Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-27

Diseño e implementación de políticas de seguridad a nivel de firewall perimetral y proxy en la red LAN del semillero OTM Bloque O Sede Fraternidad ITM

Diana Marcela Correa Bedoya

Leady Giraldo Echeverri

Ingeniería de sistemas de información

Javier Mauricio Durán Vásquez

INSTITUTO TECNOLÓGICO METROPOLITANO

2017-11-14

RESUMEN

Este proyecto tiene como finalidad diseñar e implementar políticas de seguridad en un firewall perimetral para mitigar riesgos en los servidores del Virtual DataCenter ubicado en el bloque O del semillero observatorio de telecomunicaciones para la ciudad de Medellín (OTM) del Instituto Tecnológico Metropolitano (ITM), se enfocará sobre el nivel de Capa de Transporte y Capa de Red del Modelo OSI (Modelo de interconexión de sistemas abiertos), las cuales permitirán que la institución en general pueda aplicar controles de seguridad informática, enfocados en la protección de la infraestructura computacional. Por tal razón, se iniciará realizando un inventario de los dispositivos de red que se encuentran en el bloque O, lo cual permitirá conocer el funcionamiento de cada uno de los componentes, especificaciones técnicas y sus condiciones lógicas. Una vez se tenga identificado lo anterior, se levantarán los requerimientos de seguridad informática asociados a la red, a partir del conocimiento de la arquitectura y servicios que presta la red, para luego definir las políticas de seguridad a aplicar mediante un firewall de software libre. Así mismo, se implementarán políticas de navegación mediante un servidor Proxy, el cual hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor, debido a que la red bloque O no cuenta con los controles de seguridad informática para proteger los dispositivos de red de usuarios externos a ella y/o de aplicaciones y archivos maliciosos, aunque se puede usar para mejorar el rendimiento de las conexiones a Internet, también se puede usar con fines de seguridad. El proyecto tomará elementos de la metodología Fases Prepare, Plan, Design, Implement, Operate and Optimize (PPDIOO) que fue desarrollada por la compañía de Cisco para definir actividades mínimas que se requieran para la instalación y operaciones de tecnología. El enfoque principal de esta metodología es definir las actividades mínimas requeridas, por tecnología y complejidad de red, que permitan asesorar de la mejor forma posible.

Palabras Claves: Firewall, Proxy, Reglas, LAN, WAN, Modelo OSI, TCP, UDP, Políticas de Seguridad, Open Source, Capa de Transporte, Capa de Red, Servidor Proxy,

Vulnerabilidades, pfSense, Control de Acceso, Navegación Segura, Seguridad perimetral, Filtrado de Contenido, protección firewall, servidores.

RECONOCIMIENTOS

“Primeramente, quiero agradecerle a Dios por brindarme la paciencia y entendimiento para llevar a cabo este proyecto y culminarlo con el mismo entusiasmo.
A mi familia, amigos y pareja que estuvieron dispuestos a apoyarme en todo momento que intente desfallecer por el cansancio y tiempo que conlleva realizar este trabajo.
Quiero agradecer a mi compañera de tesis, asesor y monitor que me guiaron en todas la dudas e inconvenientes que se presentaron durante todo ciclo del proyecto para sacar adelante esta propuesta”. - ***Leady Johana Giraldo Echeverri***

“En primer lugar, quiero dar gracias a Dios por llenarme de valor, paciencia y sabiduría a la hora de afrontar todos los problemas en los momentos más difíciles, como segundo a mi madre y abuelos por brindarme todo su apoyo incondicional a lo largo de mi vida y de este trabajo y por haberme inculcado una gran educación, agradecimientos especiales a una gran persona, a mi amiga Leady Giraldo, al administrador de la red del Bloque O Cristian Gaviria y asesor al Javier Durán, ya que sin él no hubiese sido posible la realización de este proyecto, gracias por darnos su confianza en la realización de este trabajo, por todos los recursos que nos brindó, por su responsabilidad y disponibilidad para resolver nuestras dudas y ayudarnos en lo que fuese necesario.” - ***Diana Marcela Correa Bedoya***

ACRÓNIMOS

CAN Campus Area Network o red de área de campus.
DMZ Demilitarized Zone o Zona Desmilitarizada.
DNS Domain Name System o Sistema de Nombres de Dominio.
FTP File Transfer Protocol o Protocolo de Transferencia de Archivos.
HTTP Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertexto.
HTTPS Protocolo de Transferencia de HiperTexto Seguro.
ISO Organización Internacional para la Estandarización.
IP Internet Protocol o Protocolo de Internet.
IPSec Internet Protocol Security
LAN Local Area Network o Red de Área Local.
MAN Metropolitan Area Network.
OSI Open System Interconnection.
PAN Personal Area Network (PAN) o Red de Área Personal.
PPDIOO Prepare, Plan, Design, Implement, Operate and Optimize.
PPTP Point-to-Point Tunneling Protocol
SI Sistema de Información.
SMTP Simple Mail Transfer Protocol o Protocolo para Transferencia Simple de Correo.
SSH Secure Shell.
TCP Transmission Control Protocol o Protocolo de Control de Transmisión.
TCP/IP Protocolo de Control de Transmisión o Protocolo de Internet.
TI Tecnología de la información.
UDP User Datagram Protocol o Protocolo de Datagrama de Usuario.
UTM Unified Threat Management o Gestión Unificada de Amenazas.
VM Máquina Virtual.
VLAN Red de área local virtual.
VPN Red Privada Virtual.
WAN Wide Area Network o Red de Área Amplia.

TABLA DE CONTENIDO

INTRODUCCIÓN

La mayoría de las aplicaciones que se utilizan normalmente en un ordenador, indiferente de su funcionalidad e interfaces de usuarios tienen algo en común al momento de comunicarse dentro una red y/o fuera de esta. Esta característica en común consiste en que al momento de comunicarse a través de la red utilizan los servicios de la Capa de Transporte para definir e identificar el servicio dentro del HOST encapsulando los datos que se desean transmitir bajo el protocolo TCP o UDP, y adicionalmente también se utilizan los servicios de la Capa de Red para identificar mediante una dirección específica a un HOST de forma única en la red.

De lo anterior la importancia de controlar y monitorear los flujos de datos que se intercambian en una red utilizando estos mecanismos y de implementar de forma correcta las políticas de seguridad en un firewall.

Cada implementación de seguridad en una red de datos tiene un firewall como la primera línea de defensa perimetral, protegiendo los activos de información de la organización contra las amenazas comunes del Internet y accesos desde orígenes no autorizados a los servicios de la organización. Entonces, teniendo en cuenta lo mencionado, no se puede dejar de considerar la seguridad de la red y el sistema operativo, si se pretende que la información que hasta hoy era considerada privada, no caiga en manos equivocadas, así que se marcaran como objetivos principales de la tesis los siguientes:

- ✓ Levantar el inventario de activos y servicios de la red del Bloque O a partir de un análisis a nivel de Capa de Red y Capa de Transporte del Modelo OSI.
- ✓ Diseñar las políticas de seguridad a nivel de firewall y de navegación para la red del bloque O del semillero OTM a partir del inventario de activos y servicios.
- ✓ Instalación y configuración de solución UTM de software libre. Implementar las políticas de seguridad para firewall y proxy a partir de la instalación de una

herramienta seleccionada.

- ✓ Evaluar el funcionamiento de las políticas definidas para el Firewall y en la navegación en internet.

Por esto se planea que la tesis se divide en varias secciones. En la primera se explicará detalladamente el marco teórico, en donde se sustenta nuestro trabajo de grado, conceptos, teoría fundamentada y desarrollada partiendo de lo más específico a lo más general, en base al planteamiento del problema que se ha realizado.

En la segunda parte se aplicará la metodología PPDIOO en donde se permite formalizar el ciclo de una red, el enfoque principal de esta metodología es definir las actividades mínimas requeridas, por tecnología y complejidad de red, instalando y operando exitosamente las tecnologías. Así mismo se logra optimizar el desempeño a través del ciclo de vida de la red.

MARCO TEÓRICO

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de "una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo". (Seguridad., 2007)

Una red de datos se constituye de una serie de elementos, (ordenadores, routers, switch, Access Point, dispositivos móviles, etc.), son autónomos y están interconectados entre sí por medios físicos y lógicos, y que están en la capacidad de compartir recursos.

Actualmente existe una gran variedad de redes no sólo por el número sino también por la diversidad de protocolos que ellas utilizan. "Considerando el tamaño o la envergadura de una red, podemos clasificarlas de la siguiente manera:" (Marín, 2014)

a) **"LAN –** Este tipo de redes soportan los servicios de pequeñas y medianas compañías, en las que se pretende compartir la información de sus ordenadores. Son las redes más habituales y de las cuales trata el presente manual.
b) **MAN –** Este tipo de redes soportan los servicios a compañías que tienen sus centros en una misma área metropolitana.
c) **WAN –** Este tipo de redes tienen cobertura global. Soportan los servicios de las compañías multinacionales." (Marín, 2014)

Las redes de computadoras surgieron como una necesidad de interconectar los diferentes HOSTS de una empresa o institución para poder así compartir recursos y equipos específicos. "Pero los diferentes componentes que van a formar parte de una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red."**Fuente especificada no válida.** La disposición de los diferentes componentes de una red se

conoce con el nombre de topología de la red.

La topología que se prefiera para "una red local influirá en su funcionamiento y en su rendimiento. A la hora de elegir la topología de una red hay que tener en cuenta factores como el número de nodos que formarán parte de la red, el tipo de acceso al medio, etc." (Ternero, Redes Locales, 2014)

"La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías LAN y WAN se pueden ver de dos maneras: La topología Física y La topología Lógica." (Ternero, Redes Locales, 2014). Hay una gran cantidad de variaciones de topologías físicas, en la cual realizaremos una enunciamos las principales:

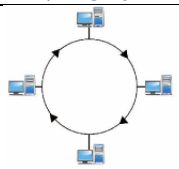
Topología de bus Esta es la topología más sencilla. En las redes que tienen esta topología todos los nodos están conectados directamente a un canal de comunicación común llamado bus que suele ser un cable coaxial.	 *Figura 1:Topología física en Bus*
Topología en anillo En esta topología cada nodo está conectado con sus dos nodos adyacentes por enlaces punto a punto, formando un anillo cerrado o círculo por el cual viaja la información. Es habitual el uso de fibra óptica como medio físico.	 *Figura 2:Topología física en Anillo*
Topología en árbol En esta topología, también llamada topología jerárquica, la mayoría de los nodos están conectadas a concentrados secundarios. Estos concentradores secundarios, así como algunos otros nodos están conectados a un concentrador primario o central, que puede ser un switch o un hub.	 *Figura 3:Topología física en Árbol*

Tabla 1. Topología en malla completa (Ternero, Redes Locales, 2014)

Sobre una topología física se puede implementar multitud de tipos de topología lógicas, en función de cómo sea el flujo de información. "La topología lógica indica la forma en la fluye información. De esta forma, sobre una misma topología física podemos implementar

distintas topologías lógicas.” (Ternero, Redes Locales, 2014)

Al igual que en la comunicación humana, los diversos protocolos informáticos y de red deben poder interactuar y trabajar en conjunto para que la comunicación de red se lleve a cabo correctamente. “Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina “suite de protocolos”. Los hosts y los dispositivos de red implementan las suites de protocolos en software, hardware o ambos. Los protocolos de red definen un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos. Algunos protocolos de red comunes son IP, HTTP y DHCP.” (Molina, 2012)

Los distintos protocolos trabajan en conjunto para asegurar que ambas partes reciben y entienden los mensajes. Algunos ejemplos de estos protocolos son:

- “**Protocolo de aplicación:** el protocolo de transferencia de hipertexto (HTTP) es un protocolo que rige la forma en que interactúan un servidor Web y un cliente Web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor Web implementan el HTTP como parte de la aplicación. HTTP depende de otros protocolos para regular la forma en que los mensajes se transportan entre el cliente y el servidor.
- **Protocolo de transporte:** el protocolo de control de transmisión (TCP) es el protocolo de transporte que administra las conversaciones individuales entre servidores Web y clientes Web. TCP divide los mensajes HTTP en partes más pequeñas, llamadas “segmentos”. Estos segmentos se envían entre los procesos del servidor y el cliente Web que se ejecutan en el host de destino. TCP también es responsable de controlar el tamaño y la velocidad a los que se intercambian los mensajes entre el servidor y el cliente.
- **Protocolo de Internet:** IP es responsable de tomar los segmentos con formato de TCP, encapsularlos en paquetes, asignarles las direcciones adecuadas y enviarlos a través del mejor camino hacia el host de destino.
- **Protocolos de acceso a la red:** los protocolos de acceso a la red describen dos

> funciones principales, la comunicación a través de un enlace de datos y la transmisión física de datos en los medios de red. Los protocolos de administración de enlace de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los estándares y protocolos de los medios físicos rigen la forma en que se envían las señales y la forma en que las interpretan los clientes que las reciben. Ethernet constituye un ejemplo de un protocolo de acceso a la red." (Molina, 2012)

Debido a la compleja interacción entre las telecomunicaciones y la informática ha sido necesario establecer estándares que permitan poner las diferentes entidades en condiciones de conectarse entre sí por medio de un lenguaje común de referencia. La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI.

El modelo OSI, se compone de siete niveles de proceso, "mediante el cual los datos se empaquetan y se transmiten desde una aplicación emisora, viajando a través de medios físicos hasta llegar a una aplicación receptora," (Tolosa, 2014) además, proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. El modelo TCP/IP, está compuesto por cuatro capas, en la que cada una "se encarga de determinados aspectos en la comunicación y a su vez cada una brinda un servició especifico a la capa superior." (Tolosa, 2014)

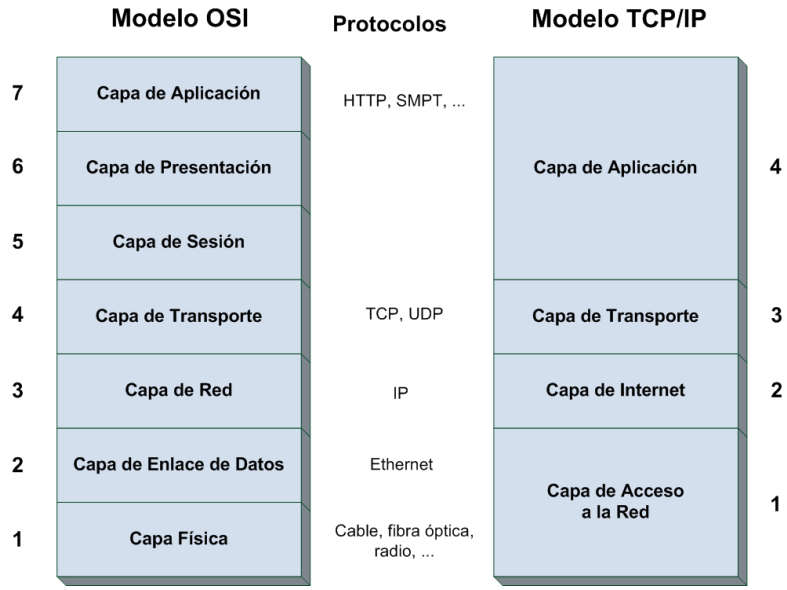


Figura 1. Modelo OSI - Modelo TCP/IP

"Cada uno de los niveles tiene una serie de vulnerabilidades y se le puede aplicar unas medidas de protección para evitar la materialización de amenazas." (López, 2010) El objetivo de la seguridad en redes en mantener la integridad, disponibilidad, confidencialidad (sus aspectos fundamentales) control y autenticidad de la información que es almacenada, procesada e intercambiada en una red de datos, a través de procesamiento basados en una política de seguridad tales que permitan el control adecuado.

La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlado por el administrador de red. Tiene como objetivo de mantener el intercambio de información libre de riesgo y proteger los recursos informáticos de los usuarios y las Organizaciones. Generalmente, se encuentra amenazada por riesgos que van de la mano con el aumento del uso de Internet en las Instituciones de todos los ámbitos. Dependiendo del enfoque que se le dé a la seguridad informática, un sistema informático está expuesto al peligro por medio de dos factores: Las amenazas y las vulnerabilidades.

La vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un

atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Globalmente clasificamos las vulnerabilidades en:

- **"Vulnerabilidades de desbordamiento de buffer**: Se produce cuando un programa no controla la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Se puede aprovechar para ejecutar código que nos de privilegios de administrador.
- **Vulnerabilidades de condición de carrera (race condition):** La condición de carrera se da principalmente cuando varios procesos acceden al mismo tiempo a un recurso compartido, por ejemplo, una variable, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.
- **Vulnerabilidades de error de formato de cadena (format string bugs):** La principal causa de los errores de cadena de formato es aceptar sin validar la entrada de datos proporcionada por el usuario. Es un error de programación y el lenguaje más afectado es C/C++. Un ataque puede conducir de manera inmediata a la ejecución de código arbitrario y a revelación de información.
- **Vulnerabilidades de Cross Site Scripting (XSS):** Abarcaban cualquier ataque que permitiera ejecutar scripts como VBScript o JavaScript, en el contexto de otro sitio web. Estos errores se pueden encontrar en cualquier aplicación que tenga como objetivo final presentar la información en un navegador web. Un uso de esta vulnerabilidad es hacer phishing. La víctima ve en la barra de direcciones un sitio, pero realmente está en otro. La víctima introduce su contraseña y se la envía al atacante.
- **Vulnerabilidades de Inyección SQL:** Una inyección SQL se produce cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.
- **Vulnerabilidades de denegación del servicio:** La denegación de servicio provoca que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la

víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- **Vulnerabilidades de ventanas engañosas (Window Spoofing):** Las ventanas engañosas son aquellas que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que des información. Hay otro tipo de ventanas que, si las sigues, obtienen datos del ordenador para luego realizar un ataque." (Mentor, 2017)

La amenaza es el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático. "Un evento producido en el sistema informático que constituye una amenaza asociada a una vulnerabilidad del sistema, produce un impacto sobre él. Si queremos eliminar las vulnerabilidades del sistema informático o queremos disminuir el impacto que puedan producir sobre él, hemos de proteger el sistema mediante una serie de medidas que podemos llamar defensas o salvaguardas." (Mentor, 2017)

Lo primero que hemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas más específicas.

Los mecanismos de seguridad se dividen en tres grupos:

- **"Prevención:** Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

- **Detección:** Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.
- **Recuperación:** Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento." (Mentor, 2017)

Además, "cuando se trata de estaciones de trabajo y servidores, no hay medidas de seguridad sólidas que mantengan un nivel de seguridad adecuado. Por este motivo, se diseñado los cortafuegos o Firewalls. Es un sistema compuesto por uno o varios dispositivos cuya función principal es la separación entre la LAN de un sistema de información y WAN para impedir la entrada de ataques y aumentar el nivel de seguridad de la organización o institución." (Tejada, 2014)

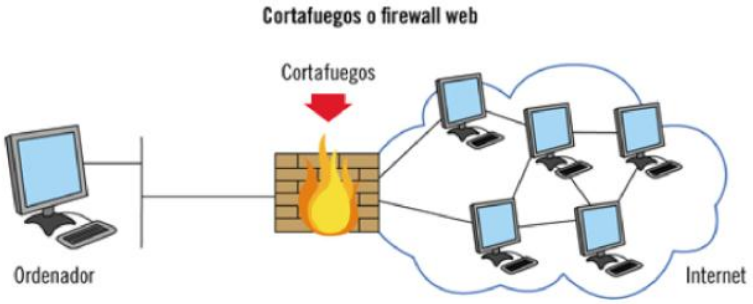


Figura 2. Cortafuegos o Firewall Web

En otras palabras, es un sistema cuya funcionalidad principal es efectuar un control de accesos entre dos redes: la red interna y la red externa o Internet.

"Los cortafuegos utilizan los conceptos de perímetro de seguridad y zona de riesgos para determinar las redes interna y externa de un sistema de información:

- **Perímetro de Seguridad:** Espacio protegido por los cortafuegos, suele ser propiedad de la organización y se corresponde con su red interna.
- **Zona de Riesgo:** Es la red frente a la que se protege el perímetro de seguridad con los cortafuegos." (Tejada, 2014)

Un sistema de seguridad perimetral tiene como premisa la protección de todo el sistema informático desde el exterior, es decir, colocar una coraza que proteja todos los elementos sensibles de ser vulnerados, sean estos: datos, configuraciones, accesos, etc. “Esto quiere decir que todo el tráfico que vaya a fluir por nuestra red, previamente debe de ser analizados, aceptado o rechazado en función de las reglas que hayamos previsto para determinar el potencial riesgo de seguridad para nuestra red.” (Erazo, 2015)

La seguridad debe ser una de las principales preocupaciones cuando los dispositivos de la red interna acceden a Internet, ya que la “red es una importante área de exposición a riesgos, en consecuencia, los atacantes suelen dirigirse a la red como punto de partida para acceder a otros activos de TI. La seguridad de red consiste en defender la red y los recursos relacionados frente a amenazas.”**Fuente especificada no válida.** Para conseguir un nivel de protección aceptable, se necesita una política de seguridad para evitar que usuarios sin autorización tengan acceso a los recursos de la red y protegerla contra la explotación sin autorización de la información confidencial.

Por lo tanto, es indispensable que desde la Ingeniería se brinden herramientas que contribuyan a minimizar los riesgos de seguridad asociados a la red. Con la finalidad de buscar estrategias para administrar de forma sencilla y accesible la seguridad de la red.

METODOLOGÍA

Para la elaboración de este proyecto se usó una adaptación de la metodología PPDIOO la cual "permite formalizar el ciclo de una red; esta metodología cuenta con seis fases Planeación, Preparación, Diseño, Implementación, Operación y Optimización" (Espinoza, 2015). De esta metodología se tomaron algunos elementos de cada fase los cuales suplen el alcance que abarco el proyecto planteado.

A continuación, se explicará lo que se realizó en cada una de las etapas para cumplir con los objetivos de este proyecto y cuáles fueron los entregables adoptados de las mismas:

En la ***fase de Preparación*** se deben "establecer los requisitos de la organización, desarrollar una estrategia de red y proponer una arquitectura conceptual de alto nivel que identifique las tecnologías que mejor pueden soportar la arquitectura. La fase de preparación puede establecer una justificación financiera para la estrategia de red mediante la evaluación del caso comercial de la arquitectura propuesta" (Sivasubramanian, Frahim, & Froom, 2010).

El entregable que se contempló para esta etapa es el Documento de requisitos del cliente, el cual se detalla en el *Apéndice1. "CRD - Diseño e implementación de políticas de seguridad a nivel de firewall perimetral y proxy en la red LAN/WAN del semillero OTM Bloque O Sede Fraternidad ITM."* En este documento se describe la situación actual de la red del Bloqueo O y la necesidad que se tiene para mitigar los riegos de seguridad que se pueden presentar en una red desprotegida.

Ya que, existía una infraestructura de servidores desplegada en la red del Bloque O, se tomó como referente dicha infraestructura ver *Apéndice2. "Diagrama Topológico de la red del semillero OTM Bloque O anterior a la implementación y configuración del Firewall"*, en la cual se diagrama el conjunto de servidores y su segmento de red, esto ayudó a tener un amplio conocimiento de los activos que fueron parte de la solución de protección del firewall y en base a esta topología existente se realizó el diseño y la arquitectura necesaria para incluir y posicionar dentro de la red la solución de firewall perimetral que permitirá la aplicación de las políticas de seguridad diseñadas para la red.

En la ***fase de Planeación*** se deben "identificar los requisitos iniciales de la red en función de los objetivos, las instalaciones, las necesidades del usuario, etc. La fase de planeación implica caracterizar los sitios y evaluar las redes existentes y realizar un análisis de brechas para determinar si la infraestructura del sistema existente, los sitios y el entorno operativo pueden soportar el sistema propuesto. Un plan de proyecto es útil para ayudar a administrar las tareas, las responsabilidades, los hitos críticos y los recursos necesarios para implementar cambios en la red." (Sivasubramanian, Frahim, & Froom, 2010).

Los entregables seleccionados para esta fase fueron, especificación de requisitos técnicos de sitio y plan de pruebas de soluciones, los cuales serán descritos a continuación:

Ya que esta fase se abarca diferente dependiendo de si se tiene o no una red montada, para el caso de este proyecto se parte de que sí existe una infraestructura instalada, y por ende se analizaron los requisitos técnicos que debía tener el ambiente donde se instaló el firewall seleccionado.

Teniendo en cuenta la arquitectura y topología actual y su esquema de virtualización basado en XenServer, se definieron las necesidades en cuanto recursos de cómputo para la implementación virtual de la solución de firewall y proxy pfSense. Para lo cual es necesario contar como mínimo con los siguientes recursos de cómputo:

Requisito	**Descripción**
CPUs	Procesador de un núcleo.
RAM	4GB de memoria RAM como mínimo.
Espacio en Disco Duro	60 GB de disco local.
Red	Por lo menos tres interfaces de red. Dirección IP estática asignada.

Tabla 2. Especificación de requisitos técnicos de sitio

Se estableció seguir un plan de pruebas para el ambiente simulado de forma local mediante programas de virtualización y simulación como VMware y GNS3, en los cuales se implementó una simulación del esquema definitivo antes de la fase de implementación en el ambiente productivo, para de esta forma mitigar la mayor cantidad de posibles incidencias en un ambiente productivo.

Plan de pruebas
1. Crear una máquina virtual con las especificaciones técnicas antes descritas.
2. Configurar la puerta de enlace de la máquina virtual para que sea igual a la interfaz del pfSense y al realizar alguna petición está pase por el Firewall aplicando las reglas configuradas en él. Esto para que los paquetes originados desde las máquinas clientes sean enviados a través del firewall y este pueda ejecutar el análisis de estos de acuerdo a las políticas de seguridad definidas.
3. Realizar un escaneo de puertos a la máquina creada.
4. Instalar y configurar el firewall.
5. Diseñar las políticas de seguridad a tener en cuenta y configurar las reglas de seguridad en el firewall.
6. Cierre de puertos detectados en el escaneo que no sean necesario para la máquina.
7. Realizar un nuevo escaneo de puertos para verificar que las políticas de seguridad aplicadas fueron efectivas, de acuerdo a lo definido para cada servidor.
8. Bloqueo de Ping a la máquina desde la red WAN.
9. Realizar Ping a la máquina creada desde un servidor direccionado en la red WAN y así verificar que este no responda al llamado.
10. Instalar y configurar el paquete de Proxy (Squidguard).
11. Diseñar y configurar las políticas de Proxy.

Tabla 3. Plan de pruebas de la solución

Adicionalmente en esta fase de realizó una investigación de herramientas firewall existentes para tener una visión clara de cuál era la ideal para implementar en la solución de este proyecto. En el *Apéndice3 "Ventajas y desventajas herramientas Firewall"*, se aprecian los pro y contras de las herramientas consultadas y seleccionadas para realizar el comparativo que dio como resultado elegir el cortafuego pfSense por sus grandes ventajas (descritas en el *Apéndice3*) y facilidad de mantenimiento. PfSense ofrece características de filtrado de paquetes statefull, facilidad en administración, instalación e implementación de proxy(Squid), además cuenta con una interface web amigable e intuitiva para su configuración, transformándose en un poderoso firewall eficaz y seguro.

A diferencia de otros firewall open source analizandos, pfSense representa la herramienta más completa de acuerdo a las necesidades requeridas por la estructura de la red del

semillero OTM del Bloque O, ya que usa múltiples componentes de balanceo de carga para distribuir el trabajo entre varios ordenadores u otros recursos, no todos los productos comparados soportan el equilibrio de carga. Otra característica que debemos resaltar de pfSense, es la personalizacion de reglas tanto para el firewall como para el proxy, un ejemplo de ellas es aceptar tráfico de un determinando sistema operativo.

PfSense es basicamente un firewall o cortaguegos de red que engloban múltiples funcionalidades en una máquina de protección perimetral. Algunos de estos servicios son:

- Función de un firewall de inspeccion de paquetes.
- Función de VPN (Ipsec, OpenVPN, PPTP)
- Antispam
- Deteccion/Prevención de intrusos.

En la ***fase de Diseño*** se deben lograr que "los requisitos iniciales que se derivaron en la fase de planificación impulsan las actividades de los especialistas en diseño de redes. La especificación de diseño de red es un diseño detallado que cumple con los requisitos comerciales y técnicos actuales, e incorpora especificaciones para admitir disponibilidad, confiabilidad, seguridad, escalabilidad y rendimiento. La especificación de diseño es la base para las actividades de implementación".

Según la topología analizada durante la planeación, para esta fase de diseño se definió la nueva infraestructura de red implementando el firewall y las políticas de seguridad, con el fin de tener mayor claridad de cómo quedaría estructurada y conocer el uso de segmentos de red que éste protegerá. En el *Apéndice4. "Diagrama Topológico de la red del semillero OTM Bloque O después de la implementación y configuración del Firewall"* se puede observar el resultado del diseño del firewall en la infraestructura existente y el cual será proporcionando como entregable en esta etapa (Diseño de bajo nivel).

En la ***fase de implementación*** "la red está construida o se incorporan componentes adicionales de acuerdo con las especificaciones de diseño, con el objetivo de integrar dispositivos sin interrumpir la red existente ni crear puntos de vulnerabilidad" (Sivasubramanian, Frahim, & Froom, 2010).
Esta fase consta de varios puntos importantes que se realizaron para llevar a cabo la solución planteada.

Como primera instancia se realizó un escaneo de la red del semillero OTM por medio de la

herramienta NMAP (("Network Mapper") fuente libre y de código abierto para el descubrimiento de redes y la auditoría de seguridad) ((Nmap: the Network Mapper - Free Security , s.f.)) para conocer los servicios que presentaba cada uno de los servidores presentes en la infraestructura. En el *Apéndice5. "Escaneo de la red del semillero OTM Bloque O"*, se puede observar las direcciones de los servidores, su nombre, descripción y puertos escaneados cada uno con su estado.

Para completar la información descrita en el *Apéndice5*, se realizó una entrevista con los administradores de la red para conocer cada uno de los servidores, logrando documentar cada uno de los activos, y obteniendo un conocimiento más amplio de estos.

Una vez obtenida esta información, se procedió a configurar las políticas de seguridad para Firewall y Proxy de cada uno de los servidores en la herramienta pfSense, las cuales son necesarias para que la infraestructura y servicios de red presentes en la red del semillero OTM del bloque O estén protegidos contra amenazas externas, así como los estudiantes que hacen uso de estos servicios, las reglas a aplicar están basadas en:

Reglas de Control de Acceso: Medidas de control de acceso para los activos que componen la red del bloque O, estas contienen los siguientes aspectos:
Autorización de acceso a los sistemas de información.
Control de acceso a la red que utilizan los sistemas de información.

Restricciones y Prohibiciones: Están completamente prohibidas las siguientes actividades:

- Internet restringido, los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación.
- La prohibición al acceso de páginas no autorizadas.

Para mitigar errores, se recreó un ambiente de preproductivo con las especificaciones técnicas y siguiendo el plan de pruebas descritos en la fase de planeación, las pruebas dieron un acercamiento del compartimento de Firewall y Proxy en cuanto a su configuración y tempo invertido para ello. En el *Apéndice6. "Reglas del Firewall de la red del semillero OTM Bloque O",* se puede observar la máquina virtual instalada y su segmento de red configurado para que todas las solicitudes desde y a hasta ella pasen por el firewall el cual aplicará las políticas establecidas.

Como se evidencia en esta etapa, lo entregables son: Prueba de red lista para usar y registro de la implementación la cual se puede constatar con el *Apéndice5. "Escaneo de la red del semillero OTM Bloque O".*

RESULTADOS Y DISCUSIÓN

Como resultados de la implementación del firewall o cortafuegos en el bloque O, se logró evidenciar que se defiende perimetralmente la red del semillero, contra ataques a la infraestructura que provee los servicios del bloque O, puesto que antes de la implementación del Firewall se realizó el escaneo de la red y, se detectaron múltiples puertos "abiertos", en cada una de las máquinas, que no eran necesarios para presentar su respectivo servicio, las cuales fueron mitigadas con la implementación de este trabajo de grado.

Para dar solución a este inconveniente, el principal objetivo de este trabajo de grado fue la correcta definición e implementación de políticas de seguridad tanto para el firewall como para el proxy, para que los estudiantes accedan a internet de forma segura, confiable y que la red interna esté protegida de accesos no autorizados, las reglas aplicadas en el Firewall pueden ser consultas en el *Apéndice6. "Reglas del Firewall de la red del semillero OTM Bloque O"*

Al implementar esta solución en la comunidad del ITM, logramos brindarles confianza al momento de trabajar en la red del semillero del bloque O, la cual es una gran ventaja para todos como consumidores de los servicios que contiene esta red.

Como consecuencia de implementar un firewall o cortafuegos a la red se vio la necesidad de modificar la topología existente de la red del semillero del bloque O como se puede consultar en la *Apéndice2. Diagrama Topológico de la red del semillero OTM Bloque O anterior a la implementación y configuración del Firewall*, el cual se deberá tener en cuenta para nuevos proyectos que afecte la infraestructura de dicha red.

A continuación, se presenta los resultados producto de la configuración de las políticas de seguridad:

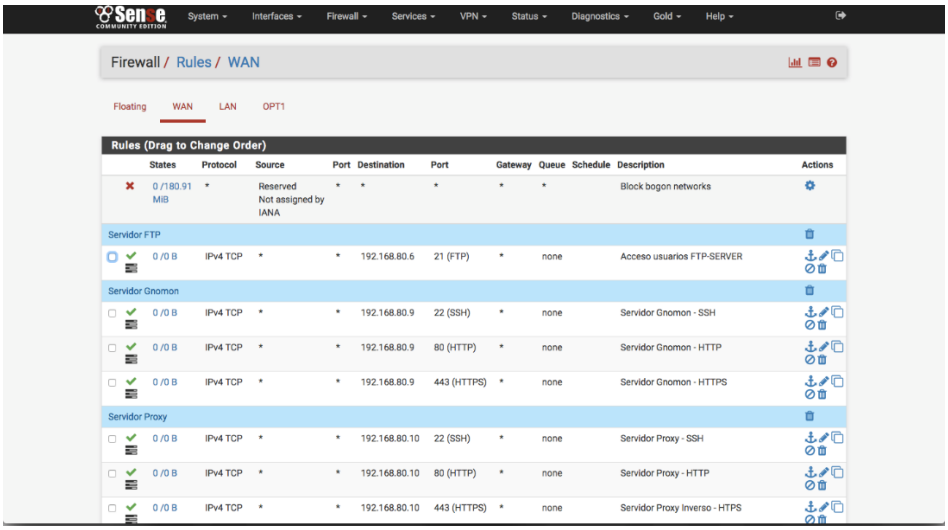


Figura 3. Reglas de políticas de Seguridad pfSense

De acuerdo a las reglas implementadas en firewall, se realiza de nuevo un escaneo a uno de los servidores al que se le aplicaron las reglas, desde la WAN:

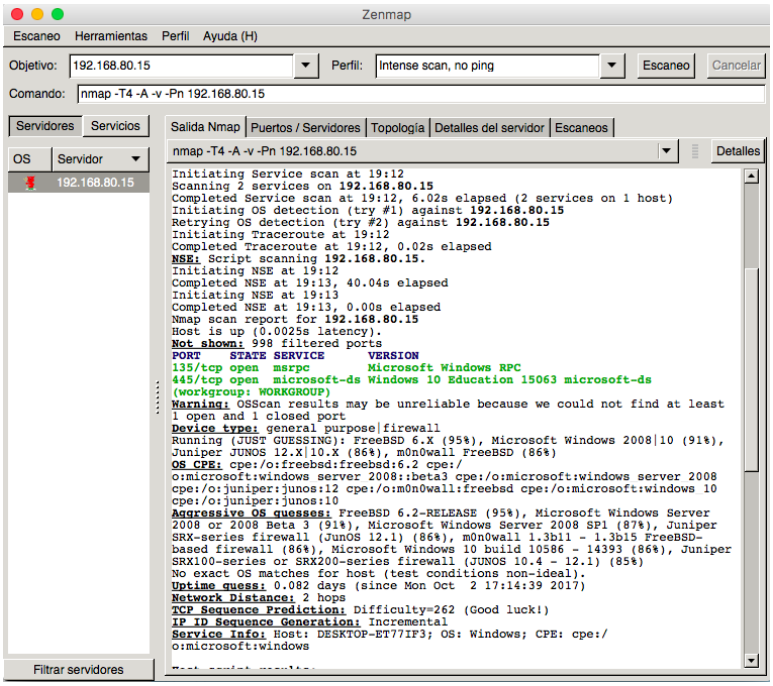


Figura 4. Escaneo de puertos al servidor 192.168.80.15

Como se puede visualizar en la ilustración, solo se habilitaron dos puertos “abiertos”, lo que indica que son los dos puertos que se dejaron permitidos en el firewall:

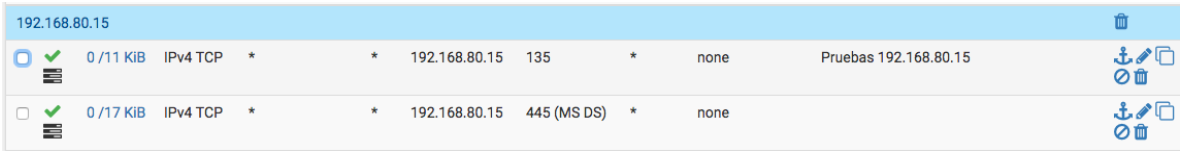


Figura 4. Reglas del Servidor 192.168.80.15

Antes de aplicar las reglas del firewall, se realizó un escaneo de los servidores, los resultados son mostrados en el *Apéndice5. “Escaneo de la red del semillero OTM Bloque O”*, en la ilustración se podrá ver los puertos “abiertos” que se encontraba en el servidor antes de configurar el firewall:

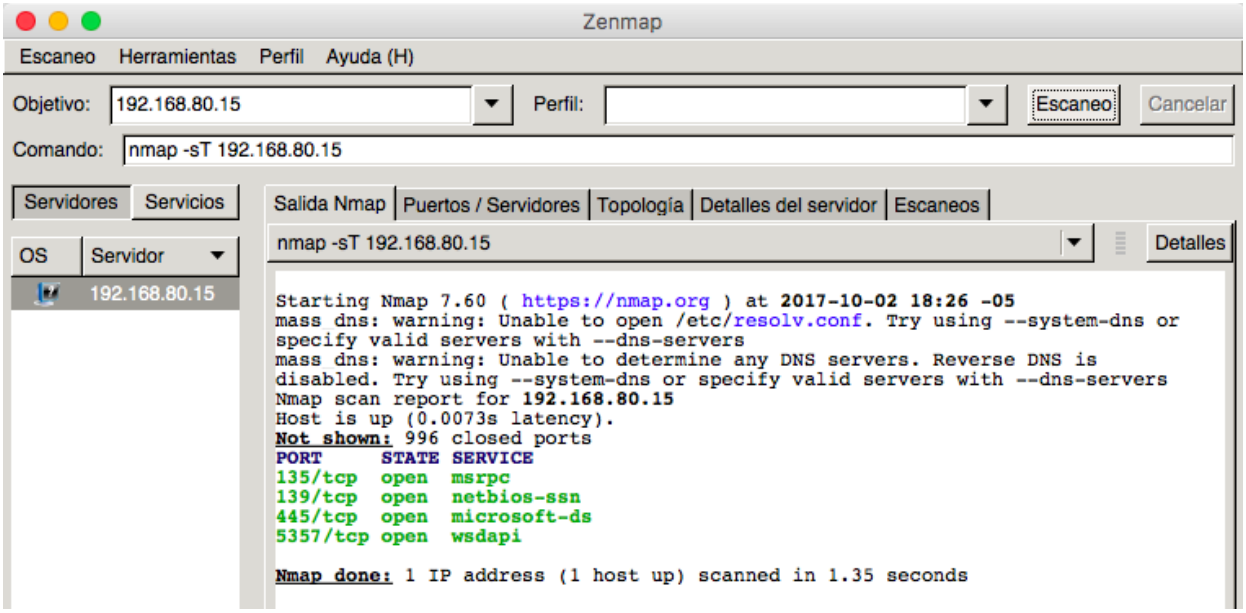


Figura 5. Escaneo de puertos al servidor 192.168.80.15

Además, se realiza la validación de que el ping se encuentre bloqueado, y no retorne respuesta:

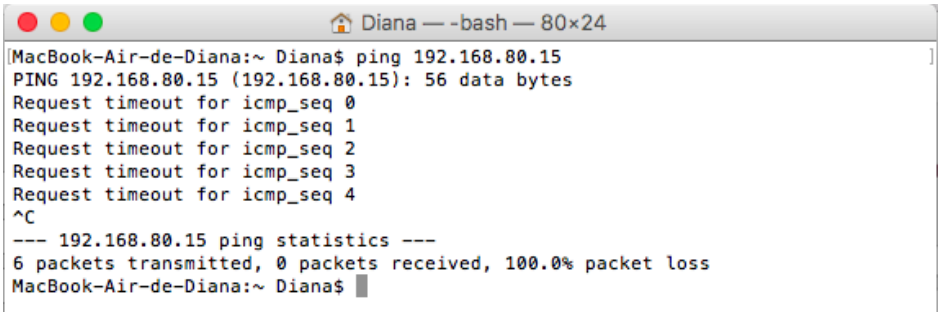


Figura 6. Ping al servidor 192.168.80.15

También, se realizaron las validaciones con el funcionamiento del proxy, en donde validará el control de acceso y el bloqueo de accesos a los sitios web malicioso. Para esto, se necesita realizar configuraciones del proxy en el firewall:

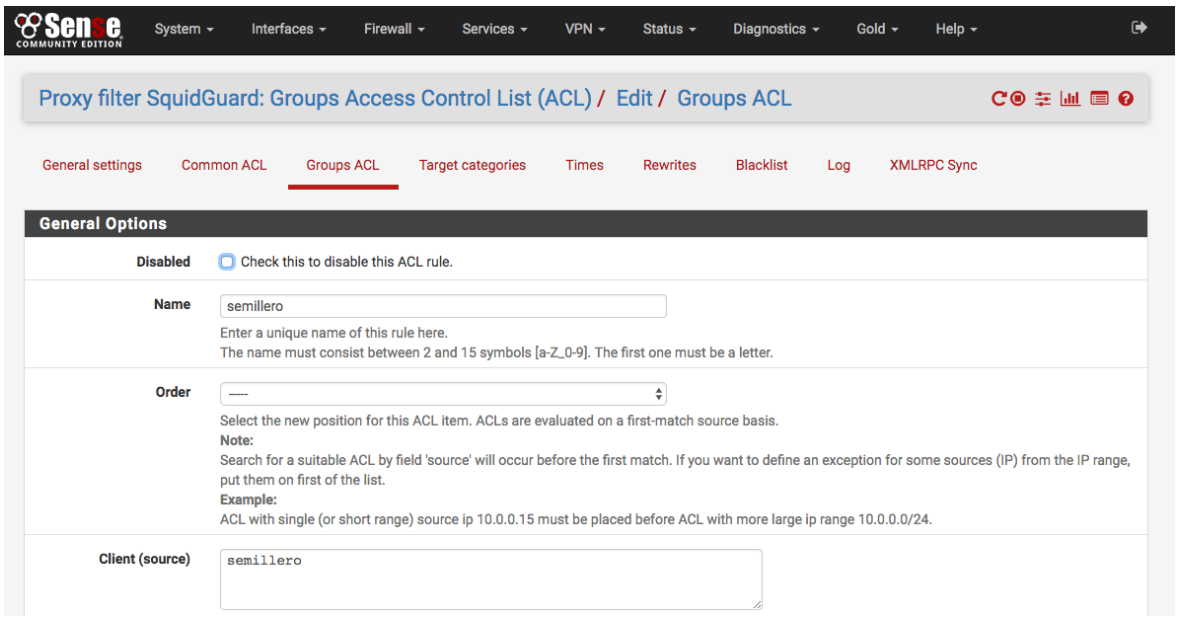


Figura 7. Implementación del proxy en el Firewall

Se realizaron las verificaciones necesarias, realizando las configuraciones del proxy en el servidor:

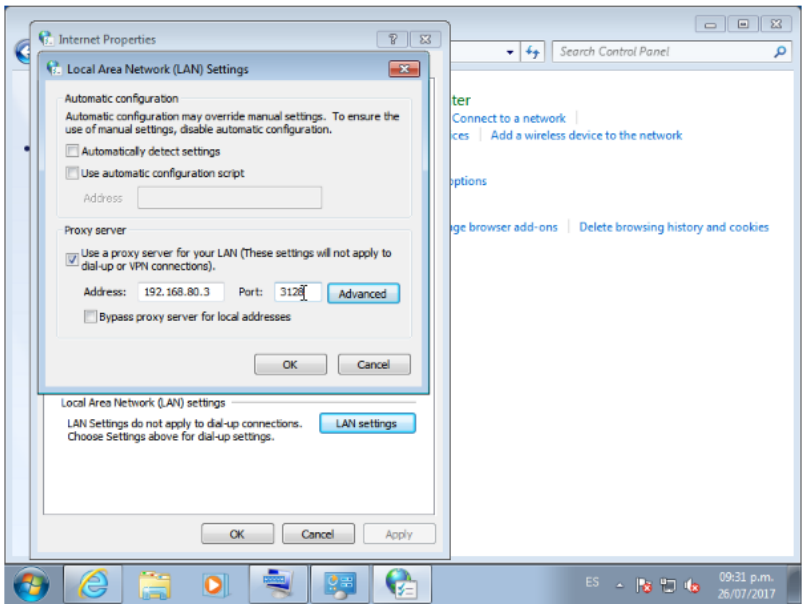


Figura 8. Configuración del proxy.

No se podrá acceder al internet, si no se inicia sección en el servidor proxy:

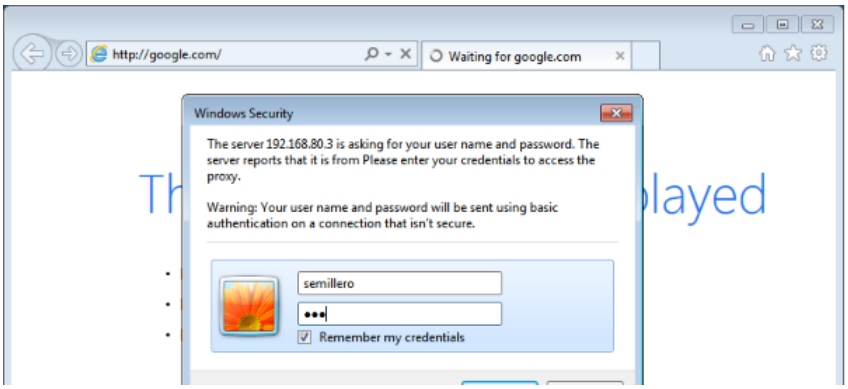


Figura 9. Inicio de Sección del proxy

Además, se implementan las reglas de proxy, en donde se controla el acceso a ciertas páginas web, definidas en categorías que agrupan diferentes sitios web de acuerdo a su contenido. En el Dashboard de configuración se presenta la opción de permitir o no permitir el acceso a las categorías presentes en el firewall, tales como se puede ver en el *Apéndice7. "Tabla de categorías para la configuración de las reglas en el proxy."*

Las categorías filtradas de la solución de seguridad fueron definidas por el administrador de la red del semillero, las cuales corresponden a las siguientes categorías: alcohol, dynamic, models, porn, ringtones y socialnet.

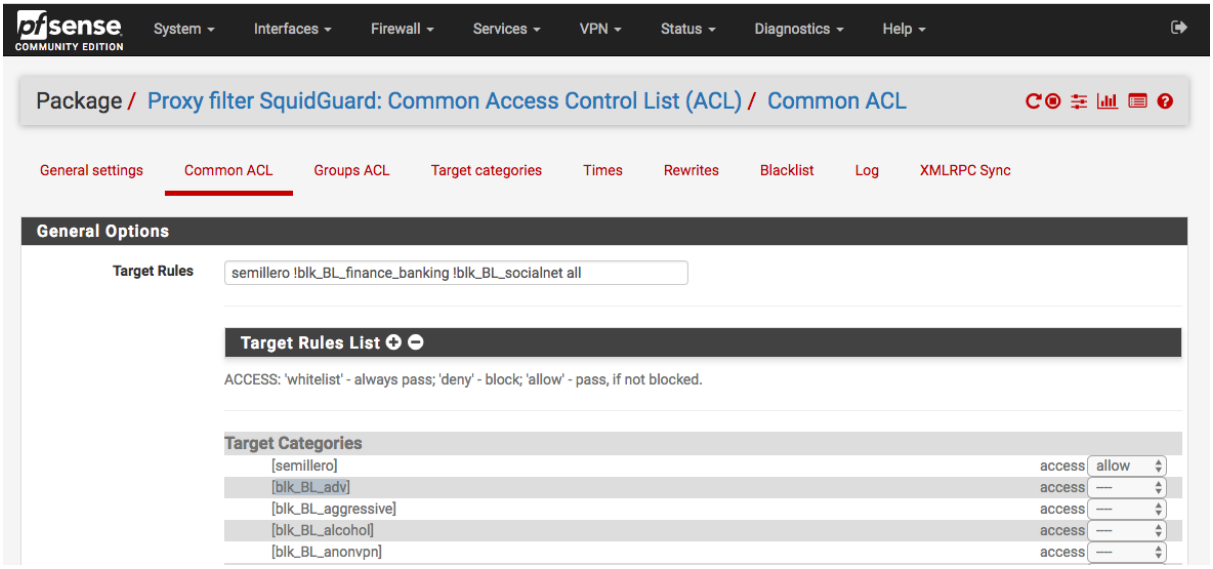
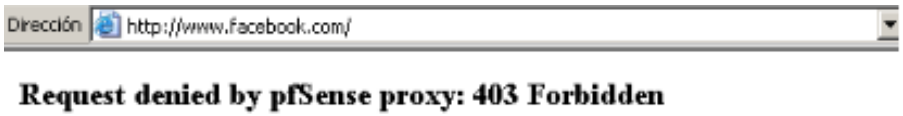


Figura 10. Configuración de las reglas en el proxy

En la siguiente ilustración, se podrá visualizar el ingreso a la una página web denomina, con redes sociales:



Request denied by pfSense proxy: 403 Forbidden

Figura 11. Bloque a las redes sociales

CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

Al realizar el diseño de las políticas de seguridad de una red de datos, es de vital importancia siempre primero definir los requerimientos de seguridad según las necesidades de la red para que de esta manera las políticas respondan de forma correcta. Sin embargo, antes de definir los requerimientos de seguridad de cualquier red de datos, primero se debe tener una idea general o conocer la estructura y los servicios que se administrarán en esta, puesto que los requerimientos se deben diseñar para que se adapten al crecimiento de la institución.

Las políticas creadas se pudieron implementar en el servidor pfSense teniendo en cuenta sus características de firewall, capaz de inspeccionar conexiones a nivel de la capa 3(Red) y de la capa 4 (Transporte). Por otra parte el pfSense también cuenta con un servicio proxy, el cual es muy recomendable utilizar en la red del Bloque O para filtrar y crear restricciones hacia los sitios de internet a los cuales se pueden conectar los usuarios y bloquear contenido no permitido en la red por cuestiones de seguridad.

El mejor proxy a implementar en una red de datos con la topología analizada en las prácticas realizadas y de acuerdo a las políticas creadas, es el servidor pfSense con el servicio Squid, justificado en que permite la fácil adaptación del servidor proxy y que no solo ayuda al rendimiento de la red, sino que además permite la mitigación de riesgos presentes en la infraestructura a proteger. Squid además de prestar grandes beneficios a la red, dispone de complementos que le permiten ser una herramienta aún más potente, para cumplir con los requerimientos de seguridad y almacenamiento caché para el acceso a internet.

- Squid permite el control de las conexiones y autenticación, debido a que es posible configurarlo para que este realice conexiones solamente con sitios permitidos así como también puede interactuar con servidores de autenticación. Además, permite restricciones por IP, por cuentas de usuario, por tiempo, por expresiones y por tráfico, entre muchas otras.
- Para el diseño de un esquema de red adecuado, se debe tener en cuenta el crecimiento exponencial de la infraestructura de la institución, la demanda creciente de servicios en producción, la diversificación constante y el incremento latente de estudiantes de la institución, lo cual exigirá que la solución a implementar sea robusta y fácilmente escalable para adaptarse a estas consideraciones.
- Luego de realizar un análisis de requerimientos informáticos para mejorar la seguridad de la información y de comparar varias posibles alternativas de software para uso en el Data Center del Semillero del OTM, se determinó que pfSense es el indicado, teniendo en cuenta que pertenece a la línea de software libre, se encuentra entre los primeros 3 mejores programas de seguridad a nivel mundial y es compatible con el hardware de la institución, manejando niveles óptimos de seguridad.
- Con la instalación del firewall PfSense, implementado sobre la plataforma de virtualización VMWARE, se obtuvo como resultado que dichos sistemas son compatibles y que cumple con la misma funcionalidad que un firewall de nivel físico. Además, la ventaja de tener servidores virtualizados optimiza la utilización de recursos de hardware.

RECOMENDACIONES

- Realizar actualizaciones periódicas del sistema pfSense, con la finalidad de mantener niveles altos de protección y desempeño.
- Revisar periódicamente las actualizaciones de Blacklist para los servidores proxys, ver qué novedades trae y que nuevo contenido se puede bloquear.
- Mantener actualizado los paquetes de Squid y SquidGuard porque de estos depende la administración de la navegación web dentro de la red del Semillero

OTM.

- Mantener los niveles de seguridad siempre monitorizados y actualizados, haciendo pruebas periódicas de los puertos que están ofreciendo servicios a la red.
- Es imprescindible aplicar técnicas de ataques informáticos de acuerdo con la versión del sistema firewall, con el propósito de obtener nuevos métodos de defensa para la seguridad de la información.

TRABAJO FUTURO

- Es importante tener en cuenta que esta implementación se realizó en la red de datos del semillero OTM del Bloque O, la cual es solo un fragmento pequeño de toda la red que contiene el semillero OTM y que da soporte a todos sus servicios de investigación a los estudiantes del ITM. Por lo cual aún quedan otros fragmentos de la red que debe ser protegidos y pueden ser analizando en otro trabajo de grado.
- Se sugiere como trabajo futuro, diseñar procesos y procedimientos que permita la solución de seguridad implementada continúe su proceso de madurez dentro de la red del semillero del Boqueo O.

REFERENCIAS

- Aula Mentor. (2017). Aula Mentor - Aprendizaje a lo largo de la vida. 2017, de Aula Mentor Sitio web: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html.
- Bilib Centro de Apoyo Tecnológico de Castilla – La Mancha (2012). Análisis de aplicación: Cortafuegos de IPCop. Mayo 2012, bilib Sitio web: https://www.bilib.es/recursos/catalogo-de-aplicaciones/analisis/doc/analisis-de-aplicacion-cortafuegos-de-ipcop/docctrl/show/Documento/
- Carlos Silva Ponce (2009). Seguridad de las redes y sistemas de telecomunicaciones críticos. AHCIET Revista de Telecomunicaciones.
- Capacity Information Technology (2013). Conoce ClearOS, simplificando la gestión de los servidores. Diciembre 2013, Capacity Sitio web: http://blog.capacityacademy.com/2013/12/03/ipfire-firewall-open-source/
- Daniel José Saa Borrero. (2016). ONTROL TRABAJO FINA. Mayo 2016, de Universidad del Valle Sede Palmira "La Carbonera" Sitio web: https://es.scribd.com/doc/314532872/Instalacion-PfSense
- Edgar Rubén Pilacuán Erazo. (2015). Implementación de un sistema de seguridad perimetral para las empresas Teamsourcing Cia. Ltda. Con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar ISO-27001. Sangolquí, Ecuador: Bachelor's thesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería Electrónica en Redes y Comunicación de Datos.
- Felix Molina. (2012). Cisco Networking Academy. 26/08/2012, de Espacio Común Virtual de Ingeniería
- Francisco García Marín. (2014). Mantenimiento de infraestructuras de redes locales de datos. ELES0209. Antequera, Málaga: IC Editorial.
- Hewlett Packard. (2017). Qué es la seguridad de red. Hewlett Packard Sitio web: https://www.hpe.com/mx/es/what-is/network-security.html.

- JOSÉ LUIS VILLACÍS MENDOZA. (2009). ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA EN EL COLEGIO INTERNACIONAL SEK-QUITO, CONSIDERANDO ASPECTOS DE SEGURIDAD DENTRO DEL ÁREA PERIMETRAL. QUITO: UNIVERSIDAD INTERNACIONAL SEK.
- Purificación Aguilera López. (2010). Seguridad informática. Madrid, Alarcón: Editex.
- María Del Carmen Romero Ternero. (2014). Redes Locales. España, Madrid: Ediciones Paraninfo.
- Lignux (2015). Conoce ClearOS, simplificando la gestión de los servidores. Diciembre 2015, Lignux Sitio web: https://lignux.com/conoce-clearos-simplificando-la-gestion-de-los-servidores/
- Balaji Sivasubramanian; Erum Frahim; Richard Froom. (2017). Ciscopress. 15 Julio, de Cisco Sitio web: http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3
- Técnico en Redes y Seguridad. (2007). Introducción a las redes informáticas. RedUSERS, 1, 4-5.
- Tejada, E. C. (2014). Auditoría de seguridad informática. IFCT0109. IC Editorial.
- Tolosa, G. (2014). Protocolos y Modelo OSI.
- Nmap: the Network Mapper - Free Security Scanner. Nmap.org. 4 octubre 2017. https://nmap.org/

APÉNDICE

Título del requerimiento	**Diseño e implementación de políticas de seguridad a nivel de firewall perimetral y proxy en la red LAN del semillero OTM Bloque O Sede Fraternidad ITM.**		
Solicitante	**Fecha de Solicitud**		
	DD	**MM**	**AAAA**
Javier Durán	30	11	2016

INFORMACIÓN BÁSICA

Objetivo general

Implementar políticas de firewall y proxy para la red de datos del semillero OTM, a partir del análisis de los controles requeridos para la mitigación de riesgos informáticos a nivel de capa de transporte y capa de red sobre los activos involucrados en las comunicaciones LAN-WAN (Local Area Network- Wide Area Network).

Usuarios involucrados

- Comunidad ITM
- Administrador red Bloque O

Situación actual

En la actualidad el Instituto Tecnológico Metropolitano (ITM) cuenta con unos bloques de laboratorios diseñados y construidos para que los estudiantes puedan practicar y ejecutar las habilidades adquiridas durante su educación en la institución, estos bloques contienen todos los equipos y las tecnologías necesarias para poder darle ejecución a estas actividades, ofreciendo a los estudiantes un acceso libre a todas estas.

Al interior de estas instalaciones se encuentra el bloque O, perteneciente a la red del semillero OTM, el cual en este momento, no cuenta con un sistema de seguridad que permita la gestión adecuada de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta la

información presente en cada uno de los procesos y sistemas internos del semillero, además no se tienen documentados ni estandarizados controles que lleven a mitigar los riesgos presentes como delitos informáticos o amenazas a los que están expuestos los datos comprometiendo sus características de integridad, confidencialidad y disponibilidad.

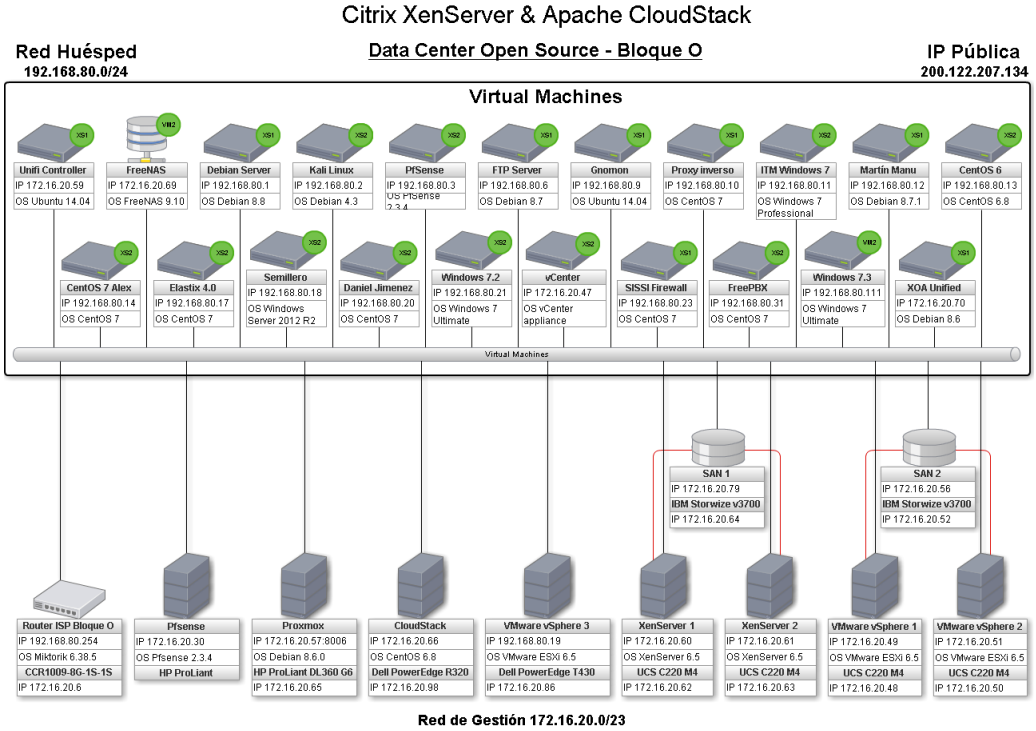
Para esto es necesario adoptar y crear políticas de seguridad que regulen el comportamiento de los sistemas y que garantice las buenas prácticas en cada una de las transacciones, procesos y recursos relacionados con la información, para esto es indispensable realizar el análisis de riesgos de la seguridad de la información sobre los activos tecnológicos presentes en el bloque O como lo son switches, routers, computadores y servidores.

Descripción del requerimiento

Se requiere diseñar e Implementar políticas de firewall y proxy para la red del semillero OTM perteneciente al bloque O del ITM, y así tener mayor seguridad sobre el tráfico entrante y saliente de cada uno de los servidores con respecto a la red LAN y WAN.
Para llevar a cabo esta solicitud se deberán cumplir los siguientes requerimientos:

1. Se deberá levantar el inventario de activos y servicios de la red del Bloque O a nivel de Capa de Red y Capa de Transporte del Modelo OSI.
2. Se deberá diseñar políticas de seguridad a nivel de firewall y de navegación para la red del bloque O del semillero OTM a partir del inventario de activos y servicios. Para definir que tipo de firewall se usara se deberá evaluar en el mercado que tipos existen y sus características.
3. Se deberá realizar el modelo de la red con la implantación de firewall, es decir, donde quedará ubicado y cuál será la nueva topología de la red.
4. Se requiere Implementar las políticas de seguridad para firewall y proxy diseñadas anteriormente.
5. Realizar pruebas correspondientes a la implementación solicitada.

Apéndice1. CRD - Diseño e implementación de políticas de seguridad a nivel de firewall perimetral y proxy en la red LAN/WAN del semillero OTM Bloque O Sede Fraternidad ITM.

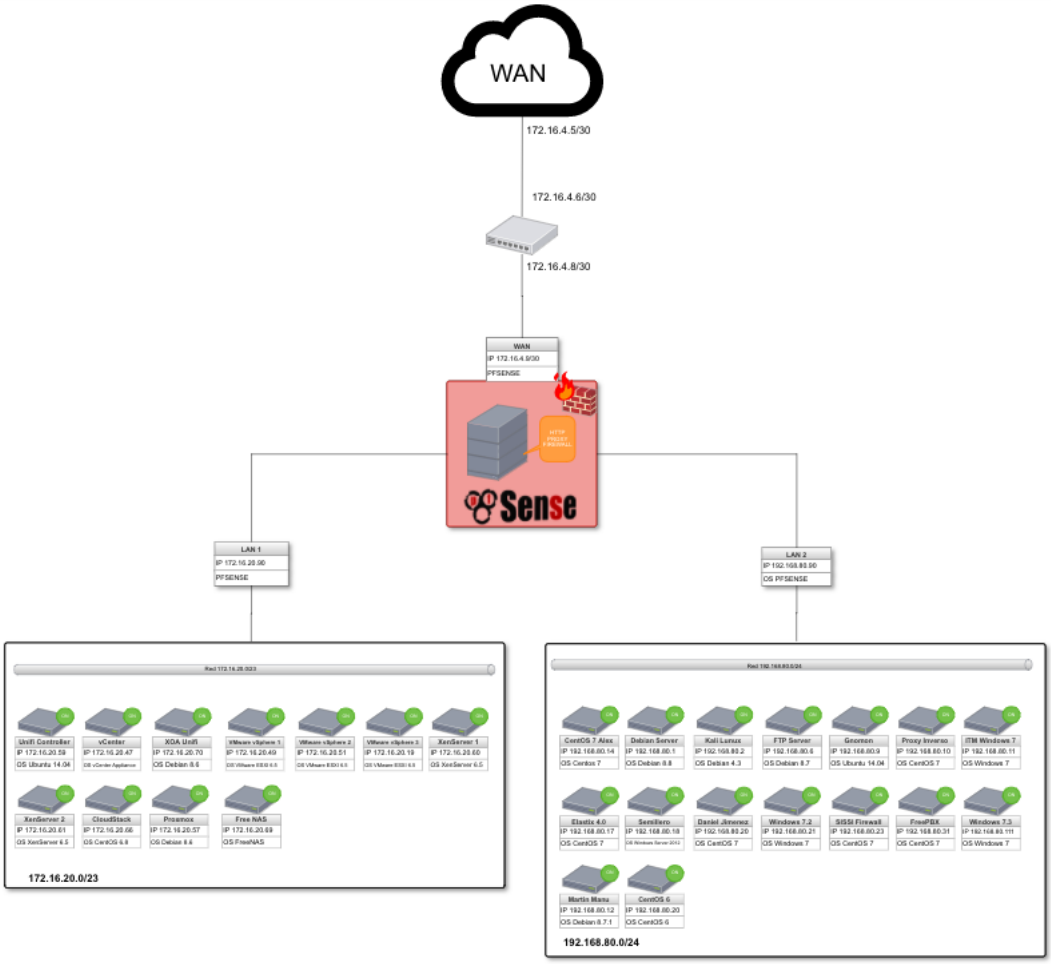


Apéndice2. Diagrama Topológico de la red del semillero OTM Bloque O anterior a la implementación y configuración del Firewall

Firewall	Características	Ventajas
ClearOS	Se basa en una interfaz web muy cuidada, potente y flexible. Es un sistema operativo orientado a Pymes (pequeñas y medianas empresas), con lo que cuenta con todo el software necesario para su funcionamiento y gestión.	• "Se encarga de escanear el spam y los virus para tráfico http, al igual que en pop imap, y smtp (semejante al plugin copfilter de ipcop). • Cuenta con firewall simple que logra detectar intrusiones. • Ofrece la filtración contenidos/protocolos a través de proxy de una forma rápida y eficaz. • Cuenta con Servidor FTP (ProFTPD), MySQL con dirección mediante el proyecto phpMyAdmin y WEB (apache 2) • Servidor LDAP con autenticación de SAMBA (muy sencillamente configurable). • Proporciona informe de logs en relación a cada uno de los servicios. Tiene un sistema recursos compartidos (sistema de ficheros e impresoras) a través de SAMBA y de impresión (CUPS)." (Lignux, 2015)

IPFire	Es un firewall minimalista que viene integrado con un manejador de paquetes llamado Pakfire. Su función principal es actualizar el sistema de manera sencilla permitiéndonos instalar los últimos parches de seguridad y mejoras.	• "Servidor proxy con filtro de contenido y funcionalidad de caché para actualizaciones (es decir, actualizaciones de Microsoft Windows y antivirus) • Sistema de detección de intrusiones (Snort) con tutor de prevención de intrusiones • VPN a través de IPsec y OpenVPN • Servidor DHCP • Servidor de nombre de caché • Servidor de tiempo • DNS Dinámico • Calidad de servicio • Cortafuegos saliente Supervisión del sistema y análisis de registros" (Capacity, 2013).
pfSense	Se basa en el filtrado de paquetes con estado. Tiene una amplia gama de características que normalmente sólo se encuentran en los cortafuegos muy caros.	• "Filtrado de origen a destino de IP, protocolo IP, puerto de origen y destinación para TCP y UDP tráfico. · • Habilitación de límites para conexiones simultaneas con reglas de base. · • pfSense utiliza p0f, una avanzada herramienta de red para huellas dactilares digitales que habilita la filtración a través el sistema operativo al inicio de la conexión. · • Opción para conectar o no conectar el tráfico descrito por cada regla. · • Políticas de enrutamiento con alta flexibilidad para la selección del Gateway sobre las reglas de base para el equilibrio de banda, failover, WAN múltiple, backup sobre mas ADSL, etc. • Posibilidad de creación de Alias de grupos de IP y nombres de IP, networks y puertas. Estas características ayudan a mantener la configuración limpia y fácil de entender, especialmente con configuraciones con varios IP públicos y numerosos Servers. · • Filtración transparente Layer 2. Posibilidad de puentear interfaces y filtrar el tráfico entre estas. • Normalización de paquetes. Descrito en la documentación de pf Scrub. Habilitado por defecto. Es posible desactivarlo si es necesario. · • Posibilidad de inhabilitar la filtración (firewalling) para utilizar pfSense como solo router" (Borrero, 2016)
IPCop	Es una distribución Linux que implementa un cortafuegos y proporciona una simple interfaz web de administración basándose en una computadora personal.	• "Soporte a DHCP como cliente y como servidor. • Cliente y servidor NTP. • Soporte a VPN. • Soporte Proxy para navegación web y direccionamiento DNS. • Administración y configuración a través de interfaz web, con posibilidad de visualización de gráficas." (bilib, 2012)

Apéndice3. Ventajas y desventajas sobre las herramientas Firewall



Apéndice4. Diagrama Topológico de la red del semillero OTM Bloque O después de la implementación y configuración del Firewall

Nombre Servidor	IP Servidor	Descripción Servidor	Protocolo TCP/UDP	Puerto
FTP Server	192.168.80.6	Es un servidor Ubuntu Server 16.04.2, que presta un servicio FTP. Es un protocolo de transferencia de archivos a través de la red entre sistemas conectados a través de conexiones TCP. Este protocolo se basa en una	**TCP**	**21**
			TCP	22
			TCP	111

		arquitectura cliente-servidor, donde el cliente solicita acceso al servidor y una vez garantizado, le permite descargar o subir archivos. El protocolo FTP consta principalmente de dos puertos, el puerto 21, utilizado para conectarse de forma remota a un servidor y autenticarse en él y el puerto 20, que se utiliza para las transferencias de archivos una vez autenticado. Por lo tanto, el servidor solo requiere tener abierto el puerto TCP 22 (Secure SHell) en la administración del servidor.	UDP	111
			UDP	979
			UDP	50492
Gnomon	192.168.80.9	Es un servidor Ubuntu Server 14.04.2, que presta un servicio Web. Son el conjunto de aplicaciones o tecnologías con capacidad para interpolar en la Web. Estas tecnologías intercambian datos entre ellas con el fin de ofrecer unos servicios. Este servicio debe poder ser accesible a través de la Web, para ello debe utilizar protocolos de transporte estándares como HTTP (80) o HTTPS (443).	**TCP**	**22**
			TCP	**80**
			TCP	**443**
			UDP	161
			UDP	43526
			UDP	45853
Proxy Inverso	192.168.80.10	Es un servidor CentOS 7, que presta un servicio Web. Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 22 (Secure SHell) en la administración del servidor, TCP 80 (HTTP) y TCP 443 (HTTPS). Los demas puertos abiertos encontrados se procederán a cerrar.	**TCP**	**22**
			TCP	**80**
			TCP	**443**
ITM Windows	192.168.80.11	Es un servidor Windows 7, que presta un servicio VPN (Virtual Private Network). Es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 3389(Remote Desktop Protocol) el cual permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor Windows, el puerto TCP 139 (NetBIOS Servicio de sesiones) es una especificación de interfaz para acceso a servicios de red	TCP	135
			TCP	**139**
			TCP	**445**
			TCP	**3389**
			TCP	7070
			TCP	49152
			TCP	49153
			TCP	49154
			TCP	49155
			TCP	49160
			TCP	49161

		y el puerto TCP 445(Microsoft-DS) compartición de ficheros. Los demas puertos abiertos encontrados se procederán a cerrar.	UDP	137
			UDP	138
			UDP	161
			UDP	500
			UDP	514
			UDP	4500
			UDP	5355
			UDP	55843
			UDP	55844
			UDP	55845
			UDP	56095
			UDP	56096
			UDP	56097
			UDP	56098
			UDP	56099
			UDP	56100
			UDP	60628
			UDP	60629
			UDP	60630
Martin UdeA	192.168.80.12	Es un servidor Ubuntu Server 16.04.2, que presta un servicio Web. Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 22 (Secure SHell) en la administración del servidor, el puerto TCP 80 (HTTP) y el puerto TCP 443 (HTTPS). Los demas puertos abiertos encontrados se procederán a cerrar.	**TCP**	**22**
			TCP	**80**
			TCP	**443**
Centos6	192.168.80.13	Es un servidor CentOS 6, que presta un servicio Web. Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 22 (Secure SHell) en la administración del servidor y el puerto TCP 80 (HTTP). Los demas puertos abiertos encontrados se procederán a cerrar.	**TCP**	**22**
			TCP	**80**
Centos7	192.168.80.14	Es un servidor CentOS 7, que presta un servicio Web. Por lo tanto, el servidor solo requiere tener abiertos los	**TCP**	**22**

		puertos TCP 22 (Secure SHell) en la administración del servidor y el puerto TCP 80 (HTTP). Los demas puertos abiertos encontrados se procederán a cerrar.	**TCP**	**80**
Elastix 4	192.168.80.17	Es un servidor Ubuntu, que presta un servicio VoIp (Voz por protocolo de internet), es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP (Protocolo de Internet). Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 22 (Secure SHell) en la administración del servidor, el puerto TCP 80 (HTTP), el puerto TCP 443 (HTTPS), el puerto UDP 68 (Cliente de protocolo de arranque) , el puerto UDP 69 (Trivial file transfer Protocol) y el puerto UDP 5060 (Session Initiation Protocol). Los demas puertos abiertos encontrados se procederán a cerrar.	**TCP**	**22**
			TCP	25
			TCP	**80**
			TCP	110
			TCP	143
			TCP	**443**
			TCP	993
			TCP	995
			TCP	3306
			TCP	4445
			UDP	**68**
			UDP	**69**
			UDP	2727
			UDP	4520
			UDP	4569
			UDP	5000
			UDP	**5060**
			UDP	5353
			UDP	33817
			UDP	49957
Semillero	192.168.80.18	Es un servidor Windows Server 2012 R2, que presta un servicio como controlador de dominio. Es el centro neurálgico de un dominio Windows, tal como un servidor Network Information Service (NIS) lo es del servicio de información de una red Unix. Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 53 (Domain Name System), el puerto TCP 80 (HTTP), el puerto TCP 88 (Kerberos), el puerto TCP 135 (epmap) , el puerto TCP 139 (NetBIOS-SSN), el puerto TCP 389 (LDAP), el puerto TCP 445 (MS DS), el	**TCP**	**53**
			TCP	**80**
			TCP	**88**
			TCP	**135**
			TCP	**139**
			TCP	**389**
			TCP	**445**
			TCP	**464**
			TCP	593
			TCP	**636**

		puerto TCP 464 (Kerberos change/set password), el puerto TCP 636, el puerto TCP 3268, el puerto TCP 3269, el puerto TCP 3389(MS RDP), el puerto UDP 53(DNS), el puerto UDP 123(NTP) y el puerto UDP 137(NetBIOS-NS). Los demas puertos abiertos encontrados se procederán a cerrar.	**TCP**	**3268**
			TCP	**3269**
			TCP	**3389**
			TCP	49154
			TCP	49155
			TCP	49157
			TCP	49158
			TCP	49159
			UDP	**53**
			UDP	**123**
			UDP	**137**
Daniel Jimenez	192.168.80.20	Es un servidor CentOS 7, el servidor solo requiere tener abierto el puerto TCP 22 (Secure SHell) en la administración del servidor.	**TCP**	**22**
Windows 7	192.168.80.21	Es un servidor Windows 7. Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 3389 (MS RDP) y el puerto UDP 500 (ISAKMP). Los demas puertos abiertos encontrados se procederán a cerrar.	TCP	135
			TCP	139
			TCP	445
			TCP	554
			TCP	2869
			TCP	**3389**
			TCP	10243
			TCP	49152
			TCP	49153
			TCP	49154
			TCP	49155
			TCP	49156
			TCP	49158
			UDP	137
			UDP	138
			UDP	**161**
			UDP	**500**
			UDP	1900
			UDP	4500
			UDP	5004

			UDP	5005
			UDP	5355
			UDP	59853
Windows 7,2	192.168.80.111	Es un servidor Windows 7.2 Por lo tanto, el servidor solo requiere tener abiertos los puertos TCP 135, el puerto TCP 445 (MS DS) y el puerto TCP 3389 (MS RDP). Los demas puertos abiertos encontrados se procederán a cerrar.	**TCP**	**135**
			TCP	**445**
			TCP	**3389**
Load Balancer	192.168.80.23	Es un servidor Linux, por lo tanto, el servidor solo requiere tener abierto el puerto TCP 22 (Secure SHell) en la administración del servidor.	**TCP**	**22**
UCS C220 M4	172.16.20.48	Es un servidor Cisco UCS C220 M4, donde está instalado VMWare ESXi 6.5. Por lo tanto, el servidor solo requiere tener abiertos los puertos UDP 389 y el puerto UDP 443; desde la red LAN se requiere el puerto TCP 161(Simple Network Management Protocol) este abierto. Los demas puertos abiertos encontrados se procederán a cerrar.	UDP	123
			UDP	**161**
			UDP	**389**
			UDP	**443**
			UDP	636
			UDP	3268
			UDP	3269
VMware vSphere 1	172.16.20.49	Es un servidor Hipervisor. Por lo tanto, el servidor solo requiere tener abierto el puerto UDP 53(DNS), desde la red LAN se requiere el puerto TCP 161(Simple Network Management Protocol) abierto. Los demas puertos abiertos encontrados se procederán a cerrar.	**UDP**	**53**
			UDP	68
			UDP	**161**
			UDP	427
			UDP	546
			UDP	8200
			UDP	12345
			UDP	23451
			UDP	123
UCS C220 M4	172.16.20.50	Es un servidor Cisco UCS C220 M4, donde está instalado VMWare ESXi 6.5. Por lo tanto, el servidor solo requiere tener abiertos los puertos UDP 389 y el puerto UDP 443; desde la red LAN se requiere el puerto TCP 161(Simple Network Management Protocol) este abierto.	**UDP**	**161**
			UDP	**389**
			UDP	**443**
			UDP	636
			UDP	3268
			UDP	3269

		Los demas puertos abiertos encontrados se procederán a cerrar.		
VMware vSphere 2	172.16.20.51	Es un servidor Hipervisor. Por lo tanto, el servidor solo requiere tener abierto el puerto UDP 53(DNS), desde la red LAN se requiere el puerto TCP 161(Simple Network Management Protocol) abierto. Los demas puertos abiertos encontrados se procederán a cerrar.	U**DP**	**53**
			UDP	68
			UDP	**161**
			UDP	427
			UDP	546
			UDP	8200
			UDP	12345
			UDP	23451
IBM Sorwize v3700	172.16.20.52	Es un servidor de almacenamiento, por lo tanto, solo requiere abierto desde la red LAN el puerto TCP 161(Simple Network Management Protocol).	UDP	42
			UDP	53
			UDP	**161**
SAN 2	172.16.20.56	Es un servidor de almacenamiento, por lo tanto, solo requiere abierto desde la red LAN el puerto TCP 161(Simple Network Management Protocol).	**UDP**	**161**
Proxmox	172.16.20.57	Es un servidor Hipervisor y los puertos que debe tener abiertos no aparecieron en el escaneo, por lo tanto, se cierran los que se detectarón ya que no se conoce su funcionalidad.	UDP	111
			UDP	1018
			UDP	39212
			UDP	5062
XenServer 1	172.16.20.60	Es un servidor XenServer 1-Citrix XenServer y los puertos que debe tener abiertos no aparecieron en el escaneo, por lo tanto, se cierran los que se detectarón ya que no se conoce su funcionalid	TCP	22
			TCP	443
			TCP	5900
			TCP	3389
UCS C220 M4	172.16.20.62	Es un servidor Cisco UCS C220 M4- donde está instalado Citrix XenServer Por lo tanto, el servidor solo requiere tener abiertos los puertos UDP 389 y el puerto UDP 443, y desde la red LAN se requiere el puerto TCP 161(Simple Network Management Protocol). Los demas puertos abiertos encontrados se procederán a cerrar.	UDP	123
			UDP	161
			UDP	389
			UDP	443
			UDP	636
			UDP	3268
			UDP	3269
UCS C220 M4	172.16.20.63	Es un servidor Cisco UCS C220 M4- donde está instalado Citrix XenServer	UDP	123
			UDP	**161**

		Por lo tanto, el servidor solo requiere tener abiertos los puertos UDP 389 y el puerto UDP 443, y desde la red LAN se requiere el puerto TCP 161(Simple Network Management Protocol). Los demas puertos abiertos encontrados se procederán a cerrar.	**UDP**	**389**
			UDP	**443**
			UDP	636
			UDP	3268
			UDP	3269
			UDP	
			UDP	
IBM Storwize v 3700	172.16.20.64	Es un servidor de almacenamiento, por lo tanto, solo requiere abierto desde la red LAN el puerto TCP 161(Simple Network Management Protocol).	UDP	42
			UDP	53
			UDP	101
			UDP	**161**
			UDP	427
HP ProLiant DL360 G6	172.16.20.65	Es un servidor HP ProLiant DL360 G6, Por lo tanto, el servidor solo requiere abierto desde la red LAN el puerto TCP 161(Simple Network Management Protocol).	UDP	0
			UDP	**161**
CloudStack	172.16.20.66	Encargada de coordinar de manera centralizada el aprovisionamiento automático de capacidades de cómputos y sus dependencias (almacenamiento, redes y sistemas operativos).	All 65536 scanned ports on 172.16.20.66 are filtered (65257) or open|filtered (279)	
FreeNAS	172.16.20.69	Es un servidor de almacenamiento, por lo tanto, solo requiere abierto desde la red LAN el puerto TCP 161(Simple Network Management Protocol). Los demas puertos abiertos encontrados se procederán a cerrar.	UDP	0
			UDP	111
			UDP	123
			UDP	137
			UDP	138
			UDP	611
			UDP	773
			UDP	832
			UDP	872
			UDP	1031
			UDP	5353
			UDP	34350
SAN 2	172.16.20.79	Es un servidor de almacenamiento, por lo tanto, solo	UDP	42

		requiere abierto desde la red LAN el puerto TCP 161(Simple Network Management Protocol). Los demas puertos abiertos encontrados se procederán a cerrar.	UDP	53
			UDP	**161**
Dell PowerEdge R320	172.16.20.98	Es un servidor de almacenamiento, por lo tanto, solo requiere abierto desde la red LAN el puerto TCP 161(Simple Network Management Protocol). Los demas puertos abiertos encontrados se procederán a cerrar.	**UDP**	**161**
			UDP	623

Apéndice5. Escaneo de la red del semillero OTM Bloque O

LAN/WAN	Protocolo (TCP, UDP, IMCP)	Action(Pass, Block, Reject)	Source	Port	Destination	Port
WAN	ANY	Block	Reserved Not assigned by IANA	ANY	ANY	ANY
Servidor FTP						
WAN	TCP	Pass	ANY	ANY	192.168.80.6	21
Servidor Gnomon						
WAN	TCP	Pass	ANY	ANY	192.168.80.9	22
WAN	TCP	Pass	ANY	ANY	192.168.80.9	80
WAN	TCP	Pass	ANY	ANY	192.168.80.9	443
Servidor Proxy						
WAN	TCP	Pass	ANY	ANY	192.168.80.10	22
WAN	TCP	Pass	ANY	ANY	192.168.80.10	80
WAN	TCP	Pass	ANY	ANY	192.168.80.10	443
Servidor ITM Windows						
WAN	TCP	Pass	ANY	ANY	192.168.80.11	139
WAN	TCP	Pass	ANY	ANY	192.168.80.11	445
WAN	TCP	Pass	ANY	ANY	192.168.80.11	3389
Servidor MartinUdeA						
WAN	TCP	Pass	ANY	ANY	192.168.80.12	22
WAN	TCP	Pass	ANY	ANY	192.168.80.12	80
WAN	TCP	Pass	ANY	ANY	192.168.80.12	443
Servidor CentOS6						

WAN	TCP	Pass	ANY	ANY	192.168.80.13	22
WAN	TCP	Pass	ANY	ANY	192.168.80.13	80
Servidor CentOS7						
WAN	TCP	Pass	ANY	ANY	192.168.80.14	22
WAN	TCP	Pass	ANY	ANY	192.168.80.14	80
Servidor Elastix4						
WAN	TCP	Pass	ANY	ANY	192.168.80.17	22
WAN	TCP	Pass	ANY	ANY	192.168.80.17	80
WAN	TCP	Pass	ANY	ANY	192.168.80.17	443
WAN	TCP	Pass	ANY	ANY	192.168.80.17	69
WAN	TCP	Pass	ANY	ANY	192.168.80.17	68
WAN	TCP	Pass	ANY	ANY	192.168.80.17	5060
Servidor Semillero						
WAN	TCP	Pass	ANY	ANY	192.168.80.18	53
WAN	TCP	Pass	ANY	ANY	192.168.80.18	80
WAN	TCP	Pass	ANY	ANY	192.168.80.18	88
WAN	TCP	Pass	ANY	ANY	192.168.80.18	135
WAN	TCP	Pass	ANY	ANY	192.168.80.18	139
WAN	TCP	Pass	ANY	ANY	192.168.80.18	389
WAN	TCP	Pass	ANY	ANY	192.168.80.18	445
WAN	TCP	Pass	ANY	ANY	192.168.80.18	464
WAN	TCP	Pass	ANY	ANY	192.168.80.18	636
WAN	TCP	Pass	ANY	ANY	192.168.80.18	3268
WAN	TCP	Pass	ANY	ANY	192.168.80.18	3269
WAN	TCP	Pass	ANY	ANY	192.168.80.18	3389
WAN	UDP	Pass	ANY	ANY	192.168.80.18	53
WAN	UDP	Pass	ANY	ANY	192.168.80.18	123
WAN	UDP	Pass	ANY	ANY	192.168.80.18	137
Servidor Daniel Jimenez						
WAN	TCP	Pass	ANY	ANY	192.168.80.20	22
Servidor Windows 7						
WAN	TCP	Pass	ANY	ANY	192.168.80.21	3389

WAN	TCP	Pass	ANY	ANY	192.168.80.21	500
Servidor Windows 7.2						
WAN	TCP	Pass	ANY	ANY	192.168.80.111	135
WAN	TCP	Pass	ANY	ANY	192.168.80.111	445
WAN	TCP	Pass	ANY	ANY	192.168.80.111	3389
Servidor Load Balancer						
WAN	TCP	Pass	ANY	ANY	192.168.80.23	22
Servidor UCS C220 M4						
WAN	TCP	Pass	ANY	ANY	192.168.80.48	389
WAN	TCP	Pass	ANY	ANY	192.168.80.48	443
Servidor Vmware vSphere 1						
WAN	TCP	Pass	ANY	ANY	192.168.80.49	53
Servidor UCS C220 M4						
WAN	TCP	Pass	ANY	ANY	192.168.80.50	389
WAN	TCP	Pass	ANY	ANY	192.168.80.50	443
Servidor Vmware vSphere 2						
WAN	TCP	Pass	ANY	ANY	192.168.80.51	53
Servidor XenServer 1						
WAN	TCP	Pass	ANY	ANY	192.168.80.60	22
WAN	TCP	Pass	ANY	ANY	192.168.80.60	443
WAN	TCP	Pass	ANY	ANY	192.168.80.60	5900
WAN	TCP	Pass	ANY	ANY	192.168.80.60	3389
Servidor UCS C220 M4						
WAN	TCP	Pass	ANY	ANY	192.168.80.62	389
WAN	TCP	Pass	ANY	ANY	192.168.80.62	443
Servidor UCS C220 M4						
WAN	TCP	Pass	ANY	ANY	192.168.80.63	389
WAN	TCP	Pass	ANY	ANY	192.168.80.63	443
Bloqueo						
WAN	ICMP	Block	ANY	ANY	ANY	ANY
WAN	ANY	Block	ANY	ANY	ANY	ANY

Apéndice6. Reglas del Firewall de la red del semillero OTM Bloque O

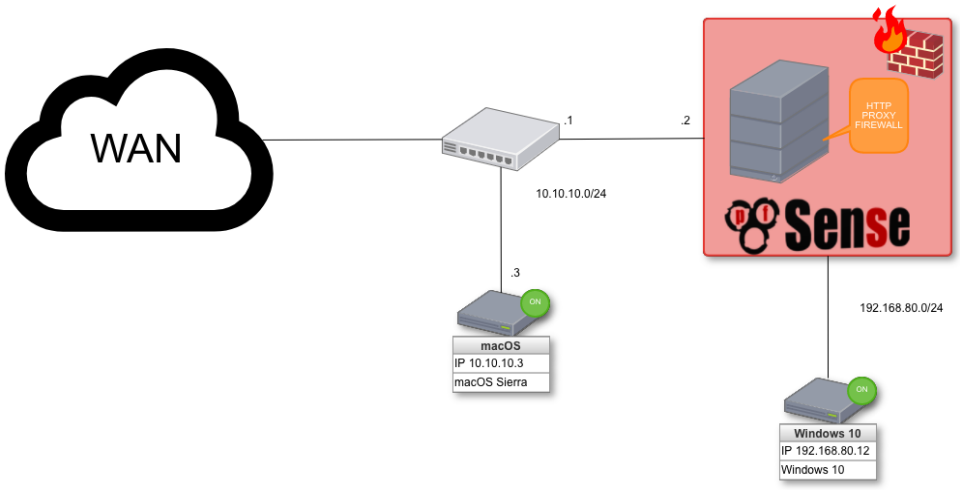
Categoria	Descripción
adv	Todo sobre publicidad: incluye sitios que ofrecen pancartas y creación de pancartas, así como sitios que ofrecen pancartas para mostrar en páginas web. Las compañías de publicidad también están en la lista.
aggressive	Sitios de contenido agresivo obvio. Esto abarca el discurso de odio y todo tipo de racismo.
alcohol	Sitios de cervecerías, bodegas y destilerías. Esta categoría también cubre sitios que explican cómo hacer cerveza, vinos y licores.
anonvpn	Esta categoría cubre los sitios que brindan servicios de VPN al público. La atención se centra en los sitios VPN utilizados para ocultar el origen del tráfico como los nodos Tor (red de anonimato). La categoría no incluye los accesos VPN de la compañía.
automobile/bikes	Todo alrededor de motocicletas. Se incluyen sitios de proveedores, revendedores, páginas de aficionados y pasatiempos, así como también proveedores. Scooters incluidos.
automobile/boats	Todo alrededor de lanchas motoras. Se incluyen sitios de proveedores, revendedores, páginas de aficionados y pasatiempos, así como también proveedores. No se incluyen consejos de viaje (esto se puede encontrar en recreación / viaje).
automobile/cars	Todo alrededor de los autos. Se incluyen las compañías automotrices y los proveedores automotrices.
automobile/planes	Todo alrededor de aviones que van desde uno y dos asientos hasta los aviones de gran tráfico, viejos y nuevos, privados, comerciales y militares. Proveedores están incluidos (los aeropuertos no lo son). Los sitios de helicópteros también están incluidos.
chat	Sitios para chat en tiempo real y mensajería instantánea. Todo lo que no está en tiempo real está incluido.
costtraps	Sitios que atraen a los usuarios con servicios gratuitos pero que luego le brindan una solución costosa (escrita en algún lugar con letras minúsculas casi ilegible).
dating	Sitios para contactar personas por amor y vivir juntos. Él la busca, ella lo busca y así sucesivamente.
downloads	Esto cubre principalmente los sitios de intercambio de archivos, P2P y torrente. También se incluyen otros sitios de descarga (para software, fondos de pantalla, ...).
drugs	Sitios que ofrecen medicamentos o explican cómo hacerlos (legales y no legales). Cubre tanto tabaco como viagra y sustancias similares.
dynamic	Todos los dominios donde las personas inician sesión desde una que obtiene una dirección IP dinámica. Los sitios dinámicos pueden ser más inofensivos, así como llevar a los proxies de redirección para eludir el filtro web o la pornografía, los juegos o cualquier otra cosa que pueda ser inapropiada.
education/schools	Páginas de inicio de escuelas, colegios y universidades.
finance/banking	Página de inicio de las empresas bancarias se enumeran aquí. Esto no está restringido a la banca en línea.
finance/insurance	Sitios de compañías de seguros, sobre información sobre seguros y colecciones de enlaces relacionadas con este tema.
finance/moneylending	Los sitios pueden solicitar préstamos e hipotecas o pueden obtener información sobre este negocio.
finance/realestate	Sitios sobre todo tipo de bienes raíces, venta y venta de casas, búsqueda de apartamentos en alquiler y venta.
finance/trading	Sitios sobre el mercado bursátil, negociación de acciones y opciones sobre acciones, así como sitios relacionados con este tema.
finance/other	Todas las páginas financieras que no se ajustan a las categorías financieras anteriores.

fortunetelling	Todos los sitios sobre astrología, horóscopos, numerología, lectura de manos y demás; sitios que ofrecen servicios para proponer el futuro.
forum	Sitios de discusión. Cubierto sitios de foros explícitos y algunos blogs. Sitios donde las personas pueden discutir y compartir información de una manera no interactiva / en tiempo real. Los debates en tiempo real están cubiertos.
gamble	Sitios que ofrecen la posibilidad de ganar dinero. Poker, Casino, Bingo y otros juegos de azar, así como sitios de apuestas. Difiere de afición / juegos en el aspecto de ganar o perder dinero o ser atraído por hacerlo.
government	Sitios pertenecientes al gobierno de un país, condado o ciudad.
hacking	Sitios con información y discusiones sobre debilidades de seguridad y cómo explotarlos. Se enumeran los sitios que ofrecen exploits y los sitios que distribuyen programas que ayudan a detectar fugas de seguridad.
hobby/cooking	Sitios relacionados con la comida y la preparación de alimentos.
hobby/games-misc	Sitios relacionados con juegos. Esto incluye descripciones, noticias e información general sobre juegos. No hay sitios de apuestas.
hobby/games-online	Sitios sobre juegos en línea (todo tipo de juegos basados en navegador). Los juegos son solo por diversión (sin apuestas).
hobby/gardening	Sitios sobre jardinería, plantas en crecimiento, bichos y todo lo relacionado con la jardinería.
hobby/pets	Sitios sobre todos los temas relacionados con mascotas: descripción, aumento, comida, apariencia, ferias, historias favoritas de mascotas, etc.
homestyle	Sitios sobre todo lo necesario para crear una casa acogedora (diseño de interiores y ambientes).
hospitals	Sitios de hospitales e instalaciones médicas.
imagehosting	Sitios especializados en alojamiento de imágenes, fotoláminas, etc.
isp	Páginas de inicio de los proveedores de servicios de Internet. También se están agregando sitios de compañías que ofrecen espacio web solamente.
jobsearch	Portales de ofertas de trabajo y buscadores de empleo, así como las páginas de empresas y trabajos para nosotros.
library	Bibliotecas en línea y sitios donde puede obtener y / o leer libros electrónicos. Las tiendas de libros no están en la lista aquí, sino en las compras.
military	Sitios de instalaciones militares o relacionados con las fuerzas armadas.
models	La agencia modelo, el modelo y las páginas de admiradores de la supermodelo y otros sitios modelo que presentan fotos modelo. No hay fotos porno
movies	Sitios que ofrecen programas de cine, información sobre películas y actores. También se incluyen sitios para descargar videoclips / películas (siempre que sea legal).
music	Sitios que ofrecen la descarga de música, información sobre grupos de música o música en general.
news	Sitios que presentan noticias. Páginas principales de periódicos, revistas y revistas, así como algunos blogs.
podcasts	Sitios que ofrecen podcasts o servicios de podcast.
politics	Sitios de partidos políticos, organizaciones políticas y asociaciones; sitios con discusiones políticas.
porn	Sitios sobre todo tipo de contenido sexual que van desde pechos desnudos hasta pornografía hardcore y sm.

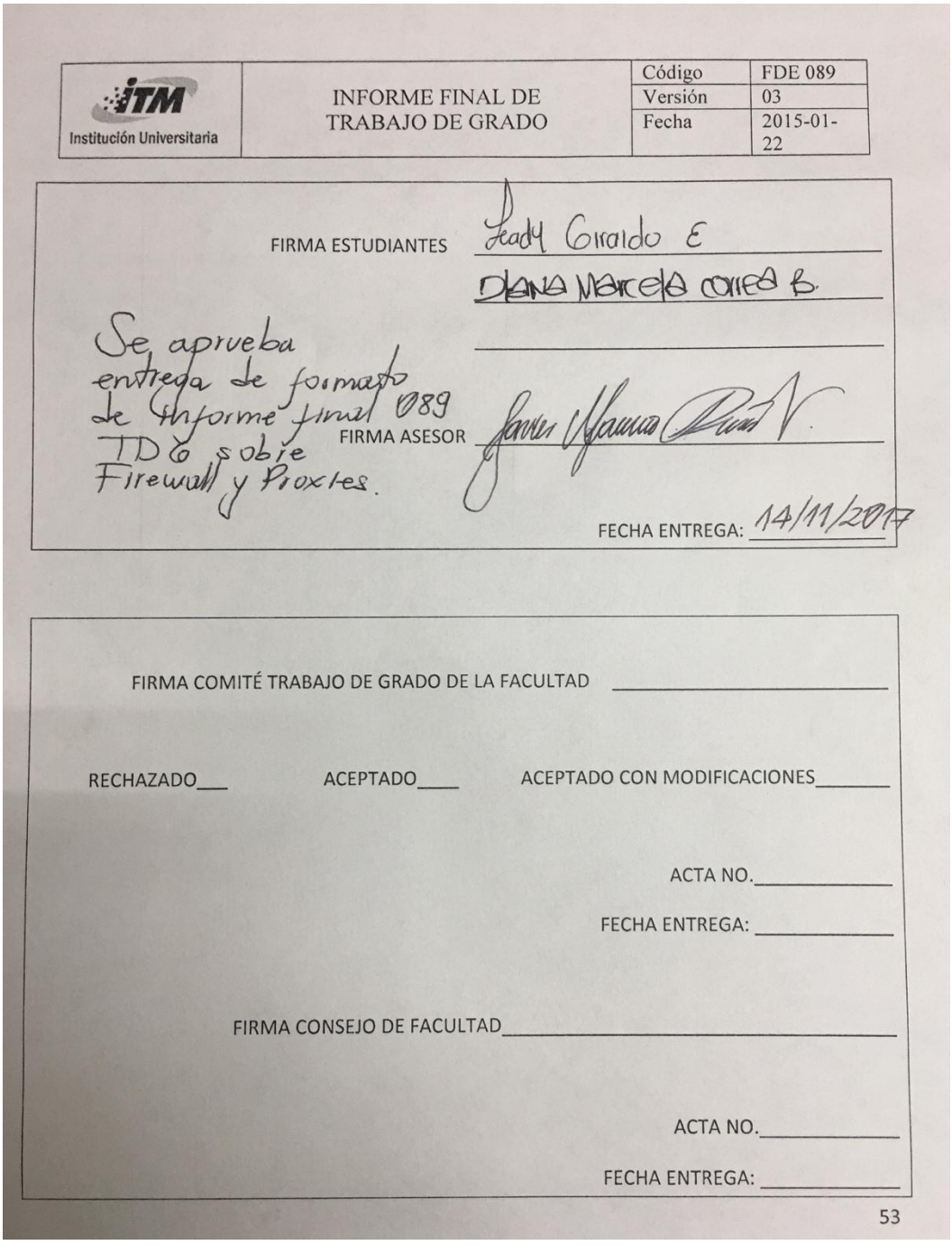
radiotv	Dominios y direcciones URL de estaciones de TV y radio, independientemente de si ofrecen algún programa en el sitio o simplemente muestran una página estática. Los sitios que ofrecen transmisiones aún se recopilan en webradio y webtv, respectivamente.
recreation/humor	Páginas humorísticas, historietas, historias divertidas, todo lo que hace reír a la gente.
recreation/martialarts	Los sitios dedicados a las artes marciales como el karate, el kung fu, el taek ganan y también los sitios de deportes de combate como el ufc. Todos los sitios enumerados en esta categoría también son parte de los deportes. Esta categoría está dirigida a usuarios que desean practicar deportes, pero no a deportes "agresivos".
recreation/restaurants	Sitios de restaurantes, descripciones de restaurantes y comentarios.
recreation/sports	Todo sobre deportes: equipos deportivos, debates deportivos, así como información sobre deportistas y los diversos deportes.
recreation/travel	Sitios con información sobre países extranjeros, compañías de viajes, tarifas de viajes, accomondations y todo lo demás que tiene que ver con los viajes, incluidos los blogs de viajes.
recreation/wellness	Aquí: Sitios sobre tratamientos para sentirse interna y externamente sanos y hermosos de nuevo.
redirector	Sitios que ayudan activamente a omitir los filtros de URL mediante la aceptación de URL a través del formulario web y juegan un papel de aproximación y redirección.
religion	Sitios con contenido religioso: todo tipo de iglesias, sectas, interpretaciones religiosas, etc.
remotecontrol	Sitios que ofrecen el servicio para acceder de forma remota a las computadoras, especialmente (pero no limitado a hacerlo) a través de firewalls. Esto incluye usar una computadora de un tercero. La VPN tradicional no está cubierta.
ringtones	Sitios que ofrecen la descarga de tonos de llamada u otras informaciones sobre tonos de llamada.
science/astronomy	Sitios de instituciones, así como de aficionados sobre todos los temas de la astronomía.
science/chemistry	Sitios de instituciones y de aficionados sobre todos los temas de la química.
searchengines	Colección de motores de búsqueda y sitios de directorio.
sex/education	Sitios que explican las funciones biológicas del cuerpo en relación con la sexualidad y la salud sexual; esto también cubre sitios para adolescentes con preguntas sobre el primer amor, el primer sexo y temas relacionados con este tema. Esta categoría no cubre el porno
sex/lingerie	Sitios que venden y presentan lencería sexy o lencería sexy.
shopping	Sitios que ofrecen compras en línea y comparaciones de precios.
socialnet	Sitios que unen a las personas (redes sociales) ya sea por amistad o por negocios.
spyware	Sitios que intentan intentar activamente instalar software (o atraer al usuario haciéndolo) para espiar el comportamiento de navegación (o algo peor). Esta categoría incluye sitios de troyanos y phishing. El sitio de inicio del hogar donde se envía la información de recopilación también figura en la lista.
tracker	Sitio vigilando dónde navegas y qué haces de forma pasiva. Cubre errores web, contadores y otros mecanismos de seguimiento en páginas web que no interfieren con la computadora local y que aún recopilan información sobre la persona que practica surf para análisis posteriores. Los sitios que espían activamente al internauta instalando software o llamando a sitios de inicio no están cubiertos con el rastreador, pero con spyware.

updatesites	Tipo de lista blanca para permitir las descargas necesarias de los proveedores. Pensamiento como una corrección a la categoría de descargas.
urlshortener	Dominios que se pueden usar para acortar URL largas. Se accederá a la URL original (larga) después de que se haya solicitado la URL corta del acortador. Esto distingue esta categoría del redirector donde nunca se accede directamente a la URL original.
violence	Sitios sobre matar y dañar a las personas. Cubre todo sobre la brutalidad y la bestialidad.
warez	Colección de sitios que ofrecen programas para romper claves de licencia, claves de licencia, software descifrado y otro material protegido por derechos de autor.
weapons	Sitios que ofrecen todo tipo de armas o accesorios para armas: armas de fuego, cuchillos, espadas, arcos, ... Se incluyen tiendas de armería, así como sitios con información general sobre armas (fabricación, uso).
webmail	Sitios que ofrecen servicios de correo electrónico basados en la web.
webphone	Sitios que permiten al usuario hacer llamadas a través de Internet / WWW. Cualquier sitio donde los usuarios puedan chatear entre ellos (los sitios normales de chat, donde los usuarios escriben sus mensajes son parte del chat, no del teléfono web).
webradio	Sitios que ofrecen escuchar radiostreams en vivo.
webtv	Colección de sitios que ofrecen transmisiones de TV en vivo a través de Internet.

Apéndice7. Tabla de categorías para la configuración de las reglas en el proxy.



Apéndice8. Diagrama Topológico de la red del semillero OTM Bloque O después de la implementación y configuración del Firewall



Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

FIRMA ESTUDIANTES Leady Giraldo E

DIANA MARCELA CORREA B.

Se aprueba entrega de formato de informe final 089 TD6 sobre Firewall y Proxies.

FIRMA ASESOR

FECHA ENTREGA: 14/11/2017

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____

53