliente de la red de datos, esto nos ayudara a crear reglas de prueba para ayudar a tener una mejor visibilidad del trafico bloqueado y aceptado. Con el apoyo de una laptop podremos realizar pruebas de navegación web y usar protocolos de red para generar tráfico en la red de prueba y pueda ser visibles en los log del firewall.

2.1 Esquema Lógico de la red

Debido a que el entorno es una topología de pruebas propia, y se quiere buscar un entorno cómodo y fácilmente manejable para realizar pruebas, se optará por una red de clase C con capacidad para un máximo de 254 equipos cada una.

Se elige la red 192.168.1.0 con máscara 255.255.255.0 para la zona de Acceso a Internet y por último la red 192.168.2.0 con mascara de red 255.255.255.0 para la Zona LAN.

La asignación de IP por la que se opta para realizar las pruebas, se muestra en la siguiente tabla 1 con la cual se configurara en los equipos de pruebas esto ayudar a tener un mejor control para la configuración:

Equipo	IP
PC_1	192.168.2.2
PC_2	192.168.2.3
Firewall LAN	192.168.2.1
consola	192.168.2.1
MGMT	192.168.1.1
Firewall WAN	192.168.1.146
Modem	192.168.1.1

Tabla 1. Equipos e IPs.

Se utilizó las siguientes características de equipos para realizar las pruebas:

- Laptop que se configurara la IPs de PC_1 y PC_2:
  - Modelo: Acer
  - Core i5
  - RAM: 4 GB
  - Disco duro: 120 SSD
  - Sistema operativo: Windows 10
- Firewall:
  - Modelo: Checkpoint 4800 NGFW
  - RAM: 4 GB
  - Disco duro: 250 HHD
- Cables de red: Rj45

Se creó una red LAN pequeña como anteriormente se menciona con el fin de realizar pruebas de navegación de internet segura como se muestra en la figura 1:

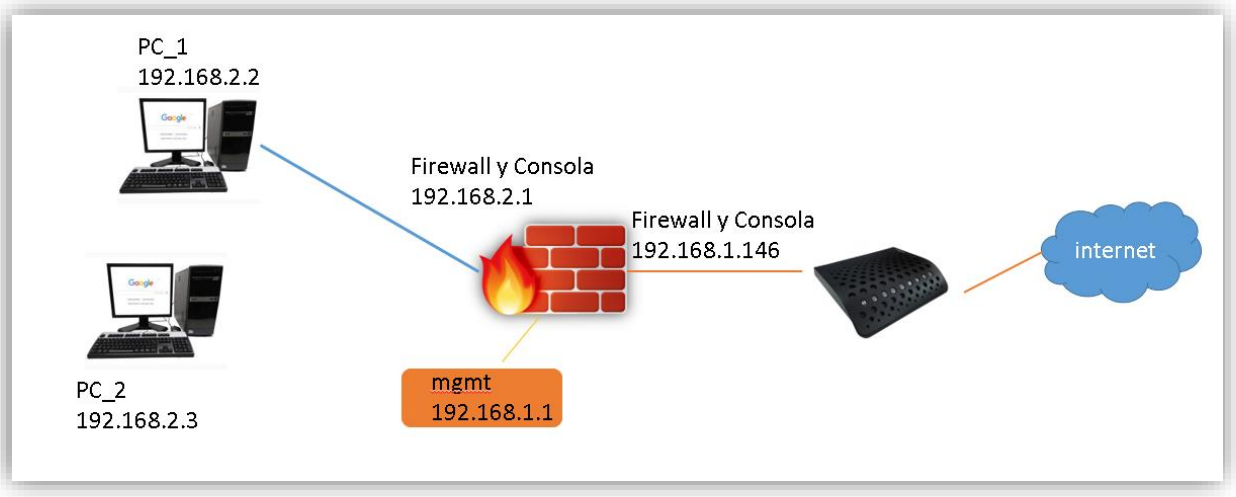


Figura 1.2. Diagrama de red.

A partir de la figura 1.2

Dentro de la red LAN propuesta, solo se realizará pruebas con dos IPs configuradas manualmente en la laptop, primero se configurará la IP de la PC_1 para configurar el firewall y tener conexión, después se usará la segunda IP de la PC_2 para generar tráfico para realizar pruebas y la IP 192.168.2.1 se asignará a la interfaz del firewall y para la red WAN se utilizará la IP 192.168.1.146 a la interfaz del firewall conectada hacia el modem de internet como se mostró en la tabla anterior y el mgmt es la interfaz de administración.

También mencionar que este pequeño diagrama de la figura 1. Me sirve de apoyo de cómo para identificar la interconexión para las pruebas del acceso.

2.2 Configuración del firewall

Primero se reseteo de fábrica el firewall esto nos ayudar a borrar toda la configuración que anteriormente tenia para un mejor desempeño, para esto se tuvo que conectar una Laptop al puerto de consola del Firewall mediante un cable RJ45, para entrar al menú de boot y así seleccionar el reinicio de fábrica.

Ya conectados al quipo mediante un cable de Rj45 hacia el puerto de consola, se reinicia el firewall y abrimos el PuTTy (es un emulador de terminal que permite conectarse a servidores remotos de forma segura) para emular la terminal y poder conectarnos al equipo mediante SSH que s un protocolo para las conexiones a las que se accede por línea de comando, esto ayudara a tener más visibilidad del menú del firewall y poder resetear.

Depuse ya conectados hacia el firewall mediante **PuTTy** nos aparecerá un menú que muestra diferentes opciones para reiniciar, se escoge el **reset to Factory defaults**, esto ayudará a reiniciar al firewall como se muestra en la figura 1.3, con las configuraciones básicas para empezar hacer nuestra configuración.

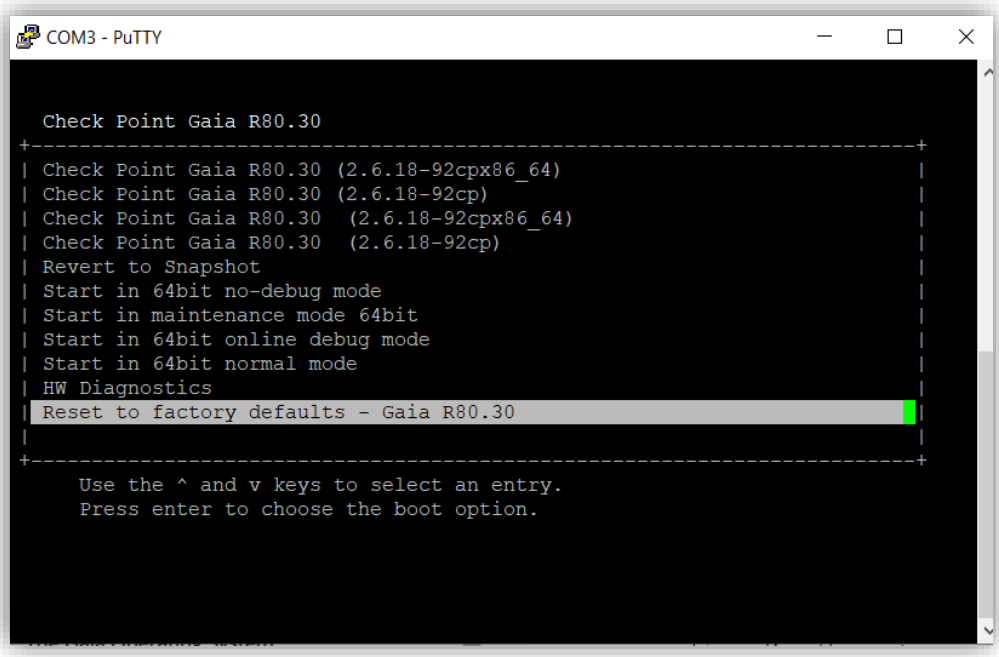


Figura 1.3. Pantalla de inicio de Firewall

Después de terminar el reinicio se mostrará el nombre por default del equipo indicando que ya podemos iniciar a la nueva configuración como se muestra en la en la figura 1.4:

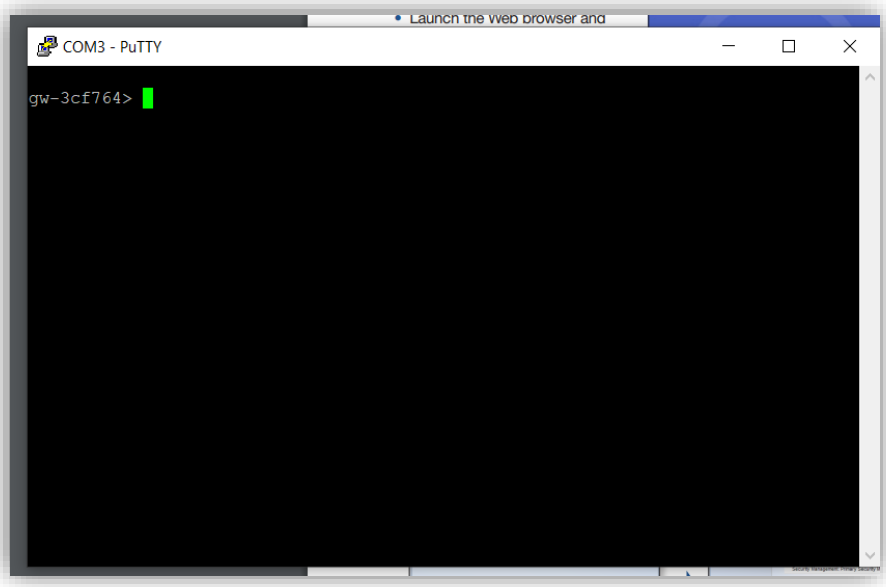


Figura 1.4. Pantalla de inicio de configuración en el Firewall.

Una vez reseteado el equipo firewall, se configuro la tarjeta de red de la laptop con una IP del segmento que tiene el firewall para poder estar en la misma red que asigna por default el firewall y se conecta al puerto de MMGT mediante el cable RJ45 como s emeusta5r en la figura 1.5.

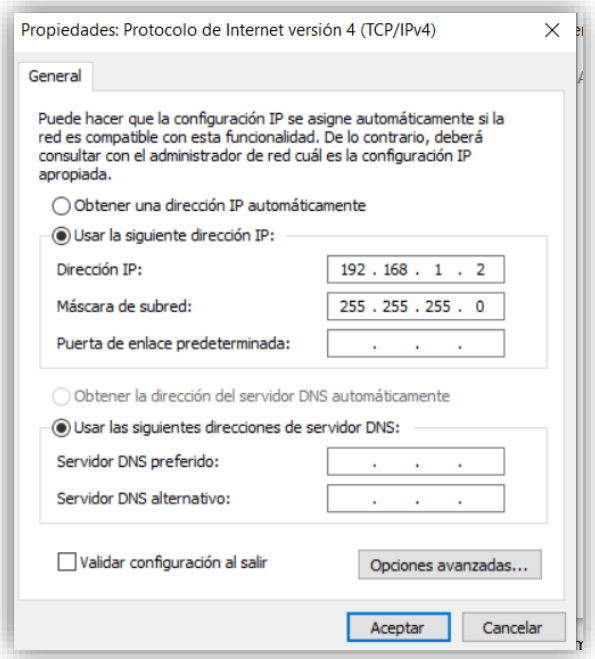


Figura 1.5. Configuración de tarjeta de red de laptop.

Validamos con un ping del protocolo ICMP (protocolo mensajes de control de internet), esta herramienta será muy útil para diagnosticar problemas de conexión, una vez ejecutado el ping hacia la IP del firewall podemos probar que se están comunicando en la misma red ambos equipos como se muestra en la figura 1.6

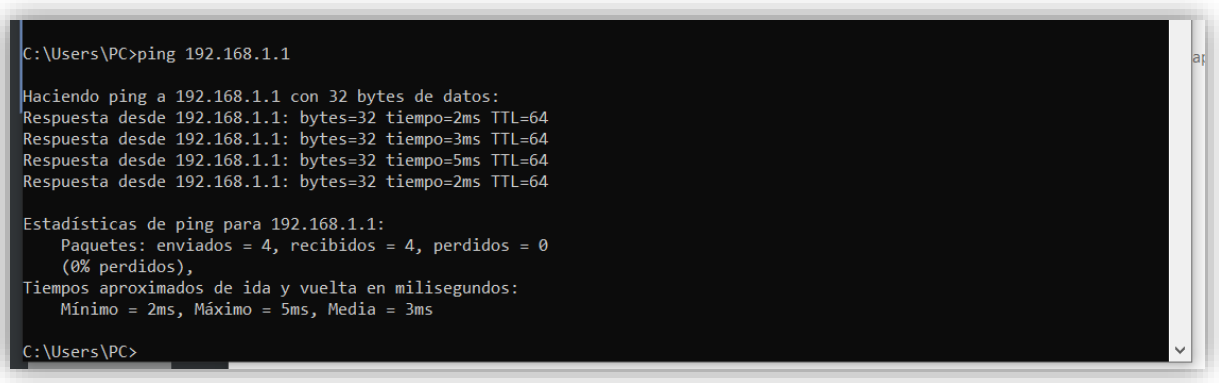


Figura 1.6. Validación ping.

Se procede a abrir un navegador web para poder ingresar vía web al firewal con la IP https://192.168.1.1 que viene por default para iniciar la configuración, pidiendo usuario y contraseña como se muestra en la figura 1.7.

Se ingresa los siguientes parámetros de acceso:

Usuario: **admin**

Contraseña: **admin**

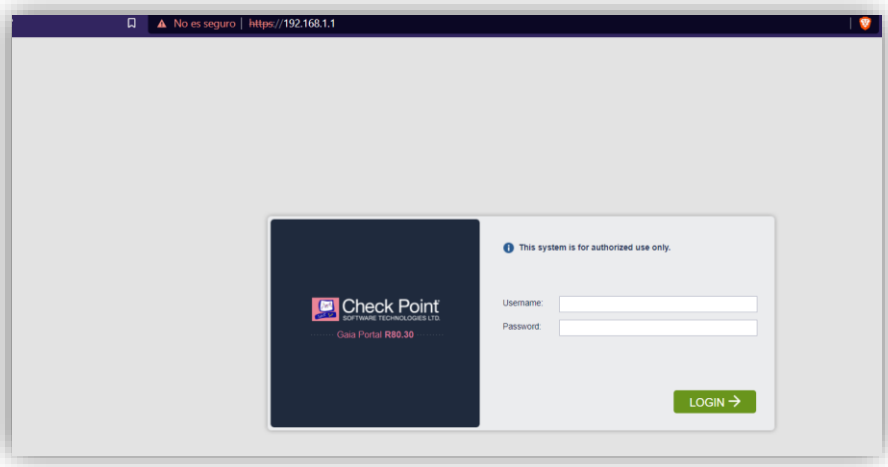


Figura 1.7. acceso vía web.

Una vez ingresado vía web con el usuario y contraseña nos saldrá la configuración del Wizard esto es para una sencilla configuración, este tipo de configuración se caracteriza por ser un modo fácil e intuitivo de guiar al usuario paso a paso en la instalación y configuración del dispositivo como se muestra en la figura 1.8.

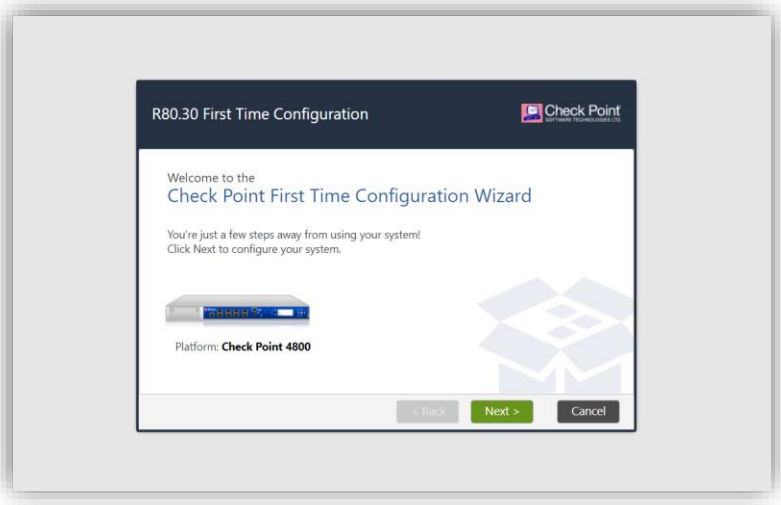


Figura 1.8. Inicio de configuración del Firewall.

Des pues nos aparecerá una ventana para ingresar el usuario y contraseña nuevas de administrador que nos servirá para conectarnos al firewall vía web y por línea de comando, como se muestra en la figura 1.9, estas credenciales hay que guardarla bien para futuros cambios yo use la credencial que se muestra.

Usuario: **admin**

Contraseña: **admin$1**

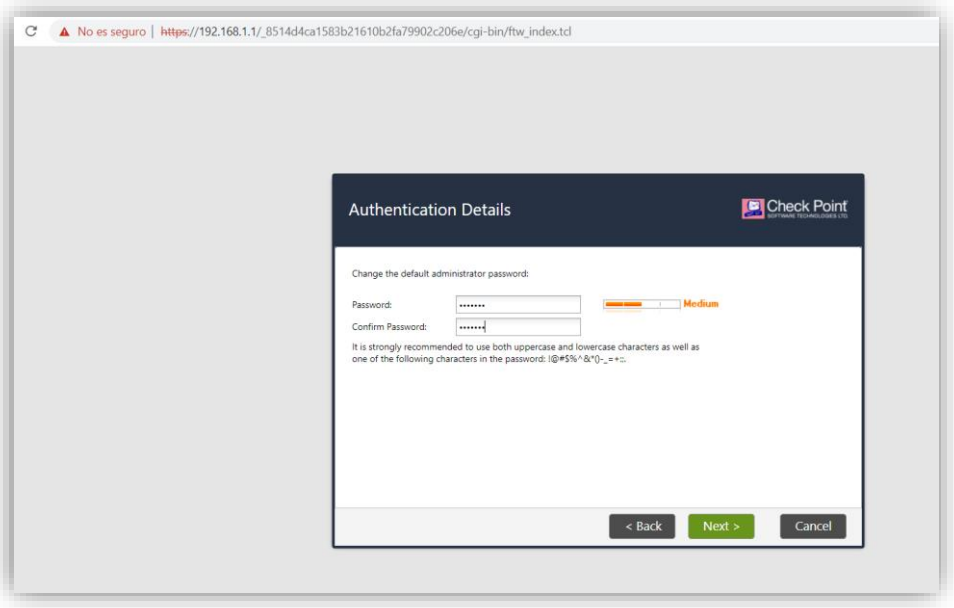


Figura 1.9. usuario y contraseña de administrado.

Después nos saldrá una ventana para seleccionar el tipo de configuración o implementación del firewall, se selecciona la opción continue witch R80.30 configuración para mantener la misma versión y se le da clic a next.

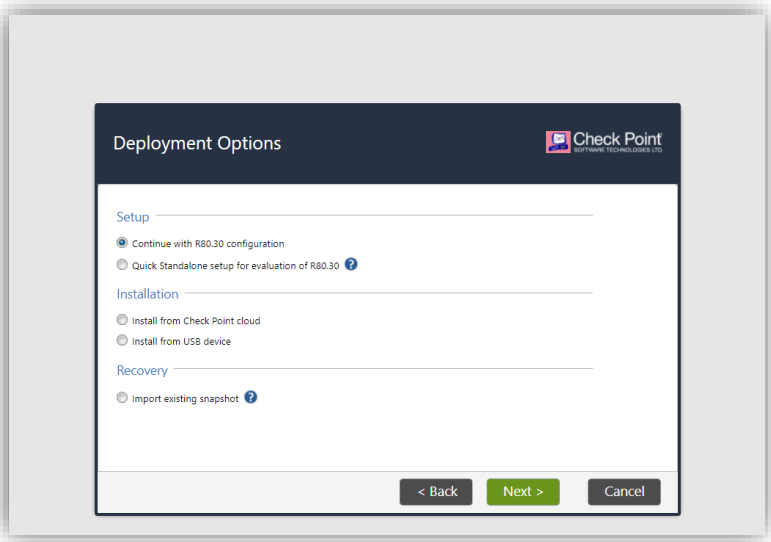


Figura 1.10. Tipo de versión.

Después se configura los parámetros de red que va tener Firewall como anteriormente se mostró el diagrama de la red, estos parámetros ayudaran conectarse vía web al firewall y por línea de comandos. Como se muestra en la siguiente figura 1.11.

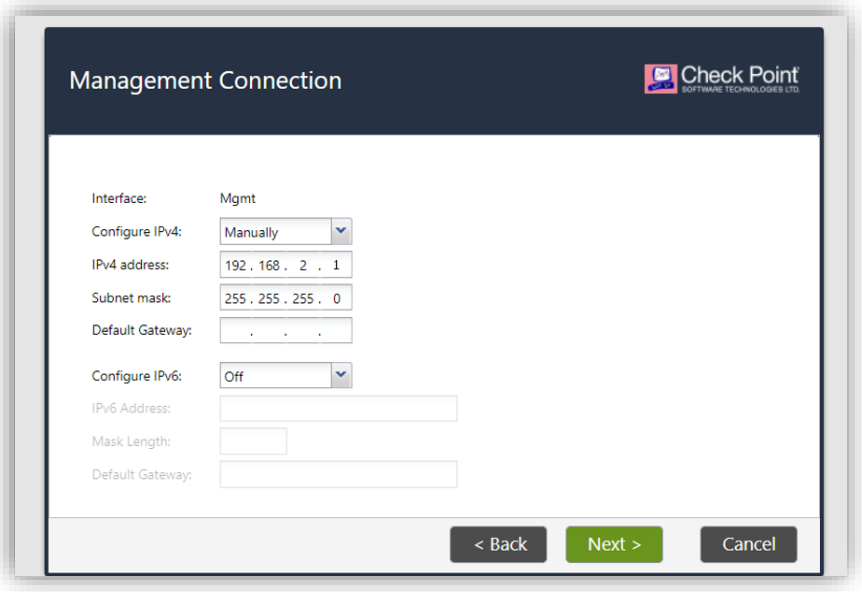


Figura 1.11. Configuración de IP de administración.

Una vez configurado los parámetros de red del Firewall saldrá una ventana para configuración de la interfaz que tendrá salida a internet, Se seleccionó la interfaz 2 del Firewall donde entrará y saldrá el tráfico hacia internet.

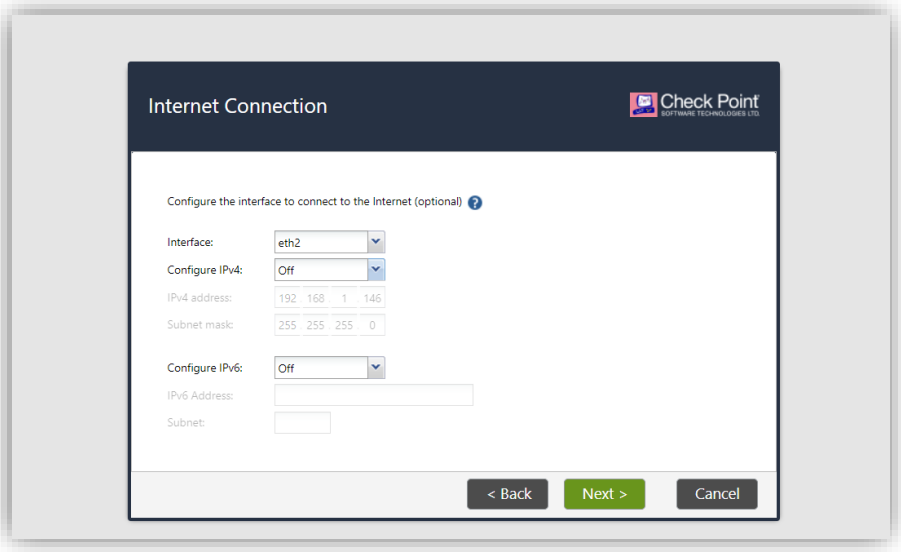


Figura 1.12. Entrada y salida del tráfico.

Después saldrá una ventana para cambiar parámetros y nombre del equipo, se nombra el equipo como FW y se agrega un DNS de internet como se muestra en la figura 113.

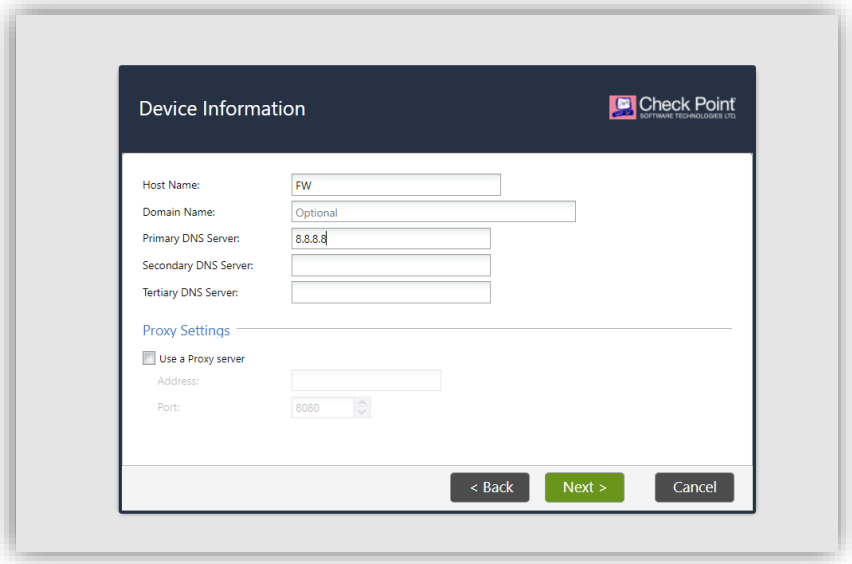


Figura 1.13. Nombre de host y DNS.

Después no saldrá una ventana para configuración del horario y se procede a configurar la hora y zona horaria:

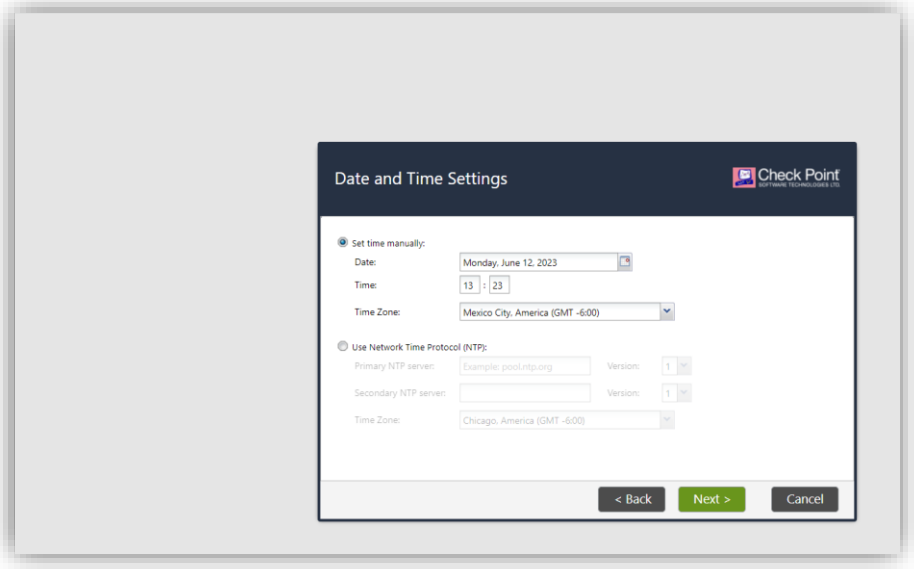


Figura 1.14. Zona horaria.

Después saldrá una venta de la configuración que muestra el tipo de operación estar realizando el Firewall, se selecciona que va estar como administrador de seguridad y se deja palomeado las descargas automáticas de firmas como se muestra en la figura 1.15.

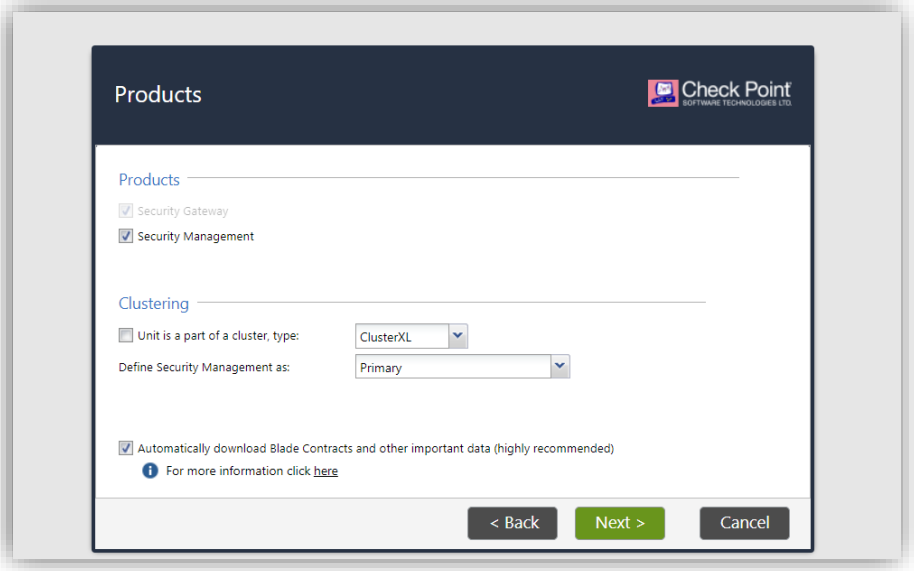


Figura 1.15. Tipo de firewall.

Después se selecciona que cualquier IP puede accesar a la interfaz gráfica dentro de la red interna, esto es debido a que se va a realizar pruebas.

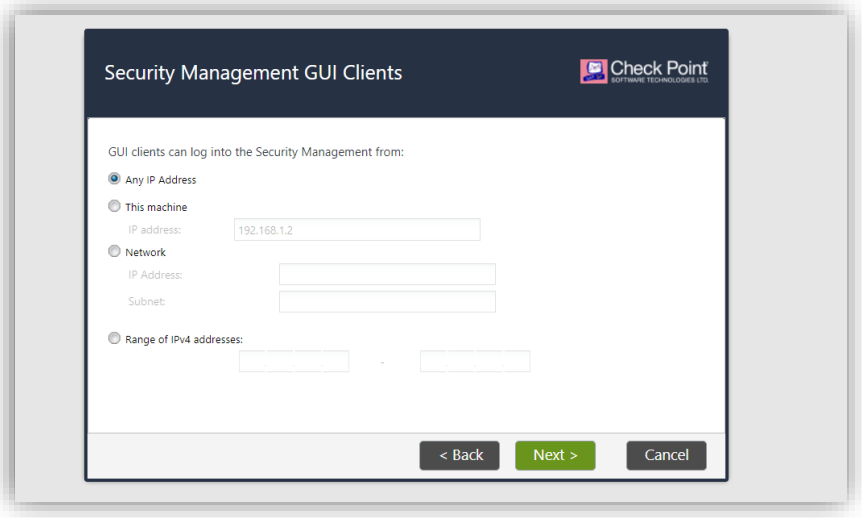


Figura 1.16. Acceso a la interfaz Gráfica.

Después saldrá una ventana de como quedo la configuración y se le da clic en **finish** como se muestra en la figura 1.17.

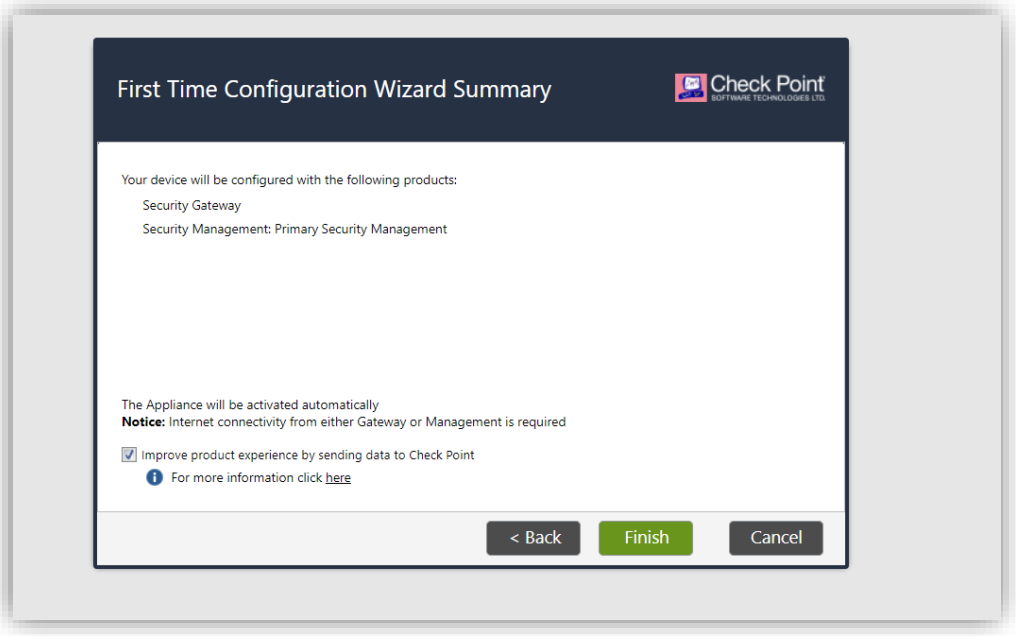


Figura 1.17. Como se configuro el Firewall.

Una vez echo la configuración básica nos saldrá la ventana de la ejecución y proceso de la configuración del Firewall como se muestra en la figura 1.18.

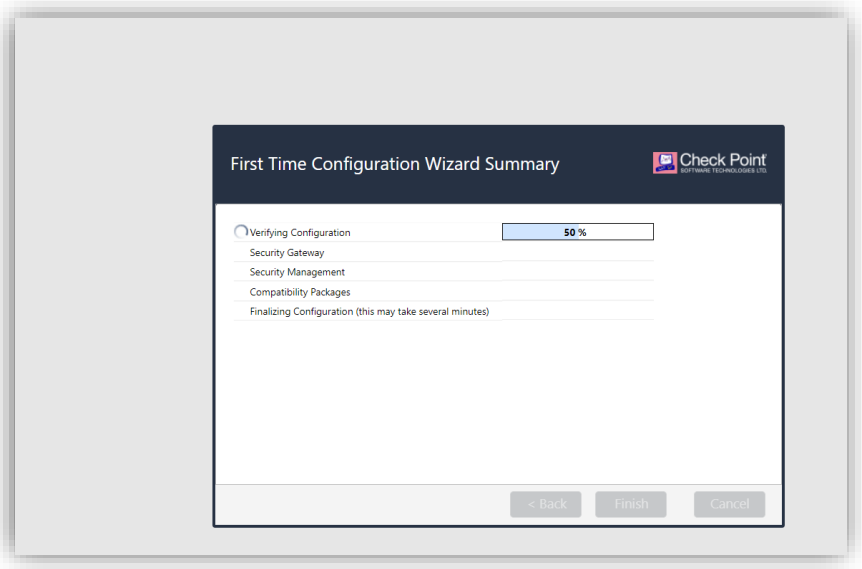


Figura 1.18. Proceso de configuración en el Firewall.

Cada vez que vaya terminado la ejecución de la configuración previa del Firewall no saldrá una palomita color verde de validación como se muestra en la figura 1.19.

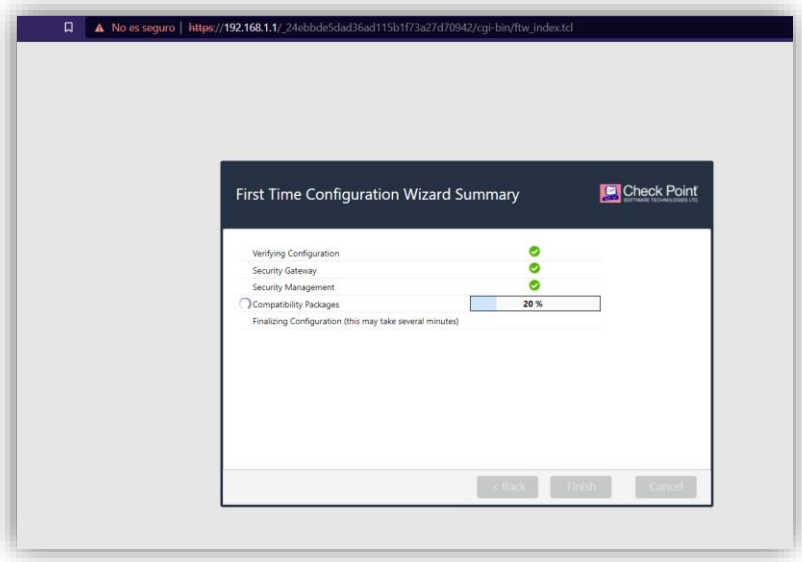


Figura 1.19. Proceso de validación.

Cuando ya se haya cargó la configuración en el Firewall correctamente no saldrá una venta como la figura 1.20 de que ya finalizo la configuración:

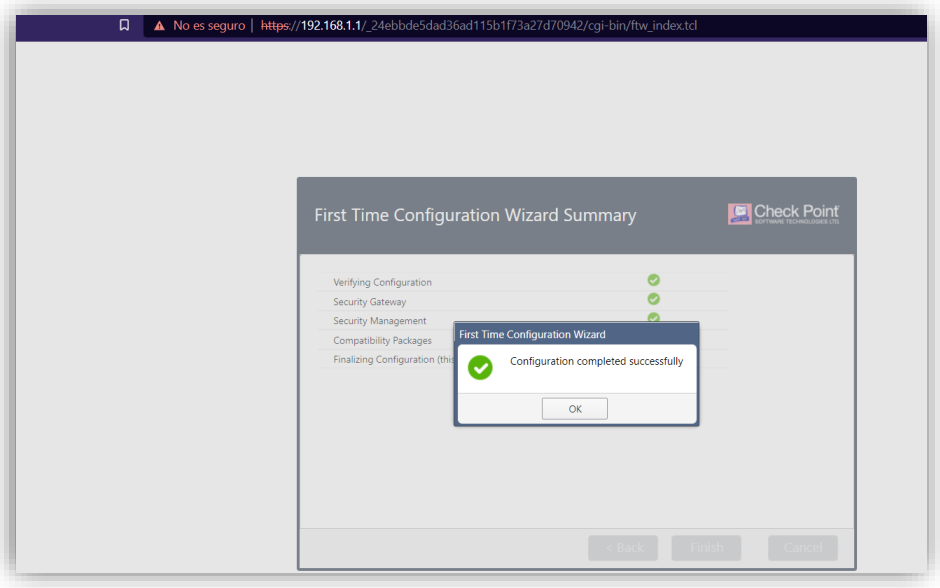


Figura 1.20. Configuración completada.

Después de haber concluido la configuración, se entra por la aplicación **PuTTY** para comprobar que se cambió el nombre del equipo con el usuario y contraseña que se asignó anteriormente para la administración como se muestra en la figura 1.21.

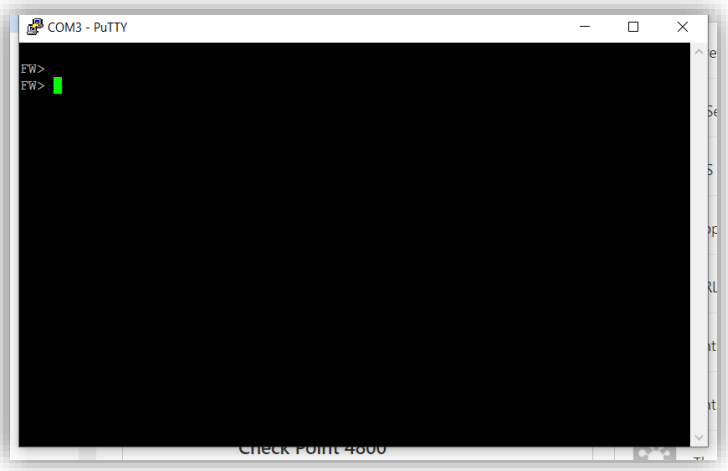


Figura 1.21. Ver cambio de nombre del equipo por PuTTY.

Después se configura la tarjeta de red al segmento de la red LAN que se asignó para poder alcanzar al Firewall conectada la laptop a la interfaz MGMT.

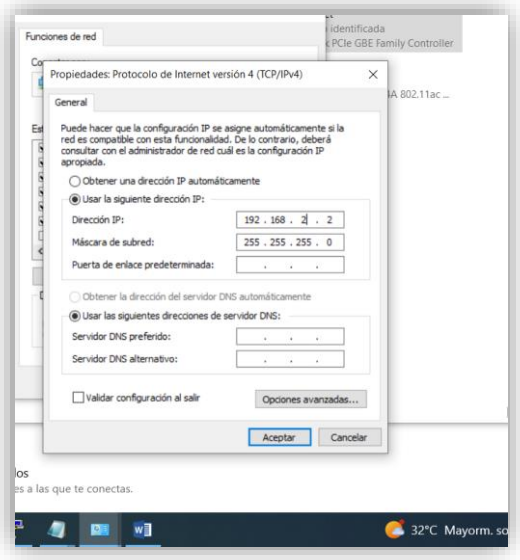


Figura 1.22 configuración de tarjeta de red.

Se ingresa vía web con **https://192.168.2.1** la IP es con la cual se le asigno desde el inicio y que se le configuro al Firewall como se muestra en la figura 23, esto es para iniciar la configurar la interfaz eth2 donde estará entrando y saliendo el tráfico de internet también en la figura 1.23, podemos configurar rutas estáticas u otras interfaces que lleguemos enaceitar a futuros cambios, también podemos configurar más segmentos y dividirlos entre las interfaces.

La interfaz eth2 tendrá la IP 192.168.1.146

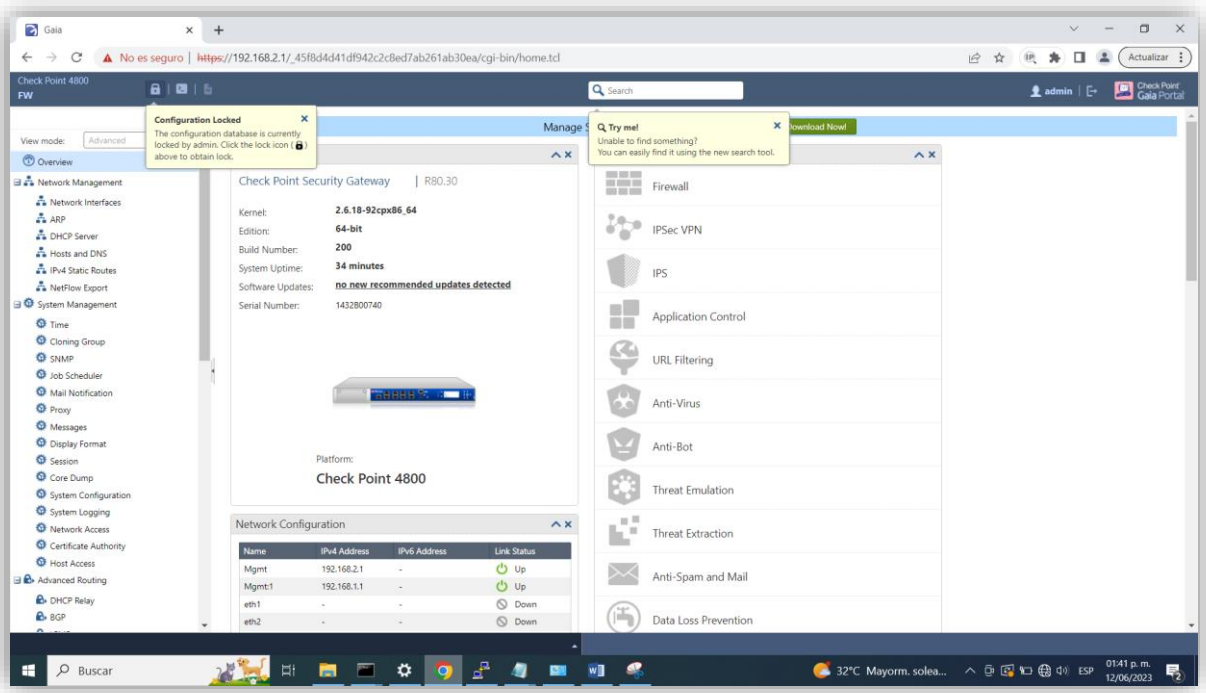


Figura 1.23. Interfaz web.

La interfaz Web está bloqueada se necesita dar clic en el candado de la figura anterior para poder configurar. Se le da clic al apartado de **network** interfaces y después se le da clic en eth1, se le da clic en **enable** para habilitar la interfaz s ele nombra LAN y se ingresa la IP del mismo del mismo segmento de la red LAN y después e hace lo mismo para la interfaz eth2 con dirección IP 192.168.1.146 que tendrá segmento hacia internet del modem.

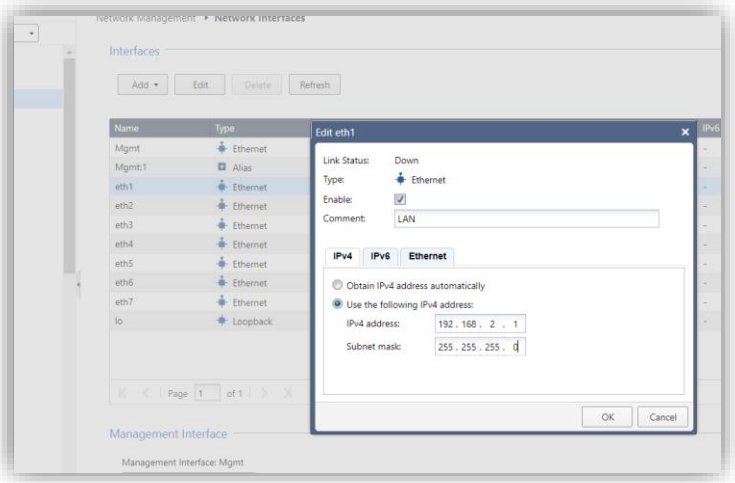


Figura 1.24. Editar interfaz.

Una vez configuradas ambas interfaces se puede logar ver que están en Up cada interfaz así mismo saber que están conectadas ambas. Aunque aparece en rojo la interfaz Mgmt porque ya no es necesario tenerla conectada debido que ya se tiene conectado el FW directamente mediante la red LAN.

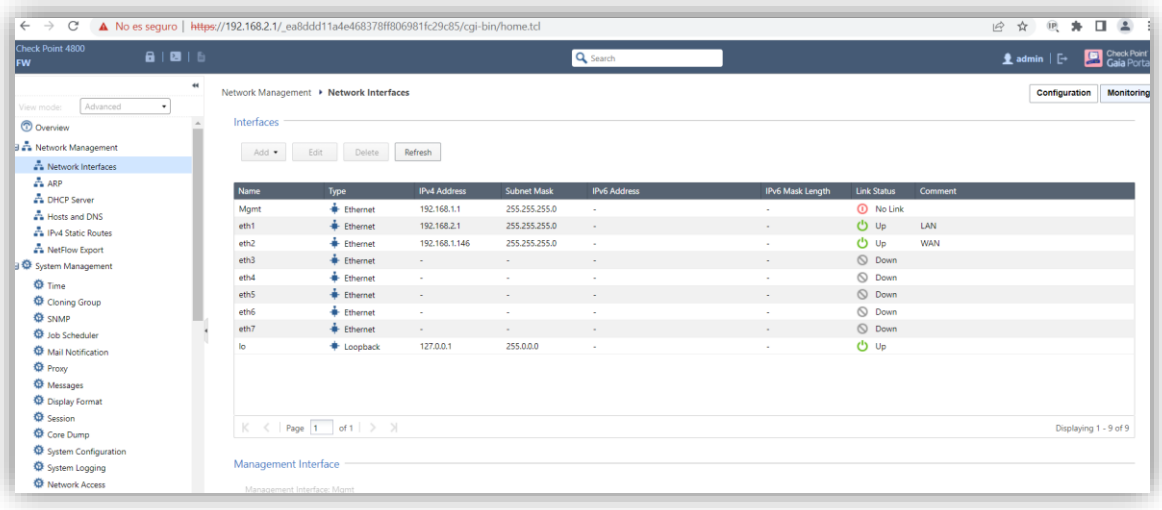


Figura 1.25. Configuración de Interfaz eth1, eth2.

Una vez echo la configuración de la interfaz eth1 y eth2, se procese a descargar el ejecutable de la consola de administración de Checkpoint que es compatible con modelo del firewall que se usó, se puede buscar desde cualquier navegador dicha información.

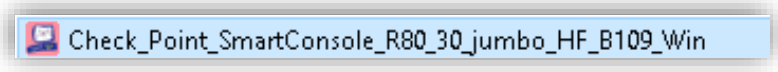


Figura 1.26. Ejecutable de consola de administración.

Se ejecuta y se espera a que se empiece a instalar como se muestra en la figura 1.27:

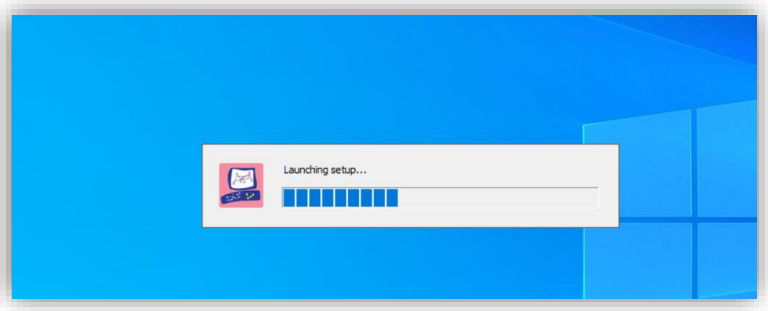


Figura 1.27. Ejecución de la Instalación de consola de administración.

En la figura 1.28 muestra el inicio para la instalación y ubicación del archivo a ejecutar.

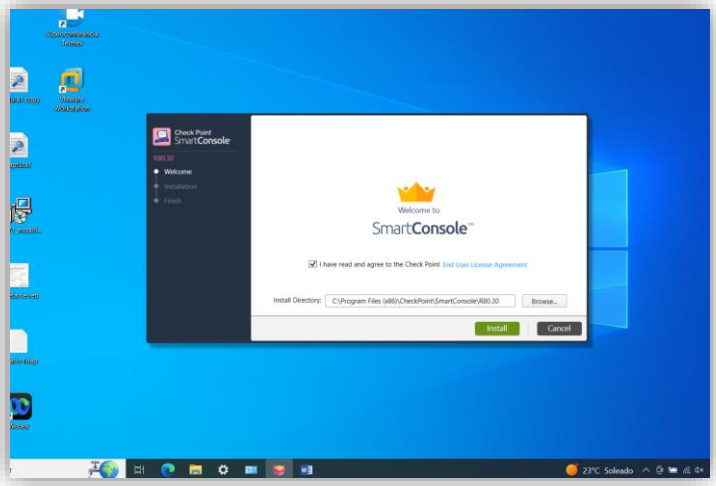


Figura1. 28. Instalación de la consola de administración.

En la figura 1.29, se muestra el porcentaje de la instalación.

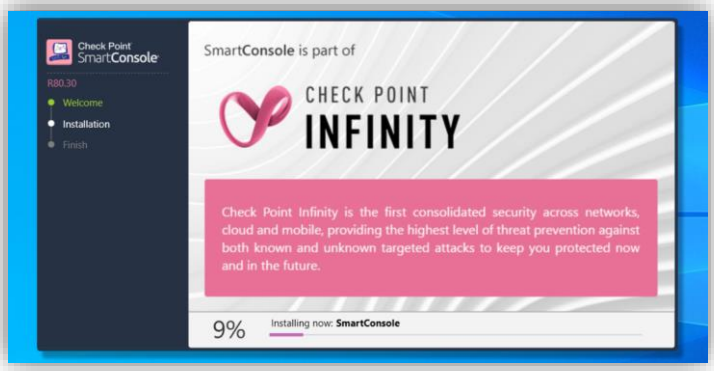


Figura 1.29. Procesando instalación.

Una vez terminada la instalación le damos clic en **Finish**.

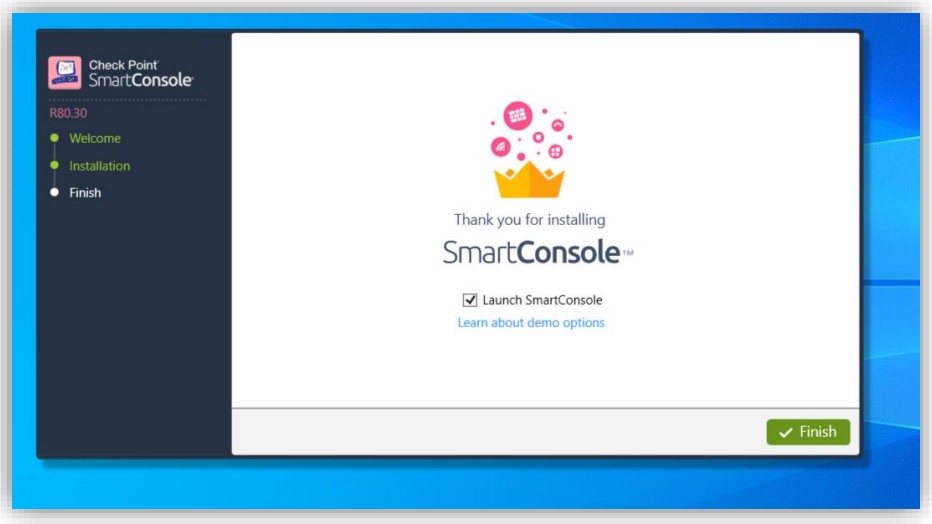


Figura 1.30. Finalización de instalación.

Entramos con nuestras credenciales que anteriormente se mencionó y se teclea la IP 192.168.2.1 del Firewall para ingresar a la consola de administración del equipo que previamente se instaló en el Firewall como se muestra en la figura 1.31.

En esta parte se crea una contraseña nueva: **admin$1**

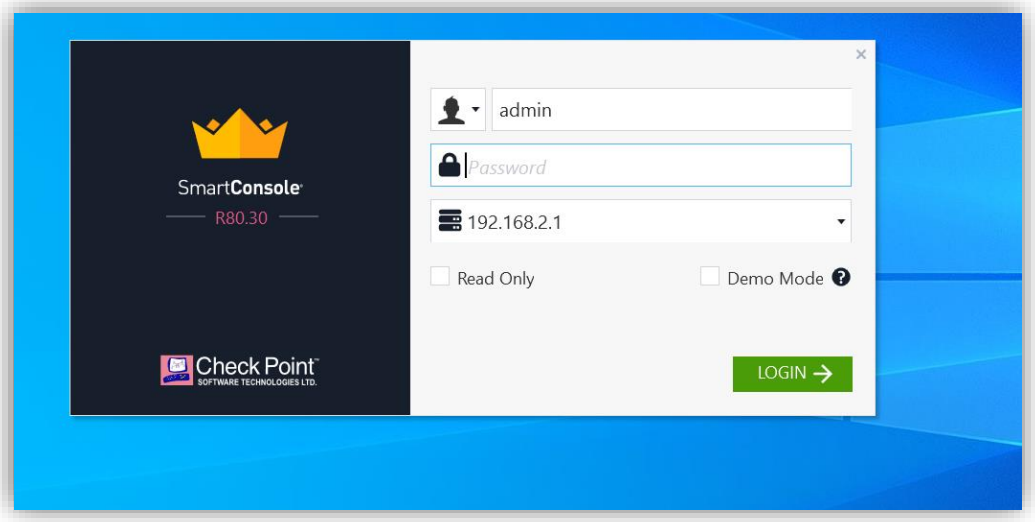


Figura 1.31. Acceso a la consola de administración del Firewall

En la siguiente figura se muestra el inicio de la consola de administración y breves explicaciones para el uso del Firewall como ver los logs, control de acceso, prevenir ataques, etc. como se muestra en la figura 1.32.

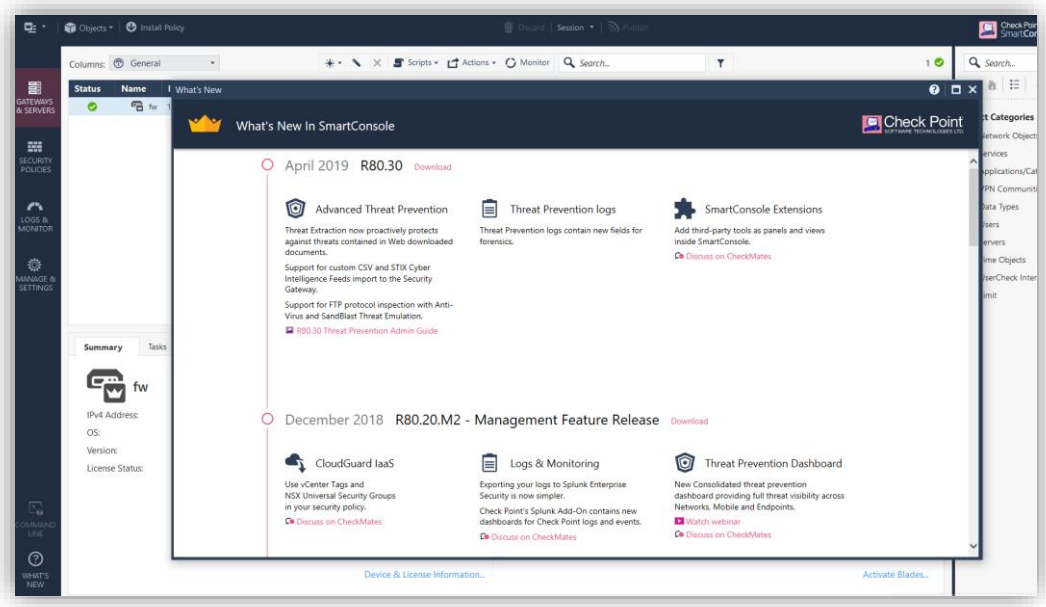


Figura 1.32. Inicio de la consola de administración.

Una vez cerrando la ventana de explicación, se muestra en la consola de administración el FW que se tiene dado de alta para empezar la configuración de políticas, también se puede ver del lado derecho el buscador de hots y grupos para generar los mismos, del lado izquierdo se puede apreciar a ver la opción de Gateways, la opción de políticas de seguridad y poder ver los logs, como se muestra en la figura 1.33.

En la opción Gateways podemos ver que ya está sincronizado nuestro Firewall con la consola y con una paloma en verde que está en línea, también podemos ver la IP que le asigno nuestros Firewall anteriormente y como está el estatus de su CPU.

Arriba podemos apreciar ver la opción de objetos que se pudieran a necesitar y lo más importante la instalación para cualquier cambio nuevo.

Al final de la figura 1.33. también nos muestra el modelo del equipo y su versión.

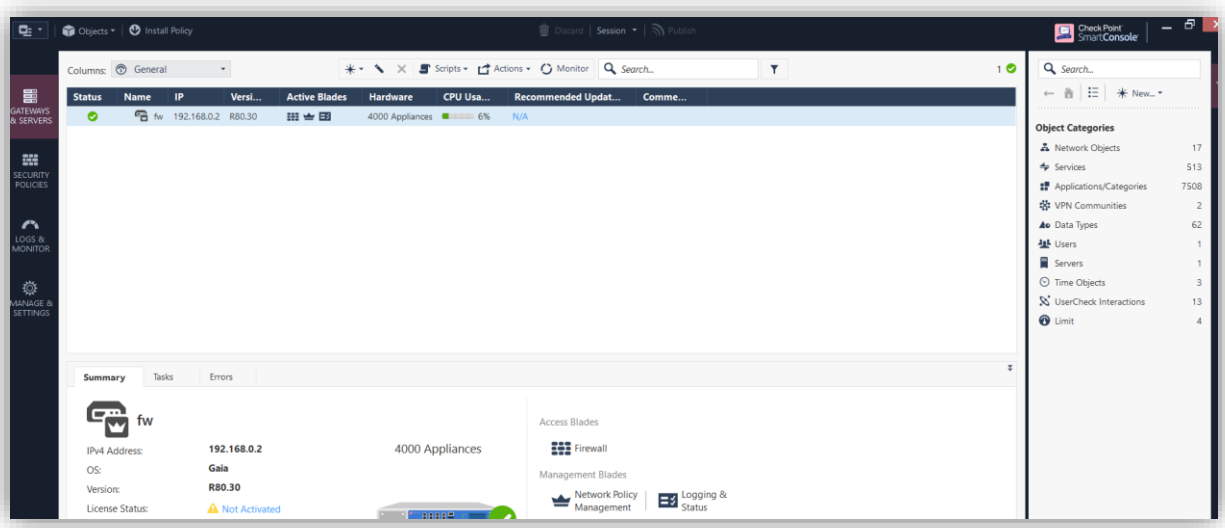


Figura 1.33. Firewall sincronizado con la consola.

2.3 Creación de reglas y validación

Para empezar a realizar la creación de reglas, primero se realizó una prueba de mandar un **ping** desde la IP 192.168.2.2 que anteriormente se había ejecutado hacia la IP 192.168.2.1 del FW como se muestra en la figura 1.34:

```
C:\Users\PC>ping 192.168.2.1

Haciendo ping a 192.168.2.1 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.2.1:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\PC>
```

Figura 1.34. Mandando ping al Firewall.

Se aprecia a ver en la figura 34, que no se puede alcanzar a ver la IP del FW debido a que por default el FW bloque cualquier protocolo.

Nos vamos a la consola de administración al apartado del lado izquierdo donde dice **SECURITY PÓLICES** ahí podemos apreciar en policy que la primera regla por default está bloqueando todo el tráfico de entrada a cualquiera como se muestra en la figura 1.35.

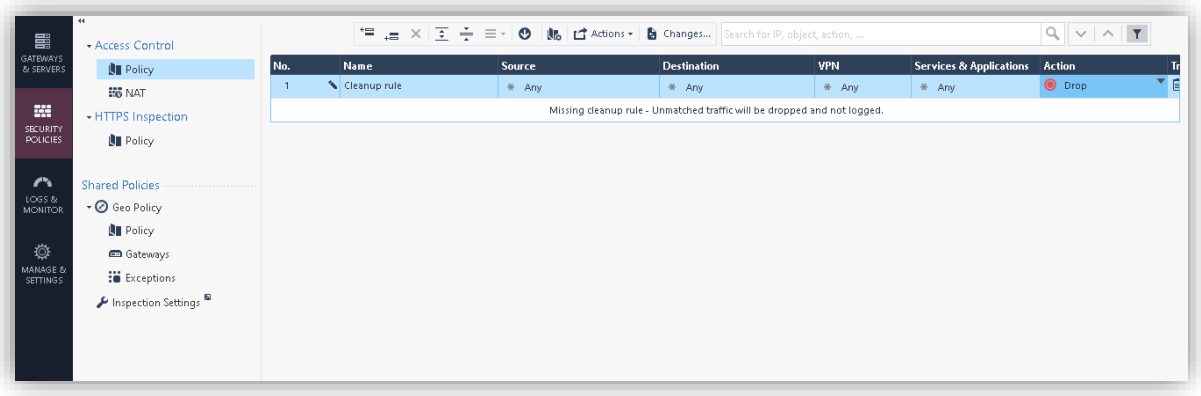


Figura 1.35. Regla que bloquea todo el tráfico.

Después donde se encuentra la primera regla le damos clic derecho para después crear una etiqueta que separa las reglas y la nombramos **Administrador** como se muestra en la figura 1.36:

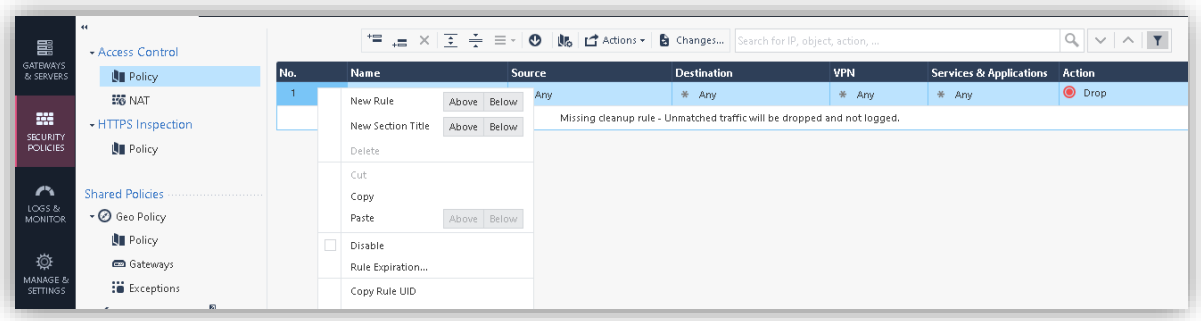


Figura 1.36. Creando etiqueta.

Ya creada la etiqueta de Administrador, después se le da clic derecho para seleccionar nueva regla:

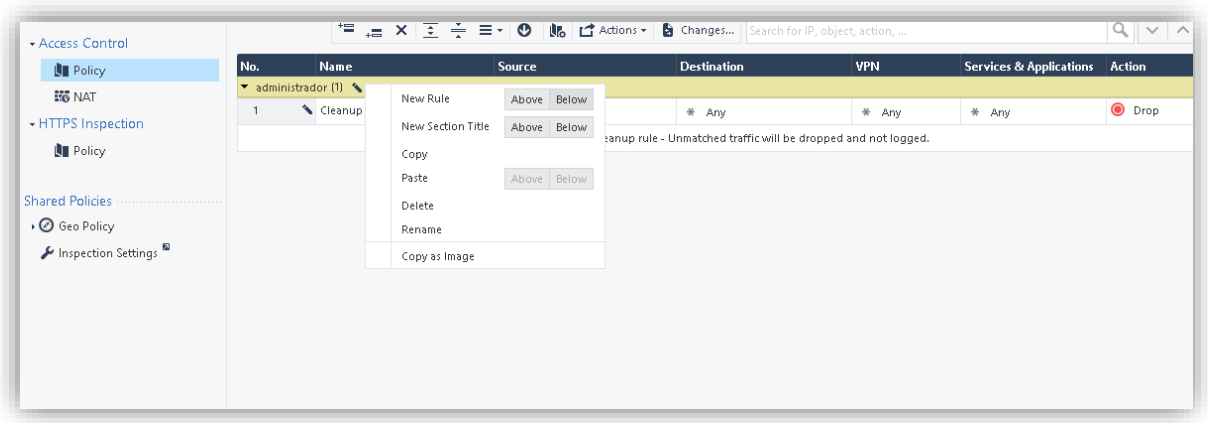


Figura 1.37. Creando regla.

Una vez creada la regla, se le da el nombre de ping (esto se realizó para crear la regla de prueba) esta regla ayudara a permitir el acceso al protocolo ICMP esta como se muestra en la figura 1.38.

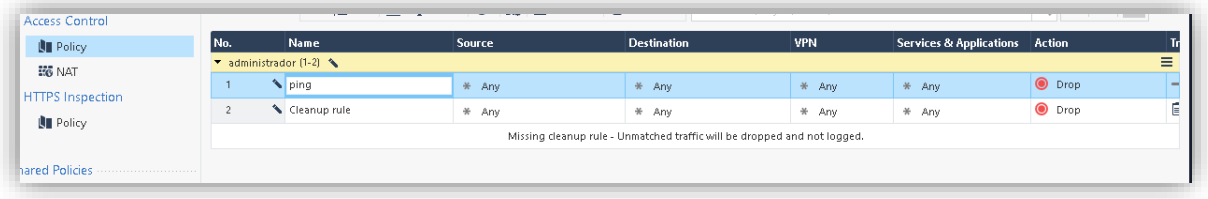


Figura 1.38. Comentando regla.

Se empieza creando un objeto nuevo del lado derecho dándole clic en host como se muestra en la figura 1.39:

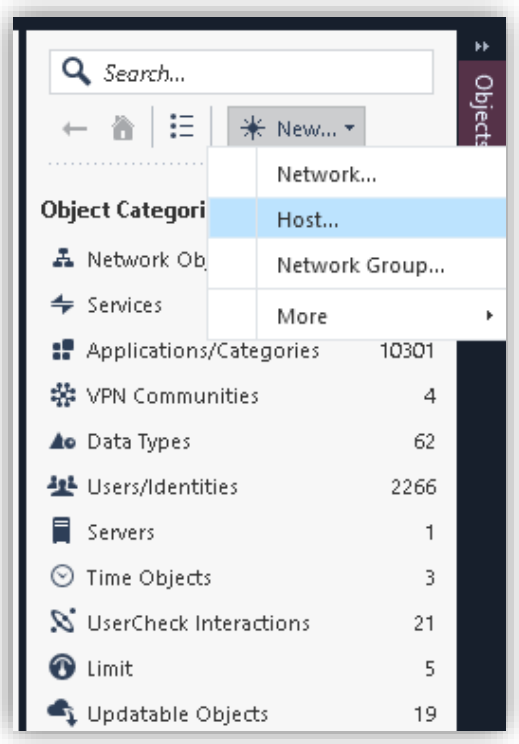


Figura 1.39. Creando host.

Se asigna un nombre para identificar el nuevo objeto y la dirección IP que se desea que tendrá comunicación por **ping** como se muestra en la siguiente figura 1.40:

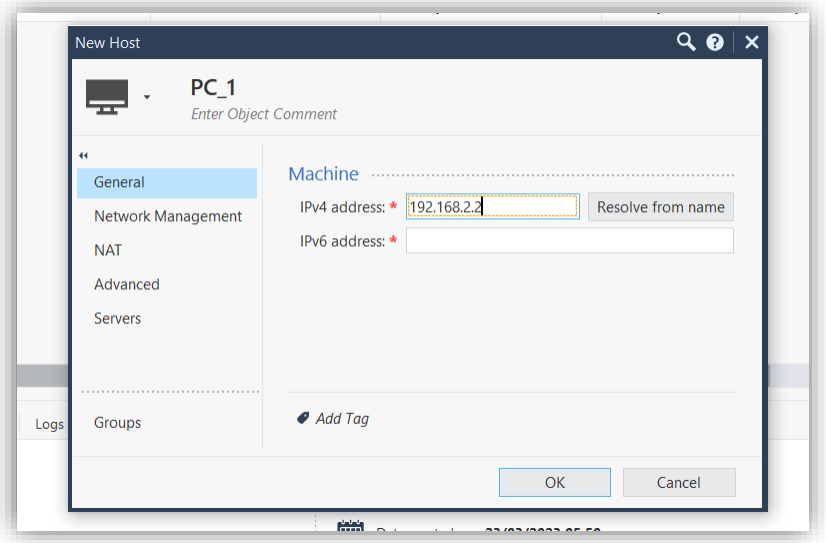


Figura 1.40. configurando IP de host.

Ya creado el host u objeto en la regla se empieza asignar en **source** el origen dándole clic izquierdo en el signo de más para que no se muestre una pequeña ventana donde buscaremos el host que se creó anterior mente con la IP 192.168.2.2 cómo se muestra en la figura 1.41 y se selecciona para añadirlo a la regla.

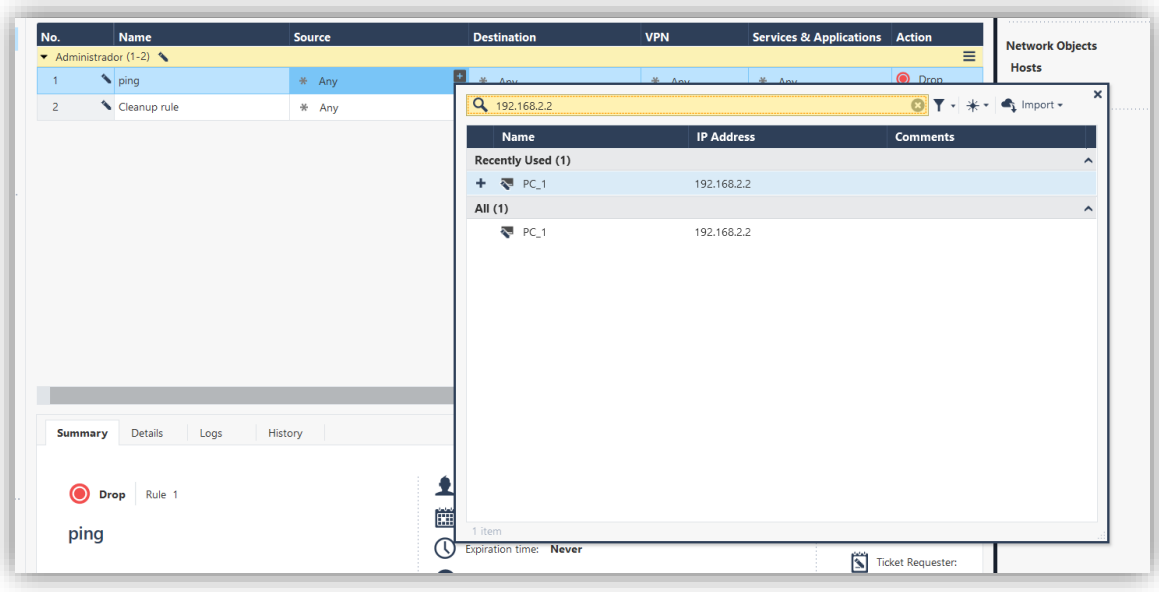


Figura 1.41. Agregando host.

Después en **destiation** de igual manera con clic izquierdo se busca el FW y se añade como se muestra en la figura 1.42.

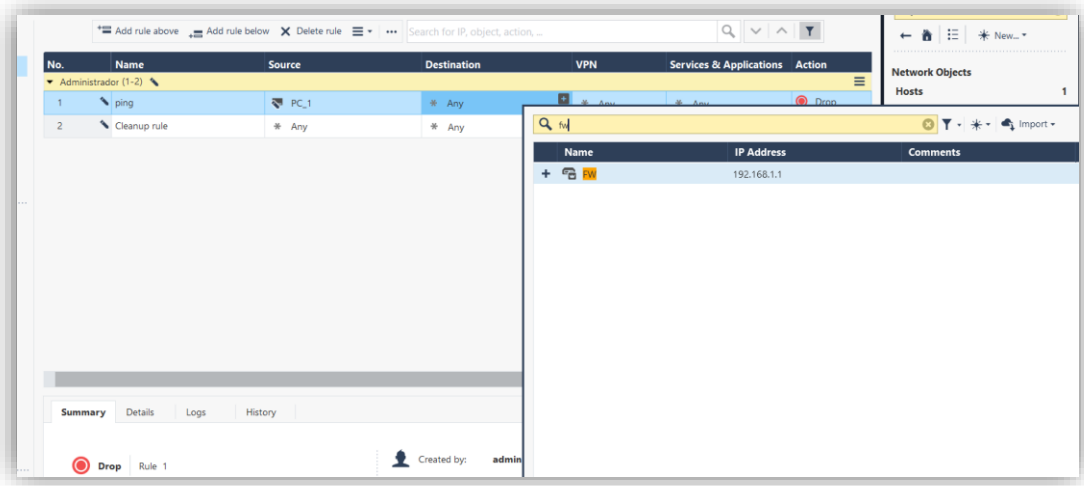


Figura 1.42. Agregando destino.

En **action** se le da clic izquierdo y se busca el protocolo ICMP para añadirlo como se muestra en la siguiente figura 1.43.

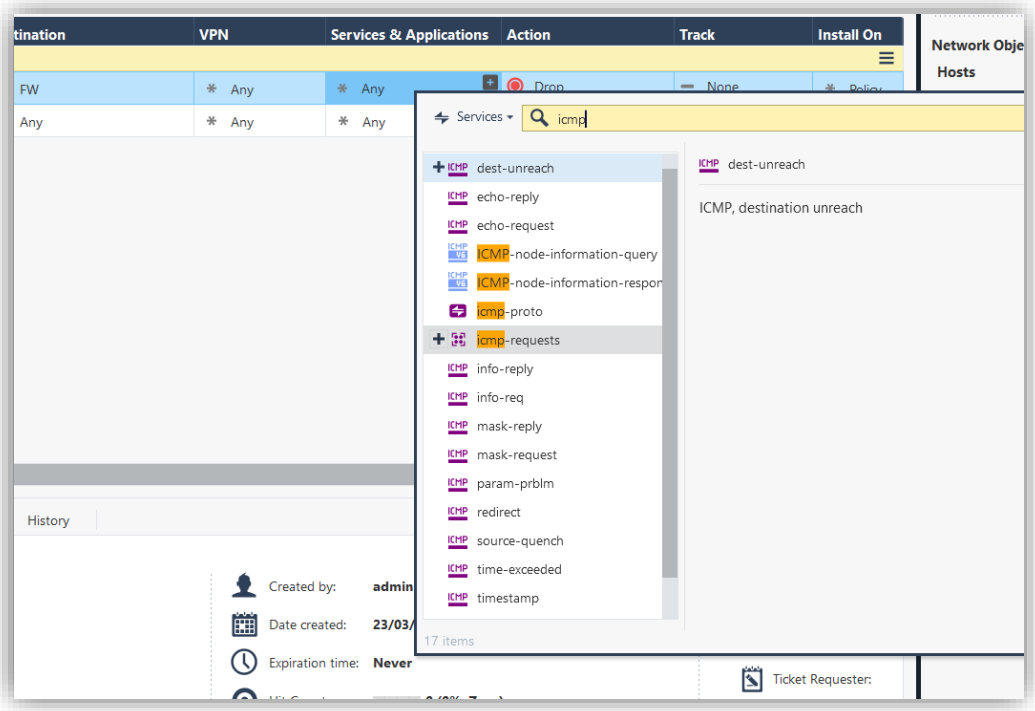


Figura 1.43. Agregando protocolo

En **log** se le da clic derecho para selecciona log y tener log en la consola de la regla que se creó como se muestra en la figura 1.44:

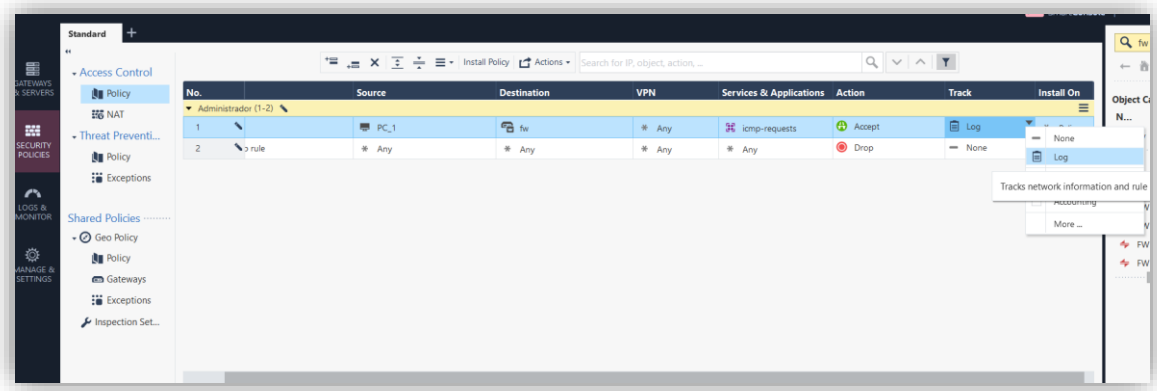


Figura 1.44. Habitando log.

Por ultimo en **install on** se le da clic derecho y se selecciona el FW que se configuro y donde se instalara la política como se muestra en la figura 1.45.

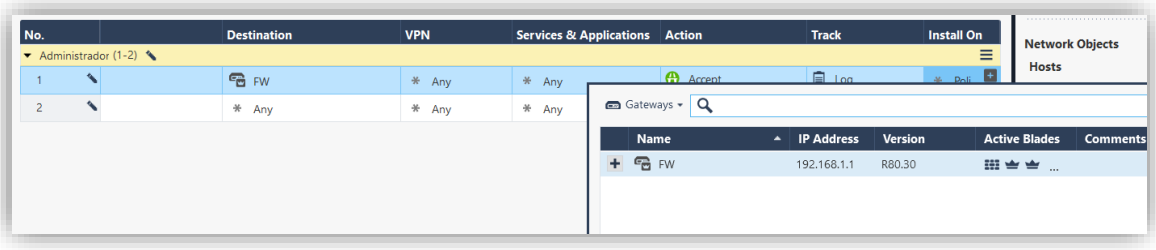


Figura 1.45. Seleccionando el firewall para la instalación.

Una vez echo los pasos anteriores la regla quedaría:

Que cuando Pc_1 quiera ir al FW por el protocolo IMCP será aceptada la petición y serán mostrados los log en el FW como se muestra la figura 1.46:

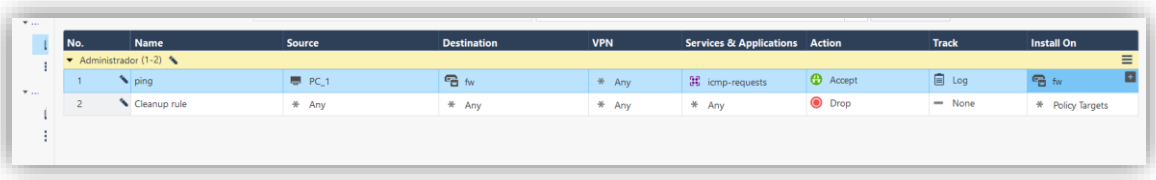


Figura 1.46. Como debe quedar la regla.

Después se mostrará en la parte arriba de la consola los cambios que se realizaron en color amarillo y se le da clic lado izquierdo donde dice **install policy** esto es para instalar la política que se realizó anteriormente, como se muestra en la figura 1.47.

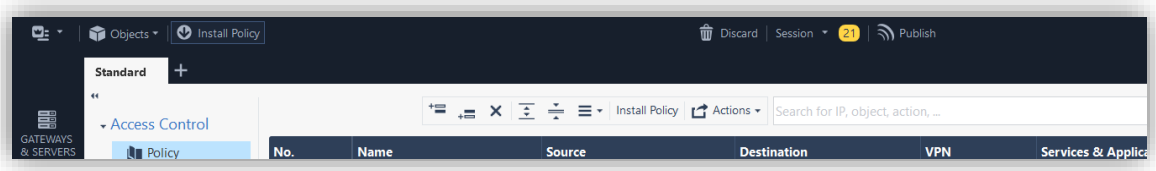


Figura 1.47. De cambios realizados.

Después de instalar la política nos aparecerá una venta de que si estamos de acuerdo en instalar los cambios que se realizaron y le damos clic en **publish & install** como se muestra en la figura 1.48.

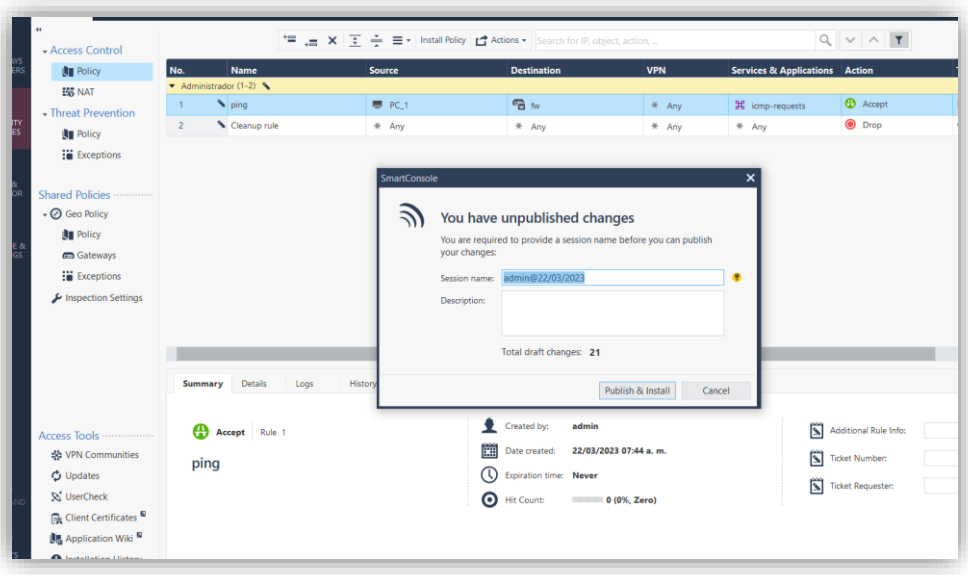


Figura 1.48. Mensaje antes de mandar a instalar política

Después aparecerá una ventana donde se muestra el tipo de política que se instalará y en que FW y tipo de versión que se está usando y le damos clic en **install** como se muestra en la figura 1.49:

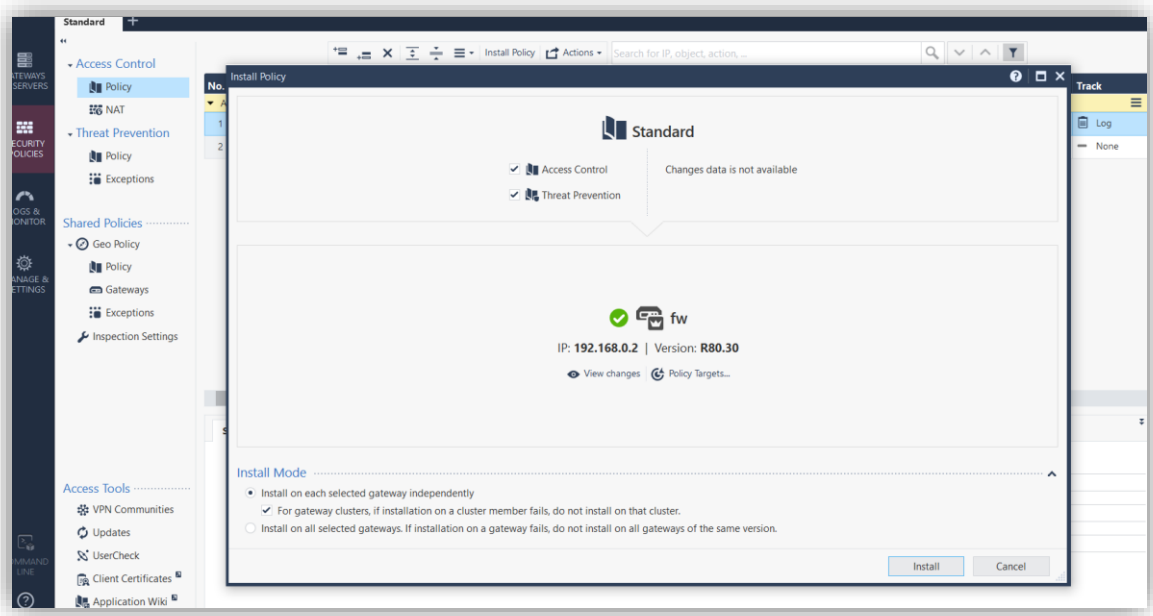


Figura 1.49. Instalar política.

De lado izquierdo abajo se aprecia ver una barra que indica el porcentaje de instalación en el FW que cuando termine de instalar en el FW se mostrara una paloma en verde como se muestra en la figura 1.50.

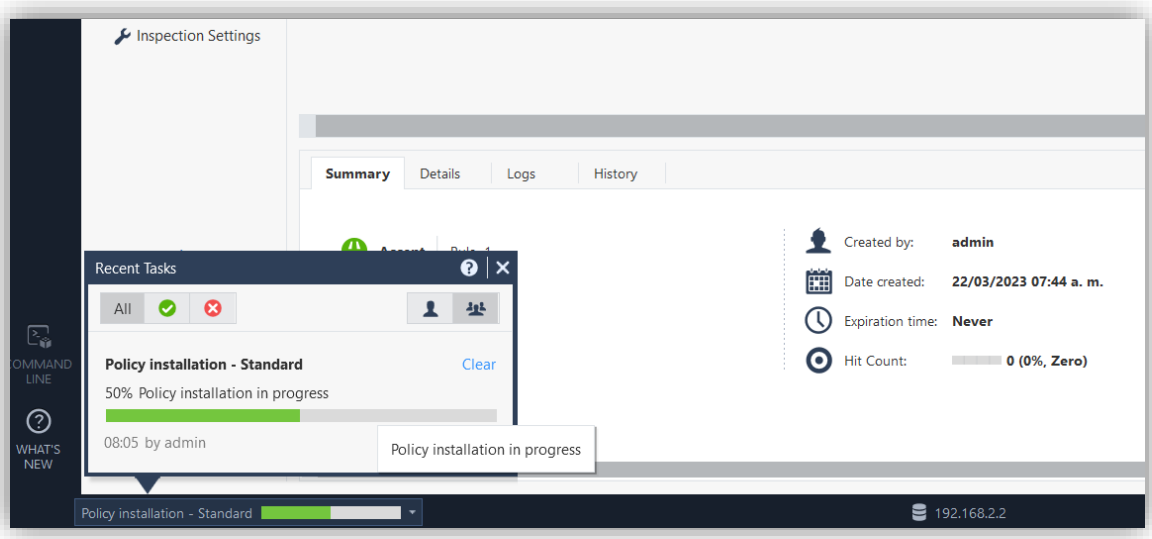


Figura 1.50. Instalando política.

Nuevamente se realiza una prueba de mandar un ping desde la IP 192.168.2.2 hacia la IP 192.168.2.1 del FW donde se ve que empieza a contestar como se muestra en la siguiente figura 1.51.

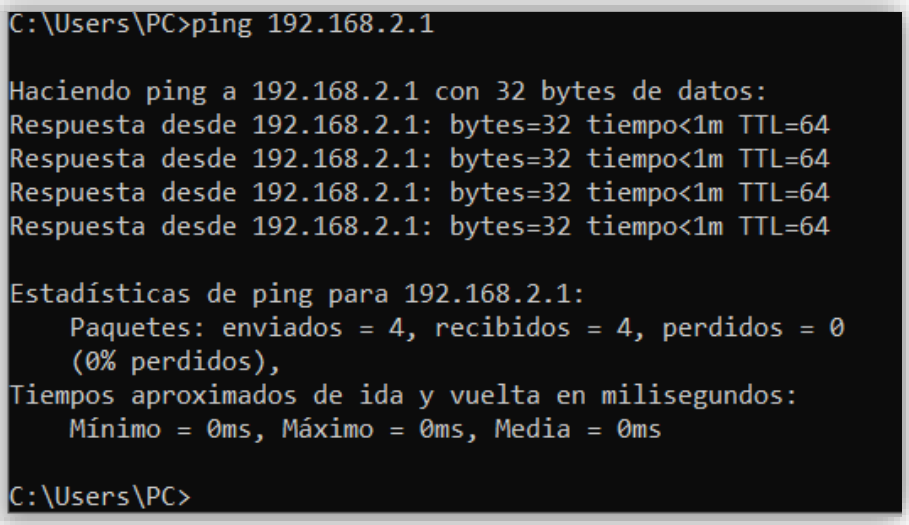


Figura 1.51. Contestación del ping hacia el FW.

Se procede a revisar los **logs** del FW, se le da clic del lado izquierdo en la opción de **logs y monitor** en la consola, se puede apreciar a ver la aceptación de las peticiones del *ping* hacia el FW como se muestra en la parte sombreada dé la figura 1.52.

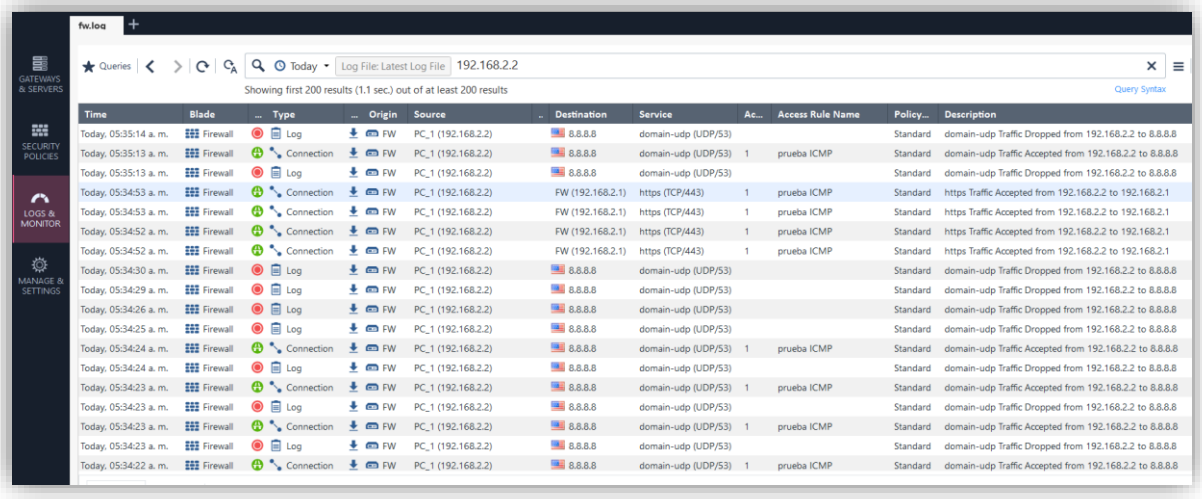


Figura 1.52. Logs del FW

Una vez validado que la que la **PC_1** va ser la única PC que va tener acceso al FW se crea una regla de administración. Como se muestra la figura 1.53, esto ayudara a futuro para solo añadir las PC o IPs que tengan acceso a la administración de FW y el control del acceso a internet.

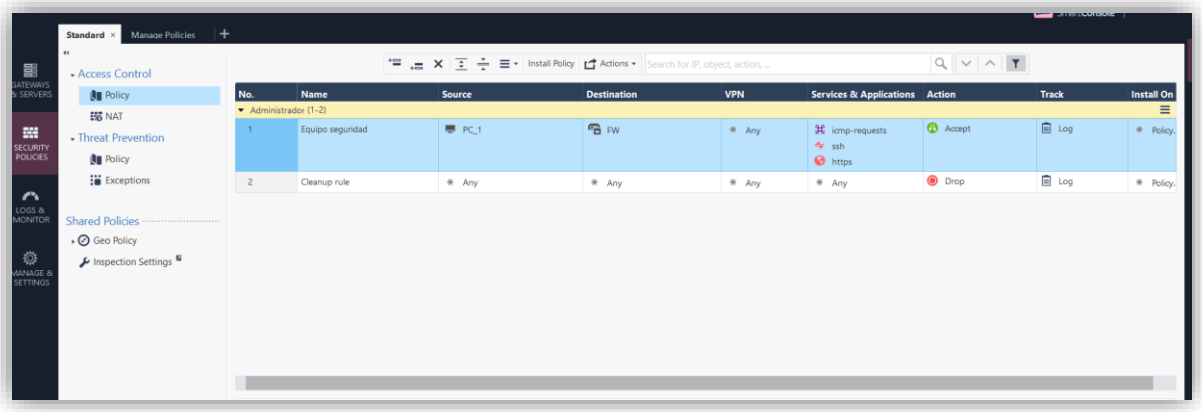


Figura 1.53. Regla de administración.

Una vez terminado la regla de administración, se usa la PC_2 y se configura la IP 192.168.2.3 y se pone la IP 8.8.8.8 en el DNS (sistema de nombres de dominio) primario que son de google en la tarjeta de red de la laptop, cómo se muestra en la figura 1.54 de abajo, esa IP se usará para realizar pruebas salida hacia internet.

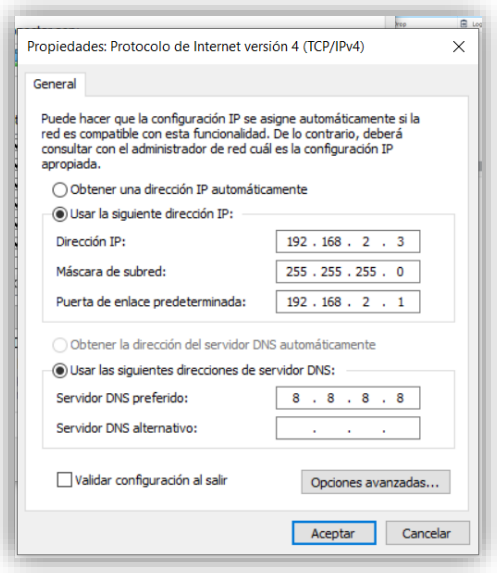


Figura 1.54. Configuración de PC_2

Se procede a verificar que el FW tenga salida a internet para realizar pruebas con la PC_2, se conecta al FW por línea de comando mediante **PUTTY** con el usuario y contraseña que al inicio se le asignó al equipo como se muestra en la figura 1.55.

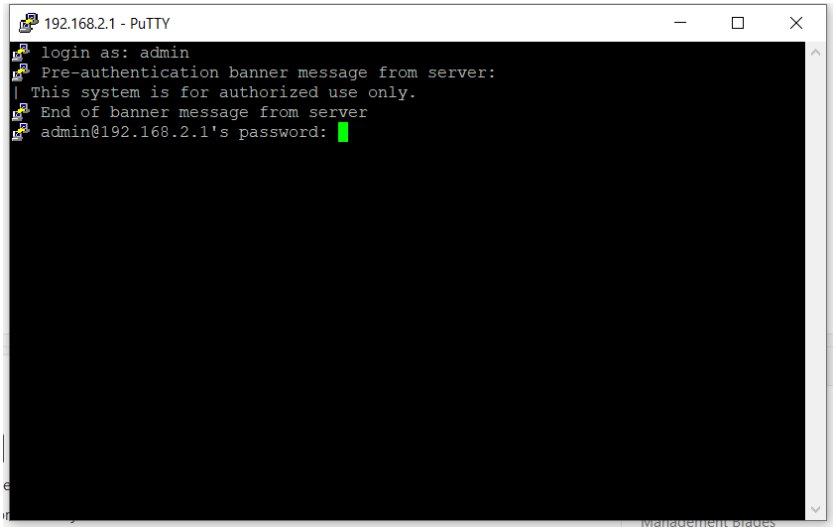


Figura 1.55. Acceso al FW mediante PUTTY.

Una vez dentro de la línea del FW se realiza un ***//ping a 8.8.8.8*** para ver que tenga salida hacia internet como se muestra en la figura 1.56, mostrando la contestación de dicho protocolo de comunicación, esto quiere decir que ya está listo el FW para dar acceso a internet.

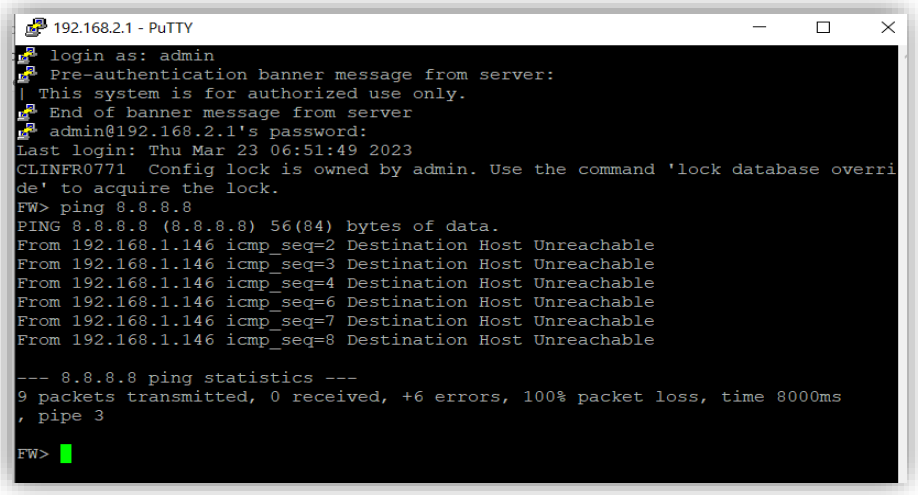


Figura 1.56. Ping hacia 8.8.8.8

Después de comprobar que tiene salida el FW, se crea una regla de salida para la PC_3, en esto se agrega el nombre del host, en el destino se agrega hacia internet y en servicios y aplicaciones se añade el protocolo https o puerto 443 como se muestra en la figura 1.57.

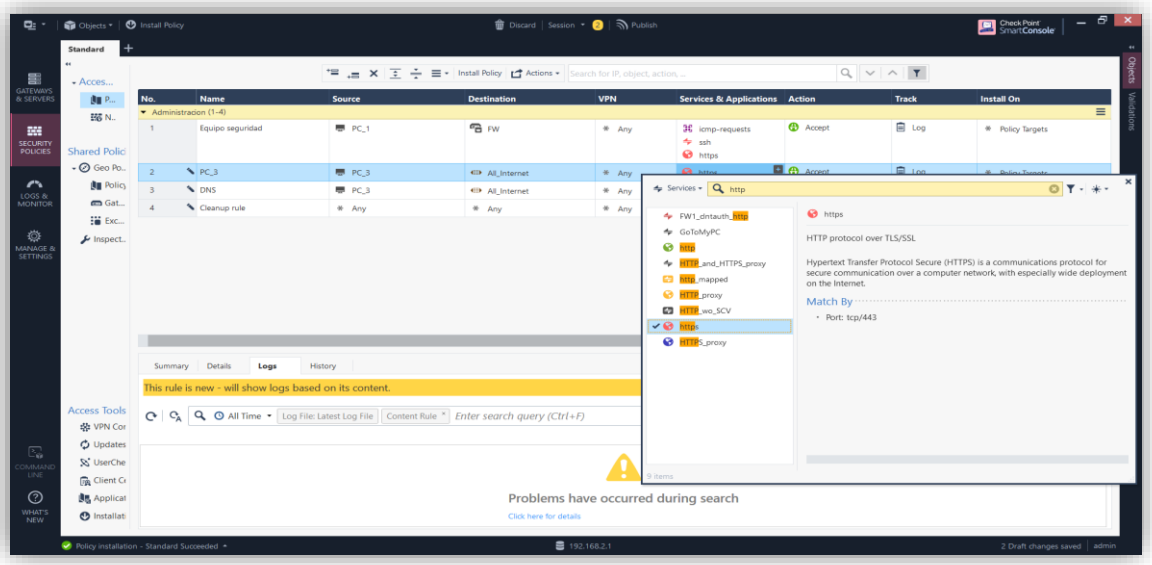


Figura 1.57. Agregando el protocolo HTTPS o puerto 443.

La regla de acceso a internet para la PC_3 que daría como se muestra en la figura 1.58 y se procede a instalar la política como anteriormente ya se había explicado.

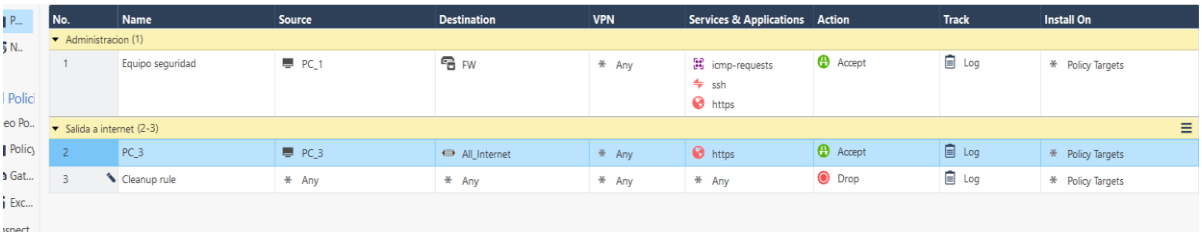


Figura 1.58. Regla de acceso a internet ya terminada.

Después de terminar la instalación de la política, se realiza una prueba de navegación web, pero marca error de nombre de DNS la página web como se muestra en la figura 1.59.

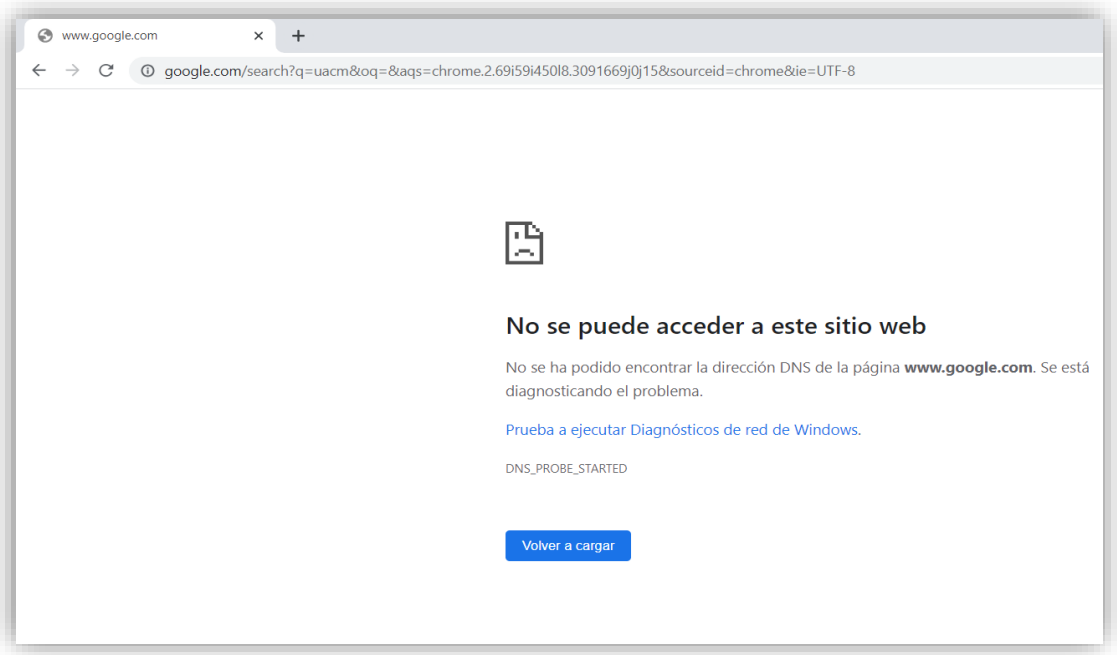


Figura 1.59. Error de DNS

Se procede a revisar los log del FW para ver qué es lo que está sucediendo con la petición. Una vez revisando los logs se logra ver que en el FW si acepta la petición de la salida hacia internet esto está de color verde, pero está bloqueando la petición hacia el DNS de google en color rojo como se muestra en la figura 1.60, esto se debe a que nos hace falta otra configuración en nuestro FW en la salida hacia internet.

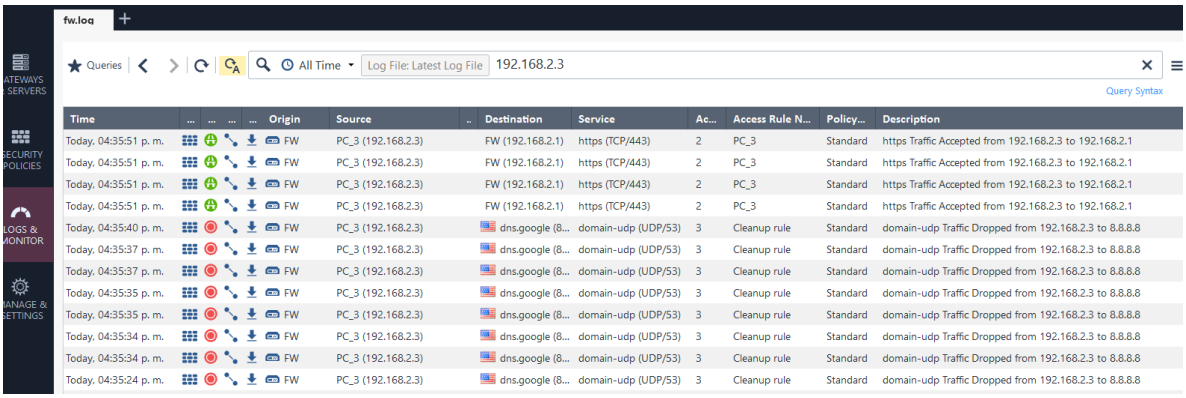


Figura 1.60. Logs del FW.

Se procede a crear otra regla de acceso con el protocolo de **DNS** agregando en servicio y aplicaciones el protocolo que hace falta como se muestra en la figura 1.61.

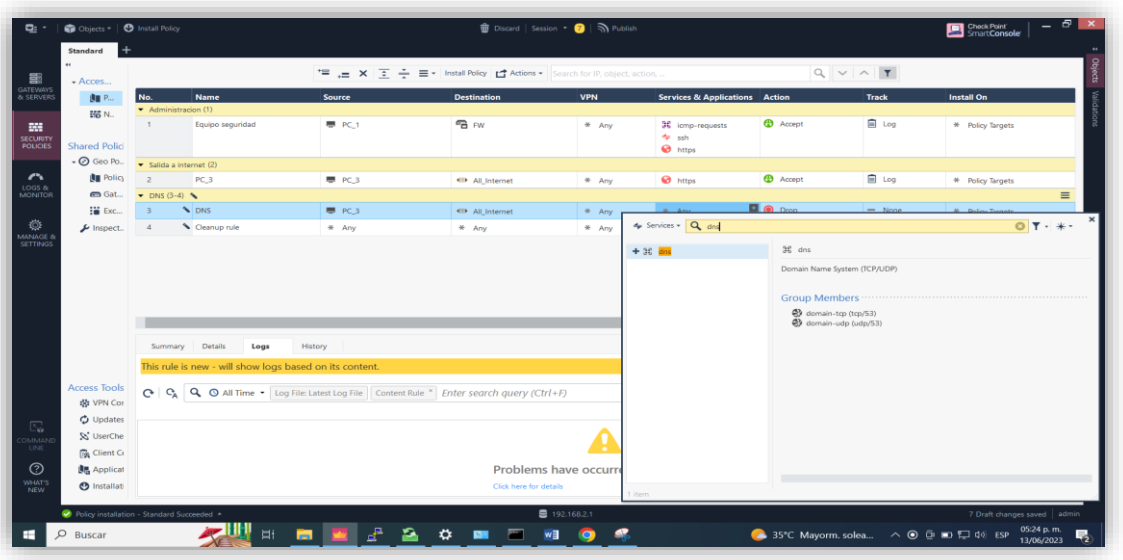


Figura 1.61. Regla de DNS.

Después de a ver creado la regla de DNS e instalado, se procede a hacer nuevamente la prueba en el navegador web y el resultado es satisfactorio. Como se nuestra en la figura 1.62.

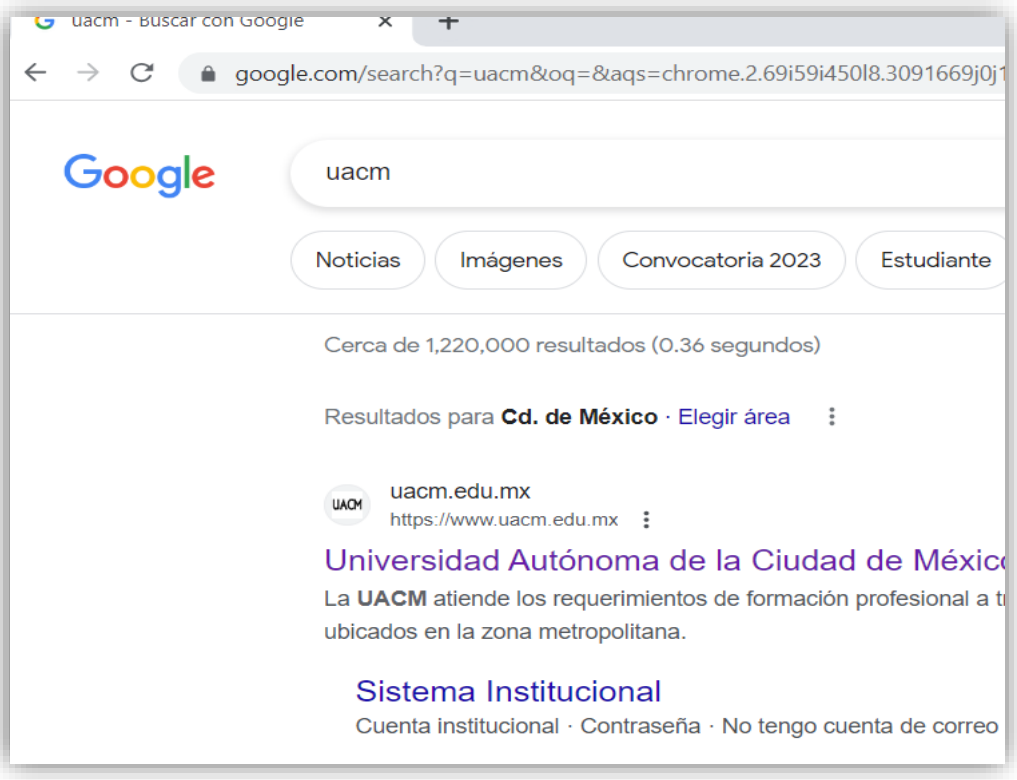


Figura 1.62. Buscando página web.

Ya teniendo visibilidad de la navegación web de la PC_3 correcta y de que está funcionando la navegación web, se abre la página web de la UACM y se busca la IP publica con una herramienta instalada en el navegador web, como se muestra en la figura 1.63.

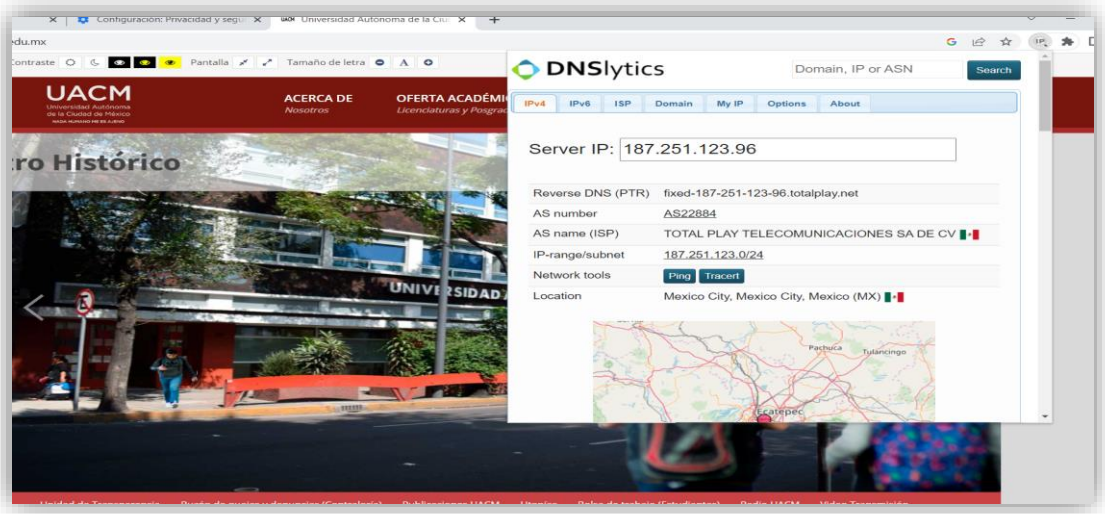
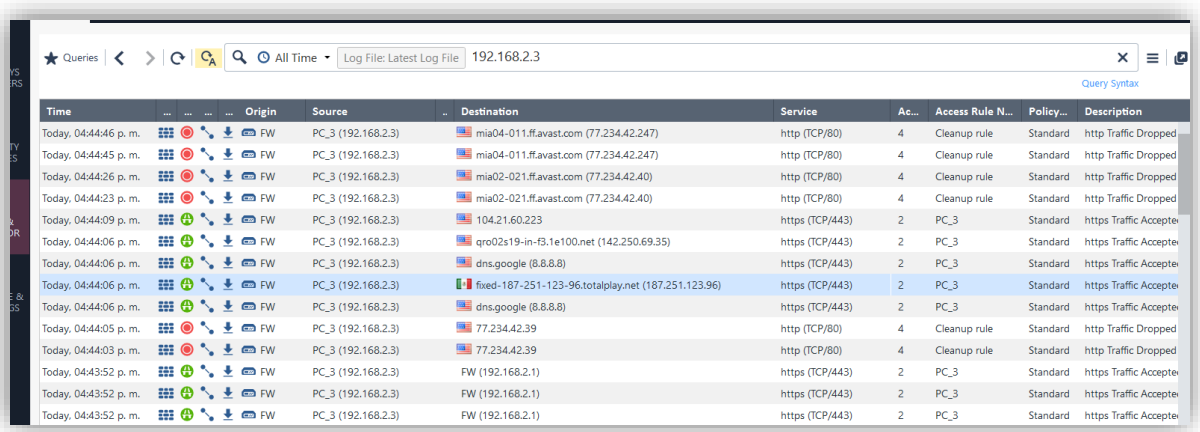


Figura 1.63. Página web y IP pública.

Para concluir se revisa los logs del FW para comprobar que se tiene peticiones aceptadas de color verde hacia la IP publica yaciendo en la regla que se configuro anteriormente de la página web como se muestra en la siguiente figura 1.64 en lo sombrero.



Time	Origin	Source	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 04:44:46 p. m.	FW	PC_3 (192.168.2.3)	mia04-011.ff.avast.com (77.234.42.247)	http (TCP/80)	4	Cleanup rule	Standard	http Traffic Dropped
Today, 04:44:45 p. m.	FW	PC_3 (192.168.2.3)	mia04-011.ff.avast.com (77.234.42.247)	http (TCP/80)	4	Cleanup rule	Standard	http Traffic Dropped
Today, 04:44:26 p. m.	FW	PC_3 (192.168.2.3)	mia02-021.ff.avast.com (77.234.42.40)	http (TCP/80)	4	Cleanup rule	Standard	http Traffic Dropped
Today, 04:44:23 p. m.	FW	PC_3 (192.168.2.3)	mia02-021.ff.avast.com (77.234.42.40)	http (TCP/80)	4	Cleanup rule	Standard	http Traffic Dropped
Today, 04:44:09 p. m.	FW	PC_3 (192.168.2.3)	104.21.60.223	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte
Today, 04:44:06 p. m.	FW	PC_3 (192.168.2.3)	qro02s19-in-f3.1e100.net (142.250.69.35)	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte
Today, 04:44:06 p. m.	FW	PC_3 (192.168.2.3)	dns.google (8.8.8.8)	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte
Today, 04:44:06 p. m.	FW	PC_3 (192.168.2.3)	fixed-187-251-123-96.totalplay.net (187.251.123.96)	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte
Today, 04:44:06 p. m.	FW	PC_3 (192.168.2.3)	dns.google (8.8.8.8)	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte
Today, 04:44:05 p. m.	FW	PC_3 (192.168.2.3)	77.234.42.39	http (TCP/80)	4	Cleanup rule	Standard	http Traffic Dropped
Today, 04:44:03 p. m.	FW	PC_3 (192.168.2.3)	77.234.42.39	http (TCP/80)	4	Cleanup rule	Standard	http Traffic Dropped
Today, 04:43:52 p. m.	FW	PC_3 (192.168.2.3)	FW (192.168.2.1)	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte
Today, 04:43:52 p. m.	FW	PC_3 (192.168.2.3)	FW (192.168.2.1)	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte
Today, 04:43:52 p. m.	FW	PC_3 (192.168.2.3)	FW (192.168.2.1)	https (TCP/443)	2	PC_3	Standard	https Traffic Accepte

Figura 1.64. Logs de salida a internet.

Conclusiones

En base a este trabajo, se concluye lo siguiente:

1. Todo lo que aprendí en la carrera no fue suficiente para poder completar esta tesis debido a que se necesitó reforzar conocimientos en algunos temas como redes, seguridad perimetral, el cómo es el funcionamiento en diferentes ambientes de trabajo dentro de una red local para interconectar: Switch, computadoras, servidores y otros dispositivos de seguridad informática.
2. En el ámbito laboral aprendí el correcto funcionamiento de un Firewall perimetral y su arquitectura, mediante una consola de administración que tiene un conjunto de reglas y aplicaciones para mantener un control del acceso de usuarios, esto también ayuda a tener una monitoreo del tráfico de entrada y salida, mi experiencia obtenida en lo laboral me ayudo a plasmar la configuración de un Firewall en este trabajo de tesis y poder compartirla con el fin de mejoras a futuras.
3. Para poder plasmar la configuración, me apoye de las materias de la carrera como redes, seguridad informática y proyectos que anteriormente había desarrollado para darle un mejor visón a la tesis.
4. Se configuro un Firewall con la arquitectura presentada y se implementaron políticas propuestas para pruebas las cuales permitieron el control de acceso a atreves del firewall, funcionando correctamente como se mostró.
5. Se concluye que la seguridad informática tiene como finalidad la confidencialidad, integridad y disponibilidad de la información para aplicarlo en cualquier organización. El trabajo que se realizo es un ejemplo de una red local de pruebas, para demostrar que se puede proteger mediante la puesta de operación de un firewall en un punto estratégico perimetral. Realizando reglas de control de acceso, esto ayuda a tener una mejor administración en la organización de un sistema y monitoreo para prevenir ataques de diferentes tipos, como evitar acceso a sitios maliciosos y poner en riesgo la organización o fuga información entre otros.
6. En este trabajo se propusieron reglas para realizar pruebas de acceso como salir a internet , consultar un DNS y poder usar el protocolo ICMP con un control más seguro, pero no quiere decir que son suficientes para tener una seguridad sólida, también se pueden crear reglas basando se en grupos de IPs con diferentes perfiles de navegación por ejemplo crear reglas para acceso para sitios de búsqueda de información, de redes sociales, video y entre otros, también hay que tener en cuenta que se debe revisar que puertos se van utilizar para determinar la regla de acceso en conjunto con el tipo de navegación a usar.
7. En este trabajo se logra tener un resultado con una mayor visión de conexiones del tráfico de una red LAN hacia una red WAN con seguridad mediante un firewall que controla el acceso mediante las reglas propuestas,

ya que es de gran valor para la organización mantener la seguridad perimetral y evitar el robo de información, por dicha razón es importante mantener o implementar políticas de seguridad para una organización acorde a las necesidades del usuario y evitar el robo de información y mantener protegidos los usuarios me diente un firewall perimetral ya que es la puerta principal.

8. Se propone reforzar la seguridad interna con un antivirus moderno instalado en las PCs de los usuarios debido a que es una solución de seguridad confiable con múltiples capas de avanzadas puede detectar, neutralizar y eliminar incluso el malware profundamente incrustado en la PC del usuario, proteger a los usuarios contra ransomware, spyware, spam, phishing y otras técnicas de ingeniería social, y también puede identificar los intentos de los atacantes de explotar vulnerabilidades en el sistema ya que el firewall solamente protegerá el perímetro de ataques y acceso a sitios maliciosos.
9. La ciberseguridad con inteligencia artificial es un nuevo surgimiento con el aprendizaje automático, esto se vuelve una herramienta valiosa con aplicaciones de amplio alcance. Debido a que a medida que la IA avance, se convertirá cada vez más en una parte central del panorama de la seguridad. La IA tiene aplicaciones tanto ofensivas como defensivas, y se utiliza para desarrollar nuevos tipos de ataques y crear defensas contra ellos.
10. Se espera que este trabajo de tesis sirva con la IA a que en un futuro la ciberseguridad se desempeña cada vez más con un papel fundamental en la lucha contra ciberamenazas más avanzadas y automatizadas. Debido a que la IA aprende continuamente de los datos a los que está expuesta, las nuevas tecnologías basadas en procesos y técnicas de IA son cruciales para identificar las amenazas más recientes y evitar que los piratas informáticos aprovechen las nuevas vulnerabilidades en el tiempo más rápido posible.

Bibliografía

1. CISCO. (2021). Tipos de Firewalls. 2021, de CISCO Sitio web: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
2. Recomendación X.800.(Aprobada en 1991-03-22) Sitio web: https://www.itu.int/rec/T-REC-X.800-199103-I/es
3. Recomendación X.200.(Aprobada en 1994-07-01) Sitio web: https://www.itu.int/rec/T-REC-X.200-199407-I/es
4. CISCO. Sitio web: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html
5. CISCO. Sitio web: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html
6. CISCO. Sitio web: https://www.cisco.com/c/dam/global/es_es/pdfs/fy17q2/DNA-HPA_ES_perimetro-de-la-red.pdf
7. Repositorio libro virtual FUNDAMENTOS DE SEGURIDAD LOGICA. página web: https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/4487/Jose_Tesis_Titulo_2014.pdf?sequence=1&isAllowed=y
8. Libro Inicio y Evolución de la Seguridad Informática en el Mundo, Fernando A. Rentería Echeverry. Nació en Quibdó Chocó, el 19 de Agosto de 1979.
9. Proofpoint, pagina web: https://www.proofpoint.com/es/threat-reference/cybersecurity-network-security
10. 3Com Corporation, Seguridad de Redes: Una guía para implementar Firewalls pawina web: http://lat.3com.com/lat/technology/technical_papers.html
11. PICOUTO Fernando, LORENTE Iñaki. Hacking y Seguridad en Internet. México: Alfaomega Grupo Editor, S.A, 2008. P 346
12. ARROYO José. Linux Máxima Seguridad edición especial México: Prentice Hall 2000 P 520
13. CISCO SYSTEMS. Currícula CCNA 4.0 Discovery - Networking para el Hogar y Pequeñas Empresa