UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

"SIMULACIÓN DE UN PERIMETRO DE SEGURIDAD LOGICA EMPLEANDO NUEVA GENERACION DE FIREWALLS PARA PREVENIR ATAQUES EXTERNOS E INTERNOS A LA GRANJA DE SERVIDORES DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN UNA RED IP-MPLS"

AUTOR:

Ing. Gordillo López Patricio Leonardo

Trabajo de titulación previo a la obtención del grado de

Magister en Telecomunicaciones

TUTOR:

Ing. Romero Paz Manuel de Jesús, MSc.

Guayaquil, a los 29 días del mes Noviembre año 2016

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por Gordillo López Patricio Leonardo como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

_____

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA

_____

MSc. Manuel Romero Paz

Guayaquil, a los 29 días del mes Noviembre año 2016

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, GORDILLO LÓPEZ PATRICIO LEONARDO

DECLARÓ QUE:

El trabajo de Titulación "**Simulación de un perímetro de seguridad lógica empleando nueva generación de firewalls para prevenir ataques externos e internos a la granja de servidores de un proveedor de servicios de internet en una red IP-MPLS**", previa a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 29 días del mes Noviembre año 2016

EL AUTOR

_____

Ing. Gordillo López Patricio Leonardo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

YO, GORDILLO LÓPEZ PATRICIO LEONARDO

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación**, en la biblioteca de la institución del Trabajo de Titulación: "**Simulación de un perímetro de seguridad lógica empleando nueva generación de firewalls para prevenir ataques externos e internos a la granja de servidores de un proveedor de servicios de internet en una red IP-MPLS**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

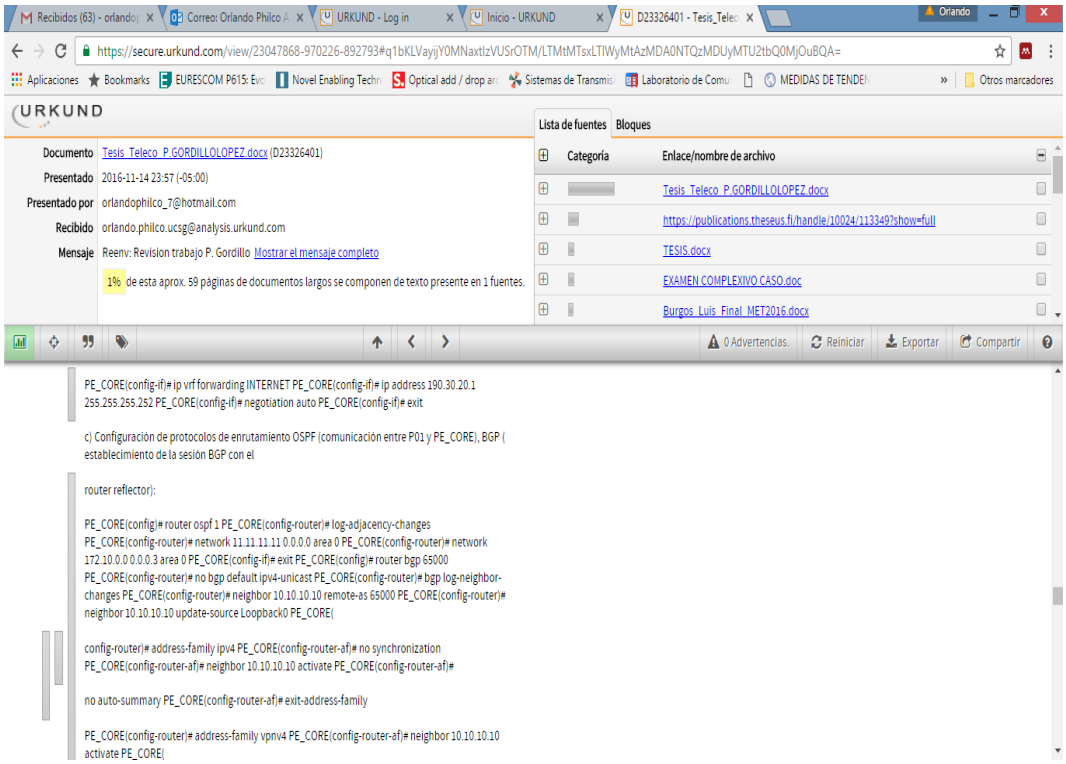
Guayaquil, a los 29 días del mes Noviembre año 2016

EL AUTOR

_____

Ing. Gordillo López Patricio Leonardo

REPORTE URKUND



Reporte Urkund Tesis "Simulación de un perímetro de seguridad lógica empleando nueva generación de firewalls para prevenir ataques externos e internos a la granja de servidores de un proveedor de servicios de internet en una red IP-MPLS" del Ing. Gordillo López Patricio Leonardo.

El resultado es 1% de coincidencias.

Atentamente.

Msc Orlando Philco A.

Dedicatoria

Este trabajo de titulación está dedicado a mis queridos abuelos: Manuel, Delfina, Julio, Rosa, José y Juana, quienes sembraron en mis padres y en mí el gran amor a Dios, al trabajo y a los estudios, gracias a ellos puedo escribir grandes historias que perduren toda una vida…

A mi dulce y amada esposa Verónica y a mi tierno hijo Santiago, quienes con su gran amor y sus oraciones fueron los primeros en ayudarme en mi conversión a la Iglesia Católica…

Agradecimientos

A Cristo rey quien es nuestro hermano mayor, y a mi santa madre la Virgen María llamada para siempre la bienaventura…

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

MSc. Manuel Romero Paz
TUTOR

f. _____

MSc. Manuel Romero Paz
DIRECTOR DEL PROGRAMA

f. _____

MSc. Orlando Philco Asqui
REVISOR

f. _____

MSc. Luis Córdova Rivadeneira
REVISOR

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo 2: Fundamentación Teórica

Capítulo 3: Diseño del perímetro de seguridad lógica empleando nueva generación de firewalls en una red IP-MPLS

Capítulo 4: Simulación y resultados de ataques externos e internos a la granja de servidores de un ISP en la red IP-MPLS empleando el software GNS3

ÍNDICE DE TABLAS

Capítulo 2: Fundamentación Teórica

Capítulo 3: Diseño del perímetro de seguridad lógica empleando nueva generación de firewalls en una red IP-MPLS

Resumen

En el presente trabajo de titulación, se exponen los fundamentos teóricos de la red MPLS, la cual, es considerada como una red de transporte para clientes de un ISP; también se analiza las condiciones necesarias para el respectivo control y acceso hacia los servidores del proveedor de internet mediante la implementación de un firewall de última generación, además, se detallan los diferentes tipos de ataques realizados por los hackers, como el de denegación de servicio DDoS, TCP flood, UDP flood y reconocimiento de puertos, que generan tráfico ilegitimo en la red de datos; finalmente se realiza una simulación de diferentes ataques informáticos ocasionados por cibercriminales localizados en cualquier parte de la red, pretendiendo dejar fuera de servicio los servidores de comunicación localizados detrás del firewall del ISP, sin embargo, el gateway instalado en el core de la red impedirá este tipo de accesos no legítimos, asegurando la operatividad de la red para todos sus clientes.

Palabras Claves: IP-MPLS, Firewall, Seguridad Informática, Hacker

Abstract

In the present work, theoretical foundations of MPLS network are explained, which is considered as a transport network for ISP's customers; besides, the necessary conditions for the respective control and access to Internet provider's servers, by implementing a next-generation firewall, are also analyzed, also, the different types of attacks made by hackers, such as denial of service DDoS, TCP flood, UDP flood and port recognition, which generate illegitimate traffic in the data network; finally a simulation of different computer attacks, caused by cybercriminals located anywhere on the network, is carried out, pretending to leave out of service to the communication servers located behind the firewall of the ISP, however, the gateway installed in the core network will prevent this type of not legitimate access, ensuring the operation of the network to all its customers.

Key words: IP-MPLS, Firewall, Information security, Hacker

Capítulo 1: Descripción del proyecto de intervención.

En el presente capítulo se menciona la justificación del problema a investigar, antecedentes, definición del problema, los objetivos generales y específicos, hipótesis y tipo de metodología de investigación.

1.1. Justificación del problema a investigar.

Gracias al crecimiento exponencial de internet, las comunicaciones se pueden realizar en cuestión de segundos, beneficiando a la población mundial en varios aspectos de su vida cotidiana, sin embargo, existe una desventaja primordial que es el intercambio de información confidencial en redes IP (Internet Protocol) inseguras y de poca fiabilidad.

En este tipo de redes, hackers están atentos a las vulnerabilidades que existen en las redes de datos, provocando pérdidas millonarias no solo a empresas privadas y/o públicas, sino también al público en general que navega en internet accediendo a cuentas bancarias, redes sociales, correos electrónicos, servidores web, compras online, etc.

Los atacantes informáticos tienen como objetivo principal buscar agujeros de seguridad en la red de los proveedores de servicios de internet, que por lo general, tienen una plataforma IP-MPLS (Internet Protocol Multiprotocol Label Switching) para todo el core de la red de datos. Debido a la vulnerabilidad lógica que presenta la granja de servidores de un proveedor de internet, es necesario brindar una solución factible y viable en seguridad informática, siendo el firewall el equipo ideal que brindaría una seguridad perimetral a todos los servidores que posee la empresa.

Con la simulación propuesta se disminuirían los riesgos ante las elevadas tasas de ataques externos e internos a los ISPs (Internet Service Provider), provocando el colapso por varias horas del servicio de datos ofrecido por las compañías que se dedican a este tipo de negocios.

Es necesario simular la red IP-MPLS del ISP, debido a que las estadísticas de empresas de seguridad informática a nivel mundial muestran ataques internos dentro de una organización en particular, violando la seguridad de la información. El diseño de una red que brinde un perímetro de seguridad empleando firewalls de última generación es de gran relevancia tecnológica para los proveedores de internet, ya que ayudaría a los administradores de la red a limitar el acceso de clientes internos y externos a la red IP-MPLS que posea el ISP y a contrarrestar todo tipo de ataque informático por parte de hackers que se pueden encontrar en cualquier parte del mundo.

1.2. Antecedentes.

Varias empresas dedicadas a la seguridad informática presentan sus reportes semestrales y/o anuales resaltando las vulnerabilidades más comunes en la nube de internet como son malware (código dañino), phishing (suplantación de identidad), spam (correos no deseados); estas empresas utilizan sistemas inteligentes basados en software y hardware monitoreando permanentemente el desempeño de las redes de datos de ciertas industrias y organizaciones, demostrando así, que la ciber delincuencia está a la orden del día.

Investigaciones realizadas por una de las mejores empresas Israelitas de seguridad informática a nivel mundial indican por ejemplo que cada minuto un computador accede a un website malicioso, cada 27 minutos malwares desconocidos son descargados involuntariamente de internet, y cada 24 horas un host es infectado por un bot (virus troyanos que permiten el control del computador por el atacante).

Según estudios recientes los ataques dirigidos a grandes corporaciones mediante spear-phishing (ataques dirigidos a compañías para robar información confidencial mediante correos electrónicos falsos) se han incrementado considerablemente, provocando así el robo de diferentes propiedades intelectuales, secretos comerciales y datos financieros de gran relevancia para las empresas (Check Point Company, 2015).

Las redes IP MPLS se consideran escalables, seguras y de alta confiabilidad, sin embargo, se ha demostrado que el ciber espionaje vulnera estas seguridades y ataca a los servidores de los proveedores de internet, ya que estas empresas tienen una plataforma MPLS (Multiprotocol Label Switching) en su core.

Algunas de estas compañías han invertido miles de dólares en equipos de seguridad informática como firewalls de última generación con su respectiva redundancia e IPS (Intrusion Prevention System) para defenderse de ataques, evitando así las filtraciones de datos y la pérdida de servicios que afectarían directamente a todos sus clientes internos y externos de la red.

1.3. Definición del problema

Existen amenazas de agentes internos o externos a la red IP-MPLS del ISP que afectan el correcto desempeño de la granja de servidores del proveedor de servicios de internet, ataques lógicos como DDoS (Distributed Denial of Service), flood ICMP (flood Internet Control Message Protocol), flood UDP (flood User Datagram Protocol), flood SYN TCP (flood sync Transmission Control Protocol) hacia los servidores del ISP, provocan pérdida de comunicación hacia los clientes del proveedor.

La ausencia de un perímetro de seguridad pone en riesgo la confidencialidad de la información que es enviada desde/hacia los sistemas o servidores de la compañía, descalificando así, el prestigio, integridad y confidencialidad del ISP.

La vulnerabilidad presente en dicha granja provoca la modificación a direccionamientos IP’s, infiltración en la infraestructura lógica de la empresa y caída de enlaces, perjudicando de manera significativa los servicios ofrecidos por el proveedor de internet.

1.4. Objetivos

A continuación se detalla el objetivo general y los objetivos específicos:

1.4.1. Objetivo General:

Simular un perímetro de seguridad lógica empleando nueva generación de firewalls para prevenir ataques externos e internos a la granja de servidores de un proveedor de servicios de internet en una red IP MPLS.

1.4.2. Objetivos específicos:

- ✓ Describir los fundamentos teóricos de las redes IP MPLS mencionando sus características y ventajas, así como su implicación en ambientes de seguridad perimetral en redes de datos.
- ✓ Analizar la configuración adecuada de los routers, switches y máquinas virtuales para la correcta comunicación a nivel de capa de red de varios clientes en la nube IP-MPLS.
- ✓ Diseñar la implementación de un firewall virtual para la seguridad logica de una granja de servidores de un proveedor de servicios de internet en una red IP MPLS.
- ✓ Establecer políticas de seguridad lógica en el firewall de acuerdo a las diferentes vulnerabilidades que se encuentran actualmente en la red IP-MPLS del proveedor de internet.
- ✓ Comprobar, mediante una simulación, la correcta funcionalidad del diseño del perímetro de seguridad lógica a nivel de firewall’s para la granja de servidores de un proveedor de servicios de internet en una red IP MPLS.

1.5. Hipótesis

La simulación de un perímetro de seguridad lógica para la granja de servidores de un proveedor de servicios de internet en una red IP MPLS debería estar basado en la integración de un firewall administrable en el core de la red y solucionaría el problema de la vulnerabilidad de ataques cibernéticos que presenta la granja de servidores de un ISP.

1.6. Metodología de investigación.

Esta investigación es descriptiva porque pretende utilizar la información obtenida en el desarrollo del Estado del Arte, para analizar, diseñar y evaluar la simulación de un perímetro de seguridad lógica para la granja de servidores de un proveedor de servicios de internet en una red IP MPLS.

Además, esta investigación es del paradigma **"EMPÍRICO-ANALÍTICO"** con un enfoque **"CUANTITATIVO"** porque se utilizan cálculos matemáticos y estadísticas para presentar los indicadores que permitan caracterizar esta investigación.

Para el desarrollo de este trabajo de investigación se empleará una metodología de tipo experimental, porque se va a comprobar los cambios que surgen al modificar la variable independiente (origen de ataques provocados por hackers en la red IP MPLS), midiendo estos efectos sobre la variable dependiente (consecuencias de ataques cibernéticos en la granja de servidores de un proveedor de internet); en el trabajo se introducirán determinadas manipulaciones mediante diferentes tipos de ataques provocados por ciber delincuentes, evaluando así, la robustez, confiabilidad y seguridad que ofrece un equipo de seguridad informática (firewalls) para la granja de servidores de un proveedor de internet; todos estos experimentos se realizarán en simuladores y software de máquinas virtuales para recrear ambientes inseguros en redes MPLS.

En el siguiente capítulo se examinará conceptos de redes IP-MPLS y se detallarán los parámetros teóricos necesarios para poseer una defensa lógica perimetral en los servidores de un proveedor de servicios de internet.

Capítulo 2: Fundamentación Teórica

En este capítulo se estudiará el modelo TCP/IP, los diferentes protocolos de enrutamiento de redes de datos, los componentes y operación de la red MPLS, y la seguridad informática bajo la arquitectura de la marca CheckPoint.

2.1. Introducción al modelo TCP/IP

La comunicación entre computadores se realiza gracias a un modelo esquemático que permite la conexión de extremo a extremo, a este modelo se denomina TCP/IP (Transmission Control Protocol / Internet Protocol) el cual fue desarrollado por el Departamento de Defensa de los EEUU en la década de 1970; gracias a este modelo, los equipos pueden comunicarse en la red enviando información encapsulada como direcciones origen, direcciones destino, y puertos de comunicación.

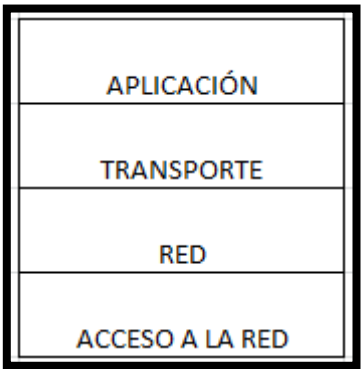


Figura 2. 1: Capas del modelo TCP/IP
Elaborada por: El Autor.

En la figura 2.1 se puede observar las diferentes capas del modelo TCP/IP, cada una con una función en particular que se detalla a continuación:

Capa de aplicación: En la cual existe un control de dialogo entre el usuario final y el protocolo a emplear en determinada comunicación.

Capa de transporte: Se encarga del transporte seguro de extremo a extremo, emplea una conexión lógica entre emisor y receptor para asegurarse de que el

paquete llegue a su destino, empleando diferentes métodos como tamaño de ventana, acuse de recibo, windowing; así mismo en esta capa de transporte existe el protocolo UDP (User Datagram Protocol) que, a diferencia de TCP, no es orientado a conexión, ya que no ofrece confiabilidad en el momento de la transferencia de la información, carece de windowing, ack (acknowledgement), tamaño de ventana.

Capa de red: Es la responsable de enrutar el paquete y escoger la mejor de las rutas para enviar el datagrama (paquetes de datos) al destino determinado, en esta capa es posible incluir el protocolo IP el cual se considera un protocolo no orientado a conexión debido a que no garantiza la integridad del paquete, tampoco posee mecanismos de ack para asegurarse de que el paquete ha llegado a su destino.

Capa de acceso a la red: Se ocupa del acceso al medio de transmisión, es decir, de los dispositivos físicos que interactúan para acceder a la red; en esta capa las tramas de datos se convierten a bits de información, asignando direcciones IP a las direcciones físicas, definiendo la conexión a los entornos físicos de la red.

El modelo TCP/IP se asemeja al modelo OSI (Open System Interconnection) de red, donde existen 7 capas como se detalla en la tabla 2.1, en la cual se observa la funcionabilidad de cada capa, sus servicios y el tipo de encapsulación que se ejecuta en cada una de ellas.

El modelo OSI es de gran importancia porque es un estándar a nivel mundial ya que facilita la normalización de los componentes de red y la compatibilidad de tecnologías diseñadas por empresas de todo el planeta.

2.1.1. Direcciones IP

Las comunicaciones entre host se realizan gracias al direccionamiento IP del modelo TCP/IP, se establecen sesiones y el intercambio de información se realiza mediante datos que son encapsulados con sus respectivos campos.

Tabla 2. 1: Capas del modelo OSI

CAPA	ENCAPSULACION	FUNCION	SERVICIOS	EQUIPO
7.- APLICACIÓN	DATOS	Establece disponibilidad de recursos.	FTP, SMTP, Telnet, POP3	
6.- PRESENTACION	DATOS	Comprime, encripta y desencripta datos.	JPEG, GIF, MPEG	
5.- SESION	DATOS	Estable, mantiene y termina las sesiones.	SQL, NFS	
4.- TRANSPORTE	SEGMENTOS	Establece conexión de extremo a extremo, usa circuitos virtuales.	TCP, UDP	
3.- RED	PAQUETES	Determina la mejor ruta para enviar el paquete	RIP, IP, IPX	Router
2.- ENLACE DE DATOS	TRAMAS	Transporta datos en una conexión física, detecta errores.	Frame Relay, PPP, HDLC	Switch / Bridge
1.- FISICA	BITS	Coloca datos en el cable.		Hub / Repeater

Elaborada por: El Autor.

Una dirección IP versión 4 se representa con 4 bytes (conjunto de 32 bits), posee 4 grupos de números decimales, cada grupo se representa en 8 dígitos binarios, son asignadas a host, y sirven para identificarse dentro de la red (Dordoigne, 2011).

Existe el direccionamiento IP público y privado; las direcciones IP públicas son únicas en el mundo, y se obtienen a través de un proveedor de internet, que a su vez, estas compañías solicitan a entes internacionales como LACNIC (responsable del direccionamiento IP público para Latinoamérica y el Caribe) un bloque de direcciones IP según la disponibilidad y estudios técnicos; mientras que las direcciones IP privadas son de uso interno en la red y pueden coexistir en el mismo bloque de direcciones en diferentes proveedores de internet. Las direcciones IPs privadas están separadas en clases como se detalla en la tabla 2.2,

mientras que las direcciones IPs públicas son el complemento de este rango de direccionamiento.

Tabla 2. 2: Clases de direcciones IPs privadas

Clase	Rango de Direcciones
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Elaborada por: El Autor.

Para optimizar un determinado segmento de red se usan técnicas matemáticas como subnetting o VLSM (Variable Length Subnet Mask) que evitaría el consumo innecesario de direcciones IPs, obteniendo así el direccionamiento justo y necesario para una determinada cantidad de tarjetas de red, interfaces físicas e interfaces lógicas que se emplearían en una red IP en particular.

2.2. Dispositivos de comunicación.

Existen varios dispositivos de red que permiten una rápida comunicación de datos teniendo como marco de referencia el modelo OSI, estos equipos almacenan en su configuración tablas de enrutamiento, direccionamiento IP, tablas de mac address, configuración de autenticación y seguridad de acceso, etc, que permiten la rápida conmutación del paquete a su destino determinado. Entre los equipos más relevantes para el desarrollo de una red IP se encuentran los routers y switches, los cuales se detallan a continuación:

2.2.1. Routers

Es un dispositivo que funciona en la capa de red del modelo OSI, y se utiliza para comunicar diferentes tipos de redes bajo ciertos protocolos de enrutamiento configurados en el equipo, además, el router separa dominios de broadcast (área lógica de host que puede enviar información entre si ya que están en la misma

subred), la figura 2.2 muestra un icono estándar para representar a un router en los diagramas de red.

Figura 2. 2: Router
Elaborada por: El Autor.

2.2.2. Switches

Es un equipo de red que trabaja en la capa de enlace de datos del modelo OSI, y sirve para conectar varios segmentos de red en base a la dirección MAC (Media Access Control) de destino, ya que el switch almacena tablas de MAC Address.

Si un host en particular desea enviar los datos a otro host, el switch verifica que la dirección MAC del equipo destino se encuentre en su tabla de Mac Address, si es asi, entonces el switch conmuta el paquete de datos, caso contrario inunda todos los puertos (menos al puerto que los recibió) para verificar donde está el host destino. La figura 2.3 muestra un icono del switch utilizado en la mayoría de diagramas de red.

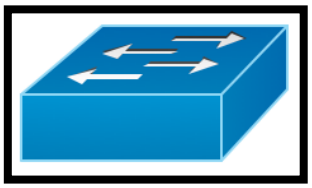


Figura 2. 3: Switch
Elaborada por: El Autor.

2.3. Protocolos de enrutamiento

Las comunicaciones entre diferentes segmentos de red se realizan gracias a los protocolos de enrutamiento, los cuales están divididos en protocolos vector distancia y protocolos de estado de enlace.

2.3.1. Protocolo vector distancia

Ocupan mayor ancho de banda debido a que las actualizaciones en su tabla de enrutamiento se realizan a cada instante, son más fáciles de configurar, convergen lentamente y envían las actualizaciones a manera de broadcast; entre los protocolos más comunes de este tipo se tiene RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol) patentado por la compañía americana Cisco.

2.3.2. Protocolos de estado de enlace

Convergen rápidamente ya que poseen una visión común de toda la topología de la red, utilizan menor ancho de banda para sus actualizaciones y envían paquetes hello a todos sus vecinos cuando detectan cambios en la red, también requieren mayor procesamiento en los routeadores; los protocolos OSPF (Open Shortest Path First) y EIGRP (Enhanced Interior Gateway Routing Protocol) son claros ejemplos de protocolos de estado de enlace.

2.4. Plataformas IP / MPLS

El enrutamiento tradicional en redes de datos se fundamenta en decisiones que hace el router para enviar el paquete de datos a su destino, este equipo envía el paquete al siguiente salto consultando siempre su tabla de enrutamiento, configurados con protocolos estáticos o dinámicos. Este enrutamiento típico en los routers posee ciertas desventajas como la escalabilidad y la flexibilidad en las redes de datos.

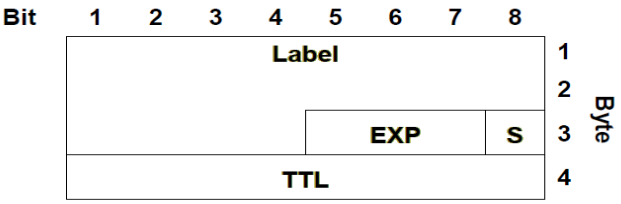
Con el desarrollo de MPLS se lograron grandes ventajas en las redes IP, debido a que es una tecnología de gran alcance, reduce costos y soporta varios tipos de aplicaciones como voz, video y datos integrándola en una red de fácil administración. (Moran Rivera, 2015) menciona las principales ventajas de las redes IP MPLS, las cuales se indican a continuación:

a) Virtual Private Networks (VPN's).- Este tipo de redes se caracteriza por compartir el mismo segmento de red dentro de la nube MPLS gracias al etiquetamiento entre la capa de enlace de datos y de red del modelo OSI, son redes seguras y equivalentes a una red LAN (Local Area Network) privada.
b) Quality of Service (QoS).- Se puede garantizar el ancho de banda a un determinado tipo de tráfico gracias a la calidad de servicio, tomando en cuenta siempre las prioridades que posea determinada empresa al momento de transmitir información de alta relevancia dentro de su red de datos.
c) Ingeniería de tráfico.- Es posible optimizar la utilización del ancho de banda en caminos subutilizados y concentra el tráfico en determinadas partes de la red.
d) Escalabilidad.- Asocia un gran número de redes IP a un número reducido de etiquetas, gracias a la tecnología MPLS las redes IP privadas se pueden reutilizar entre los clientes del ISP, debido a que la comunicación se realiza a través de etiquetas diferentes.

2.4.1. Arquitectura MPLS

Básicamente MPLS en una tecnología que trabaja entre la capa 2 y 3 del modelo OSI donde la transmisión de paquetes se realiza mediante etiquetas, éstas se asignan cuando el paquete ingresa a la red MPLS y son insertadas entre la capa de enlace de datos y la de red; en el enrutamiento tradicional se utilizan direcciones IPs, mientras que en el enrutamiento en MPLS se agregan etiquetas a las direcciones IPs.

La cabecera de la etiqueta MPLS: Consta de 32 bits, las cuales están divididas en 20 bits para la etiqueta (representada entre los valores de 0 y 1048575), 3 bits para identificar la clase de servicio en el campo EXP, 1 bit de Pila (Stack) para agrupar etiquetas de forma jerárquica en el campo S, y 8 bits que representan el tiempo de vida del paquete, la figura 2.4 muestra un detalle de los bits distribuidos en la etiqueta MPLS.



Label	Valor de la etiquete (20 bits)
EXP	Clase de servicio (3 bits)
S	Boton de pila (1 bit)
TTL	Tiempo de vida del paquete

Figura 2. 4: Cabecera de la etiqueta MPLS
Elaborada por: El Autor.

A manera de ejemplo y utilizando una herramienta de captura de paquetes, en la figura 2.5 se observa la conectividad exitosa desde el host 192.168.1.1 al equipo 192.168.4.1 dentro de la nube MPLS empleando el protocolo ICMP (Internet Control Message Protocol), se puede notar los valores de la cabecera de la etiqueta (MPLS label: 19, MPLS EXP: 0, MPLS STACK:1, MPLS TTL:254)

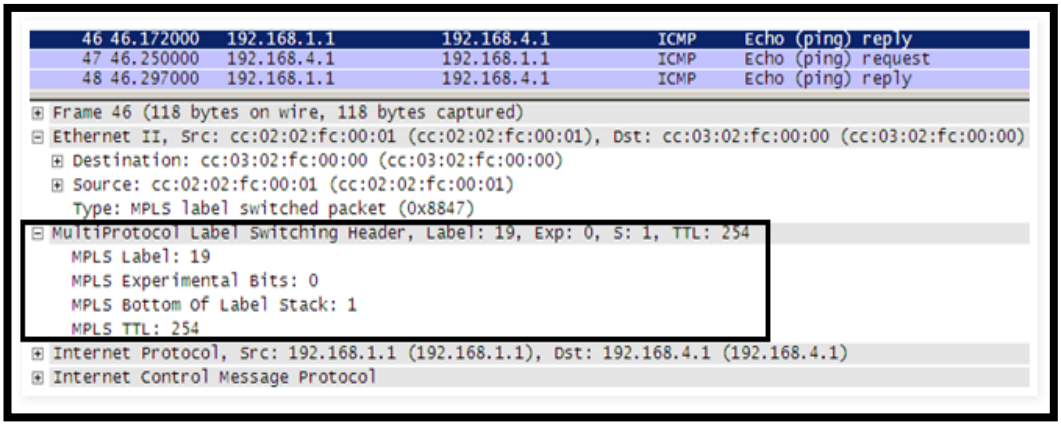


Figura 2. 5: Captura de paquetes en una red MPLS
Fuente: (Go-Mpls, 2009)

Componentes en una red MPLS: Existen varios elementos dentro de una nube MPLS que están involucrados en la transmisión y recepción de paquetes IP, entre los cuales se tiene:

a) Label Switch Router (LSR), estos routers reciben un paquete etiquetado y lo conmutan al destino determinado con una etiqueta de otro valor.

b) Edge Label Switch Router (ELSR), en este tipo de routers los paquetes son etiquetados al ingresar a la red MPLS, también se encargan de remover las etiquetas del paquete al salir de dicha red.
c) Label Switched Path (LSP), se define como todo el trayecto que toma el paquete a través de los routers LSR en una nube MPLS con un nivel jerárquico determinado y son unidireccionales, este encaminamiento se realiza por medio de los diferentes enrutamientos dinámicos configurados en el equipo.
d) Forwading Equivalence Class (FEC), es un conjunto de paquetes IP que son enviados por el mismo LSP y solicitan un servicio en común como VPN, QoS, ingeniería de tráfico.

Operación de la red MPLS: Existen varios procesos para el etiquetamiento del paquete IP en la red MPLS, entre los cuales se tienen las siguientes operaciones:

- **PUSH**: en este proceso se le asigna una etiqueta al paquete IP cuando ingresa a la red MPLS
- **SWAP:** aquí la etiqueta es mapeada y reemplazada por otro valor en la pila superior
- **POP**: se define a la operación realizada para remover la etiqueta y entregar el paquete IP fuera de la red MPLS

En la figura 2.6 se observa como un paquete IP ingresa a la red MPLS por medio de los diferentes elementos de la misma; el router A desea comunicarse con el router B, estos routers se conocen como CE (Costumer Edge) y son los equipos de propiedad de los diferentes clientes instalados en la red, en este tramo la comunicación es a nivel de IP y no existe el etiquetamiento respectivo, el rectángulo de color amarillo representa el paquete que se origina en los routers CE e ingresan a su próximo salto que es el router ELSR conocido como routers PE (Provider Edge), en este sector empieza el proceso de etiquetamiento MPLS, el router ELSR-2 se encarga de agregar al paquete IP las 2 etiquetas respectivas empleando la operación PUSH, una etiqueta se asigna para buscar el router ELSR destino mediante algún tipo de protocolo IGP (Interior Gateway Protocol) y la

otra etiqueta se utiliza para direccionar el paquete al router CE destino (representadas de color verde y rojo respectivamente).

Este conjunto de bits previamente etiquetados ingresan al router LSR-1 conocido como router P (Provider) donde se reemplaza las etiquetas recibidas por otras de diferente valor, este proceso se conoce como SWAP; estos paquetes se dirigen hacia el router LSR más próximo a su destino (router LSR-2) realizando el proceso POP, es decir remueve las etiquetas para conmutar el paquete al router ELSR más cercano del cliente final, en este caso el router ELSR-4, finalmente este router realiza otra operación POP para eliminar la etiqueta restante y entregar el paquete IP fuera de la red MPLS previamente conociendo su destino mediante los diferentes protocolos de enrutamiento configurados en los equipos.

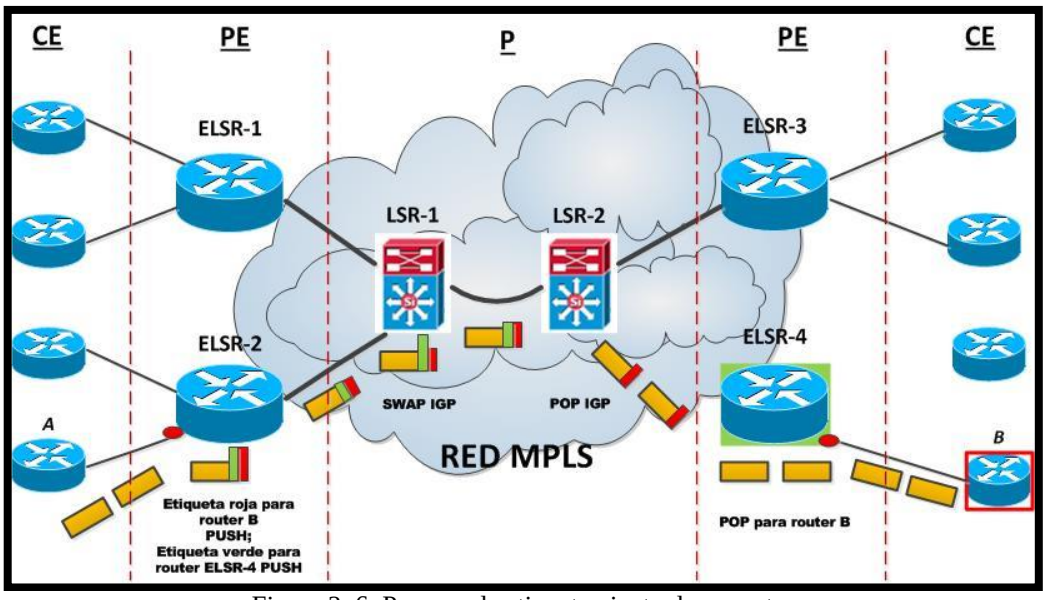


Figura 2. 6: Proceso de etiquetamiento de paquetes
Elaborada por: El Autor.

Label Distribution Protocol (LDP): es un conjunto de métodos que permiten a los routers LSR compartir una etiqueta en particular y asociarla con otro LSR, en estos equipos se mantiene una sesión LDP permitiendo a cada uno de ellos aprender información a nivel de etiquetamiento del otro, convirtiendo a este protocolo en un sistema bidireccional. Al establecerse la sesión LDP se descubren los vecinos LSRs directamente conectados a través de paquetes hello y se envían

paquetes multicast a todos los routers en una subred determinada, una vez que el descubrimiento LDP es realizado, las sesiones son establecidas sobre el puerto TCP 646.

En un enrutamiento tradicional, se usa protocolos dinámicos como OSPF, BGP, IS-IS para aprender prefijos de otros routers, todo esto es almacenado en la RIB (Routing Information Base), que representa la tabla de enrutamiento; la información de RIB es usada para construir la FIB (Forwarding Information Base) y se usa para enviar los paquetes IP a la red, sin embargo para redes MPLS se usa LDP como plano de control, es decir se genera localmente una etiqueta por cada prefijo que se encuentra en RIB, esta información es agregada a FIB, y es usada para construir la LFIB (Label Forwarding Information Base); cuando un router envía un paquete con la etiqueta respectiva en la nube MPLS, el equipo usara la LFIB para tomar la decisión de forwarding.

2.4.2. Protocolos de enrutamiento en MPLS

Para transportar los prefijos de red a través de la nube MPLS, es necesario emplear protocolos de gateway interior y exterior; se establecen los protocolos de enrutamiento OSPF e IS-IS (Intermediate System to Intermediate System) para la comunicación entre los ELSR y LSR, mientras que para el enrutamiento entre los routers CE y ELSR se configuran los protocolos RIP, static, IGRP y BGP (Border Gateway Protocol); para la simulación a realizar en el desarrollo de este trabajo se utilizará los protocolos BGP, MP-BGP (Multi Protocol Border Gateway Protocol), OSPF, static.

BGP: Antes de definir el protocolo BGP se debe tener claro el concepto de AS (Autonomous System), el cual es un conjunto de redes bajo la misma organización técnica, es un numero de 16 bits definido en el RFC (Request for Comments) 1930 (Hawkinson & Bates, 1996) y se clasifican en AS privados y públicos, se representan en números enteros que van del 0 al 65335 y tienen un rango definido, para los privados se utiliza desde 64512 al 65534 y para los públicos se emplea el rango desde el 1 al 64495.

BGP es un protocolo de gateway exterior que se utiliza para el intercambio de rutas entre AS, considerado como el tipo de vector distancia, las actualizaciones en la tabla de enrutamiento se realizan solo cuando hay un cambio en la topología de la red, utiliza el puerto TCP (Transmission Control Protocol) 179, es un protocolo lento en su convergencia, pero de alta escalabilidad y estabilidad, posee una distancia administrativa de 20 para EBGP (External Border Gateway Protocol) o 200 para IBGP (Internal Border Gateway Protocol).

El intercambio de rutas se establece mediante sesiones con los routers vecinos en BGP llamados peers, los estados de las sesiones tienen las siguientes secuencias indicadas a continuación:

a) IDLE (desocupada).- el router inicia la conectividad con el peer.
b) ACTIVE (activa).- el router descubrió la ruta de su vecino, empieza el proceso de 3 vías handshake.
c) OPEN SENT (enviando de forma abierta).- se envía el mensaje OPEN al peer remoto incluyendo parámetros como versión de BGP, router ID, autenticación.
d) OPEN CONFIRM (confirmación de apertura).- el peer responde con un OPEN confirmando los datos recibidos, caso contrario lo manda a ACTIVE.
e) ESTABLISHED (establecida).- se establece completamente la sesión BGP entre los peers, mediante un mensaje keepalive.

En la tabla 2.3 se puede observar los principales atributos que ayudan a definir la mejor opción hacia un destino entre varias rutas posibles que utiliza el protocolo BGP.

Para escoger la mejor de las rutas en el protocolo BGP, se deben tomar en cuenta ciertos parámetros, como por ejemplo: se debe rechazar las rutas con un inaccesible siguiente salto, se prefieren las rutas con un alto valor de peso (atributo Weight) y con un alto local-preference, se escogen las rutas con el AS-PATH (trayecto de sistema autónomo) más corto, se prefiere las rutas del vecino más próximo al equipo, se escoge la ruta de mayor antigüedad, y finalmente el

router puede escoger los prefijos anunciados por el peer vecino con el menor router ID.

Tabla 2. 3: Atributos del protocolo BGP

ATRIBUTO	CATEGORIA	DESCRIPCION
Aggregator	Optional, transitive	ID y AS del router que lleva a cabo la sumarización. No se usa en el proceso de selección de caminos.
As_Path	Well-known, mandatory	Lista de todos los AS a través de los cuales ha pasado, se prefiere el más corto.
Atomic aggregate	Well-known, discretionary	Al generar una sumarización envía los AS de las rutas que componen dicha sumarizacion.
Community	Optional, transitive	Etiqueta prefijos, no se usa en el proceso de selección de caminos.
Local preference	Well-Know, discretionary	Indica el nivel de preferencia para alcanzar prefijos externos a través de los routers internos, se prefiere el valor más alto.
Weight	Optional, not communicated to peers	Propietario de Cisco, se prefiere el más alto.

Fuente: (Ariganello & Barrientos, Redes Cisco, guia de estudio para la certificacion CCNP, 2010)

MP-BGP es un protocolo extendido de BGP que permite transportar información de prefijos de red, VPNv4, IPv6; se utiliza para la distribución de las rutas en las VPN y el etiquetamiento del paquete en la red MPLS. MP-BGP solo se configuran en los routers PE, los cuales asignan las rutas aprendidas a otros routers PE de la red, en los routers P no existe configuración de MP-BGP ya que no tienen conocimiento alguno de enrutamiento en VPN.

La salida de comandos que ayudaría a resolver problemas a nivel del protocolo BGP en routeadores Cisco es la siguiente:

a) show ip bgp vpnv4 all summary: muestra el estado de la sesión BGP con todos los routers vecinos
b) show ip bgp vpnv4 all neighbors *ip router vecino* advertised-routes: indica las redes que se están publicando a un router vecino
c) show ip bgp vpnv4 all neighbors *ip router vecino* routes: indica las redes que se están aprendiendo de un router vecino
d) clear ip bgp *ip router vecino* soft in: realiza una actualización sencilla de las rutas enviadas por el router vecino
e) clear ip bgp *ip router vecino* soft out: realiza una actualización sencilla de las rutas anunciadas al router vecino

OSPF: es un protocolo de enrutamiento de estado de enlace donde se divide lógicamente la red en áreas pequeñas, agrupando los routers que ejecutan un mismo proceso ya que poseen una base de datos en común provocando el mejoramiento de la red, menor uso del procesamiento de equipos, y una mayor convergencia de datos; el área backbone se conoce como el área 0, todas las áreas están conectadas a esa área, el router ABR (Router Border Area) conecta el área regular con el área 0, de existir un cambio en el área regular, el router ABR detecta el cambio y le informa al área 0.

En OSPF la tabla de enrutamiento se actualiza únicamente si existe un cambio en la topología de la red utilizando paquetes hello para alcanzar a sus vecinos, posee una visión común de toda la red, en comparación con otros protocolos de enrutamiento IGP, OSPF es muy rápido en su convergencia ya que emplean el algoritmo SPF (Short Path First) encontrando la mejor de las rutas.

El protocolo OSPF es un protocolo open source (de código abierto) y utiliza un algoritmo denominado el algoritmo de Dijkstra que descubre el camino más corto a un nodo determinado, el router al conectarse a la red crea adyacencias con sus vecinos enviando paquetes hello en cada interface que contienen: el ID (identificador) del router, tiempo del paquete, mascara de red, prioridad del router, password en el caso de que haya autenticación; el router remoto recibe el paquete hello, enviando la respuesta del paquete, aquí se determina la relación maestro –

esclavo indicada por su prioridad, los dos envían su DBD (Database Description), finalmente la vecindad es sincronizada (estado full state) gracias a la ejecución del algortimo de Dijkstra para encontrar la mejor de las rutas, provocando una convergencia muy rápida en la red MPLS, caso contrario la sesión se convertiría en estado down causando la perdida de conectividad con el vecino OSPF. Existen varios tipos de topologías en OSPF conocidas como:

a) NBMA (Non-Broadcast Multiaccess Network).- La configuración en los equipos es manual deben de estar en la misma subred.
b) BMA (Broadcast Multiaccess).- Los routers vecinos se configuran automáticamente, no se aplica la configuración manual.
c) Point to Point (Punto a Punto).- Los routers vecinos se descubren dinámicamente, el tiempo del paquete hello es de 10 sg.

La distancia administrativa de un protocolo se representa con un valor decimal, e indica cuan fiable es un protocolo de enrutamiento entre los otros protocolos configurados en la red, la distancia administrativa de OSPF es 110; la métrica de un protocolo es una cantidad que indica la mejor de las rutas que puede tomar un paquete en la red, en OSPF la métrica se calcula en base al costo y es igual a 10^8/ancho de banda, donde el ancho de banda se expresa en bps; la métrica se utiliza con frecuencia para enlaces redundantes, es decir, el paquete de datos va a preferir la ruta con en menor costo posible, teniendo como enlace de respaldo la ruta que posea el costo más alto.

Se puede utilizar el protocolo OSPF para el enrutamiento entre el enlace PE – CE en la red MPLS; para propagar las rutas de los clientes de PE al PE, OSPF se redistribuye en IBGP y viceversa en los routers PE, el lado negativo de esto es que todas las rutas OSPF se convierten en rutas externas en el PE cuando las rutas se redistribuyen de nuevo en OSPF (De Ghein, 2007). La figura 2.7 muestra la conectividad de los clientes finales en OSPF en una red MPLS.

Enrutamiento Estático: Una ruta estática posee una distancia administrativa con el valor de 1 convirtiéndola en una ruta de alta confiabilidad frente a otros

protocolos de enrutamiento, ya que posee un menor valor con respecto a los protocolos IGP y EGP (External Gateway Protocol), es usado con mayor frecuencia para establecer el enrutamiento entre el router PE de la red MPLS y el router CE del cliente. La configuración de este protocolo es manual en el equipo y guarda el formato indicado en la figura 2.8

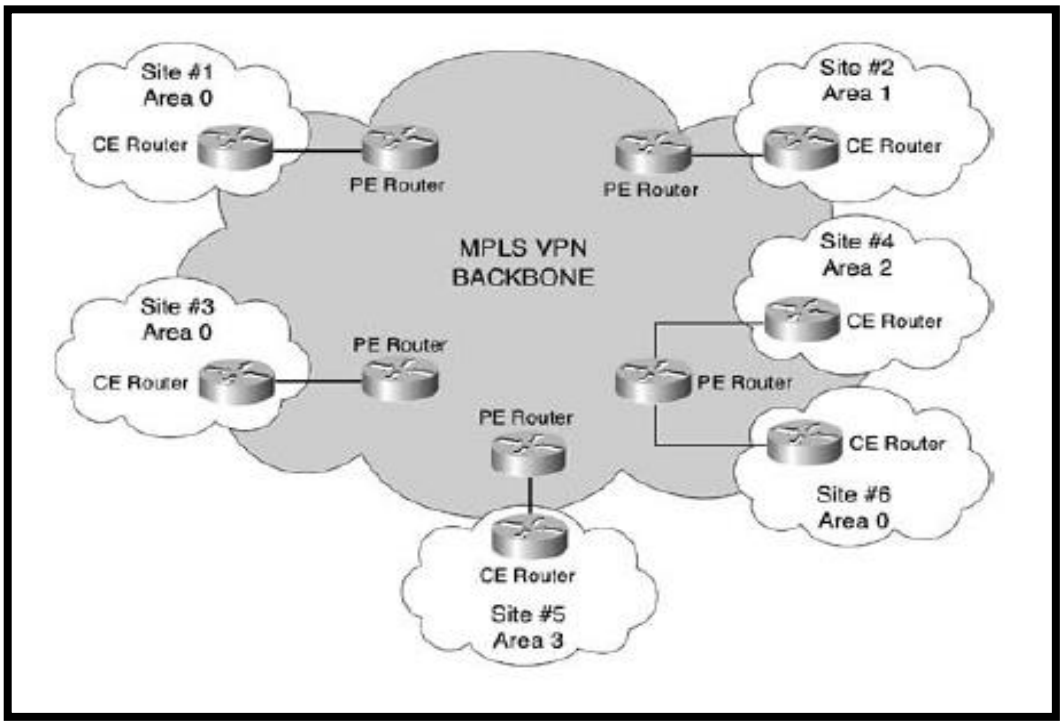


Figura 2. 7: Rutas OSPF a través de la red MPLS
Fuente: (Guichard, Pepelhjak, & Apcar, 2003)

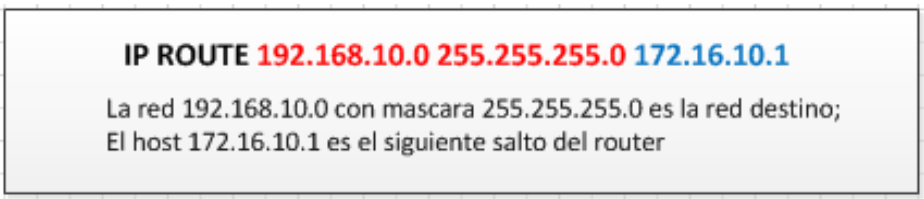


Figura 2. 8: Configuración de una ruta estática
Elaborada por: El Autor.

2.4.3. Configuración de MPLS en los routers de la red

Para proceder a habilitar MPLS se debe considerar ciertos comandos que corren en la mayoría de sistemas operativos de los routers y switches de una red de datos. Para la simulación propuesta se configurará routers Cisco para implementar la red

MPLS; los comandos básicos de configuración, resolución de problemas y monitoreo de eventos se detallan en la tabla 2.4

Tabla 2. 4: Comandos básicos en routers Cisco para MPLS

SALIDA DE COMANDO	DESCRIPCION FUNCIONAL
mpls ip (configuración global)	Habilitación global de MPLS en el router
mpls ip (configuración de la interfaz)	Habilitación de MPLS en la interfaz del router
ip cef	Habilitación de CEF (Cisco Express Forwarding, la forma rápida de ejecutar la conmutación del paquete en capa 3 en una interfaz determinada)
mpls label protocol ldp	Se habilita por defecto MPLS en todas las interfaces del equipo
show mpls interface detail	Verifica en el router las interfaces que estén configuradas MPLS y el protocolo LDP
show mpls ldp neighbor	Muestra la IP de los routers vecinos que están siendo aprendidas por el protocolo MPLS
show mpls ldp bindings	Muestra las etiquetas asignadas a los routers vecinos MPLS
shw mpls ldp discovery	Verifica si la interfaz asignada para MPLS está activa y enviando paquetes hello
show cef interface	Verifica si está habilitada CEF en la interfaz
show mpls ldp parameters	Muestra la información de los paquetes hello LDP
show mpls forwarding-table	Se observan las tablas de las etiquetas
show mpls label range	Muestra el rango de etiquetas locales disponibles en el equipo
debug mpls packets	Muestra información de paquetes etiquetados por el router
debug mpls events	Muestra información relevante acerca de diferentes eventos que ocurren en el momento de la transmisión MPLS

Elaborada por: El Autor.

2.4.4. Aplicaciones en el dominio MPLS

Existen varias aplicaciones que se pueden ejecutar gracias a la tecnología MPLS, el presente trabajo se concentrará en las configuraciones de VPN's en capa 3, ya que también existe configuraciones de VPN's de capa 2 del modelo OSI.

Los clientes demandan altos niveles de seguridad en la red, además de una rápida convergencia de datos, una alternativa ampliamente usada por las carriers y los ISP's es la configuración de VPN's en la red MPLS.

Una vez que el paquete de datos ingresa a la red MPLS se le asignan las etiquetas determinadas en el router PE, el cual almacena una tabla de enrutamiento por cada VPN que se desea transmitir, esta tabla se denomina tabla de enrutamiento de VRF (VPN Routing and Forwarding) y contienen rutas que se repiten en otras VRF's, pero con nombres totalmente distintos; la gran ventaja de tener VRFs es poseer el mismo direccionamiento IP en varios clientes, ya que las tablas de enrutamiento en VRF's son totalmente independientes, esto quiere decir que el cliente A puede tener el mismo segmento de red privado con la misma mascara de red que el cliente B en la red MPLS; el transporte de datos desde el router del cliente CE hasta el router PE se realiza mediante el protocolo MP-BGP.

A continuación las principales características que las VRF's pueden soportar (Salcedo, Pedraza, & Espinosa, 2012):

a) Las direcciones se superponen, lo que permite la reutilización de las direcciones IP en el enrutador PE para diferentes VPNs.
b) Reutilización de los puertos TCP/UDP lo cual permite usar los mismo puertos en diferentes VRFs.
c) El Backbone MPLS puede interactuar en dos planos diferentes de implementación: plano de encaminamiento y plano de control de datos.

En la figura 2.9 se muestra paso a paso las configuraciones correspondientes a una VRF en un router PE; en el paso 1 dentro de la configuración global del router se define un nombre para identificar la VRF del cliente, en este caso se identifica con el nombre CLIENTE_A, luego se configurará los route distinguer o rd, que son identificaciones locales en el router, para el ejemplo se muestra 3:106, donde 3 puede ser el código del router PE configurado y 106 el código del CLIENTE_A, luego se configuran los route-target export e import, en los cuales se declaran las redes que se exportan e importan en la red MPLS; en el paso 2, dentro de la

configuración de BGP 65000, se procederá a crear el address-family del cliente, que se usa para el intercambio de información de enrutamiento con el router vecino en unicast y como el transporte en MPBGP para los prefijos de la red IPv4 en la red MPLS; en el paso 3 se configura la subinterfaz en el router PE con un tipo de encapsulación en dot1q, se le asigna la VRF creada previamente y un direccionamiento IP con máscara de red de 30 bits, de esta manera la primera IP utilizable de este segmento está configurada en el router del cliente y la última IP en el router PE del ISP o carrier.

Es necesaria la configuración de una ruta estática en el router PE para alcanzar la red LAN del cliente, esta ruta estática configurada dentro de la VRF, debe indicar que la red destino del cliente es alcanzada por la dirección IP del siguiente salto, es decir, por la IP que tenga el router CE conectado al router PE de la red MPLS.

Paso # 1: Se creará la vrf en el router PE cercano al cliente

```
Configure terminal
ip vrf CLIENTE_A
 rd 3:106
 route-target export 1:106
 route-target import 1:106
```

Paso # 2: Se creará el address-family para dicha vrf con la configuración básica.

```
router bgp 65000
address-family ipv4 vrf CLIENTE_A
redistribute connected
redistribute static
no synchronization
exit-address-family
```

Paso # 3: Se creará la subinterfaz con el direccionamiento para el cliente.

```
interface GigabitEthernet0/1/0.1066
 description RPV-TMX-ACC-1066
 encapsulation dot1Q 1066
 ip vrf forwarding CLIENTE_A
 ip address 172.31.128.65 255.255.255.252
 no ip directed-broadcast
 no ip proxy-arp
 no cdp enable
end
```

Figura 2. 9: Configuración de VRF en un router PE
Elaborada por: El Autor.

Para realizar un correcto troubleshooting (eliminación y solución de problemas) a nivel de VRF's, se procederá a señalar los diferentes comandos que corren en los sistemas operativos de los routers Cisco:

a) show ip vrf: indica todas las VRF's configuradas en el router

b) show ip route vrf CLIENTE_A : se observa las tablas de enrutamiento de la VRF con el nombre CLIENTE_A
c) show running-config vrf CLIENTE_A : muestra la configuración global de la VRF del CLIENTE_A
d) ping vrf CLIENTE_A *ip router destino*: ayuda a probar la conectividad por el protocolo ICMP a una dirección ip destino determinado en la VRF CLIENTE_A configurada en el equipo.
e) telnet *ip router destino* / vrf CLIENTE_A: comprueba la conectividad en capa 7 del modelo OSI, ingreso remoto a una dirección IP del equipo CPE del cliente en una VRF determinada.

2.5. Seguridad informática.

Se define como seguridad informática a la implementación de políticas virtuales de defensa para una red de datos con el objetivo de mitigar el acceso a la red de sistemas no autorizados que buscan alterar, corromper y destruir información confidencial de usuarios internos y externos quienes en algunas ocasiones desconocen que son víctimas de ataques cibernéticos.

Hoy en día, es de vital importancia poseer ambientes de seguridad perimetral para los servidores de las empresas, ya que estos se convierten en blanco atractivo para los delincuentes informáticos, debido a que pueden modificar su funcionamiento para beneficio propio como por ejemplo: anuncios publicitarios de manera gratuita, captura de información de entidades financieras, e interrupción de servicios online, provocando así pérdidas millonarias a las empresas y el desprestigio a nivel mundial de las mismas. El objetivo de la seguridad informática puede declararse en tres aspectos fundamentales como son: la confidencialidad, integridad y disponibilidad de la información, esto se detalla en la norma ISO 27001.

ISO (International Organization for Standardization) es un organismo internacional que se dedica a desarrollar reglas de normalización en diferentes ámbitos, entre ellos la informática; la serie de normas ISO 27000 se denomina

“Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)” y comprenden un conjunto de normas sobre este tema, la valoración de riesgos y controles. La norma con respecto a seguridad informática es la ISO 27001 y señala que la seguridad de la información es la preservación de su confidencialidad, integridad, y disponibilidad, así como de los sistemas implicados en su tratamiento (García-Cervigón Hurtado & Alegre Ramos, 2011).

Los términos hackers y crackers son empleados con mucha frecuencia en seguridad informática; hacker es una persona que posee altos conocimientos de programación y realiza pruebas de acceso a determinados sistemas informáticos con el objetivo de hallar vulnerabilidades que por lo general son reportados al propietario de este sistema, sin buscar beneficiarse ni corromper el sistema informático auditado, esto es lo que se conoce como el hacking ético; se puede definir como cracker a un individuo que penetra a los sistemas informáticos en línea buscando alterar, corromper y destruir información confidencial con el objetivo de perjudicar económicamente o alterar el desempeño de computadores de victimas a nivel mundial.

Por lo general, los hackers y crackers siguen determinados patrones para desarrollar un ciber ataque: primero indagan información sobre el objetivo a ser atacado, como direcciones IPs de servidores de comunicación, y también las políticas de seguridad implementadas en la red, luego realizan un análisis de sus vulnerabilidades, después hurtan identidades legitimas para ingresar a los sistemas informáticos haciéndose pasar por usuarios legalmente registrados, finalmente realizan la intromisión al sistema reportando las falencias halladas (en el caso del hacker) o alterando el sistema para beneficio propio donde en múltiples ocasiones dejan fuera de servicio al sistema informático atacado (en el caso del cracker).

Por esta razón es de vital trascendencia crear hábitos de preservar información en los empleados de una compañía, como por ejemplo: brindar capacitación al personal de una empresa de los últimos ataques concebidos en una red, envío de correos electrónicos indicando una vulnerabilidad presente en la web, e

implementar estrategias a todo el personal en el caso de que se sufra un atentado a la información confidencial de la compañía.

En la figura 2.10 se puede visualizar un cuadro estadístico de las principales causas de violaciones de seguridad de datos desde el año 2013; se observa un alto porcentaje de agresiones a la red originados por atacantes (durante el 2015, China fue el país donde se originó el 40% del bot malicioso en el mundo), seguido por la información confidencial publicada involuntariamente, así como por robos de equipos y hurtos de información privilegiadas dentro de una organización.

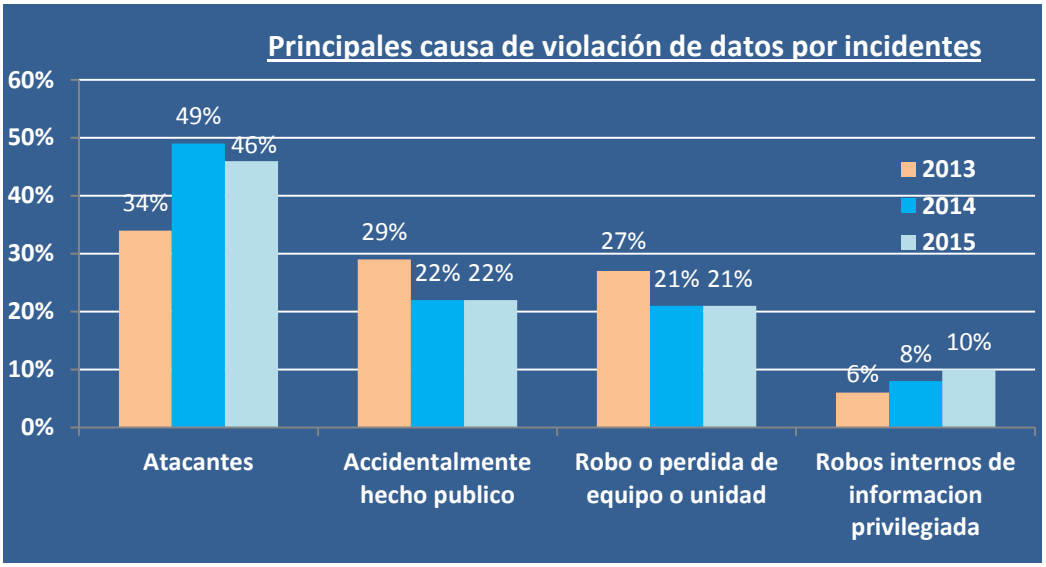


Figura 2. 10: Causas de violación de datos de los últimos 3 años
Fuente: (Symantec Corporation, 2016)

Las organizaciones deben analizar su modelo de seguridad de manera holística y obtener visibilidad y control en toda la red extendida y de toda la continuidad del ataque, durante su proceso, e incluso después de que comienza a dañar los sistemas o a robar información.

Cisco plantea seguir un modelo de seguridad donde se realicen análisis antes, durante y después de un ataque: antes del delito, los defensores necesitan sensibilidad y visibilidad integral de todo lo que contiene la red extendida a fin de implementar políticas y controles para defenderla, durante el ataque, es fundamental poder detectar continuamente el malware y bloquearlo, y después del

ataque, los defensores necesitan la seguridad retrospectiva para marginar el impacto de un ataque, se debe identificar el punto de ingreso, determinar el alcance, contener la amenaza, eliminar el riesgo de reinfección, y corregir la interrupción (Cisco System, Inc., 2014).

Existen varias preocupaciones por parte de las compañías con respecto a los ataques cibernéticos que pueden sufrir sus redes de datos, las estadísticas muestran que el factor económico no solo es el principal malestar de las empresas cuando sufren infiltraciones ilegitimas en su red, también existen factores como perdida de reputación, pérdida de clientes y corte de servicios que inciden en el desempeño y el crecimiento de la compañía, la figura 2.11 refleja un detalle de las preocupaciones de las empresas con respecto a los ataques cibernéticos durante los 2 últimos años.

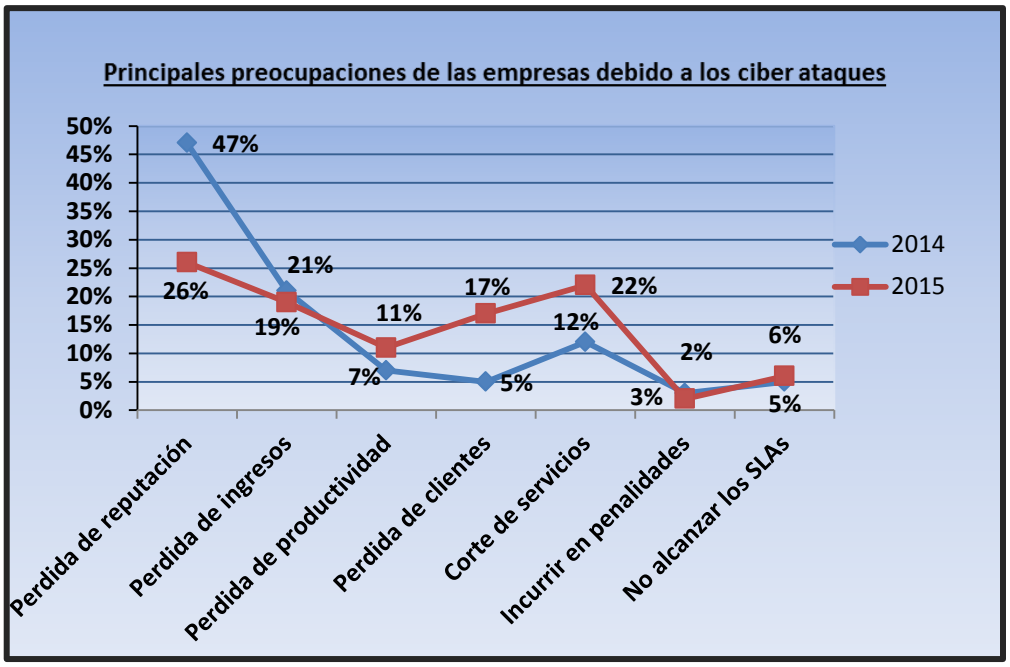


Figura 2. 11: Principales preocupaciones de las empresas debido a los ciber ataques
Fuente: (Radware Ltd., 2016)

2.5.1. Estudio de las amenazas a las redes de datos

Se entiende por virus informático a un software diseñado con el objetivo de causar un perjuicio al computador de la víctima, pretendiendo actuar de forma natural al

usuario, provocando alteración de los archivos alojados en la PC y colapsos en sistemas informáticos en línea. Existen ciertos patrones o inteligencias de estas amenazas que se tiene en las redes de datos a nivel mundial, el ejemplo más significativo de una agresión a la red de datos es la inundación de puertos aleatorios de TCP o UDP sobrecargando un servidor en particular desde varios puntos de conexión, dejándolo, en muchas ocasiones, fuera de servicio, este tipo de ataques se conoce como DDoS, y provoca lentitud de acceso a un servidor de comunicación ya que el equipo no responde correctamente a la cantidad de peticiones legitimas e ilegítimas que ingresan en la red de datos; como se observa en la figura 2.12, DDoS representa un 51% de ataques que experimentaron las diferentes compañías en el año 2015, seguido por agresiones de tipo phising, virus y gusanos, accesos no autorizados, correos spam y fraudes bancarios.

En su informe del primer trimestre del 2016, Akamai Technologies, Inc., resalta las diferentes estadísticas de ataques DDoS a aplicaciones web: se registró un aumento del 23% de ataques DDoS y un incremento de ataques del 107% en la capa de aplicación en comparación con el último trimestre del 2015, el volumen de este tipo de ataques fue de 51 Mpps (millones de paquetes por segundo) con una duración promedio de 16 horas, el sector de los juegos representa un 55% de objetivos a ser atacados por DDoS, seguido de las empresas de tecnología y software con un 25%, China figura como el país donde más se origina este tipo de ataques con un 27%, seguido por Estados Unidos con un 17%; en ataques a aplicaciones web, el 70% de estas amenazas están dirigidas a servidores instalados con el servicio http, mientras que el 30% de los ataques están dirigidos a aplicaciones https (Hypertext Transfer Protocol Secure), y el 60% de ataques a aplicaciones web son dirigidos a sitios alojados en los Estados Unidos (Akamai Technologies, Inc., 2016).

2.5.2. Protocolos y encriptación en redes de datos.

Cabe señalar que existen protocolos de seguridad de redes de datos que permiten una comunicación segura y confiable a nivel IP; IPSEC (Internet Protocol security) es un conjunto de protocolos que protegen la información cuando se

transmite la información de un punto a otro, basado en otros protocolos como IKE (Internet Key Exchange), ESP (Encapsulating Security Payload), AH (Authentication Header); posee las siguientes características:

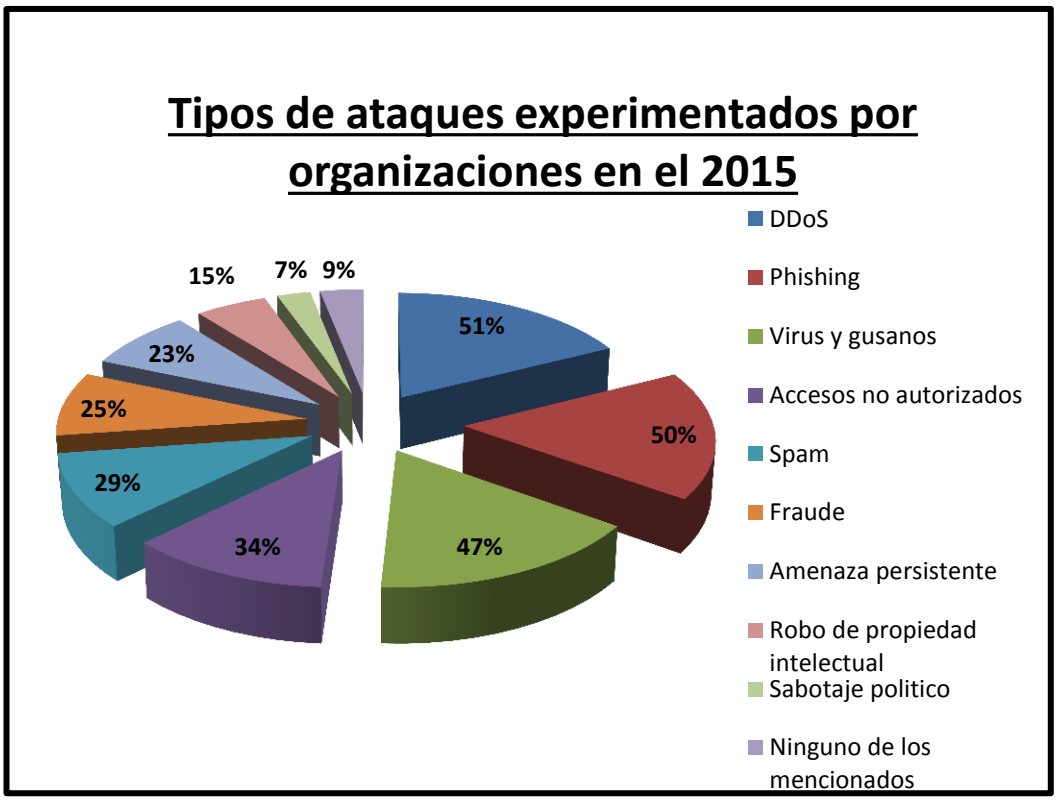


Figura 2. 12: Tipos de ataques a las redes de datos en el 2015
Fuente: (Radware Ltd., 2016)

a) Seguridad de datos: encriptación de datos para hacerlos ilegibles
b) Integridad de datos: garantiza que no han sido modificados, ni alterado los datos sobre la VPN
c) Autenticación desde el nodo origen de datos: valida el origen de la VPN IPSEC, asegura que el equipo del otro extremo es quien debe ser

El protocolo IKE se encarga de la negociación segura de las llaves de autenticación, en las VPN se realiza el intercambio de dichas llaves de seguridad; el protocolo ESP proporciona tres tipos de encriptación de los datos: DES (Data Encryption Standard), 3DES (triple Data Encryption Standard) y AES (Advanced Encryption Standard); el protocolo AH garantiza que los datos no han sido modificados o interferidos, utiliza HMAC (Hash-based Message Authentication

Code) como método de chequeo para la autenticación e integridad de la información (Ariganello & Barrientos, 2010).

Existen 2 modos para proteger los datos en IPSEC, estos son los modos transparentes (la cabecera IPSEC es insertada después de la cabecera IP) y el modo túnel (tanto la cabecera IP original como el resto de datos son protegidos). Para garantizar que la comunicación de extremo a extremo sea confiable en ambos nodos de la comunicación, existen métodos para la autenticación de vecinos en IPSEC, como usuarios y contraseñas, sistemas biométricos, certificados digitales y claves pre compartidas (Ariganello & Barrientos, 2010).

Existen 2 tipos de algoritmos de encriptación, simétrica y asimétrica, la primera se basa en el uso de una sola llave tanto para encriptar como para desencriptar los datos, DES, 3DES y AES utilizan este tipo de encriptación; la encriptación asimétrica utiliza diferentes llaves para encriptar (llave publica) y desencriptar información (llave privada).

Otro tipo de encriptación es PKI (Public Key Infrastructure) que es un proceso de intercambio y mantenimiento de llaves lógicas de seguridad permitiendo que la comunicación sea segura entre nodos, empleando certificados digitales, autoridad certificadora y mecanismos de distribución.

La característica esencial del protocolo IKE es la complejidad que posee para intercambiar de manera dinámica parámetros y claves IPSEC para el establecimiento de asociaciones de seguridad, la asociación de este protocolo está compuesta por 2 fases: la fase 1 se establece una única asociación de seguridad bidireccional, operando en modo agresivo (no protege la identidad de los nodos extremos) y en modo principal (protege la identidad de los nodos extremos), y la fase 2 establece una asociación de seguridad en una sola dirección (Ariganello & Barrientos, 2010).

2.5.3. Principales amenazas en las redes de datos

Existen una diversidad de amenazas en internet que tienen como objetivo común alterar la información alojada en el computador y dejar fuera de servicio sistemas informáticos de entidades bancarias, financieras y estatales; estos ataques son originados, en muchas ocasiones, por sistemas políticos que contratan a hackers para lograr desprestigiar a un gobierno en particular, también los ciber ataques son causados por usuarios molestos de jugadores en línea que no logran alcanzar un nivel determinado en el juego y producen ataques a los servidores en cuestión.

Las organizaciones se encuentran preparadas para resistir las amenazas de virus, gusanos, ataques DDoS en sus redes con equipos de alta gama en seguridad informática como firewalls de última generación y sistemas de prevención de intrusos, experimentando máximo un promedio de una hora de ataques cibernéticos en su core; la tabla 2.5 ilustra un listado de las principales amenazas en las redes de datos hoy en día.

2.5.4. Nueva generación de firewalls

Ante los diferentes problemas de seguridad informática que afrontaban ciertos proveedores de internet, recurrían a la instalación de firewalls sencillos en su configuración y poco fiables al momento de exponer información confidencial al mundo entero, por lo que con el pasar de los años salió a producción la nueva generación de firewalls para fortalecer la seguridad lógica en la red de datos en una empresa.

Tabla 2. 5: Principales amenazas a las redes de datos

TERMINOLOGIA	DESCRIPCION
Adware	Software malicioso cuyo objetivo es descargar publicidad no requerida por el usuario, desplegadas por ventanas emergentes en el computador; el término proviene de las siglas advertisement (anuncio) y software.

ARP Spoofing	Ataque dirigido a la tabla ARP de un dispositivo informático, inundando la red con paquetes ARP dañinos, realizando un match entre la dirección MAC física del atacante con la dirección IP legitima, de esta manera, el atacante recibirá información confidencial enviada a la víctima.
Backdoor	Es un método de infiltración a un sistema informático tratando de pasar por alto la autenticación para el acceso a la herramienta obteniendo información relevante del propietario del sistema.
Black hat SEO	Black hat significa sombrero negro en inglés y SEO (Search Engine Optimization), es una técnica usada por los atacantes para engañar a los buscadores en internet (Google, Yahoo, Bing) direccionando las palabras claves solicitadas por la victima a sitios web controladas por el atacante.
Botnet	Son creadas infectando las PC's con malware controladas bajo un atacante conocido como bot maestro, utilizando estas computadoras para actividades malintencionadas como ataques de denegación de servicio y envió de spam, por lo general los propietarios de estas PC's ignoran que son parte de los ataques por botnet.
Bootkit	Este virus se ejecuta al arrancar el sistema operativo de una PC con el objetivo de tener control total de la maquina antes de que termine el proceso de carga de la computadora infectada.
Creepware	Es un subconjunto de software espía que permite el control del micrófono y de la cámara web de la víctima.
Crimeware	Término usado por lo general para identificar ataques de malware dirigidos a entes financieros o económicos.
Caballo de Troya	Este código malicioso tiene la característica de ejecutarse dentro de un programa que a primera vista no representa riesgo alguno, sin embargo causa robos y pérdidas de información personal, creando backdoors permitiendo el acceso a la PC por un usuario no autorizado.

DDoS	Es un ataque conocido como denegación de servicio desde varios puntos de la red, generando un gran flujo de información a una PC determinada provocando congestión en el procesador del equipo y lentitud de paquetes legítimos al servidor; existen diferentes tipos de ataques DDoS como DDoS ICMP, DDoS UDP, DDoS SYNC_TCP
DNS Spoofing	Es un ataque que sufren los servidores DNS alterando las direcciones IP legitimas de estos equipos con direcciones DNS maliciosas, de esta manera las consultas a los servidores por parte de las víctimas se verán afectadas ya que son redirigidas a sitios web que el atacante desee.
Exploit	Cadena de comandos que utiliza el delincuente informático para tratar de ingresar al software conociendo una vulnerabilidad en la aplicación, se clasifican en conocidos y desconocidos (como el ataque de día zero)
Gusano	Es un software malicioso que tiene la característica de auto reproducirse sin ayuda de la víctima y puede propagarse de PC a PC en una red de datos causando graves daños a gran escala en los sistemas informáticos en línea, a diferencia del virus que solo afectan a los archivos de un computador personal.
Ingeniería Social	Conjunto de prácticas que emplean los hackers para engañar a usuarios en la red de datos mediante procedimientos psicológicos con el objetivo de persuadir a la víctima para que entregue información personal como contraseñas de acceso a cuentas bancarias, cuentas de tarjetas de crédito y cuentas de redes sociales.
Keylogger	En español significa registrador de teclas, es un malware que tiene la característica de capturar información de las pulsaciones del teclado o del mouse para hurtar información como contraseñas de correo, números de tarjeta de crédito, inclusive capturas de pantalla de la PC de la víctima.
Malware	El termino malware se compone de malicious (en español “malicioso”) y “software”, es un programa informático malicioso cuyo objetivo primordial es corromper la lógica del programa para obtener información confidencial de la víctima; se propaga mediante correos electrónicos, memorias USB, mensajes de chat. Un conjunto de malwares conocidos son los virus, gusanos, troyanos, backdoors.
Man In The Browser (MITB)	En español significa "hombre en el navegador", el atacante utiliza las vulnerabilidades del navegador de internet del usuario para averiguar el tráfico de la red capturando datos confidenciales de la víctima e inyectando códigos de programación en las páginas web visitadas; este tipo de malware es de difícil detección ya que los sitios web alterados no mantienen diferencia con las originales.

Phishing	Utiliza ingeniería social para convencer a la víctima que entregue información confidencial como cuentas de tarjetas de créditos, contraseñas; por lo general los delincuentes informáticos utilizan mensajes de correo electrónico haciéndose pasar por entidades bancarias de confianza para lograr sus objetivos.
Ransomware	Proviene de los términos ransom (rescate), y ware (software); virus informático que encripta la información confidencial alojada en el computador de la víctima con el objetivo de cobrar una cierta cantidad de dinero por el atacante para entregar la clave que ayudaría a descifrar la información.
Rootkit	Software cuyo objetivo es ingresar a un sistema informático de manera sigilosa evadiendo seguridades implantadas en el equipo, ejecutando virus informáticos sin ser detectados, apoderándose completamente del sistema.
Spam	Conocidos como correos basura o no deseado enviados de forma masiva por el atacante, tratando de llenar la bandeja de entrada de publicidad engañosa.
Spyware	Aplicación instalada involuntariamente en la PC de la víctima con el fin de recopilar información confidencial de esta persona sin usar su consentimiento, esta información es enviada al atacante obteniendo así números de tarjetas de crédito, contraseñas y cuentas de correo, códigos de cuentas bancarias.
Spoofing	Malware cuyo fin es falsificar los componentes que intervienen en una comunicación de redes datos como por ejemplo IP Spoofing (envío de paquetes de datos con dirección Ips falsas) , DNS Spoofing (respuestas a consultas de las víctimas a dirección DNS maliciosas), ARP Spoofing (modificar la tabla ARP con datos falsos para lucro del atacante).
Zero-day (dia cero)	Vulnerabilidad existente en una aplicación que es desconocido por el programador del software determinado, muchos hackers aprovechan este hueco de seguridad para alterar el desempeño de la aplicación sin ser detectados.

Elaborada por: El Autor.

Se podría definir como NGFW (Next Generation Firewall) a un server appliance que permite contralar el tráfico en la red analizando el paquete de datos por cada una de las capas del modelo OSI, por lo que se conoce como protección multicapa, además de poseer una administración central del equipo, soportando un

throughput (rendimiento) de más de 10 Gbps y las opciones de activación de módulos virtuales como IPS, antivirus, antibot, control de aplicaciones, filtro de URL's, capacidad de enrutamiento IGP y EGP, todo esto en un solo hardware mitigando todos los tipos de amenazas posibles en el core de datos.

Existe una variedad muy extensa a nivel de hardware y software con respecto a firewalls de última generación, si se desea integrar un equipo appliance NGFW que proteja la granja de servidores del core de la red, hay que enfocarse en el desempeño, administración centralizada y presupuesto que ofrezca determinado firewall; los requerimientos mínimos que debe de cumplir el equipo para que sea capaz de aminorar los diferentes ataques lógicos al core de la red son:

a) Conexiones TCP concurrentes: 5 M (millones)
b) Throughput del firewall nominal: 14 Gbps
c) Throughput del IPS: 6 Gbps
d) Monitoreo centralizado del appliance
e) Memoria ram: 10 GB
f) Disco duro: 500 GB
g) Conexiones por segundo: 140 K (mil)

La tabla 2.6 indica un detalle de las marcas más relevantes que existen en el mercado de las tecnologías de la información, siendo la marca Check Point el equipo que cumple con la mayoría de requisitos necesarios para la implementación del firewall en la red.

2.5.5. Firewall Check Point

Para lograr el objetivo propuesto, este trabajo se orientará al estudio de la tecnología en firewalls Check Point, ya que cumple con los requisitos indispensables para la protección de la granja de servidores de un ISP en la red MPLS.

Tabla 2. 6: Cuadro comparativo de NGFW

APPLIANCE			
	CISCO	FireEye Next Generation Threat Protection	Check Point SOFTWARE TECHNOLOGIES LTD.
Modelo	ASA 4110	NX10150	Checkpoint 12600
Usuarios	Sin límite de usuarios	Sin límite de usuarios	Sin límite de usuarios
Throughput del firewall	10 Gbps	4 Gbps	14 Gbps
Throughput del IPS	10 Gbps	4 Gbps	6 Gbps
Throughput de VPN	8 Gbps	No	3.5 Gbps (AES-128)
Conexiones concurrentes	4.5 M	2 M	5 M
Máxima conexiones por segundo	150 K	2 M	1.7 M / 5 M (máximo)
Conexiones por segundo	150 K	40 K	140 K
Puertos de red GE	No	8-port 10/100/1000	Modular 12-port 10/100/1000 (máximo 26 puertos con módulos de expansión)
Puertos de red SFP	24 port GE SFP	8-port GE SFP	4-port GE SFP (máximo 12 puertos con módulos de expansión)
Puertos de red 10 GE	8 port 10 GE	4 port 10GE SFP+	6 port 10GE SFP+
Puertos USB2.0	1	2	2
Capacidad de almacenamiento	200 GB	4 x 960GB SSD	500 GB disk
Memoria	4 GB	4 GB	12 GB
Interfaces virtuales (VLAN's)	1024	1024	1024
IPSEC VPN	3DES, AES	No	3DES, AES
Autenticación	Local, Radius, Tacacs	Local, Radius, Tacacs	Local, Radius, Tacacs
Routing IPV4 / IPV6	OSPF/BGP/Static	Static	OSPF/BGP/Static
Logs en tiempo real	Si	Si	Si
Eficiencia y protección en ataques de malware	80%	47%	100%
Tiempo de respuesta para el bloqueo de malware	No	2 segundos	2 segundos
Alta disponibilidad	Active/Active, Active/Standby	Active-Passive	Active/Active, Active/Standby
Soporte IPv6	Si	Si	Si
Fuente de poder	AC/DC	AC	AC/DC

Fuente: (Cisco Systems, Inc., 2015) ; (FireEye, Inc., 2016) ; (Check Point Company, 2015)

La tecnología en firewalls de última generación Check Point posee una arquitectura llamada SMART (Security Management Architecture) que es un componente central de seguridad informática unificada y ayuda a tener una administración de todos los dispositivos de seguridad desde una consola llamada smart dashboard, donde los administradores de la red pueden realizar consultas en tiempo real de los diferentes eventos del equipo y de la seguridad de la red de datos que está siendo protegida por el firewall.

Arquitectura Check Point: El core del firewall Check Point posee una arquitectura de 3 capas y está compuesto de los siguientes elementos:

a) SmartConsole: Provee una interfaz gráfica para administrar múltiples elementos de seguridad de red en ambientes Check Point.
b) Security Manager server: Es un repositorio donde se guardan las políticas de los firewalls, por alta disponibilidad se recomienda que este físicamente fuera del gateway (firewall)
c) Security Gateway: Es el firewall como tal, en este equipo se procesan las políticas de seguridad de la red.

Se conoce como arquitectura standalone a la implementación del security manager server y el security gateway dentro de un mismo equipo como muestra la figura 2.13, mientras que en la arquitectura distribuida el security manager y el security gateway se encuentran en diferentes equipos, como indica la figura 2.14

Control de tráfico en la red: Check Point utiliza tecnologías para controlar el tráfico en la red conocidas como: Packet filtering (filtrado de paquetes), Stateful Inspection (estado de inspección) y Application Intelligence (inteligencia de aplicación); en packet filtering los mensajes son divididos en paquetes que incluyen la dirección destino y son menos seguros porque no comprenden el contexto completo de la comunicación; en stateful inspection monitorea el estado de la conexión de extremo a extremo, por lo que se considera una etapa de alta confiabilidad y en application intelligence se detecta y previene ataques a diferentes aplicaciones dado un elevado número de ciber ataques que explotan

vulnerabilidades en la red puesto que no solo se presentan ataques directamente al firewall como tal.

Figura 2. 13: Arquitectura Check Point Standalone
Fuente: (Check Point Company, 2013)

Figura 2. 14: Arquitectura Check Point distribuida
Fuente: (Check Point Company, 2013)

Cuando un paquete de datos alcanza el firewall muchas cosas suceden, primero el firewall Check Point va a las reglas de anti-spoofing para asegurarse que el paquete está viniendo por la interfaz correcta, algún error y el paquete es descartado, después empieza un proceso llamado motor de inspección como se muestra en el diagrama de flujo de la figura 2.15, primero el firewall revisa en su base de reglas por un match a un determinado paquete (las reglas son analizadas de arriba hacia abajo, una a la vez) una vez que suceda esto la conexión es establecida y el firewall determina si debe pasar, dropear o rechazar el paquete, si un paquete es rechazado envía un paquete NACK (negative acknowledgment) al servidor para cerrar la conexión y dropear el paquete (Stephens, Stiefel, Watkins, Desmeules, & Faskha, 2005).

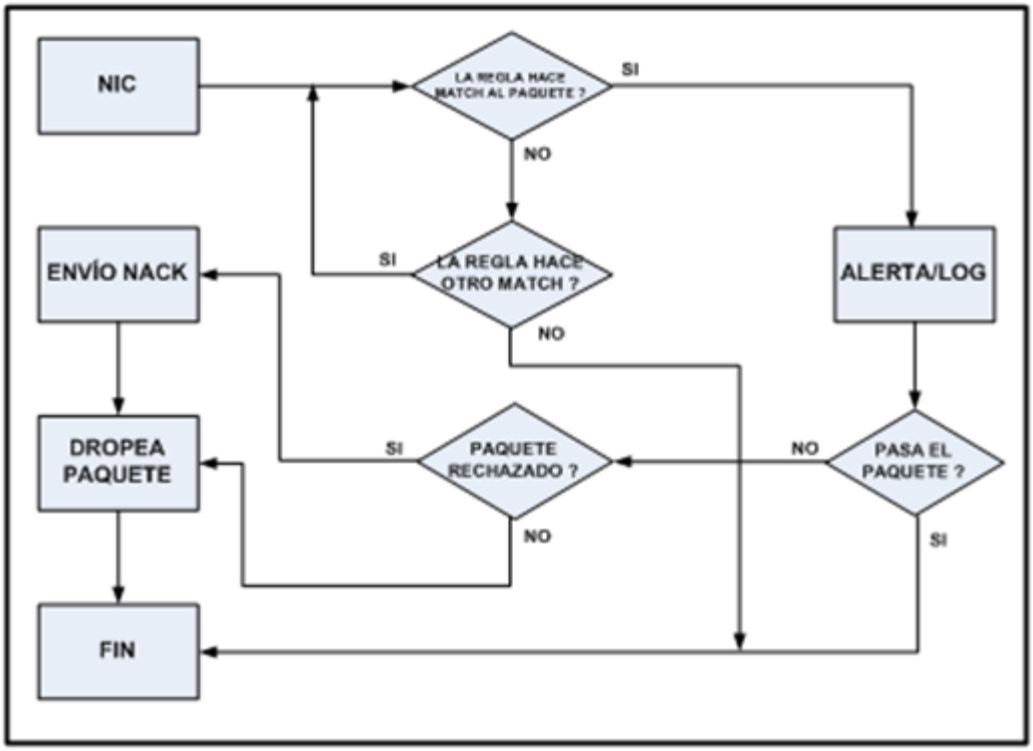


Figura 2. 15: Diagrama de flujo del motor de inspección Check Point
Fuente: (Stephens, Stiefel, Watkins, Desmeules, & Faskha, Configuring Checkpoint NGX VPN-1/Firewall-1, 2005)

Clientes SmartConsole: Para una mejor administración del NGFW Check Point existen varias alternativas amigables que evitan la ejecución de líneas de comandos en el equipo, estos clientes son administrados desde el smartconsole; las más importantes son: SmartDashboard, SmartviewTracker y SmartviewMonitor; el smartDashboard permite observar los paquetes por segundo y número de conexiones en determinado firewall, información general de políticas creadas en el equipo, y administrar los diferentes software blades como Application & URL Filtering, DataLoss Prevention, IPS, VPN; la figura 2.16 muestra la captura de pantalla del SmartDashboard, donde el cuadro señalado con el numero 1 indica opciones como grabar cambios en el equipo, editar propiedades globales, instalar políticas y abrir diferentes opciones con el SmartConsole, en el cuadro 2 se tiene los diferentes blades activados en el equipo, en el cuadro 3 se pueden escoger opciones como reglas de NAT (Network Address Translation), políticas instaladas en el equipo y una visión general del firewall, en el cuadro 4 se muestra todas las reglas instaladas en el gateway (se conoce como rule base), en el cuadro 5 señala el árbol de objetos donde están los

diferentes grupos de red, servicios y configuración de usuarios y finalmente en el cuadro 6 está la lista de objetos donde se puede buscar, en que regla reside un host en particular con las respectivas acciones a realizar.

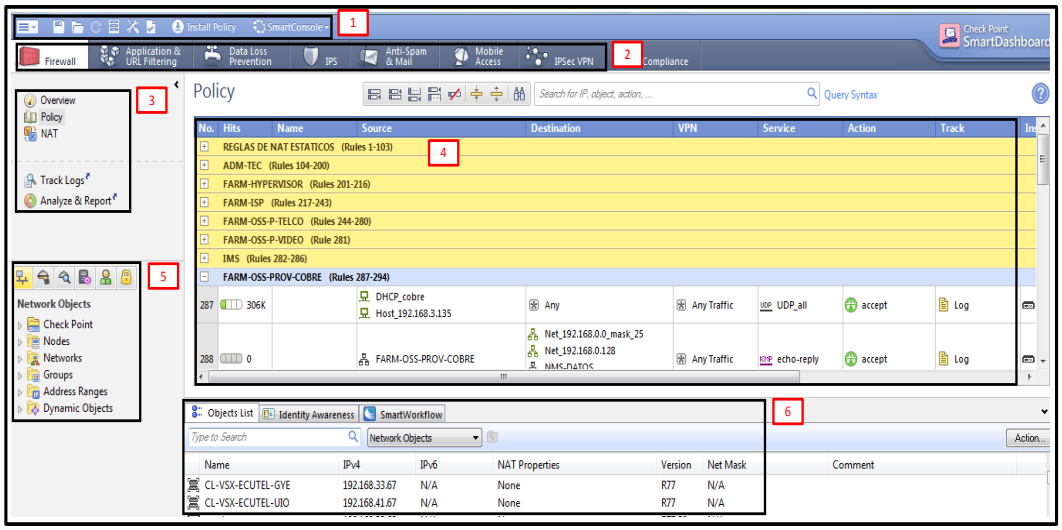


Figura 2. 16: SmartDashboard Check Point
Elaborada por: El Autor.

En el SmartviewTracker se pueden analizar los diferentes logs de una regla especifica como el día y la hora que se ejecuta dicha regla, tipo de protocolo, dirección IP fuente, dirección IP destino, numero de regla configurada en el firewall y la acción resultante que el firewall ha decidido realizar (aceptar paquete, dropear paquete o rechazar paquete), además se guardan eventos como datos de los usuarios que acceden al equipo, la figura 2.17 muestra un detalle del SmartviewTracker.

El SmartviewMonitor proporciona información de direcciones IP de los diferentes gateways, el consumo promedio del CPU, la actividad de memoria RAM y el porcentaje de disco libre de cada uno de los firewalls instalados en la red, en la figura 2.18 se observa la captura de pantalla del SmartviewMonitor.

Certificado SIC (Secure Internal Communications): La comunicación entre el security manager server y el security gateway (firewall) debe de ser encriptada y autenticada, por lo que Check Point creó el certificado SIC que asegura la comunicación entre estos 2 servidores, cada vez que el servidor manager se trata

de autenticar con el firewall se levanta este protocolo, de este manera se garantiza la confiabilidad e integridad en el momento de la transmisión de datos de equipo a equipo, ya que en ambos servidores vive este certificado compartiendo una contraseña idéntica en estos dispositivos.

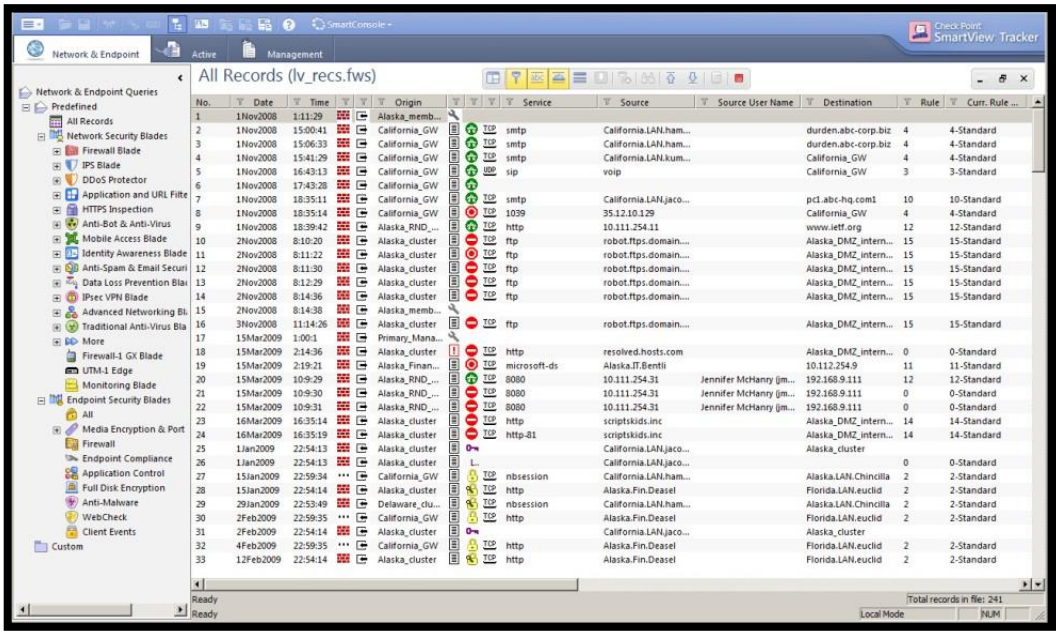


Figura 2.17: SmartViewTracker Check Point
Elaborada por: El Autor.

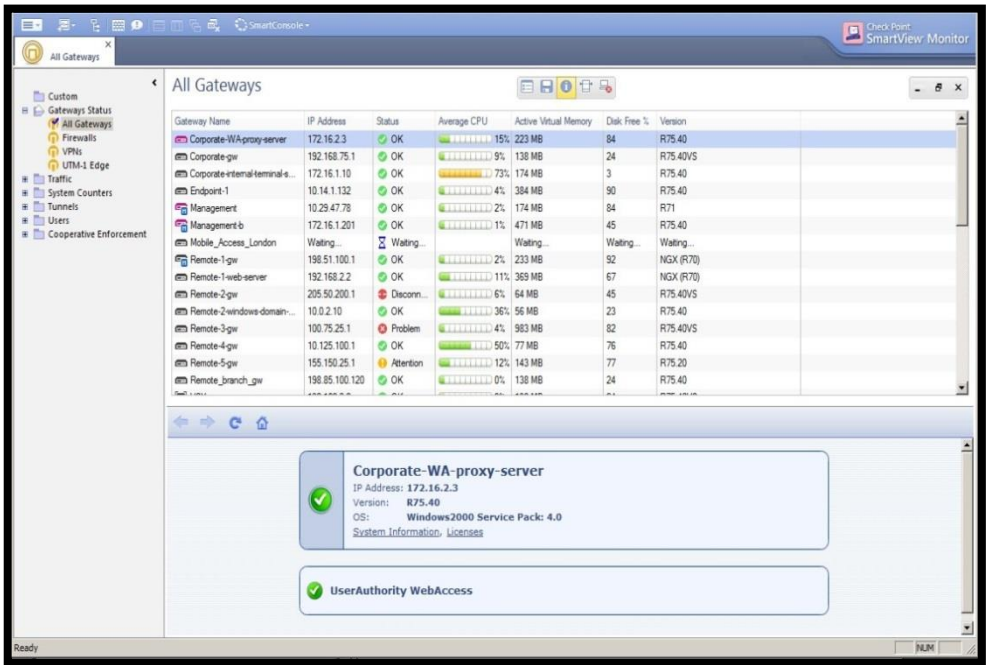


Figura 2. 18: SmartView Monitor Check Point
Elaborada por: El Autor.

Es muy importante que la comunicación entre equipos Check Point sea encriptada y autenticada ya que asegura la correcta instalación de políticas en los firewalls y

él envió de logs entre los gateways y el security manager server; cabe resaltar, que el reloj de sincronización entre los gateways y los servidores deben estar correctamente sincronizado para garantizar el establecimiento del certificado SIC.

Sistema Operativo GAIA: El sistema operativo que corre en todos los dispositivos de siguiente generación de firewalls Check Point es GAIA (su nombre se debe a que en la mitología Griega, Gaia es madre de todo lo creado), soporta un completo portafolio de firewalls, software blades y dispositivos de seguridad Check Point, además combina las mejores características del sistema operativo SecurePlatform e IPSO; SecurePlatform es un sistema operativo de firewalls, fácil de usar y de alta disponibilidad, mientras que IPSO es un sistema operativo que trabaja en equipos Nokia y la arquitectura de la configuración es centralizada. GAIA nació en la versión R75.40 caracterizándose en tener alto desempeño y robustez al momento de correr en todas las plataformas NGFW de Chek Point.

El sistema operativo GAIA incluye soporte para (Check Point Company, 2016):

a) IPv4 e IPv6.- Integridad completa en el sistema operativo.
b) Capacidad para crear sistemas virtuales.- Soporta 64 bits
c) Balanceo de carga.- En interfaces cluster e interfaces bonding.
d) Alta disponibilidad.- En interfaces bonding, VRRP, y cluster
e) Enrutamiento dinámico y multicast.- BGP, OSPF, RIP y PIM-SM (Protocol Independent Multicast - Sparse Mode), IGMP (Internet Group Management Protocol).
f) Línea de interfaz de comando fácil de usar
g) Administración basada en roles de usuarios.

La versión R77 GAIA (versión que se utilizara en ambientes virtuales para la simulación a realizar en el desarrollo de este trabajo) aumenta el desempeño del NGFW de Chek Point bloqueando ataques del dia-zero (ataques a software y aplicaciones que tienen agujeros de seguridad desconocidos por los desarrolladores) y ataques dirigidos específicamente a un servidor detrás del

firewall, las mejores de esta versión posibilitan consolidar más módulos virtuales al equipo (módulo IPS, VPN, Identity Awarereness) en el mismo firewall con un alto rendimiento del mismo, proporciona una fácil visibilidad de la red de una manera global y una administración centralizada del equipo, además se pueden ejecutar varias tareas desde el dashboard tales como restore, backup o abrir la consola shell remoto.

Administración del equipo: Existen 2 maneras para administrar los firewalls Check Point, a través de la interfaz gráfica web y por medio de comandos CLI (Command Line Interface); la interfaz gráfica proporciona acceso total a la configuración del equipo, además de poseer un ambiente amigable y de fácil configuración, el acceso a esta interfaz es por medio del protocolo https a la dirección IP del firewall, con un usuario y contraseña previamente creados se accede a esta herramienta, en la figura 2.19 se analizará con más detalles esta consola gráfica: el cuadro 1 indica una visión general de las opciones que ofrece el firewall para su administración, como políticas de enrutamiento, gestión de usuarios, alta disponibilidad del equipo, sistemas de backup, y actualizaciones de versiones del firewall, en el cuadro 2 se puede observar características del sistema instalado en el dispositivo como versión del sistema operativo, numero de kernel, edición para 32 o 64 bits y tiempo que lleva encendido el equipo, en el cuadro 3 se muestran todos los software blades que están activados en el firewall y en cuadro 4 se detalla la configuración de red del equipo como dirección IP, nombre de la tarjeta de red y estado de operación de la tarjeta.

Otra forma de administrar el appliance es vía CLI, si se ingresa via SSH (Secure Shell) a la dirección IP del firewall con un usuario y contraseña previamente creado, se tendría más de 1000 comandos disponibles en el sistema operativo GAIA para realizar las respectivas configuraciones y/o troubleshooting al equipo; cabe resaltar que el firewall posee una ayuda para los administradores de este appliance en el caso de que no recuerden la línea exacta del comando a ejecutar, esta ayuda se realiza directamente en el firewall vía CLI completando la línea con la tecla tab del computador, así el operador tendrá opción a escoger el comando

exacto para lograr el objetivo deseado; la tabla 2.7 muestra los principales comandos a ejecutar y la respectiva función que cumplen en el equipo.

Figura 2. 19: Consola de administración web del firewall
Elaborada por: El Autor.

Tabla 2. 7: Lista de principales comandos CLI para el firewall Check Point

COMANDO CLI	FUNCION
`fw unloadlocal`	Desactiva las políticas instadas en el firewall
`fw ver`	Verifica la versión del firewall
`fw stat`	Verifica si las políticas están instaladas localmente en el firewall
`fw monitor`	Monitorea el tráfico de una interfaz en particular en el firewall
`fwm lock_admi -ua`	Desbloquea todas las cuentas de administrador del server management
`fw ctl pstat`	Información estadística de memoria, conexiones y kernel del gateway
`fw ctl iflist`	Muestra la lista de las interfaces del firewall
`fw log`	Muestra los eventos de las reglas
`show route`	Muestra la tabla de enrutamiento del equipo
`show configuration`	Muestra la configuración del firewall
`show interfaces all`	Muestra información de las interfaces en el equipo

reboot	Reinicia el firewall
cpconfig	Reconfigurar productos de Check Point
save config	Guarda los cambios en el equipo
lock database override	Adquiere acceso de lectura / escritura a la base de datos del firewall
expert	Cambia el promt de la configuración a un modo avanzado (experto)
restore -file-	Restaura un archivo de backup
backup	Realiza un backup de la configuración del equipo
cd /var /CPbackup /backups	Se almacenan los backups que se realizan via webUI directamente en el server management
cplic print	Ver las licencias instaladas en el server management o en el gateway
cd /$CPDIR /conf	Los certificados SIC son almacenados en este directorio.
cd /$FWDIR /conf	Se almacenan licencias, reglas, objetos, y base de datos de usuarios
cd /$FWDIR /log	Ubicación de los logs del equipo
cpstop	Parar todos los servicios de Check Point
cpstart	Empezar todos los servicios de Chek Point
cprestart	Reinicia todos los servicios de Check Point
cp_conf sic state	Verifica el estado del certificado SIC en el equipo
cpstat fw -f policy	Muestra la tabla de paquetes dropeados y aceptados por interfaz del firewall
cpstat fw -f sync	Muestra el sincronismo del equipo
cpinfo -o date.cpinfo.txt	Archivo de soporte de diagnóstico de Check Point

Elaborada por: El Autor.

2.5.6. IPS

Estudiando las estadísticas de ataques informáticos de los últimos meses, se observa altos porcentajes de vectores de ataques dirigidos a servicios financieros, servicios legales, tecnología y software con un tiempo de duración prolongado, provocando que los activos más importantes de estas entidades sean vulnerables y de fácil acceso a la organización criminal digital de hoy en día.

Investigaciones realizadas por laboratorios Eset de Latinoamérica indican que durante el año 2015 la infección por malware ocupa el primer lugar en incidentes de seguridad a las empresas con un 40% de respuestas afirmativas, en segundo lugar se ubican los casos de phishing con el 16% y en tercer lugar el fraude interno/externo con el 13%; otro punto importante de esta encuesta es la implementación de controles tecnológicos en las empresas, donde el 77% fueron respuestas afirmativas por las compañías en la adquisición de software antivirus, seguido por los Firewalls-IPS con el 71%, y respaldos de información con el 63% (Eset Company, 2016).

Un IPS appliance detecta intrusiones lógicas a servidores corporativos o computadores de usuarios con el objetivo de alterar o corromper el desempeño de estos equipos, por lo que el IPS activa inmediatamente mecanismos de defensa como escudos de protección a través de firmas lógicas para resguardar a estos servidores de los ciber ataques detectados en la red; los bugs o vulnerabilidades de los servidores o de ciertas aplicaciones son aprovechados por cibercriminales para cometer un delito, el IPS contrarresta estos ataques a la red reduciendo considerablemente el riesgo de una caída total o parcial de un sistema informático puesto en producción.

Los firewalls de siguiente generación tienen la opción de integrar en un solo equipo tanto el módulo de IPS y el módulo de firewall, además de otros softwares blades como Antivirus, Antispam, Mobile Access, Vpn, Url Filtering que pueden ser activados dependiendo de la licencia adquirida al proveedor y de los requerimientos tecnológicos que demande determinada empresa; una de las ventajas de incorporar en un appliance los módulos de IPS y firewall es el incremento de seguridad en un solo equipo con administración centralizada y amigable, dado que se formaría un perímetro de seguridad lógica en la red, haciéndola robusta y de alta confiabilidad.

Como se indicó, un método de detección que utiliza el sistema de prevención de intrusos es el empleado por la activación de las firmas en el equipo, que son patrones que capturan y reúnen información con respecto al código malicioso que

trata de atacar a determinado servidor; una vez reunido estos reportes, los diseñadores de las firmas estudian la lógica del ataque y tratan de programar una cadena de bytes cuyo objetivo primordial es tomar una acción apropiada para contrarrestar el ataque como dropear o eliminar los paquetes ilegítimos que tratan de ingresar a la red.

Existen varios tipos de atributos que caracterizan a estas firmas como son: las aplicaciones donde van dirigidos los ataques (servidor web, servidor de correos, servidor apache), el sistema operativo donde corre la vulnerabilidad analizada (Microsoft Windows, Linux, Solaris), el tipo de riesgo que se tiene en el momento de que el paquete de datos anómalo trata de ingresar a la red de datos (alto, medio o bajo), los servicios que se verían afectados en el perímetro de la red *(*Hypertext Transfer Protocol o HTTP, Simple Network Management Protocol o SNMP, Domain Name System o DNS), y el tipo de amenaza que caracteriza al ataque (inundación de paquetes, denegación de servicios, ataques VBA (Visual Basic Applications).

Lo esencial de la funcionabilidad del motor del IPS son las varias técnicas de detección, comportamiento y análisis de datos, el IPS no solo es un motor que protege a la red en base a firmas previamente instaladas o detectando un comportamiento anómalo en la red, el IPS es un equipo de alta precisión y alto desempeño en protección específica a aplicaciones instaladas en los servidores, análisis preventivo de amenazas en el core de la red y detección lógica de intrusos bajo conductas anormales al tratar de ingresar a los sistemas informáticos que se encuentran en línea.

Dentro de esto marco, ha de considerarse la instalación y activación del software blade de siguiente generación IPS Check Point para la simulación planteada en esta tesis, por lo que se acude al ejemplo de la figura 2.20 para indicar brevemente las diferentes opciones que presenta esta herramienta de defensa virtual activada en el appliance: en la sección a se observa una visión global de varias características que posee el modulo virtual de sistema de prevención de intrusos, como gateways donde está instalado el software blade en cuestión, las diferentes

protecciones y severidades que soporta el blade activado, la protección geográfica detallando el país donde se origina el ataque, excepciones para filtrar direcciones de red licitas y conocidas que no ocasionarían problemas al momento de ingresar a la red de datos, y las actualizaciones en línea de las firmas del IPS; en la sección b se aprecia una lista de los perfiles configurados en el IPS en un gateway determinado y en la sección c se observa el estatus de seguridad de la red, segmentado en niveles bajos, medios altos y críticos, detallando el número de eventos manejados por el IPS diarios, semanales y mensuales.

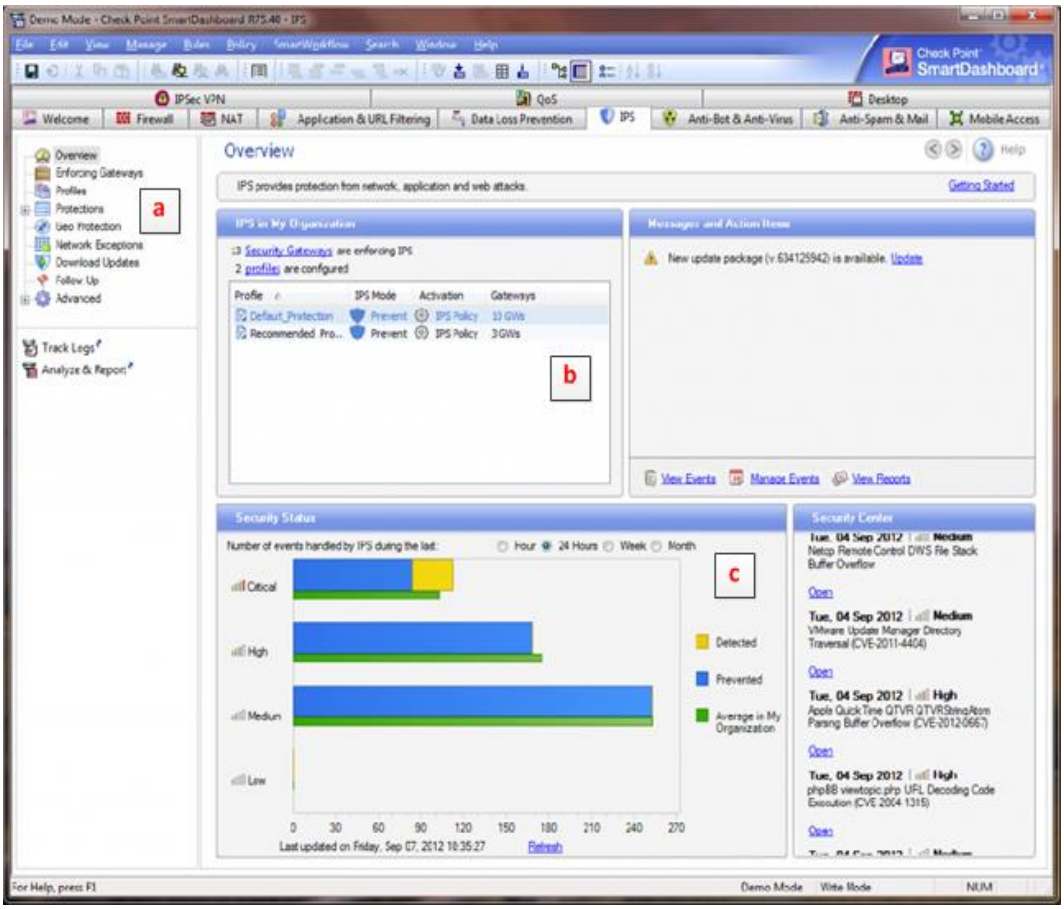


Figura 2. 20: Consola de administración del IPS Check Point
Elaborada por: El Autor.

En el siguiente capítulo se plantea el diseño de la red MPLS con su respectivo perímetro de seguridad lógica empleando el firewall CheckPoint, que protegerá la granja de servidores de un proveedor de servicios de internet.

Capítulo 3: Diseño del perímetro de seguridad lógica empleando nueva generación de firewalls en una red IP-MPLS

En el presente capítulo se analiza la situación actual del proveedor de internet en temas de seguridad informática, también se presenta una propuesta técnica factible para evitar ataques lógicos a la granja de servidores del ISP.

3.1. Análisis de la situación actual del proveedor de servicios de internet

El proveedor de internet posee una red IP-MPLS escalable y de fácil administración, ofreciendo servicios de voz, video y datos a todos sus clientes corporativos y residenciales en la ciudad de Guayaquil y Quito, interconectando los nodos de estas ciudades mediante enlaces de fibra óptica con el core del ISP. El diseño de red del proveedor de internet se sustenta en el nivel jerárquico que comprende las tres capas: núcleo, distribución y acceso; la primera es el core de la red, se encarga de conmutar el trafico lo más rápido posible para transportar grandes volúmenes de bits de manera confiable y veloz, la capa de distribución tiene como función principal proveer enrutamiento, filtrado de datos y determina que paquetes deben llegar al núcleo de la red, y la de acceso es la más cercana al usuario (Jiménez & Reuter, 2013).

3.1.1. Equipos de comunicación distribuidos por jerarquía de red del ISP

A continuación se detalla el equipamiento instalado por el proveedor de internet, ordenado en el nivel jerárquico de red:

Capa de núcleo o core de la red del ISP: Está constituido por los siguientes equipos de comunicación:

a) 1 router Cisco del modelo 7200 VXR, con un sistema operativo IOS c7200-advipservicesk9_li-mz.150-1.M.image, 512 MB de memoria RAM, 4 interfaces gigabit Ethernet (conectadas hacia el router reflector, router core,

router de distribución de Guayaquil y router de distribución de Quito); este equipo cumple las funciones de router P (provider) o LSR en la red MPLS.

b) 1 router Cisco del modelo 7200 VXR, con un sistema operativo IOS c7200-advipservicesk9_li-mz.150-1.M.image, 512 MB de memoria RAM, 3 interfaces gigabit Ethernet (conectadas hacia el router P, al router del proveedor de internet y al switch de core); este equipo cumple las funciones de router PE (provider edge) o ELSR en el core de la red MPLS.
c) 1 router Cisco del modelo 7200 VXR, con un sistema operativo IOS c7200-advipservicesk9_li-mz.150-1.M.image, 512 MB de memoria RAM, 1 interfaz gigabit Ethernet (conectadas hacia el router P); este equipo cumple las funciones de router reflector en la red MPLS, permitiendo concentrar y reflejar las rutas aprendidas en todos los routers clientes de la red MPLS.
d) 1 switch Cisco core del modelo 3650 de 48 puertos gigabit Ethernet, con un sistema operativo IOS-XE cat3k_caa-universalk9, 512 MB de memoria RAM, una interfaz gigabit Ethernet de cobre está conectado al router PE, y otras interfaces van a la granja de servidores del ISP.
e) El proveedor de internet posee servidores de correo electrónico, DNS, FTP y gestión de la red en su granja de servidores, estos equipos se comunican con las PC's de los clientes tanto internos como externos del ISP.

Capa de distribución: La red de distribución del ISP se encuentra dividida en nodos ubicados en Guayaquil y Quito, y se compone de los siguientes dispositivos en cada uno de los nodos:

a) 1 router Cisco del modelo 7200 VXR, con un sistema operativo IOS c7200-advipservicesk9_li-mz.150-1.M.image, 512 MB de memoria RAM, 2 interfaces gigabit Ethernet (conectadas hacia el router P del core, y al switch del nodo); este equipo cumple las funciones de router PE (provider edge) o ELSR en la red MPLS de distribución del ISP.
b) 1 switch Cisco core del modelo 3650 de 48 puertos gigabit Ethernet, con un sistema operativo IOS-XE cat3k_caa-universalk9, 512 MB de memoria RAM, una interfaz gigabit Ethernet de cobre está conectado al router PE del

nodo, y otra interface de fibra óptica va directamente a las oficinas del cliente del proveedor de internet.

Capa de acceso: Los siguientes equipos de comunicación integran la red de acceso del ISP:

a) 1 router Cisco del modelo 7200 VXR, con un sistema operativo IOS c7200-advipservicesk9_li-mz.150-1.M.image, 512 MB de memoria RAM, 2 interfaces gigabit Ethernet (una interfaz va hacia el switch del nodo más cercano, otra al switch dentro de las oficinas del cliente); este equipo cumple las funciones de router CE (costumer edge) en la red IP MPLS.
b) 1 switch Cisco en capa 2 que se utiliza para la conexión con la red LAN en las oficinas del cliente.

3.1.2. Protocolos de enrutamiento establecidos en la red IP MPLS del ISP

Existen varios protocolos de enrutamiento configurados en la red IP MPLS del proveedor, los cuales se detalla a continuación:

a) En los routers P, PE y router reflector de la red, está configurado el protocolo LDP para generar la distribución de las etiquetas en MPLS.
b) Se establece el protocolo OSPF para la comunicación entre el router reflector, PE core y router PE de los nodos con el router P1 core, en el área 0 conocida como backbone.
c) Se tiene configurado una sesión BGP entre los routers PE de los nodos con el router reflector, el objetivo de esta configuración es reflejar y aprender las rutas deseadas con un solo router (router reflector), evitando así el full mesh.
d) En los routers PE de los nodos, están configuradas rutas estáticas para alcanzar la red LAN de las oficinas del cliente, esta ruta estática está configurada con su respectiva VRF.
e) En los routers CE de las oficinas del cliente, existe una ruta por default hacia la dirección IP de la interfaz del router PE del nodo, así, cualquier dirección

IP destino solicitada por la PC del cliente será enrutado hacia el router PE del nodo más cercano al usuario.

3.1.3. Direccionamiento IP administrado por el proveedor de internet

En la tabla 3.1 se detalla el direccionamiento ip que utiliza el ISP en su red MPLS

Tabla 3. 1: Direccionamiento IP administrado por el proveedor de internet

EQUIPO ORIGEN	INTERFAZ ORIGEN	DIRECCION IPORIGEN	EQUIPO DESTINO	INTERFAZ DESTINO	DIRECCION IP DESTINO
ROUTER P01 CORE	G1/0	172.20.0.1/30	PE01_GYE	G1/0	172.20.0.2/30
ROUTER P01 CORE	G2/0	172.30.0.1/30	PE01_UIO	G1/0	172.30.0.2/30
ROUTER P01 CORE	G3/0	172.0.0.1/30	ROUTER REFLECTOR	G1/0	172.0.0.2/30
ROUTER P01 CORE	G4/0	172.10.0.1/30	PE_CORE	G1/0	172.10.0.2/30
ROUTER P01 CORE	Loopback0	9.9.9.9			
PE_CORE	G3/0	190.30.20.1/30	SALIDA A INTERNET		
PE_CORE	G2/0	10.128.10.1/24	HACIA SERVIDORES		
PE_CORE	Loopback0	11.11.11.11			
ROUTER REFLECTOR	Loopback0	10.10.10.10			
PE01_GYE	Loopback0	12.12.12.12			
PE01_GYE	G2/0.100	172.16.10.1/30	ROUTER_CLIENTE GYE	G0/0	172.16.10.2/30
PE01_UIO	Loopback0	13.13.13.13			
PE01_UIO	G2/0.100	172.16.20.1/30	ROUTER_CLIENTE UIO	G0/0	172.16.20.2/30
ROUTER_CLIENT E GYE	G1/0	192.168.10.1/24	RED LAN GYE		
ROUTER_CLIENT E UIO	G1/0	192.168.20.1/24	RED LAN UIO		
SERVIDOR DNS	G0/0	200.124.255.1/24	HACIA ROUTER PE_CORE		
SERVIDOR FTP	G0/0	200.125.255.2/24	HACIA ROUTER PE_CORE		

Elaborada por: El Autor.

3.1.4. Aplicaciones de MPLS ofrecidas por el ISP

Una de las aplicaciones de MPLS empleada por el proveedor de internet es la configuración realizada en los routers para VPN's en capa 3, por lo que, en los routers PE de los nodos, existe una configuración de VRF con sus respectivos

route distinguisher, import y export, para que las oficinas de los clientes en Guayaquil alcancen la red LAN de las sucursales en la ciudad de Quito; el protocolo de comunicación empleado para estas VRF's es MP-BGP.

3.1.5. Vulnerabilidades detectadas en el core de la red IP MPLS del ISP

La granja de servidores del ISP carece de un perímetro de seguridad lógica protegido por firewalls e IPS de última generación para sus equipos de comunicación, siendo así, estos servidores se encuentran vulnerables a hackers y crackers que buscarían alterar el desempeño de los equipos; estos ciber ataques no solo se originarían dentro de la red IP MPLS del proveedor, también serían víctimas de ataques externos desde cualquier parte del planeta, ya que los servidores tienen direccionamiento IP público para que sean publicados por protocolos de enrutamiento al mundo entero. En la figura 3.1 se observa el diagrama general de la red IP MPLS del proveedor de internet, con su respectivo núcleo, red de distribución en Guayaquil y Quito y la red de acceso para los clientes residenciales y corporativos.

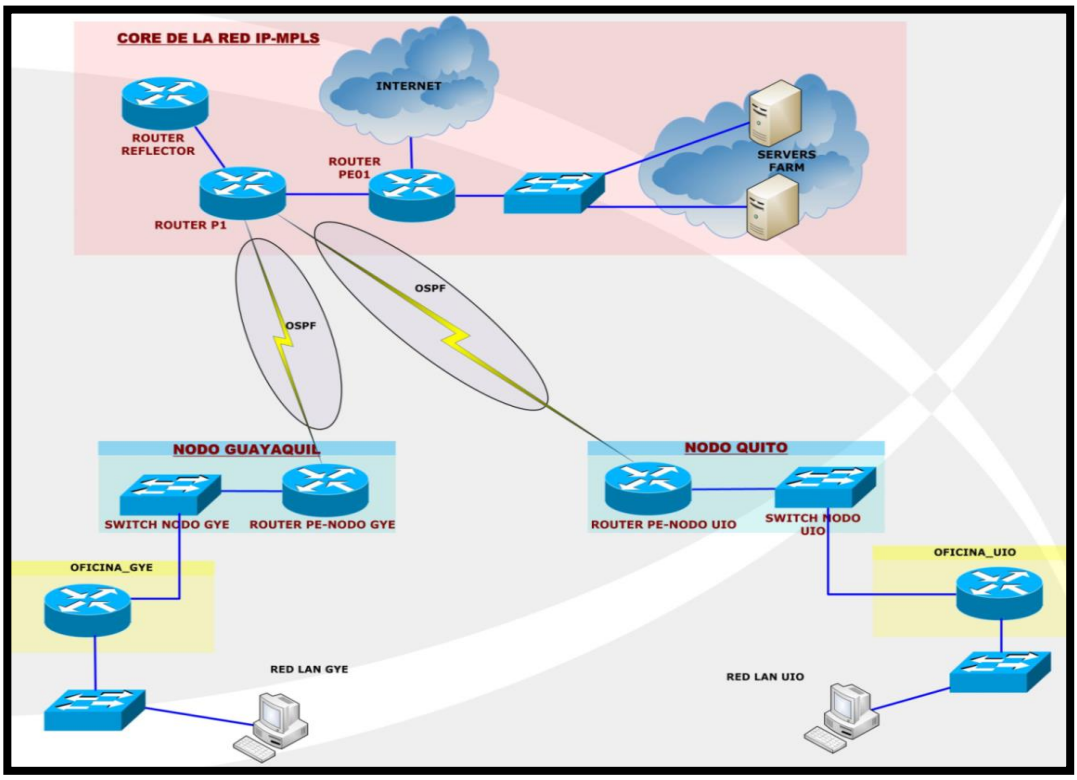


Figura 3. 1: Diagrama general de la red IP-MPLS del ISP
Elaborada por: El Autor.

3.2. Propuesta de la solución a implementar en la granja de servidores del proveedor de servicios de internet

Ante la vulnerabilidad encontrada en el core de la red del ISP, se propone una solución segura, escalable y amigable para mantener un ambiente de seguridad en los equipos de comunicación de la empresa; la cual consistiría en la instalación de un firewall de última generación de marca CheckPoint, con diferentes módulos virtuales (como el IPS) que permitiría proteger los servidores del ISP de diferentes ataques lógicos tanto internos como externos a la red IP MPLS.

3.2.1 Justificación para la adquisición del firewall Check Point

Para acreditar el desempeño de firewalls de siguiente generación en cuestiones de seguridad lógica de redes de datos de las empresas, se acude al reporte anual de la compañía Gartner (prestigiosa empresa que se dedica a la investigación de tecnologías de información a nivel mundial con sede en Estados Unidos), que indica las fortalezas y debilidades de distintos proveedores de firewalls de última generación. Los equipos de marca Check Point son los más solicitados por clientes que buscan usar este tipo de tecnologías con nuevas características para sus implementaciones complejas o en busca de alta seguridad; su amplio portafolio de servicios incluye un módulo de firewall robusto para requerimientos de sistemas de control industrial, opciones de software que proporciona informes detallados para muchos estándares de cumplimiento, posee información detallada sobre las amenazas en la red y gestión de políticas del firewall (Hils, D'Hoinne, Kaur, & Young, 2016)

Cuadrante mágico de Gartner: Este cuadrante es muy considerado por el mercado de las IT (Information Technology), por lo que se lo menciona en las investigaciones realizadas para firewalls de siguiente generación; este cuadrante representa, de una manera elegante y sencilla, una matriz de competitividad entre varios proveedores de IT. El eje X consiste en la capacidad visionaria que posee la compañía, como conocimientos del mercado actual, tácticas de marketing y si sus productos se ajustan a la necesidad de los clientes; el eje Y se fundamenta en la

capacidad de desarrollar y comercializar sus productos en el mercado, como capacidad funcional del equipo, costos del producto, licenciamiento y soluciones a futuro que implicarían actualización de dispositivos. El cuadrante mágico está separado en 4 cuadrantes: líderes, retadores, visionarios y jugadores de nicho; en líderes están las empresas mejores calificadas, ya que gozan de excelente salud como compañía y obtuvieron el mayor puntaje en capacidad de visión, los retadores no poseen una buena orientación en dirección de mercados pero tienen alta capacidad de ejecución, los visionarios son empresas con un alto índice de visión de mercado pero poseen baja capacidad de ejecución, y en los jugadores de nicho residen compañías menos favorables, pero no significa que sus soluciones sean de mala calidad. Según el cuadrante mágico de la figura 3.2, Check Point marca el liderazgo en firewalls de última generación, ya que se ubica en el cuadrante de líderes, con un elevado índice de capacidad de visión y altos niveles de capacidad de desarrollo de sus productos en el mercado.

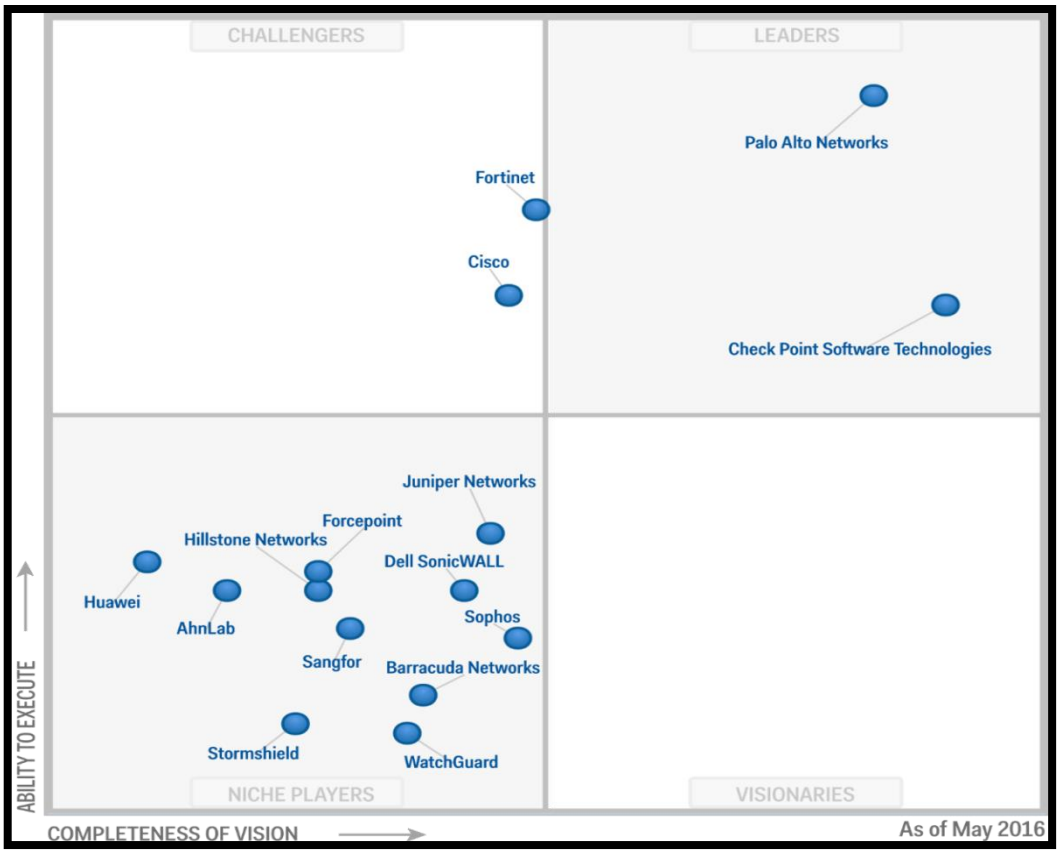


Figura 3. 2: Cuadrante mágico de la compañía Gartner para firewalls de última generación
Fuente: (Hils, D'Hoinne, Kaur, & Young, 2016)

3.2.2 Características técnicas y sistema operativo del equipo

Se sugiere implementar la arquitectura distribuida en equipos Check Point para proteger la granja de servidores del ISP, así, el security manager (servidor de gestión) estaría separado físicamente del security gateway (firewall), logrando tener administración del equipo en los escenarios que el firewall pierda conectividad con la red de datos. El firewall a instalar en el core de la red es un equipo Check Point modelo 12600, las características técnicas del equipo se detallan en la tabla 3.2

Tabla 3. 2: Características técnicas del firewall Check Point 12600

CARACTERISTICAS TECNICAS DEL FIREWALL CHECKPOINT 12600	
Firewall throughput	30 Gbps
Conexiones por segundo	130000
Sesiones concurrentes	2.5M/5.0M[2]
IPS throughput	6 Gbps
Direccionamiento	IPv4, IPv6
Interfaces vlan	1024
Alta disponibilidad	Activo/Activo
	Activo/Pasivo
Interfaces fisicas	14 interfaces 10/100/1000 Base-T port card
	1 puerto consola
Memoria RAM	6 / 12 GB
Almacenamiento	2 - 500 GB RAID
Requerimientos de energia	100-240 v AC; 60 Hz
	220 W maximo consumo de potencia
Redundancia de fuente de poder	Si
Dimensiones	2 UR (unidad de rack)
	17.24 x 22.13 x 3.46 in
Peso	23.4 Kg
Temperatura	0 a 40 grados centigrados

Fuente: **(Check Point Company, 2016)**

Se ilustran en las figuras 3.3 y 3.4 fotografías reales de la vista frontal y posterior del firewall Check Point 12600, se observa las interfaces de cobre a 1000 mbps y las fuentes de poder redundantes debidamente conectadas al equipo. La creación de políticas, redes, grupos, objetos, Nat, visor de eventos, exporte de reporteria, visor de logs, son administrados desde el security manager; el sistema operativo instalado tanto para el security manager como para el appliance firewall es GAIA R77 edition 64-bit, con la versión del kernel 2.6.18-92cpx86_64; la gestión total y

aplicación de políticas para el firewalls Check Point, se las realiza mediante el software Smart Dashboard.

Figura 3. 3: Vista frontal firewall Check Point 12600
Elaborada por: El Autor.

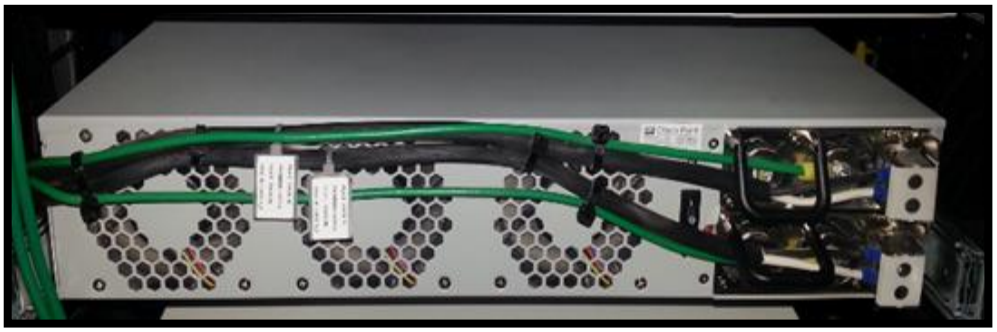


Figura 3. 4: Vista posterior firewall Check Point 12600
Elaborada por: El Autor.

3.2.3 Diseño de la solución recomendada en el core de la red del ISP

A continuación se describe el diseño a implementar bajo la arquitectura Check Point en la granja de servidores del proveedor de internet, ilustrado en la figura 3.5

a) Todos los servidores de comunicación del ISP deberán estar conectados al switch de servidores (con interfaces 10/100/1000 base-T), en el cual se deberán configurar correctamente las VLAN de comunicación en modo acceso y troncal, dependiendo del tipo de conexión.

b) Una interfaz física del firewall (10/100/1000 base-T), se conectará a una interfaz del switch de servidores, la interfaz del firewall tendrá una dirección IP que sería el default gateway de los servidores del proveedor de internet; esta es la interfaz interna.

c) Una segunda interfaz física del firewall (10/100/1000 base-T), se conectará a una interfaz del switch core, esta interfaz deberá poseer un direccionamiento IP privado, y se conoce como interfaz externa.

d) Una interfaz física del server manager (10/100/1000 base-T) se conectará a una interfaz del switch core para lograr tener gestión del firewall; tanto el direccionamiento IP del server manager como el del firewall deberían estar en el mismo segmento de red para lograr una correcta comunicación entre dispositivos.

e) Una interfaz física del switch core (10/100/1000 base-T) se conectará a una interfaz de cobre del router PE core para lograr el correcto enrutamiento en la red IP MPLS del proveedor de internet.

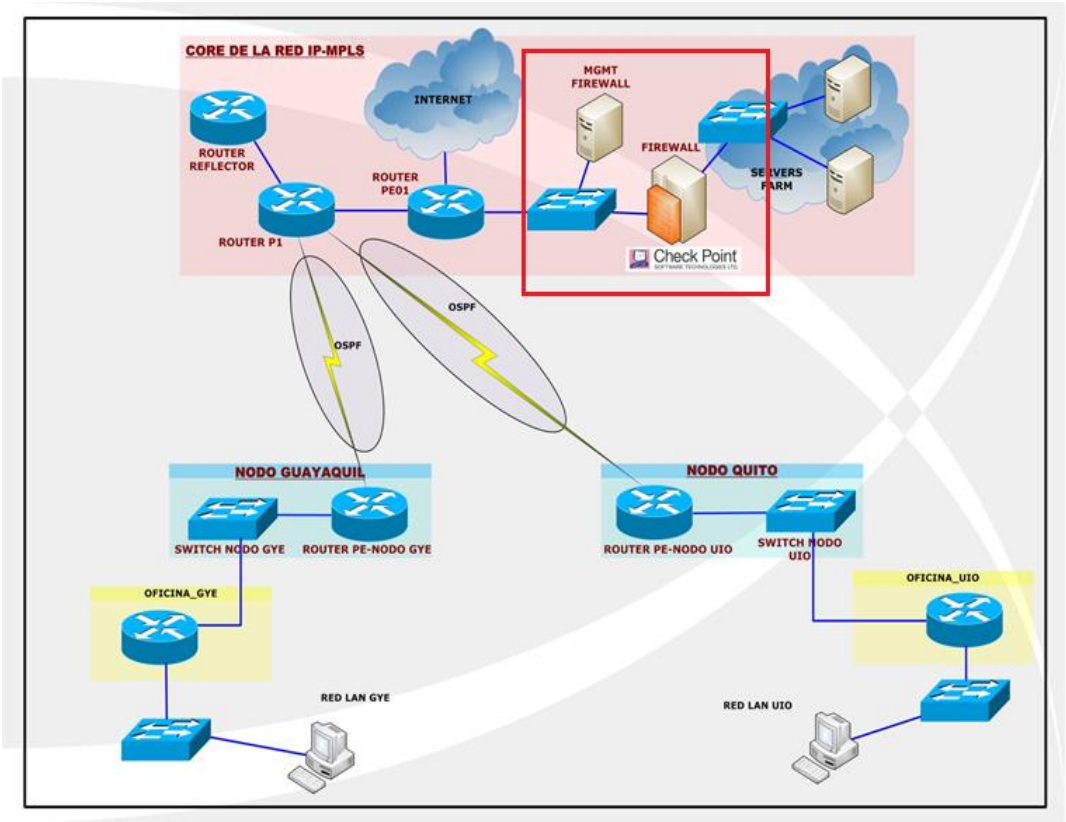


Figura 3. 5: Diagrama sugerido para establecer un perímetro de seguridad lógica en la granja de servidores del ISP
Elaborada por: El Autor.

3.3. Configuración de los equipos de comunicación y seguridad de datos

Parte de la solución de seguridad perimetral establecida en la granja de servidores del proveedor de internet, consiste en realizar la configuración detallada en cada uno de los equipos y servidores de comunicación de la red IP MPLS; se sugiere observar el grafico del anexo # 1 de este documento, en el que se ilustra el diseño y las interfaces implicadas en la configuración realizada en los equipos.

3.3.1 Configuración de routers y switch de la red IP MPLS

Se describe la configuración de los routers y switches en el core de la red MPLS

Router P01 Core:

a) Configuración del hostname y habilitación del protocolo LDP en el equipo:

```
Router# configure terminal
Router(config)# hostname P01
P01(config)# mpls label protocol ldp
```

b) Direccionamiento IP de las interfaces, descripción y habilitación de MPLS en cada una de ellas:

```
P01# configure terminal
P01(config)# interface Loopback0
P01(config-if)# ip address 9.9.9.9 255.255.255.252
P01(config-if)#  exit
P01(config)# mpls ldp router-id Loopback0
P01(config)# interface GigabitEthernet1/0
P01(config-if)#  description HACIA_PE_01-GYE
P01(config-if)#  ip address 172.20.0.1 255.255.255.252
P01(config-if)#  negotiation auto
P01(config-if)#  mpls ip
P01(config-if)#  exit
P01(config)# interface GigabitEthernet2/0
P01(config-if)# description HACIA_PE_01-UIO
P01(config-if)# ip address 172.30.0.1 255.255.255.252
P01(config-if)# negotiation auto
```

```
PO1(config-if)# mpls ip
PO1(config-if)#  exit
PO1(config)# interface GigabitEthernet3/0
PO1(config-if)# description HACIA_ROUTER_REFLECTOR
PO1(config-if)# ip address 172.0.0.1 255.255.255.252
PO1(config-if)# negotiation auto
PO1(config-if)# mpls ip
PO1(config-if)#  exit
PO1(config)# interface GigabitEthernet4/0
PO1(config-if)# description HACIA_PE_CORE
PO1(config-if)#    ip    address    172.10.0.1    255.255.255.252
PO1(config-if)# negotiation auto
PO1(config-if)# mpls ip
PO1(config-if)#  exit
```

c) Establecimiento del protocolo OSPF para las redes hacia los routers PE de los nodos y routers de core:

```
PO1(config)# router ospf 1
PO1(config-router)# log-adjacency-changes
PO1(config-router)# network 9.9.9.9 0.0.0.0 area 0
PO1(config-router)# network 172.0.0.0 0.0.0.3 area 0
PO1(config-router)# network 172.10.0.0 0.0.0.3 area 0
PO1(config-router)#  network 172.20.0.0 0.0.0.3 area 0
PO1(config-router)# network 172.30.0.0 0.0.0.3 area 0
PO1(config-router)# exit
```

d) Guardar los cambios en el equipo:

```
PO1(config)# exit
PO1# write
```

Router PE01 Core:

a) Configuración del hostname y habilitación del protocolo LDP en el equipo:

```
Router# configure terminal
Router(config)# hostname PE_CORE
PE_CORE (config)# mpls label protocol ldp
```

b) Direccionamiento IP de las interfaces, descripción y habilitación de MPLS en cada una de ellas:

```
PE_CORE(config)# interface Loopback0
PE_CORE(config-if)#  ip address 11.11.11.11 255.255.255.255
PE_CORE(config-if)#  exit
PE_CORE(config)# mpls ldp router-id Loopback0
PE_CORE(config)# interface GigabitEthernet1/0
PE_CORE(config-if)# description HACIA_ROUTER P01
PE_CORE(config-if)#  ip address 172.10.0.2 255.255.255.252
PE_CORE(config-if)#  negotiation auto
PE_CORE(config-if)#  mpls ip
PE_CORE(config-if)#  exit
PE_CORE(config)# interface GigabitEthernet2/0
PE_CORE(config-if)#  description HACIA_FIREWALL-CHECKPOINT
PE_CORE(config-if)#  ip vrf forwarding INTERNET
PE_CORE(config-if)#  ip address 10.128.10.1 255.255.255.252
PE_CORE(config-if)#  negotiation auto
PE_CORE(config-if)#  exit
PE_CORE(config)# interface GigabitEthernet3/0
PE_CORE(config-if)# description SALIDA A INTERNET
PE_CORE(config-if)#  ip vrf forwarding INTERNET
PE_CORE(config-if)#  ip address 190.30.20.1 255.255.255.252
PE_CORE(config-if)#  negotiation auto
PE_CORE(config-if)#  exit
```

c) Configuración de protocolos de enrutamiento OSPF (comunicación entre P01 y PE_CORE), BGP (establecimiento de la sesión BGP con el router reflector):

```
PE_CORE(config)# router ospf 1
PE_CORE(config-router)# log-adjacency-changes
PE_CORE(config-router)# network 11.11.11.11 0.0.0.0 area 0
PE_CORE(config-router)# network 172.10.0.0 0.0.0.3 area 0
PE_CORE(config-if)#  exit
PE_CORE(config)# router bgp 65000
PE_CORE(config-router)# no bgp default ipv4-unicast
PE_CORE(config-router)# bgp log-neighbor-changes
PE_CORE(config-router)# neighbor 10.10.10.10 remote-as 65000
PE_CORE(config-router)# neighbor 10.10.10.10 update-source Loopback0
PE_CORE(config-router)# address-family ipv4
PE_CORE(config-router-af)#  no synchronization
PE_CORE(config-router-af)# neighbor 10.10.10.10 activate
```

```
PE_CORE(config-router-af)# no auto-summary
PE_CORE(config-router-af)# exit-address-family
PE_CORE(config-router)# address-family vpnv4
PE_CORE(config-router-af)# neighbor 10.10.10.10 activate
PE_CORE(config-router-af)# neighbor 10.10.10.10 send-community
extended
PE_CORE(config-router-af)#  exit-address-family
```

d) Configuración de la VRF INTERNET, exportando e importando en la red MPLS las rutas aprendidas en los routers PE01_GYE y PE02_UIO; y configuración de la ruta estática para alcanzar la granja de servidores del ISP:

```
PE_CORE(config)# ip vrf INTERNET
PE_CORE(config-vrf)#  rd 3:100
PE_CORE(config-vrf)# route-target export 2:200
PE_CORE(config-vrf)# route-target import 2:200
PE_CORE(config-vrf)# route-target import 1:100
PE_CORE(config-vrf)# exit
PE_CORE(config)# router bgp 65000
PE_CORE(config-router)#  address-family ipv4 vrf INTERNET
PE_CORE(config-router-af)#  no synchronization
PE_CORE(config-router-af)#  redistribute connected
PE_CORE(config-router-af)#  redistribute static
PE_CORE(config-router-af)#  exit-address-family
PE_CORE(config-router)# exit
PE_CORE(config)#  ip route vrf INTERNET 200.124.255.0
255.255.255.0 10.128.10.2
PE_CORE(config)# exit
```

e) Guardar los cambios en el equipo:

```
PE_CORE# write
```

Router Reflector:

a) Configuración del hostname y habilitación del protocolo LDP en el equipo:

```
Router# configure terminal
Router(config)# hostname ROUTER_REFLECTOR
ROUTER_REFLECTOR(config)# mpls label protocol ldp
```

b) Direccionamiento IP de las interfaces, descripción y habilitación de MPLS en cada una de ellas:

```
ROUTER_REFLECTOR(config)# interface Loopback0
ROUTER_REFLECTOR(config-if)#ip address10.10.10.10 255.255.255.255
ROUTER_REFLECTOR(config-if)# exit
ROUTER_REFLECTOR(config)# mpls ldp router-id Loopback0
ROUTER_REFLECTOR(config)# interface GigabitEthernet1/0
ROUTER_REFLECTOR(config-if)# ip address 172.0.0.2 255.255.255.252
ROUTER_REFLECTOR(config-if)# description HACIA_P01
ROUTER_REFLECTOR(config-if)# negotiation auto
ROUTER_REFLECTOR(config-if)# mpls ip
ROUTER_REFLECTOR(config-if)# exit
```

c) Configuración de protocolos de enrutamiento OSPF (comunicación entre router reflector y P01), BGP (establecimiento de la sesión BGP con los router PE de la red MPLS):

```
ROUTER_REFLECTOR(config)# router ospf 1
ROUTER_REFLECTOR(config-router)# log-adjacency-changes
ROUTER_REFLECTOR(config-router)# network 10.10.10.10 0.0.0.0area0
ROUTER_REFLECTOR(config-router)# network 172.0.0.0 0.0.0.3 area 0
ROUTER_REFLECTOR(config-router)# exit
ROUTER_REFLECTOR(config)# router bgp 65000
ROUTER_REFLECTOR(config-router)# no bgp default ipv4-unicast
ROUTER_REFLECTOR(config-router)# bgp log-neighbor-changes
ROUTER_REFLECTOR(config-router)# neighbor 11.11.11.11remote-as
65000
ROUTER_REFLECTOR(config-router)# neighbor 11.11.11.11 update-
source Loopback0
ROUTER_REFLECTOR(config-router)# neighbor 12.12.12.12   remote-as
65000
ROUTER_REFLECTOR(config-router)# neighbor 12.12.12.12  update-
source Loopback0
ROUTER_REFLECTOR(config-router)# neighbor 13.13.13.13  remote-as
65000
ROUTER_REFLECTOR(config-router)# neighbor 13.13.13.13 update-
source Loopback0
ROUTER_REFLECTOR(config-router)# address-family ipv4
ROUTER_REFLECTOR(config-router-af)#  no
synchronizationROUTER_REFLECTOR(config-router-af)#  neighbor
11.11.11.11  activate
```

```
ROUTER_REFLECTOR(config-router-af)#  neighbor 12.12.12.12
activate
ROUTER_REFLECTOR(config-router-af)#  neighbor 13.13.13.13
activate
ROUTER_REFLECTOR(config-router-af)#  no auto-summary
ROUTER_REFLECTOR(config-router-af)#  exit-address-family
ROUTER_REFLECTOR(config-router)#  address-family vpnv4
ROUTER_REFLECTOR(config-route-af)#  neighbor  11.11.11.11
activate
ROUTER_REFLECTOR(config-router-af)#  neighbor 11.11.11.11 send-
community extended
ROUTER_REFLECTOR(config-router-af)#  neighbor 11.11.11.11 route-
reflector-client
ROUTER_REFLECTOR(config-router-af)#  neighbor 12.12.12.12
activate
ROUTER_REFLECTOR(config-router-af)#  neighbor 12.12.12.12 send-
community extended
ROUTER_REFLECTOR(config-router-af)#  neighbor 12.12.12.12 route-
reflector-client
ROUTER_REFLECTOR(config-router-af)# neighbor 13.13.13.13 activate
ROUTER_REFLECTOR(config-router-af)# neighbor 13.13.13.13 send-
community extended
ROUTER_REFLECTOR(config-router-af)# neighbor 13.13.13.13 route-
reflector-client
ROUTER_REFLECTOR(config-route-af)# exit-address-family
ROUTER_REFLECTOR(config-router)# end
```

d) Guardar los cambios en el equipo:

```
ROUTER_REFLECTOR # write
```

Switch Cisco Core:

a) Configuración del hostname en el switch:

```
Switch# configure terminal
Switch(config)# hostname SWITCH_CORE
SWITCH_CORE(config)#
```

b) Configuración de las interfaces del switch en modo acceso, guardar los cambios:

```
SWITCH_CORE(config)# interface Gi0/1
SWITCH_CORE(config-if)# switchport mode access
SWITCH_CORE(config-if)# interface Gi0/2
SWITCH_CORE(config-if)# switchport mode access
SWITCH_CORE(config-if)# interface Gi0/4
SWITCH_CORE(config-if)# switchport mode access
SWITCH_CORE(config-if)# end
SWITCH_CORE# write
```

Se detalla la configuración de los routers y switches en la red de distribución del ISP

Router PE_01-GYE:

a) Configuración del hostname y habilitación del protocolo LDP en el equipo:

```
Router# configure terminal
Router(config)# hostname PE_01-GYE
PE_01-GYE(config)# mpls label protocol ldp
```

b) Direccionamiento IP de las interfaces, descripción y habilitación de MPLS en cada una de ellas:

```
PE_01-GYE(config)# interface Loopback0
PE_01-GYE(config-if)# ip address 12.12.12.12 255.255.255.255
PE_01-GYE(config-if)# exit
PE_01-GYE(config)# mpls ldp router-id Loopback0
PE_01-GYE(config)# interface GigabitEthernet1/0
PE_01-GYE(config-if)# description HACIA_ROUTER_P1
PE_01-GYE(config-if)# ip address 172.20.0.2 255.255.255.252
PE_01-GYE(config-if)# load-interval 30
PE_01-GYE(config-if)# negotiation auto
PE_01-GYE(config-if)# mpls ip
PE_01-GYE(config-if)# exit
PE_01-GYE(config)# interface GigabitEthernet2/0
PE_01-GYE(config-if)# description HACIA_SWITCH-ACCES0-GYE
PE_01-GYE(config-if)# no ip address
PE_01-GYE(config-if)# load-interval 30
PE_01-GYE(config-if)# negotiation auto
PE_01-GYE(config-if)# exit
PE_01-GYE(config)# interface GigabitEthernet2/0.100
PE_01-GYE(config-if)# description HACIA_OFICINA-MATRIZ
```

```
PE_01-GYE(config-if)# encapsulation dot1Q 100
PE_01-GYE(config-if)# ip vrf forwarding CLIENTE_A
PE_01-GYE(config-if)# ip address 172.16.10.1 255.255.255.252
PE_01-GYE(config-if)# exit
```

c) Configuración de protocolos de enrutamiento OSPF (comunicación entre router PE_01-GYE y P01), BGP (establecimiento de la sesión BGP con el router reflector):

```
PE_01-GYE(config)#  router ospf 1
PE_01-GYE(config-router)# log-adjacency-changes
PE_01-GYE(config-router)# network 12.12.12.12 0.0.0.0  area 0
PE_01-GYE(config-router)# network 172.20.0.0 0.0.0.3  area 0
PE_01-GYE(config-router)# exit
PE_01-GYE(config)# router bgp 65000
PE_01-GYE(config-router)# no bgp default ipv4-unicast
PE_01-GYE(config-router)# bgp log-neighbor-changes
PE_01-GYE(config-router)# neighbor 10.10.10.10 remote-as 65000
PE_01-GYE (config-router)# neighbor 10.10.10.10 update-source Loopback0
PE_01-GYE(config-router)# address-family ipv4
PE_01-GYE(config-router-af)#  no synchronization
PE_01-GYE(config-router-af)# neighbor 10.10.10.10 activate
PE_01-GYE(config-router-af)# no auto-summary
PE_01-GYE(config-router-af)# exit-address-family
PE_01-GYE(config-router)# address-family vpnv4
PE_01-GYE(config-router-af)# neighbor 10.10.10.10 activate
PE_01-GYE(config-router-af)# neighbor 10.10.10.10 send-community
extended
PE_01-GYE(config-router-af)#  exit-address-family
PE_01-GYE(config-router)#
```

d) Configuración de la VRF CLIENTE_A, exportando e importando en la red MPLS las rutas aprendidas en los routers PE_CORE y PE02_UIO; y configuración de la ruta estática para alcanzar la red LAN de la sucursal en Guayaquil:

```
PE_01-GYE(config)# ip vrf CLIENTE_A
PE_01-GYE(config-vrf)#  rd 1:100
PE_01-GYE(config-vrf)# route-target export 1:100
PE_01-GYE(config-vrf)# route-target import 1:100
PE_01-GYE(config-vrf)# route-target import 2:200
PE_01-GYE(config-vrf)# exit
```

```
PE_01-GYE(config)# router bgp 65000
PE_01-GYE(config-router)#  address-family ipv4 vrf CLIENTE_A
PE_01-GYE(config-router-af)#  no synchronization
PE_01-GYE(config-router-af)#  redistribute connected
PE_01-GYE(config-router-af)#  redistribute static
PE_01-GYE(config-router-af)#  exit-address-family
PE_01-GYE (config-router)# exit
PE_01-GYE(config)# ip route vrf CLIENTE_A 192.168.10.0
255.255.255.0 172.16.10.2
```

e) Guardar los cambios en el equipo:

```
PE_01-GYE# write
```

Switch Cisco de distribución Guayaquil:

a) Configuración del hostname en el switch:

```
Switch# configure terminal
Switch(config)# hostname SWITCH_GYE
SWITCH_GYE(config)#
```

b) Creación de la VLAN 100 (VLAN asignada para el cliente en GYE):

```
SWITCH_GYE(config)# vlan 100
SWITCH_GYE(config-vlan)# name CLIENTE_GYE
```

c) Configuración de las interfaces del switch en modo acceso, troncal y guardar cambios en el equipo:

```
SWITCH_GYE(config)# interface Gi0/1
SWITCH_GYE(config-if)# switchport mode trunk
SWITCH_GYE(config-if)# switchport trunk encapsulation dot1q
SWITCH_GYE(config-if)# interface Gi0/2
SWITCH_GYE(config-if)# switchport mode access
SWITCH_GYE(config-if)# switchport access vlan 100
SWITCH_GYE(config-if)# end
SWITCH_GYE# write
```

Router PE_02-UIO:

a) Configuración del hostname y habilitación del protocolo LDP en el equipo:

```
Router# configure terminal
Router(config)# hostname PE_02-UIO
PE_02-UIO(config)# mpls label protocol ldp
```

b) Direccionamiento IP de las interfaces, descripción y habilitación de MPLS en cada una de ellas:

```
PE_02-UIO(config)# interface Loopback0
PE_02-UIO(config-if)# ip address 13.13.13.13 255.255.255.255
PE_02-UIO (config-if)# exit
PE_02-UIO(config)# mpls ldp router-id Loopback0
PE_02-UIO(config)# interface GigabitEthernet1/0
PE_02-UIO(config-if)# description HACIA_ROUTER_P1
PE_02-UIO(config-if)# ip address 172.30.0.2 255.255.255.252
PE_02-UIO(config-if)# load-interval 30
PE_02-UIO(config-if)# negotiation auto
PE_02-UIO(config-if)# mpls ip
PE_02-UIO(config-if)# exit
PE_02-UIO(config)# interface GigabitEthernet2/0
PE_02-UIO(config-if)# description HACIA_SWITCH-ACCES0-UIO
PE_02-UIO(config-if)# no ip address
PE_02-UIO(config-if)# load-interval 30
PE_02-UIO(config-if)# negotiation auto
PE_02-UIO(config-if)# exit
PE_02-UIO(config)# interface GigabitEthernet2/0.100
PE_02-UIO(config-if)# description HACIA_OFICINA-SUCURS-UIO
PE_02-UIO(config-if)# encapsulation dot1Q 100
PE_02-UIO(config-if)# ip vrf forwarding CLIENTE_A
PE_02-UIO(config-if)# ip address 172.16.20.1 255.255.255.252
PE_02-UIO(config-if)# exit
```

c) Configuración de protocolos de enrutamiento OSPF (comunicación entre router PE_02-UIO y P01), BGP (establecimiento de la sesión BGP con el router reflector):

```
PE_02-UIO(config)#  router ospf 1
PE_02-UIO(config-router)# network 13.13.13.13 0.0.0.0  area 0
```

```
PE_02-UIO(config-router)# network 172.30.0.0 0.0.0.3  area 0
PE_02-UIO(config-router)# exit
PE_02-UIO(config)# router bgp 65000
PE_02-UIO(config-router)# no bgp default ipv4-unicast
PE_02-UIO(config-router)# bgp log-neighbor-changes
PE_02-UIO(config-router)# neighbor 10.10.10.10 remote-as 65000
PE_02-UIO (config-router)# neighbor 10.10.10.10 update-source Loopback0
PE_02-UIO(config-router)# address-family ipv4
PE_02-UIO(config-router-af)#  no synchronization
PE_02-UIO(config-router-af)# neighbor 10.10.10.10 activate
PE_02-UIO(config-router-af)# no auto-summary
PE_02-UIO(config-router-af)# exit-address-family
PE_02-UIO(config-router)# address-family vpnv4
PE_02-UIO(config-router-af)# neighbor 10.10.10.10 activate
PE_02-UIO(config-router-af)# neighbor 10.10.10.10 send-community
extended
PE_02-UIO(config-router-af)#  exit-address-family
```

d) Configuración de la VRF CLIENTE_A, exportando e importando en la red MPLS las rutas aprendidas en los routers PE_CORE y PE01_GYE; y configuración de la ruta estática para alcanzar la red LAN de la sucursal en Quito:

```
PE_02-UIO(config)# ip vrf CLIENTE_A
PE_02-UIO(config-vrf)#  rd 2:100
PE_02-UIO(config-vrf)# route-target export 1:100
PE_02-UIO(config-vrf)# route-target import 1:100
PE_02-UIO(config-vrf)# route-target import 2:200
PE_02-UIO(config-vrf)# exit
PE_02-UIO(config)# router bgp 65000
PE_02-UIO(config-router)#  address-family ipv4 vrf CLIENTE_A
PE_02-UIO(config-router-af)#  no synchronization
PE_02-UIO(config-router-af)#  redistribute connected
PE_02-UIO(config-router-af)#  redistribute static
PE_02-UIO(config-router-af)#  exit-address-family
PE_02-UIO(config-router)# exit
PE_02-UIO(config)# ip route vrf CLIENTE_A 192.168.20.0
255.255.255.0 172.16.20.2
```

e) Guardar los cambios en el equipo:

```
PE_02-UIO# write
```

Switch Cisco de distribución Quito:

a) Configuración del hostname en el switch:

```
Switch# configure terminal
Switch(config)# hostname SWITCH_UIO
SWITCH_UIO(config)#
```

b) Creación de la VLAN 100 (VLAN asignada para el cliente en UIO):

```
SWITCH_UIO(config)# vlan 100
SWITCH_UIO(config-vlan)# name CLIENTE_UIO
SWITCH_UIO(config-vlan)# exit
```

c) Configuración de las interfaces del switch en modo acceso, troncal y guardar cambios en el equipo:

```
SWITCH_UIO(config)# interface Gi0/1
SWITCH_UIO(config-if)# switchport mode trunk
SWITCH_UIO(config-if)# switchport trunk encapsulation dot1q
SWITCH_UIO(config-if)# interface Gi0/2
SWITCH_UIO (config-if)# switchport mode access
SWITCH_UIO(config-if)# switchport access vlan 100
SWITCH_UIO(config-if)# end
SWITCH_GYE# write
```

Se ilustra la configuración de los routers en la red de acceso del proveedor de internet

Router OFICINA_GYE:

a) Configuración del hostname en el equipo:

```
Router# configure terminal
Router(config)# hostname OFICINA_GYE
OFICINA_GYE (config)# exit
```

b) Direccionamiento IP de las interfaces, descripción de las mismas:

```
OFICINA_GYE # configure terminal
OFICINA_GYE (config)# interface GigabitEthernet0/0
OFICINA_GYE (config-if)# description HACIA_PE_01-GYE
OFICINA_GYE (config-if)# ip address 172.16.10.2 255.255.255.252
OFICINA_GYE (config-if)# duplex full
OFICINA_GYE (config-if)# speed 1000
OFICINA_GYE (config-if)# media-type gbic
OFICINA_GYE (config-if)# negotiation auto
OFICINA_GYE (config-if)# exit
OFICINA_GYE (config)# interface GigabitEthernet1/0
OFICINA_GYE (config-if)# description HACIA_RED-LANOFICINA_GYE
OFICINA_GYE (config-if)# ip address 192.168.10.1  255.255.255.0
OFICINA_GYE (config-if)# negotiation auto
OFICINA_GYE (config-if)# exit
```

c) Ruta por defecto para alcanzar cualquier destino por medio del gateway

```
OFICINA_GYE (config)# ip route 0.0.0.0 0.0.0.0 172.16.10.1
OFICINA_GYE (config)# end
```

d) Guardar los cambios en el equipo:

```
OFICINA_GYE# write
```

Router OFICINA_UIO:

a) Configuración del hostname en el equipo:

```
Router# configure terminal
Router(config)# hostname OFICINA_UIO
OFICINA_UIO (config)# exit
```

b) Direccionamiento IP de las interfaces, descripción de las mismas:

```
OFICINA_UIO # configure terminal
OFICINA_UIO (config)# interface GigabitEthernet0/0
OFICINA_UIO (config-if)# description HACIA_PE_02-UIO
OFICINA_UIO (config-if)# ip address 172.16.20.2 255.255.255.252
OFICINA_UIO (config-if)# duplex full
OFICINA_UIO (config-if)# speed 1000
```

```
OFICINA_UIO (config-if)# media-type gbic
OFICINA_UIO (config-if)# negotiation auto
OFICINA_UIO (config-if)# exit
OFICINA_UIO (config)# interface GigabitEthernet1/0
OFICINA_UIO (config-if)# description HACIA_RED-LANOFICINA_UIO
OFICINA_UIO (config-if)# ip address 192.168.20.1  255.255.255.0
OFICINA_UIO (config-if)# negotiation auto
OFICINA_UIO (config-if)# exit
```

c) Ruta por defecto para alcanzar cualquier destino por medio del gateway

```
OFICINA_UIO (config)# ip route 0.0.0.0 0.0.0.0 172.16.20.1
OFICINA_UIO (config)# end
```

d) Guardar los cambios en el equipo:

```
OFICINA_UIO# write
```

En la red de acceso es opcional la instalación de un switch en las oficinas del cliente, depende del requerimiento del mismo.

3.3.2 Configuración del firewall Check Point

Previo a la configuración de los equipos de seguridad informática, se debe definir el direccionamiento IP a utilizar para estos dispositivos; en la tabla 3.3 se detallan los diferentes equipos que conforman el perímetro de seguridad para proteger la granja de servidores del ISP, así como su interfaz y la dirección IP a utilizar.

Tabla 3. 3: Direccionamiento IP asignado a los equipos de seguridad informática

Equipo	Interfaz	Dirección IP
Firewall Check Point	ethernet 0	192.168.33.65/26
Firewall Check Point	ethernet 1	10.128.10.2/30
Firewall Check Point	ethernet 2	200.124.255.254/24
Security manager	ethernet 0	192.168.33.68/26
Server Windows (smart console)	ethernet 0	192.168.33.66/26

Elaborada por: El Autor.

En el anexo # 2 de este documento se detalla la instalación del firewall Check Point, instalación del security manager y la instalación del smart console en máquinas virtuales; a continuación se describe las configuraciones realizadas en el firewall Check Point para proteger la granja de servidores del ISP:

Firewall Check Point:

a) Configuración de las interfaces y ruta por default en el equipo (interfaz gestión eth0, interfaz externa eth1, interfaz interna eth2):

```
gw-001-fwm> set hostname Firewall
Firewall> set interface eth0 state on
Firewall> set interface eth0 auto-negotation on
Firewall> set interface eth0 link-speed 1000M/full
Firewall> set interface eth0 ipv4-address 192.168.33.65 mask-
lengt 26
Firewall> set interface eth1 state on
Firewall> set interface eth1 auto-negotation on
Firewall> set interface eth1 link-speed 1000M/full
Firewall> set interface eth1 ipv4-address 10.128.10.2 mask-lengt
30
Firewall> set interface eth2 state on
Firewall> set interface eth2 auto-negotation on
Firewall> set interface eth2 link-speed 1000M/full
Firewall> set interface eth2 ipv4-address 200.124.255.254
mask-lengt 24

Firewall> set static-route default nexthop gateway address
10.128.10.1 on
Firewall> save config
```

b) Se ingresa al security manager (192.168.33.68/26) mediante el smart dashboard (instalado en el smart console), para realizar las configuraciones necesarias en el equipo: (ver figura 3.6)

Figura 3. 6: SmartDashboard Check Point
Elaborada por: El Autor.

c) Se vincula el security gateway al security manager para tener conectividad entre el firewall y el security manager; como se observa en la figura 3.7, al dar clic derecho en la opción Check Point (dentro de los objetos de red) se selecciona la opción Security Gateway/Management, para agregar el firewall en cuestión.

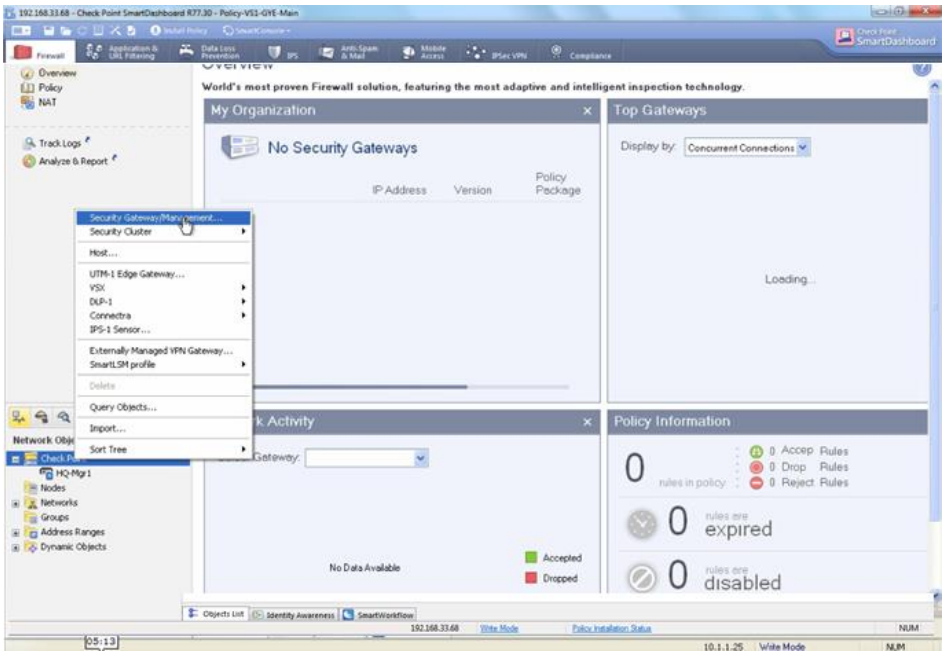


Figura 3. 7: Vinculación entre el security manager y el firewall
Elaborada por: El Autor.

d) Se selecciona la opción classic mode para realizar la configuración del firewall en el security manager, la figura 3.8 muestra la opción a escoger.

e) Se agrega los datos necesarios en las propiedades generales del gateway, mostrado en la figura 3.9; el nombre del equipo: Firewall, ipv4 address: 192.168.33.65, se configura el protocolo SIC dentro de la opción Communication con el mismo password configurado en el momento de la instalación del firewall (el estado del certificado debe indicar *trust established*), se escoge la plataforma de hardware 12000 appliance con la versión R77 del sistema operativo Gaia, se activan los módulos de: Firewall, IPS, y Monitoring que se utilizarán en la simulación propuesta.

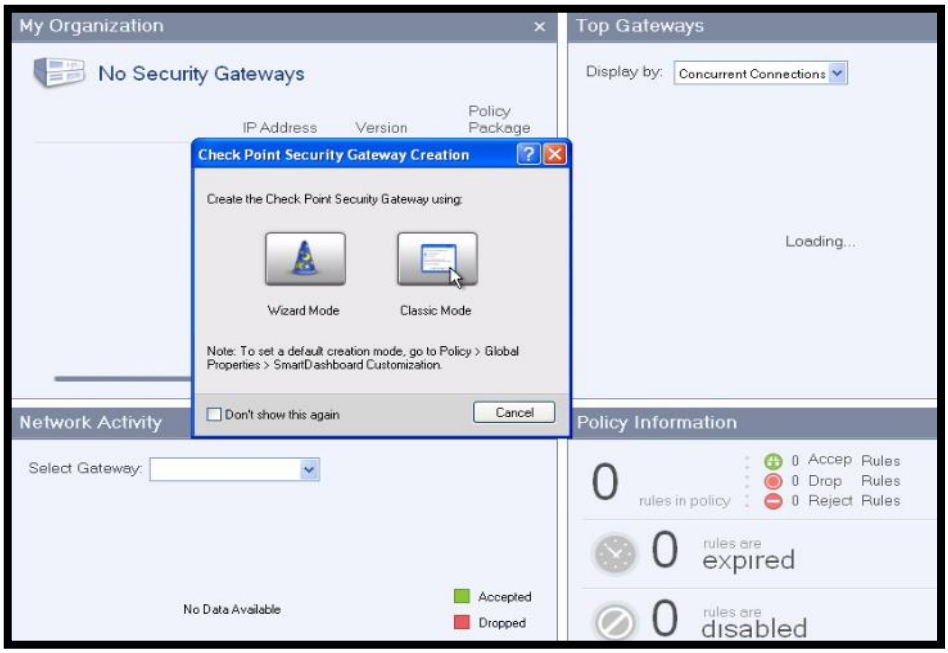


Figura 3. 8: Opción classic mode previo a la configuración del firewall
Elaborada por: El Autor.

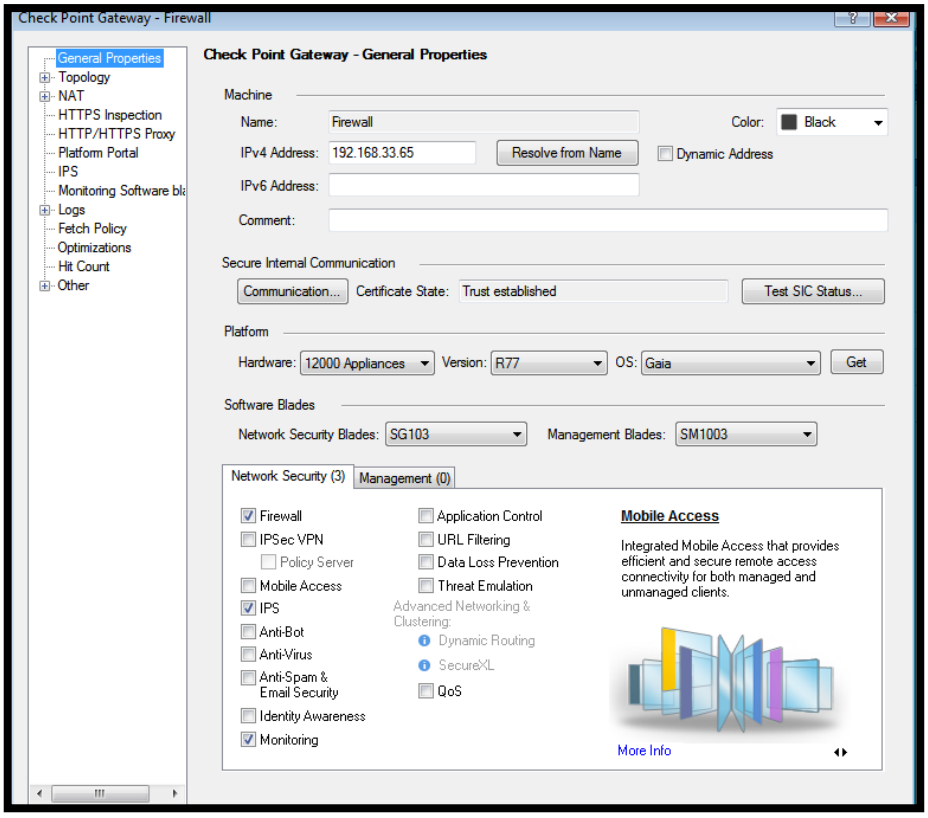


Figura 3. 9: Propiedades generales del gateway
Elaborada por: El Autor.

f) Se selecciona la opción *topology* para obtener las interfaces físicas del firewall previamente configuradas vía comandos, esto se realiza dando un clic en la opción *Get;* estas interfaces se señalan en la figura 3.10.

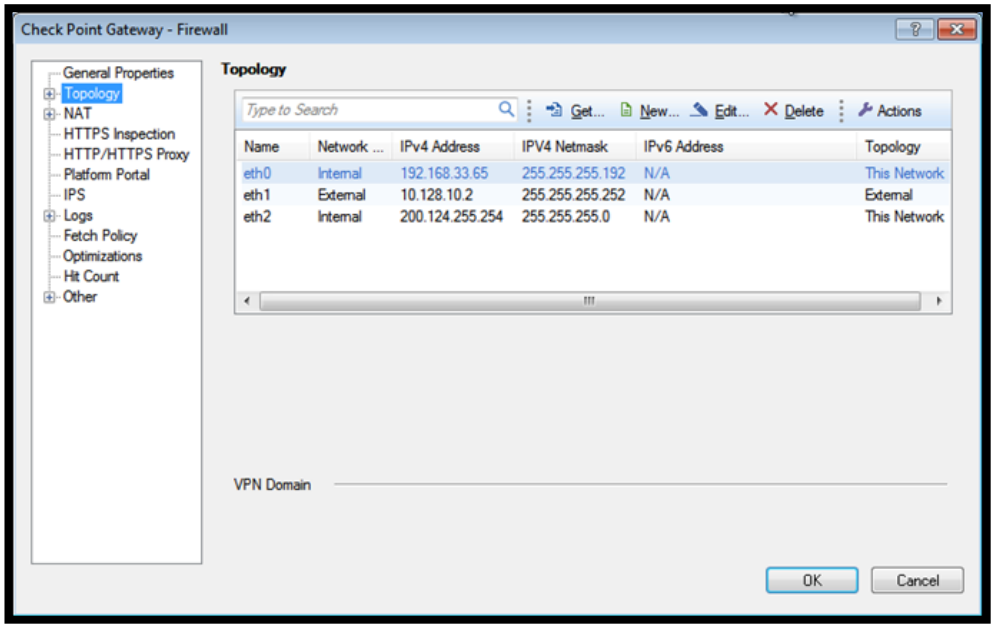


Figura 3. 10: Direccionamiento ip de las interfaces del firewall
Elaborada por: El Autor.

g) Finalmente, en las propiedades globales del dashboard, existen reglas implícitas del firewall, que deben estar habilitadas para el correcto funcionamiento del equipo; la figura 3.11 detalla estas reglas correctamente activadas.

h) Luego de las configuraciones realizadas en el equipo, se muestra en la figura 3.12, una visión global del estado del firewall luego de su implementación, como: actividad de red, dirección IP del gateway, versión instalada en el firewall, información de políticas, número de conexiones concurrentes en el equipo y objetos de red.

La configuración del security manager solo se realiza en el momento de la instalación de la máquina virtual con el sistema operativo GAIA, seleccionando correctamente el tipo de servidor indicado.

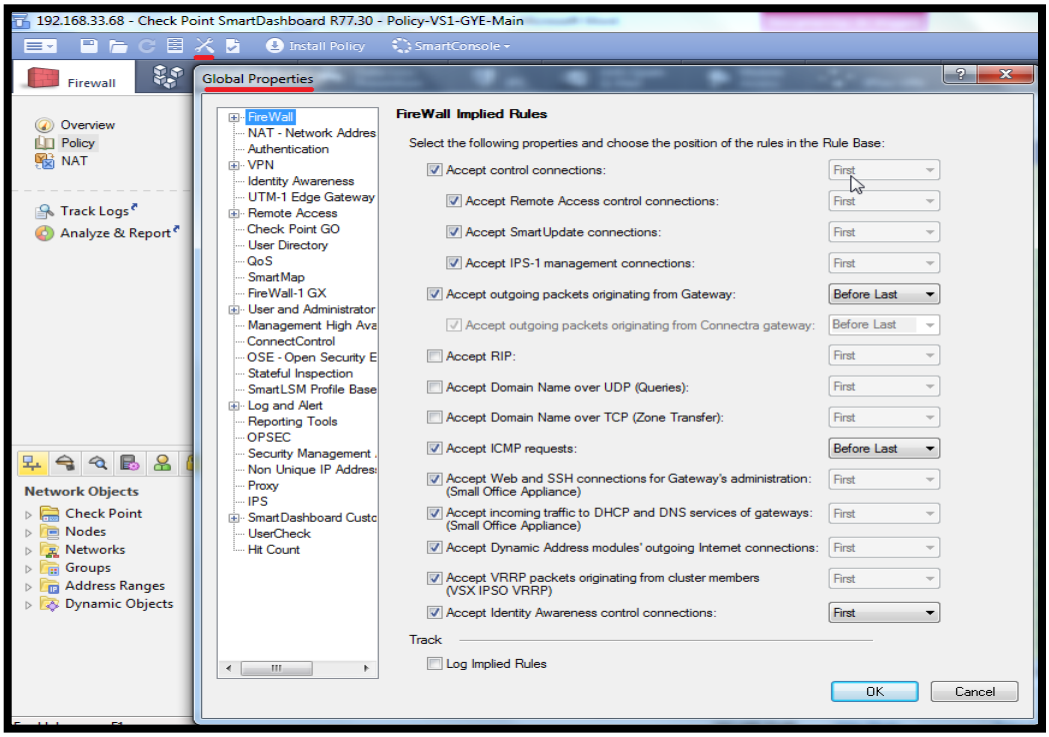


Figura 3. 11: Propiedades globales del gateway
Elaborada por: El Autor.

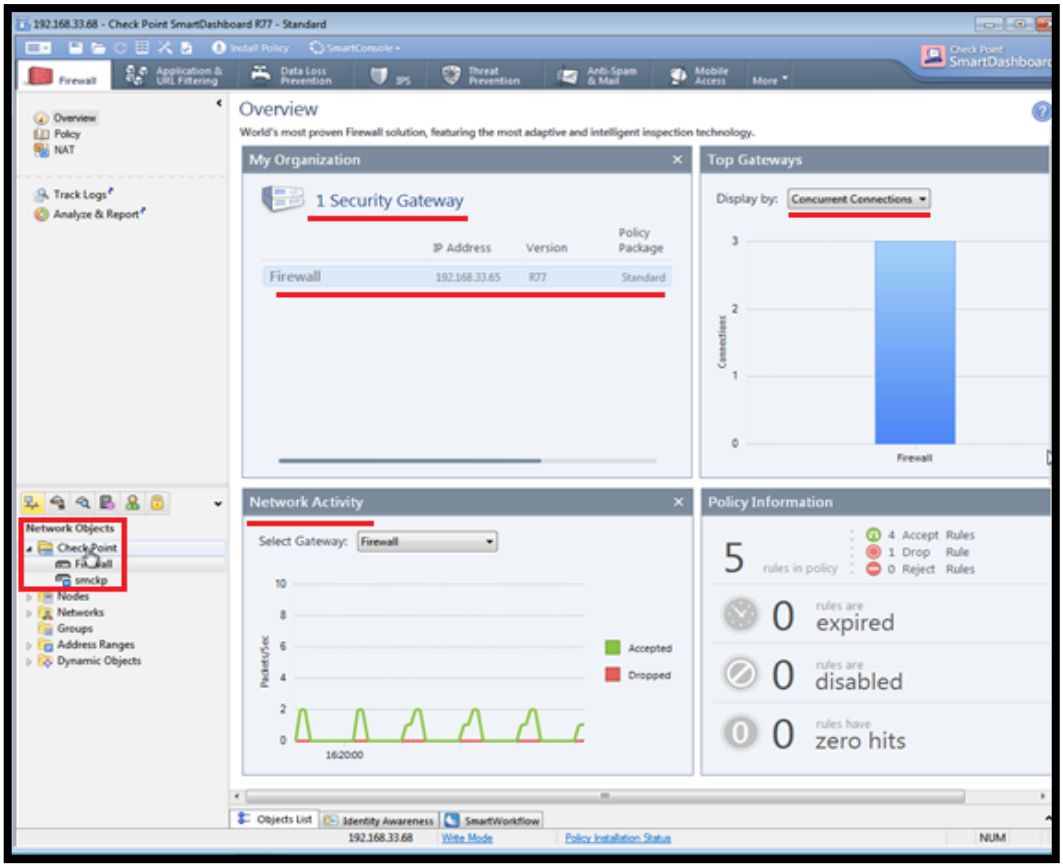


Figura 3. 12: Visión global de la configuración del firewall
Elaborada por: El Autor.

3.3.3 Configuración de un servidor web de pruebas en ambiente Linux

Se plantea la configuración de red y el servicio web en un servidor linux Centos que servirá como servidor de pruebas, puesto que será el objetivo de los ataques informáticos originados por una PC en la red MPLS del proveedor de internet (para efectos de simulación, se subieron a este servidor web Linux, las páginas html de la Espol, Universidad Católica Santiago de Guayaquil y de la red social Facebook)

Servidor Linux Centos:

a) Se ingresa al siguiente directorio donde se almacena la configuración de la tarjeta de red para modificar la dirección IP del servidor linux:

```
[root@localhost pgordillo] # vi /etc/sysconfig/network-scripts/ifcfg-enp0s3
```

b) Se cambia los parámetros de *bootpro, ipaddr, netmask,* dentro del archivo de configuración indicado; en la figura 3.13 se indican los valores a cambiar:

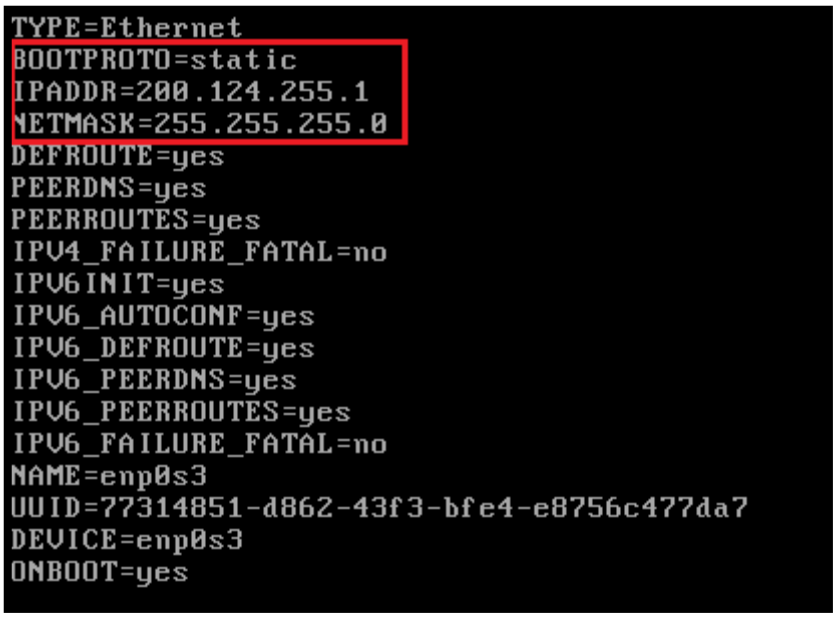


Figura 3. 13: Modificación de la dirección IP del servidor linux
Elaborada por: El Autor.

c) Se modifica la dirección IP del default gateway del servidor en el siguiente directorio:

```
[root@localhost pgordillo] # vi /etc/sysconfig/network
```

d) En la figura 3.14 se observa el valor de la dirección IP a cambiar como default gateway en el archivo de configuración indicado:

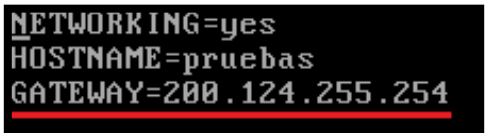


Figura 3. 14: Modificación de la dirección ip del gateway del servidor linux
Elaborada por: El Autor.

e) Se reinician los servicios de red en el servidor linux:

```
[root@localhost pgordillo] # systemctl restart network.service
```

f) Se instala el servicio de SSH para acceder al servidor mediante este protocolo y el servicio HTTPD (que sirve para almacenar las páginas web en el servidor):

```
[root@localhost pgordillo] #  yum install | grep openssh-server
[root@localhost pgordillo] #  yum install httpd
```

g) Se inicializa y habilita el servicio de ssh previamente instalado en el servidor:

```
[root@localhost pgordillo] #  systemctl start ssh.service
[root@localhost pgordillo] #  systemctl enable ssh.service
```

h) Se inicializa y habilita el servicio de http previamente instalado en el servidor:

```
[root@localhost pgordillo] #  systemctl start httpd.service
[root@localhost pgordillo] #  systemctl enable httpd.service
```

i) Se observa el estado del servicio httpd instalado en el servidor mediante la salida del siguiente comando:

```
[root@localhost pgordillo] #   systemctl status httpd
```

En la figura 3.15 se resalta la salida del comando indicado:

```
[root@localhost pgordillo]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset
: disabled)
   Active: active (running) since dom 2016-09-25 21:43:21 ECT; 1min 30s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 809 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/s
ec"
   CGroup: /system.slice/httpd.service
           ├─ 809 /usr/sbin/httpd -DFOREGROUND
           ├─1325 /usr/sbin/httpd -DFOREGROUND
           ├─1326 /usr/sbin/httpd -DFOREGROUND
           ├─1327 /usr/sbin/httpd -DFOREGROUND
           ├─1328 /usr/sbin/httpd -DFOREGROUND
           └─1329 /usr/sbin/httpd -DFOREGROUND

sep 25 21:43:16 localhost.localdomain systemd[1]: Starting The Apache HTTP Se...
sep 25 21:43:21 localhost.localdomain httpd[809]: AH00558: httpd: Could not r...
sep 25 21:43:21 localhost.localdomain systemd[1]: Started The Apache HTTP Ser...
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost pgordillo]#
```

Figura 3. 15: Estado del servicio httpd instalado en el servidor linux
Elaborada por: El Autor.

j) Finalmente se ilustra en la figura 3.16 la dirección IP y el gateway configurado en el servidor web linux, mediante los comandos *ip addr list* y *ip route show*:

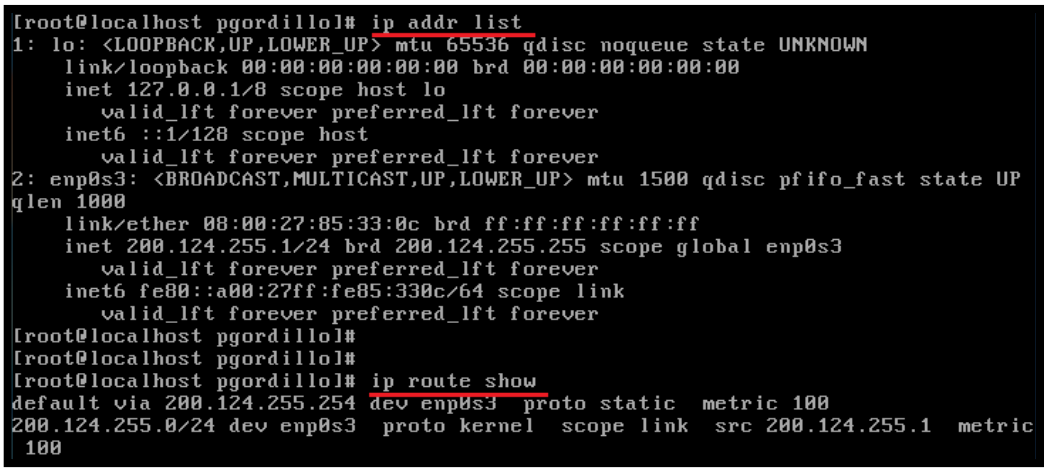


Figura 3. 16: Dirección IP y gateway del servidor web linux

Elaborada por: El Autor.

En el siguiente capítulo se exponen y analizan los resultados de la simulación planteada en el presente documento, realizado en plataformas virtuales de simulación.

Capítulo 4: Simulación y resultados de ataques externos e internos a la granja de servidores de un ISP en la red IP-MPLS empleando el software GNS3

Este capítulo contempla la comprobación del correcto enrutamiento en la red de datos IP MPLS y la simulación enunciada en este trabajo de titulación, basándose en el software GNS3. Este programa es una herramienta de simulación de redes de datos que facilita el diseño de topologías de redes complejas, creando ambientes de red con sistemas operativos, máquinas virtuales e ISOs de equipos de comunicación, tratando de recrear escenarios cercanos a la realidad, permitiendo al administrador de la red, comprobar diferentes conceptos teóricos antes de reproducirlos en equipos y servidores reales; la figura 4.1 muestra la pantalla principal de este software de simulación.

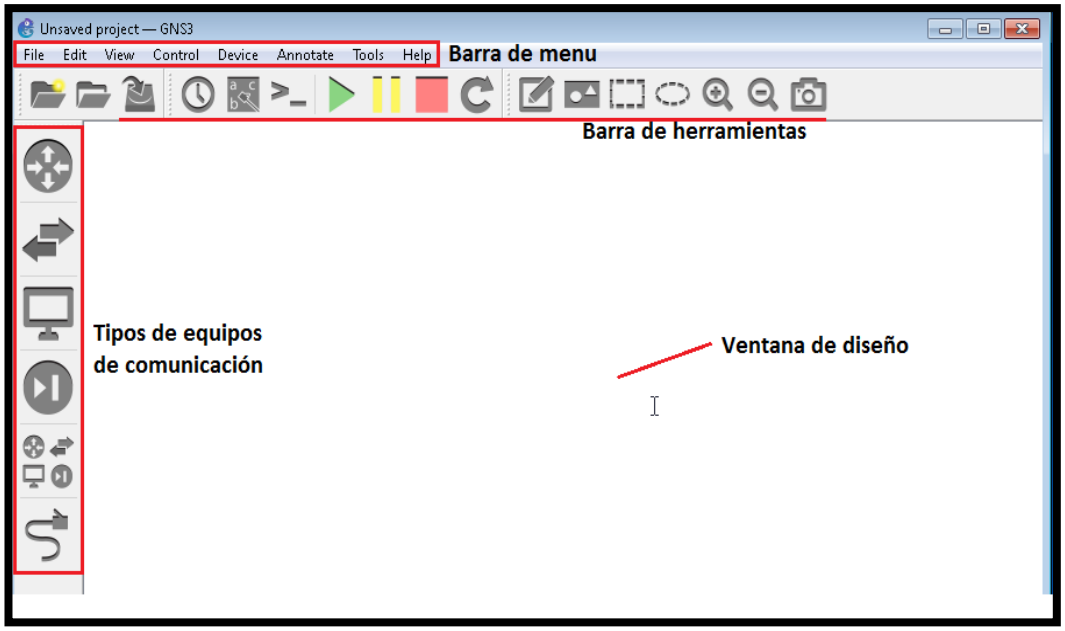


Figura 4. 1: Ventana principal del software GNS3
Elaborada por: El Autor.

4.1. Validación del enrutamiento en la red IP MPLS del proveedor de internet.

A continuación se presenta el enrutamiento de los equipos de comunicación realizado en la simulación con el software GNS3, cabe mencionar que se detalla

esta información por niveles de jerarquía en la red IP MPLS del proveedor de internet.

4.1.1. Enrutamiento en el core de la red

Se detalla el correcto enrutamiento aprendido por los equipos de comunicación que conforman el core de la red IP MPLS del proveedor de internet:

Router P01 Core:

a) Se comprueba que las interfaces del router han sido configuradas para usar el protocolo LDP (*show mpls interfaces*), ver figura 4.2:

```
P01#show mpls interfaces
Interface              IP             Tunnel   BGP Static Operational
GigabitEthernet1/0     Yes (ldp)      No       No  No     Yes
GigabitEthernet2/0     Yes (ldp)      No       No  No     Yes
GigabitEthernet3/0     Yes (ldp)      No       No  No     Yes
GigabitEthernet4/0     Yes (ldp)      No       No  No     Yes
```

Figura 4. 2: Verificación del protocolo LDP en las interfaces del equipo
Elaborada por: El Autor.

b) Se verifica el proceso de etiquetamiento MPLS en las interfaces del equipo (*show mpls forwarding-table*), ver figura 4.3:

```
P01#Show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
21         Pop Label  10.10.10.10/32   32635         Gi3/0      172.0.0.2
22         Pop Label  12.12.12.12/32   10893         Gi1/0      172.20.0.2
23         Pop Label  11.11.11.11/32   11874         Gi4/0      172.10.0.2
24         Pop Label  13.13.13.13/32   11772         Gi2/0      172.30.0.2
```

Figura 4. 3: Proceso de etiquetamiento MPLS en el router
Elaborada por: El Autor.

c) Se revisa la tabla de enrutamiento global en el equipo, el tipo de protocolo con el que se alcanzan las redes del proveedor, la interfaz del router por donde se llega al equipo destino, y el tiempo de conexión (show ip route), ver figura 4.4:

```
PO1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      9.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        9.9.9.8/30 is directly connected, Loopback0
L        9.9.9.9/32 is directly connected, Loopback0
      10.0.0.0/32 is subnetted, 1 subnets
O        10.10.10.10 [110/2] via 172.0.0.2, 01:28:01, GigabitEthernet3/0
      11.0.0.0/32 is subnetted, 1 subnets
O        11.11.11.11 [110/2] via 172.10.0.2, 01:27:41, GigabitEthernet4/0
      12.0.0.0/32 is subnetted, 1 subnets
O        12.12.12.12 [110/2] via 172.20.0.2, 01:27:51, GigabitEthernet1/0
      13.0.0.0/32 is subnetted, 1 subnets
O        13.13.13.13 [110/2] via 172.30.0.2, 01:27:18, GigabitEthernet2/0
      172.0.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.0.0.0/30 is directly connected, GigabitEthernet3/0
L        172.0.0.1/32 is directly connected, GigabitEthernet3/0
      172.10.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.10.0.0/30 is directly connected, GigabitEthernet4/0
L        172.10.0.1/32 is directly connected, GigabitEthernet4/0
      172.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.20.0.0/30 is directly connected, GigabitEthernet1/0
L        172.20.0.1/32 is directly connected, GigabitEthernet1/0
      172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.30.0.0/30 is directly connected, GigabitEthernet2/0
L        172.30.0.1/32 is directly connected, GigabitEthernet2/0
```

Figura 4. 4: Tabla de enrutamiento global en el router
Elaborada por: El Autor.

Router PE01 Core:

a) Se comprueba que esté establecida la sesión BGP con su router vecino (router reflector), así como el número de sistema autónomo, mensajes en BGP enviados y recibidos, tiempo de operatividad de la sesión BGP y cantidades de redes que se aprenden del router reflector (*show ip bgp vpnv4 all sumary*), ver figura 4.5:

```
PE_CORE#show ip bgp vpnv4 all summary
BGP router identifier 11.11.11.11, local AS number 65000
BGP table version is 12, main routing table version 12
11 network entries using 1584 bytes of memory
11 path entries using 572 bytes of memory
2/2 BGP path/bestpath attribute entries using 264 bytes of memory
2 BGP rrinfo entries using 48 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2516 total bytes of memory
BGP activity 11/0 prefixes, 11/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.10     4        65000     213     217       12    0    0 03:12:33        4
```

Figura 4. 5: Estado de la sesión bgp con el router reflector
Elaborada por: El Autor.

b) Se verifica que las subredes propias del PE_Core se envíen al router reflector para que sean propagadas por la red MPLS (*show ip bgp vpnv4 all neighbors 10.10.10.10 advertised-routes*), ver figura 4.6:

```
PE_CORE#SHow ip  bgp vpnv4 all neighbors 10.10.10.10 advertised-routes
BGP table version is 12, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 3:100 (default for vrf INTERNET)
*> 10.128.10.0/30   0.0.0.0                  0         32768 ?
*> 190.30.20.0/30   0.0.0.0                  0         32768 ?
*> 200.124.255.0    10.128.10.2              0         32768 ?

Total number of prefixes 3
```

Figura 4. 6: Redes del PE_Core anunciadas al router reflector
Elaborada por: El Autor.

c) Se observa que se aprendan todas las rutas por la VRF de INTERNET en el router PE_Core, así como el tipo de protocolo de enrutamiento que se emplea para alcanzar determinada red, el tiempo que está establecida la sesión BGP, y la interfaz del router por donde es alcanzable dicha red (*show ip route vrf INTERNET*), ver figura 4.7:

```
PE_CORE#show ip route vrf INTERNET

Routing Table: INTERNET
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.128.10.0/30 is directly connected, GigabitEthernet2/0
L        10.128.10.1/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/30 is subnetted, 2 subnets
B        172.16.10.0 [200/0] via 12.12.12.12, 00:19:38
B        172.16.20.0 [200/0] via 13.13.13.13, 00:18:27
      190.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        190.30.20.0/30 is directly connected, GigabitEthernet3/0
L        190.30.20.1/32 is directly connected, GigabitEthernet3/0
B     192.168.10.0/24 [200/0] via 12.12.12.12, 00:19:38
B     192.168.20.0/24 [200/0] via 13.13.13.13, 00:18:27
S     200.124.255.0/24 [1/0] via 10.128.10.2
PE_CORE#
```

Figura 4. 7: Redes aprendidas en el router PE_Core en la VRF de INTERNET
Elaborada por: El Autor.

Router Reflector:

a) Se valida el estado de las sesiones BGP con cada uno de los routers vecinos, así como el sistema autónomo, tiempo que está operativa la sesión y cantidad de redes aprendidas por router (*show ip bgp vpnv4 all sumary*), ver figura 4.8:

```
ROUTER_REFLECTOR#show ip bgp vpnv4 all summary
BGP router identifier 10.10.10.10, local AS number 65000
BGP table version is 8, main routing table version 8
7 network entries using 1008 bytes of memory
7 path entries using 364 bytes of memory
2/2 BGP path/bestpath attribute entries using 264 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1684 total bytes of memory
BGP activity 7/0 prefixes, 7/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
11.11.11.11     4        65000      69      69        8    0    0 00:57:29        3
12.12.12.12     4        65000      67      69        8    0    0 00:57:39        2
13.13.13.13     4        65000      68      67        8    0    0 00:56:19        2
ROUTER_REFLECTOR#
```

Figura 4. 8: Estado de las sesiones BGP con los routers vecinos
Elaborada por: El Autor.

b) Se comprueba las redes aprendidas por cada uno de los routers vecinos (*show ip bgp vpnv4 all neighbors*); se puede observar el símbolo *>*i* en cada una de

las redes alcanzables, esto significa que es una red valida, es la mejor ruta y se lo puede alcanzar dentro de la red interna, ver figura 4.9

```
ROUTER_REFLECTOR#
ROUTER_REFLECTOR#show ip bgp vpnv4 all neighbors 11.11.11.11 routes
BGP table version is 8, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 3:100
*>i10.128.10.0/30   11.11.11.11              0    100      0 ?
*>i190.30.20.0/30   11.11.11.11              0    100      0 ?
*>i200.124.255.0    11.11.11.11              0    100      0 ?

Total number of prefixes 3
ROUTER_REFLECTOR#
ROUTER_REFLECTOR#show ip bgp vpnv4 all neighbors 12.12.12.12 routes
BGP table version is 8, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:100
*>i172.16.10.0/30   12.12.12.12              0    100      0 ?
*>i192.168.10.0     12.12.12.12              0    100      0 ?

Total number of prefixes 2
ROUTER_REFLECTOR#show ip bgp vpnv4 all neighbors 13.13.13.13 routes
BGP table version is 8, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 2:100
*>i172.16.20.0/30   13.13.13.13              0    100      0 ?
*>i192.168.20.0     13.13.13.13              0    100      0 ?

Total number of prefixes 2
ROUTER_REFLECTOR#
```

Figura 4. 9: Redes aprendidas en el router reflector con cada uno de los routers vecinos
Elaborada por: El Autor.

4.1.2. Enrutamiento y conectividad en la red de distribución:

Se valida el correcto enrutamiento aprendido por los equipos de comunicación que conforman la red de distribución del ISP:

Router PE_01-GYE:

a) Se observa las rutas aprendidas en la VRF CLIENTE_A en el router PE_01-GYE, la VRF INTERNET creada en el router PE01_CORE se comunica con

la VRF CLIENTE_A (gracias a los route targer import y export) para que pueda alcanzar los equipos que se encuentran en la granja de servidores del proveedor; se observa la salida del comando *show ip router vrf CLIENTE_A*, donde se señala el tipo de protocolo de enrutamiento que se emplea para alcanzar determinada red, el tiempo que está establecido la sesión BGP, y la interfaz del router por donde es alcanzable dicha red, ver figura 4.10:

```
PE_01-GYE#show ip route vrf CLIENTE_A

Routing Table: CLIENTE_A
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      10.0.0.0/30 is subnetted, 1 subnets
B        10.128.10.0 [200/0] via 11.11.11.11, 04:18:45
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.10.0/30 is directly connected, GigabitEthernet2/0.100
L        172.16.10.1/32 is directly connected, GigabitEthernet2/0.100
B        172.16.20.0/30 [200/0] via 13.13.13.13, 04:17:36
      190.30.0.0/30 is subnetted, 1 subnets
B        190.30.20.0 [200/0] via 11.11.11.11, 04:18:45
S     192.168.10.0/24 [1/0] via 172.16.10.2
B     192.168.20.0/24 [200/0] via 13.13.13.13, 04:17:36
B     200.124.255.0/24 [200/0] via 11.11.11.11, 04:18:45
PE_01-GYE#
```

Figura 4. 10: Redes aprendidas en el router PE_01-GYE por la VRF CLIENTE_A
Elaborada por: El Autor.

b) Se prueba la conectividad ICMP desde el router en cuestión hacia el servidor detrás del firewall (*ping vrf CLIENTE_A 200.124.255.1 re 50*), ver figura 4.11:

```
PE_01-GYE#ping vrf CLIENTE_A 200.124.255.1 re 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 200.124.255.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 40/96/208 ms
```

Figura 4. 11: Conectividad ICMP al servidor Linux detrás del firewall
Elaborada por: El Autor.

Router PE_01-UIO:

a) Se muestra las rutas aprendidas en la VRF CLIENTE_A en el router PE_02-UIO, la VRF INTERNET creada en el router PE01_CORE se comunica con la VRF CLIENTE_A para que pueda alcanzar los servidores detrás del firewall; se observa la salida del comando *show ip router vrf CLIENTE_A*, donde se señala el tipo de protocolo de enrutamiento que se emplea para alcanzar determinada red, el tiempo que está establecida la sesión BGP, y la interfaz del router por donde es alcanzable dicha red, ver figura 4.12:

```
PE_02-UIO#show ip route vrf CLIENTE_A

Routing Table: CLIENTE_A
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      10.0.0.0/30 is subnetted, 1 subnets
B        10.128.10.0 [200/0] via 11.11.11.11, 04:37:32
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
B        172.16.10.0/30 [200/0] via 12.12.12.12, 04:37:32
C        172.16.20.0/30 is directly connected, GigabitEthernet2/0.100
L        172.16.20.1/32 is directly connected, GigabitEthernet2/0.100
      190.30.0.0/30 is subnetted, 1 subnets
B        190.30.20.0 [200/0] via 11.11.11.11, 04:37:32
B     192.168.10.0/24 [200/0] via 12.12.12.12, 04:37:31
S     192.168.20.0/24 [1/0] via 172.16.20.2
B     200.124.255.0/24 [200/0] via 11.11.11.11, 04:37:31
PE_02-UIO#
```

Figura 4. 12: Redes aprendidas en el router PE_02-UIO por la VRF CLIENTE_A
Elaborada por: El Autor.

b) Se prueba la conectividad ICMP desde el router en cuestión hacia el servidor detrás del firewall (*ping vrf CLIENTE_A 200.124.255.1 re 50*), ver figura 4.13:

```
PE_02-UIO#ping vrf CLIENTE_A 200.124.255.1 re 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 200.124.255.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 24/51/228 ms
PE_02-UIO#
```

Figura 4. 13: Conectividad ICMP al servidor Linux detrás del firewall
Elaborada por: El Autor.

4.1.3. Enrutamiento y conectividad en la red de acceso

Se comprueba el correcto enrutamiento aprendido por los equipos de comunicación que conforman la red de acceso del proveedor de internet:

Router OFICINA_GYE:

a) Se valida la tabla de enrutamiento global en el router OFICINA_GYE, se observa el tipo de protocolo por el cual se alcanzan las redes desde el equipo, así como las interfaces por donde se llegan a las redes destinos (*show ip route*), ver figura 4.14:

```
OFICINA_GYE#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 172.16.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.10.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.10.0/30 is directly connected, GigabitEthernet0/0
L        172.16.10.2/32 is directly connected, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0
L        192.168.10.1/32 is directly connected, GigabitEthernet1/0
OFICINA_GYE#
```

Figura 4. 14: Tabla de enrutamiento global en el router OFICINA_GYE
Elaborada por: El Autor.

b) Se comprueba la conectividad ICMP desde el router en cuestión hacia el servidor detrás del firewall (*ping 200.124.255.1 re 50*), ver figura 4.15:

```
OFICINA_GYE#ping 200.124.255.1 re 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 200.124.255.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 44/74/160 ms
OFICINA_GYE#
```

Figura 4. 15: Validación ICMP al servidor detrás del firewall desde las oficinas de Guayaquil
Elaborada por: El Autor.

Router OFICINA_UIO:

a) Se valida la tabla de enrutamiento global en el router OFICINA_UIO, se observa el tipo de protocolo por el cual se alcanzan las redes desde el equipo, así como las interfaces por donde se llegan a las redes destinos (*show ip route*), ver figura 4.16:

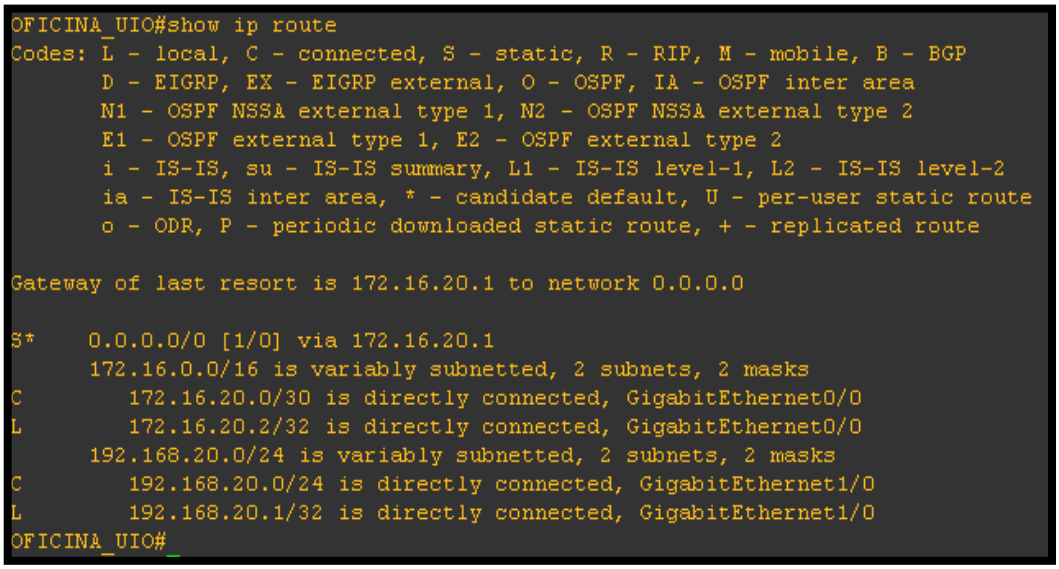


Figura 4. 16: Tabla de enrutamiento global en el router OFICINA_UIO
Elaborada por: El Autor.

b) Se confirma la conectividad ICMP desde el router en cuestión hacia el servidor detrás del firewall (*ping 200.124.255.1 re 50*), ver figura 4.17

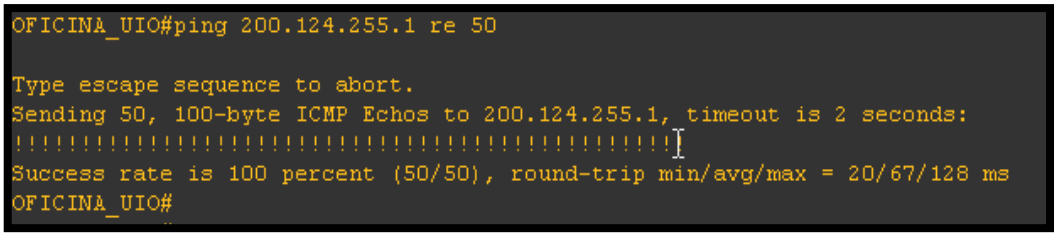


Figura 4. 17: Validación ICMP al servidor detrás del firewall desde las oficinas de Quito
Elaborada por: El Autor.

4.2. Simulación y resultados de ataques lógicos internos y externos a la granja de servidores del ISP en la red MPLS.

Para realizar la simulación planteada en esta investigación, se crearán todas las máquinas virtuales empleando el software virtual box (versión 5.0.10) para

utilizarse en la simulación (firewall Check Point, security manager, servidor web Linux, servidor Windows 7 smart console, y PC atacante) y serán agregadas en el software GNS3.

El servidor web Linux Centos virtualizado con servicios WINSCP (Windows Secure Copy) y SSH, será la victima de los ataques comunes generados con diferentes herramientas; el Security Gateway Check Point debe estar en la capacidad de bloquear, permitir, presentar estadísticas completas y generar logs del tráfico, sea éste permitido o bloqueado; para generar los ataques de red, se utilizara el software libre Raptor Attack Bot, basado en la distribución de linux Gentoo (versión 2.88); y el servidor Windows 7 servirá como smart console dentro de la arquitectura Check Point, el cual ayudará a gestionar el firewall en un ambiente amigable y de fácil administración.

Para lograr el enrutamiento adecuado en la red IP-MPLS del proveedor de internet, se vincula el sistema operativo IOS que emplean los routers Cisco a los equipos de red dentro de la simulación con el software GNS3.

A continuación se presenta la simulación y se analizan los resultados de los ataques lógicos a la granja de servidores en los escenarios que el ISP muestre carencia y presencia de firewalls de última generación en su granja de servidores de comunicación.

4.2.1. Ciberataques a los servidores del proveedor de internet sin la presencia del firewall Check Point

Se ejecutará un ataque desde el servidor Raptor Attack Bot al servidor web Linux localizado en el core del proveedor de internet, este ataque se originará dentro de la red MPLS (en la red de acceso) y simulará el ataque de un hacker desde las instalaciones de un cliente en las oficinas de Quito. El ataque lógico al servidor Linux se realizará en el escenario de que el ISP carezca de una línea de defensa propia como un firewall de protección para su granja de servidores, como se indica en la figura 4.18:

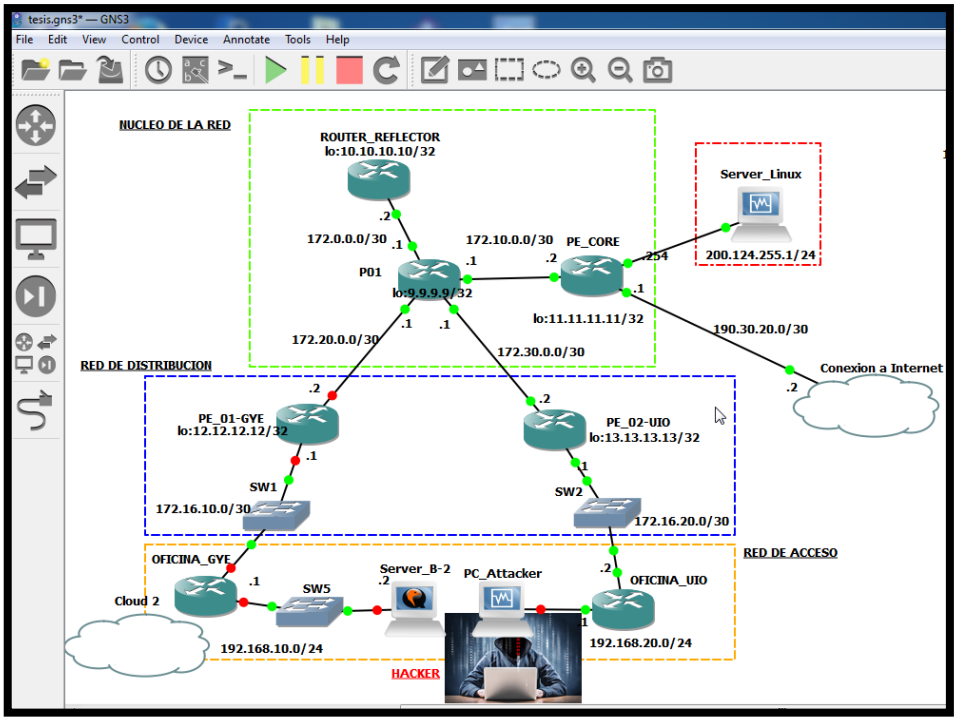


Figura 4. 18: Ataques lógicos al servidor web Linux sin la presencia del firewall Check Point
Elaborada por: El Autor.

Se enciende la máquina virtual PC_Attacker dentro de la simulación indicada (clic derecho, start), luego se carga el sistema operativo y se modifica la dirección IP empleada por el hacker en la red LAN de Quito (192.168.20.2/24, gw: 192.168.20.1), como indica la figura 4.19, después el software muestra varias opciones para generar diferentes tipos de ataques de red.

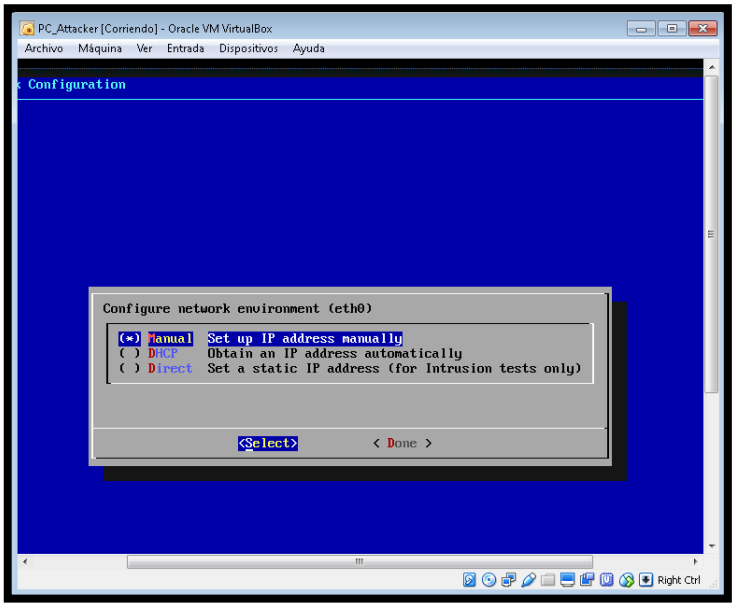


Figura 4. 19: Máquina virtual PC_Attacker administrada por el hacker
Elaborada por: El Autor.

Ataque TCP Scan vertical

Para ejecutar este tipo de ataque, se escoge (desde la máquina virtual PC_Attacker) la opción *network attacks, scans, tcp, vertical, high,* se coloca la IP del servidor web destino (200.124.255.1), el cual será el objetivo del ataque realizado por el hacker, después se realiza la ofensiva desde la PC_Attacker con el objetivo de impedir el acceso de clientes legítimos al servidor Linux, por lo que, los clientes que deseen acceder al servidor web del ISP, presentarán lentitud y perdida de comunicación con las páginas web alojadas en el servidor de la empresa (se cargó la página html de la red social facebook en el servidor web, para realizar pruebas en esta simulación). Se inicia el ataque, el hacker realiza un scaneo de diferentes puertos TCP desde la dirección ip 192.168.20.2 hacia la IP del servidor web 200.124.255.1, este equipo recibe demasiadas peticiones TCP, por lo que le es imposible responder a clientes legítimos en la red MPLS que buscan cargar el sitio web de la red social indicada (como muestra la figura 4.20); en la captura de paquetes wireshark realizada entre el router P01 y PE_02-UIO se aprecia con mayor claridad, la cantidad de puertos TCP que la PC del hacker (192.168.20.2) realiza al servidor web del proveedor de internet (ver figura 4.21).

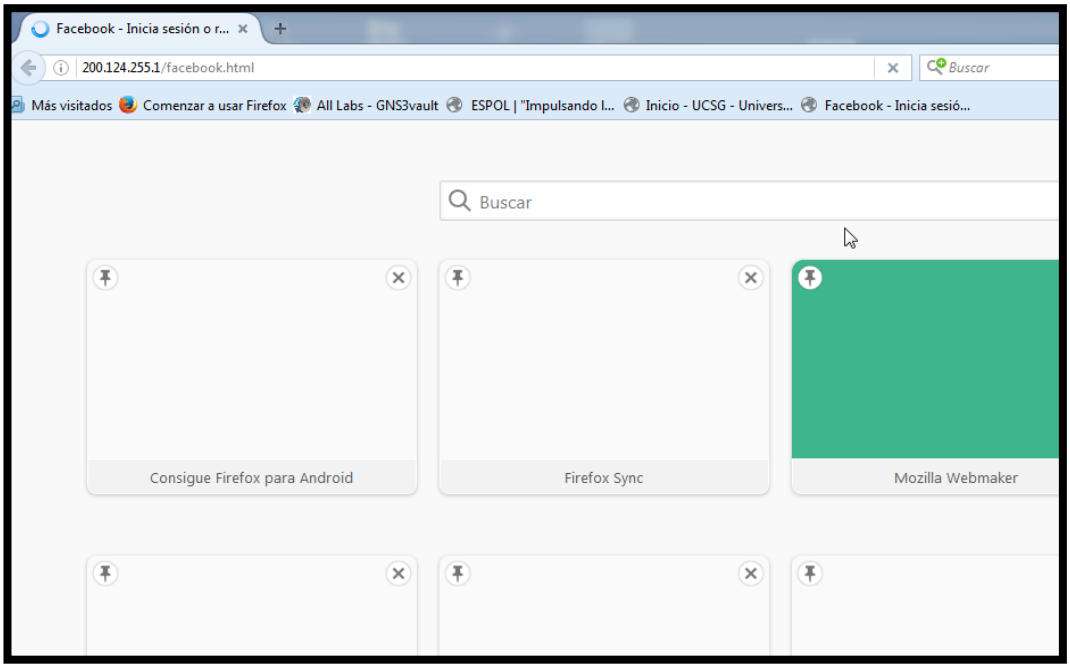


Figura 4. 20: Acceso desde un host legitimo al sitio web del servidor Linux durante el ataque
Elaborada por: El Autor.

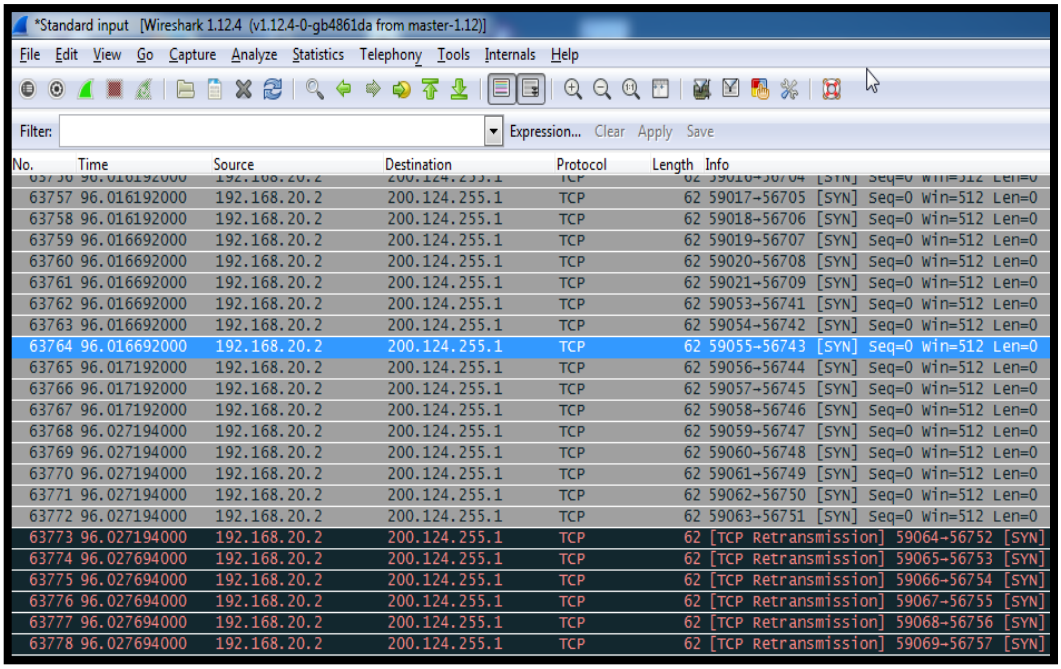


Figura 4. 21: Captura de paquetes entre el router P01 y PE_02-UIO de la red MPLS
Elaborada por: El Autor.

4.2.2. Ciberataques a los servidores del proveedor de internet bajo la presencia del firewall Check Point

Se ejecutarán varios ataques generados en la red LAN de Guayaquil, pero con la diferencia de que la granja de servidores del proveedor de internet posee un perímetro de seguridad lógica (en base al firewall Check Point) como línea de defensa, para evitar ataques de hackers que se originarían dentro o fuera de la red MPLS del proveedor de internet; la figura 4.22 muestra el diagrama de la red del ISP con el perímetro de defensa ya establecido, que incluye el firewall Check Point, securtiy manager, smart console (servidor Windows 7), y el switch de acceso para los servidores del proveedor de internet que se encuentran protegidos por el firewall.

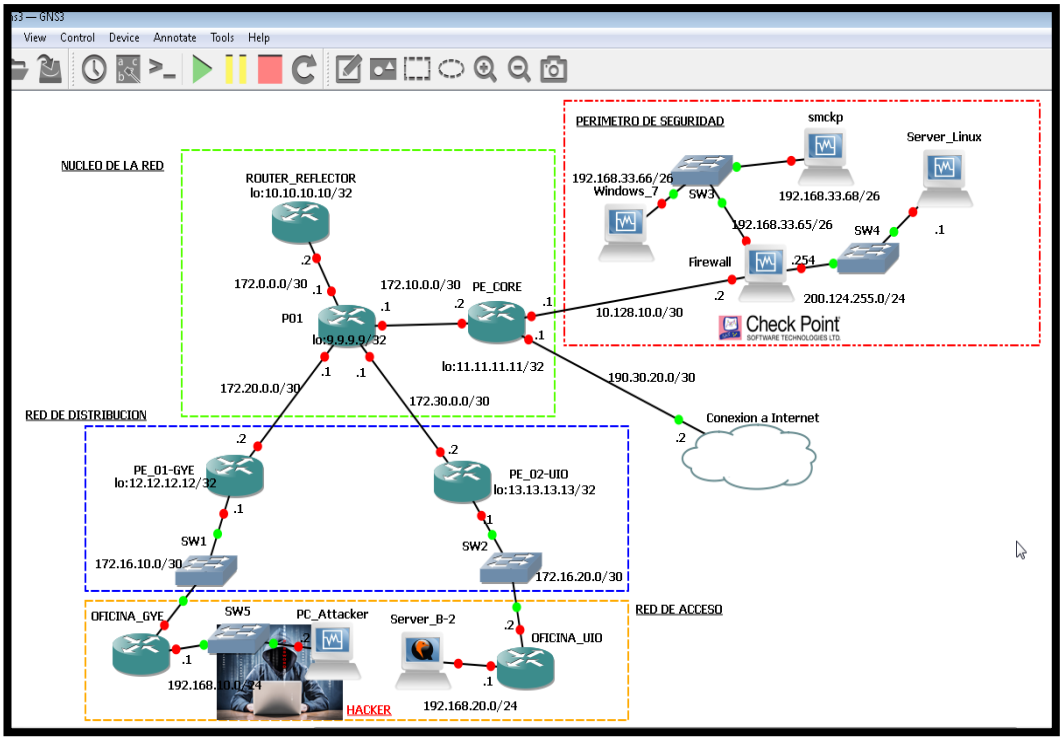


Figura 4. 22: Ataques lógicos al servidor web Linux con el firewall de protección.
Elaborada por: El Autor.

Se detallan los ataques internos (dentro de la red MPSL), realizados al servidor web Linux detrás del firewall, se captura tráfico entre origen y destino, así, se analizarán los resultados de los logs del smart view tracker (en la smart console), y del paquete IP en la captura de datos obtenidos con el software WireShark versión 1.12.4:

Ataques por reconocimiento de puertos:

Estos se realizan comprobando si el protocolo http, SSH e ICMP está habilitado en el servidor web Linux, estas pruebas se ejecutan desde un host ilegitimo (administrado por un hacker), por lo cual, el firewall Check Point deberá impedir estos accesos al servidor web. Para lograr esto, se crean políticas de seguridad en el firewall como muestra la figura 4.23; en la regla número 1 se detalla que desde el host de Guayaquil 192.168.10.3/24, al servidor web Linux del ISP 200.124.255.1/24, se habilite los puertos SSH, http e ICMP; en la regla número 2, se indica que desde el host de Quito 192.168.20.3/24, al servidor web Linux del ISP 200.124.255.1/24, se habilite los puertos SSH, http e ICMP; y en la regla

número 3 (regla de clean up), se muestra una política general de dropeo de servicio, es decir, se deniega el acceso de cualquier host en la red al servidor web Linux del ISP 200.124.255.1/24, se guardan los cambios y se instalan políticas en el firewall (ver figura 4.24).

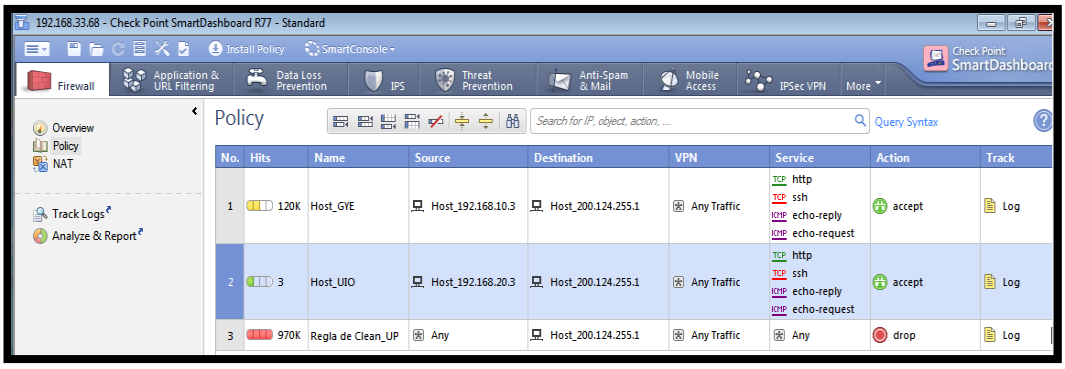


Figura 4. 23: Creación de políticas del firewall Check Point
Elaborada por: El Autor.

Se inicia el ataque desde el host ilegitimo 192.168.10.2/24, el hacker trata de acceder al servidor web Linux del proveedor de internet, tratando de escuchar los puertos que se encontrarían abiertos en este servidor, por lo que realiza consultas web, ICMP y SSH a la IP 200.124.255.1, el paquete viaja por la red MPLS hacia la granja de servidores del ISP protegido por el firewall, y el mismo dropea este tipo de peticiones ya que lo considera un ataque por la política número 3 ya establecida; en la figura 4.25 se observan logs del smart view tracker donde se resaltan datos importantes del supuesto ataque, como IP fuente y destino, puertos y regla al que hace match en el firewall.

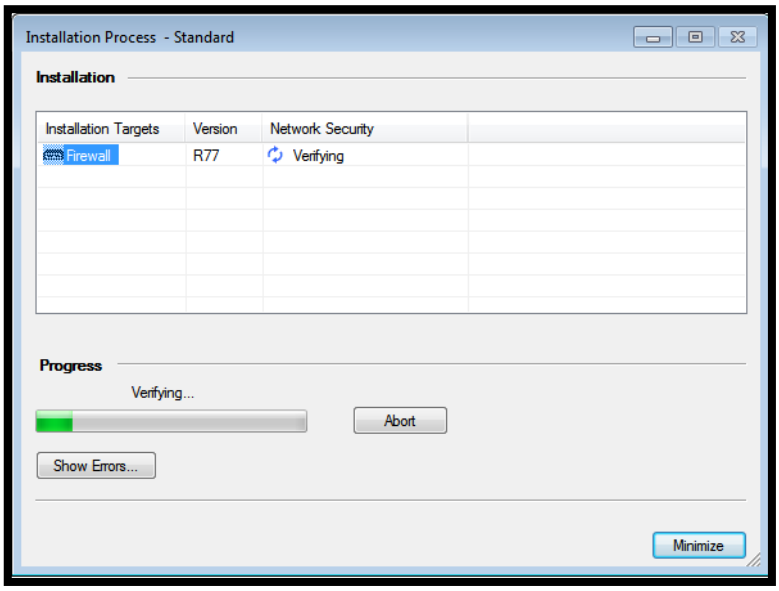
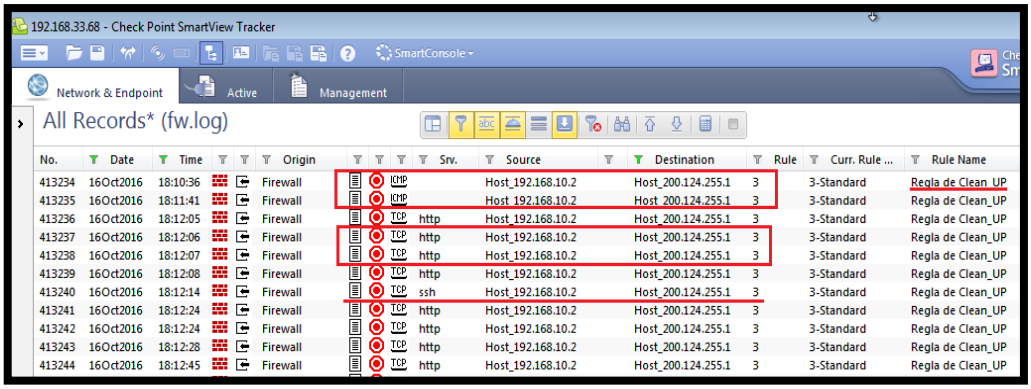


Figura 4. 24: Instalación de políticas en el firewall Check Point
Elaborada por: El Autor.



No.	Date	Time	Origin	Srv.	Source	Destination	Rule	Curr. Rule ...	Rule Name
413234	16Oct2016	18:10:36	Firewall		Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413235	16Oct2016	18:11:41	Firewall		Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413236	16Oct2016	18:12:05	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413237	16Oct2016	18:12:06	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413238	16Oct2016	18:12:07	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413239	16Oct2016	18:12:08	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413240	16Oct2016	18:12:14	Firewall	ssh	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413241	16Oct2016	18:12:24	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413242	16Oct2016	18:12:24	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413243	16Oct2016	18:12:28	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
413244	16Oct2016	18:12:45	Firewall	http	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP

Figura 4. 25: Logs capturados en el smart view tracker impidiendo el acceso al servidor web Linux desde un host ilegítimo.
Elaborada por: El Autor.

Gracias a la protección del firewall, el hacker no puede acceder al servidor web y realizar consultas vía http como indica la figura 4.26. Se realiza una captura de tráfico con el software Wireshark entre el router P01 y PE_01-GYE, donde se observa (según la figura 4.27) la solicitud de eco desde la IP del hacker (192.168.10.2) a la del servidor web destino (200.124.255.1), pero no se encuentra la respuesta (reply) desde este servidor a la IP fuente, también se aprecia que se levanta una sesión TCP entre la IP del host atacante y el servidor web (para hacer consultas vía http), pero solo existe la parte del sincronismo (sync), mas no el ACK desde el servidor Linux a la IP original, tampoco el tamaño de ventana (windowing) que son requisitos indispensables para establecer completamente una sesión TCP; además, se observa los paquetes BGP, OSPF y LDP implicados en la transmisión de datos en una red MPLS.

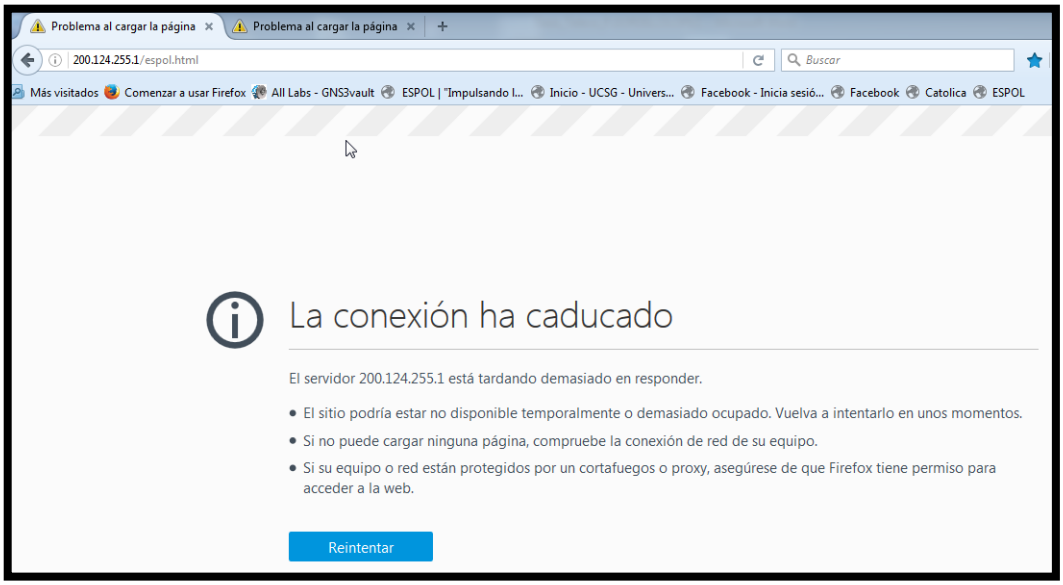


Figura 4. 26: Sitio web del servidor Linux no cargada en el host del hacker
Elaborada por: El Autor.

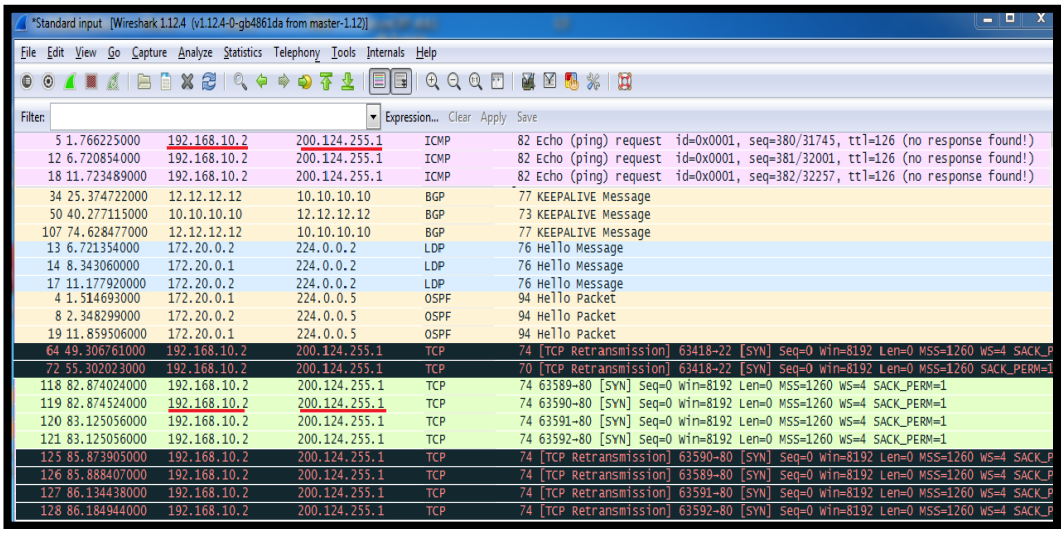


Figura 4. 27: Captura de datos en la red MPLS, empleando el software Wireshark
Elaborada por: El Autor.

Ataque TCP Scan vertical

Se fundamenta en escanear varios puertos TCP desde una PC en particular al servidor que sería la victima de este tráfico anómalo; para realizar este tipo de ataque, se selecciona (desde la máquina virtual PC_Attacker) la opción *network attacks, scans, tcp, vertical, high*, se coloca la IP del servidor web destino, el cual será el objetivo del ataque realizado por el hacker, luego, se realiza la ofensiva desde la PC_Attacker con el objetivo de incrementar los recursos del servidor web, impidiendo el acceso de clientes legítimos al servidor Linux; sin embargo, gracias a la protección del firewall Check Point y del módulo IPS habilitado en el equipo, los clientes del ISP accederán a las páginas web del servidor sin problemas.

Se inicia el ataque, el hacker realiza un scaneo de diferentes puertos TCP desde la dirección IP 192.168.10.2 hacia la del servidor web 200.124.255.1, esta petición viaja por la red MPLS y llega al firewall, el cual, activa el sistema de prevención de intrusos (IPS), y dropea este tráfico anómalo dirigido al servidor web Linux, en la figura 4.28 se muestra la cantidad de paquetes por segundo que ingresa al firewall Check Point.

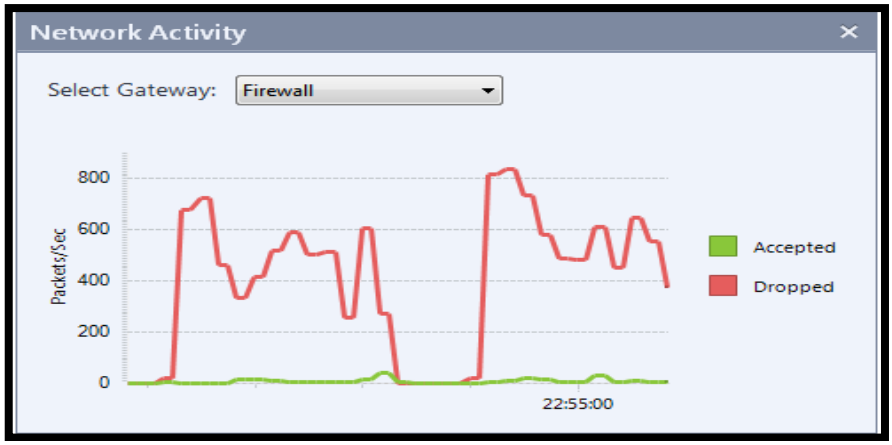


Figura 4. 28: Paquetes que dropea el firewall durante el ataque al servidor Linux
Elaborada por: El Autor.

En la figura 4.29 se aprecia los logs que muestra el smart view tracker durante el ataque, se observa la dirección IP de la PC administrada por el hacker (192.168.10.2) y los diferentes puertos que genera este tipo de ataques dirigidos al servidor web destino 200.124.255.1; también se analiza un log que fue generado por el módulo del IPS previamente activado, el firewall al recibir una solicitud http desde una dirección IP legítima en medio de un ataque, activa las firmas del IPS y deja pasar estas solicitudes al servidor web destino, la gráfica 4.30 indica con detalle las características de este blade activado (dirección IP fuente y destino, dirección web, severidad).

No.	Date	Time	Origin	Service	Source	Destination	Rule	Curr. Rule ...	Rule Name
1018...	19Oct2016	12:52:15	Firewall	29771	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29787	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29788	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29789	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29794	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29817	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29819	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29820	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29821	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29829	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29830	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29831	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29832	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29833	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29834	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29835	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP
1018...	19Oct2016	12:52:15	Firewall	29836	Host_192.168.10.2	Host_200.124.255.1	3	3-Standard	Regla de Clean_UP

Figura 4. 29: Logs de los ataques generados en el Smart view tracker
Elaborada por: El Autor.

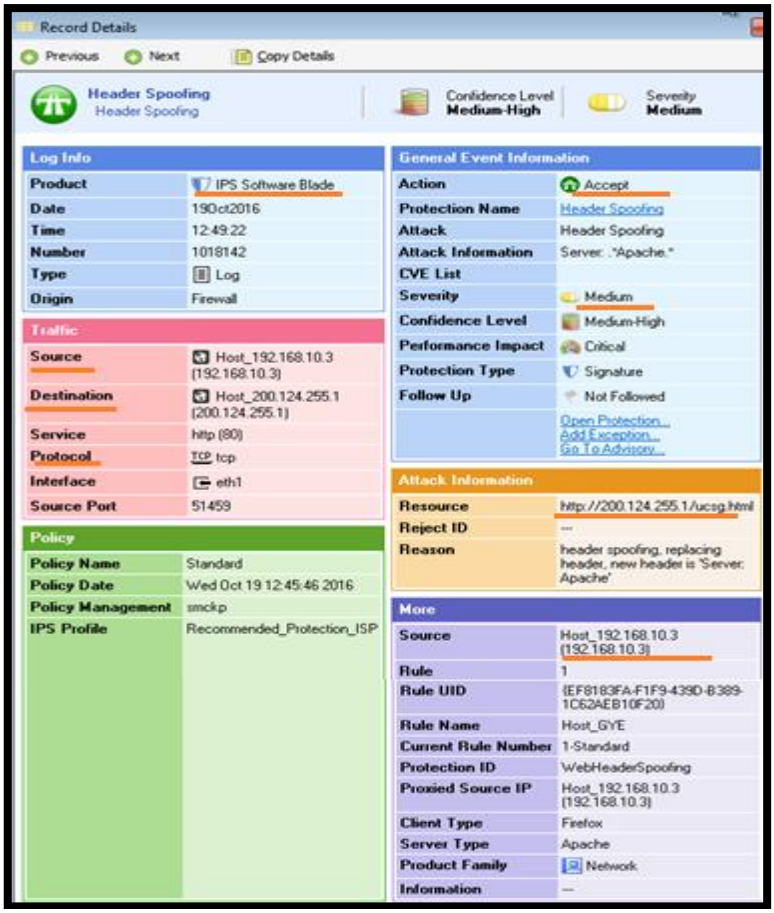


Figura 4. 30: Logs del módulo IPS activado en el firewall Check Point
Elaborada por: El Autor.

Ataque HTTP flooding

Este tipo de ataques consiste en inundar la red de paquetes TCP desde el puerto 80 a un destino destino determinado, para realizarlo se acude a la máquina virtual PC_Attacker, se escoge la opción *service attacks*, *HTTP*, *flooding*, se coloca la IP del servidor web destino (200.124.255.1), el cual será el objetivo de los ataques realizados por el hacker, luego se escribe un dominio alojado en el servidor web (se cargó la página html de la ESPOL en el servidor web, para realizar pruebas en esta simulación), y se realiza la ofensiva desde la PC atacante con el objetivo de tumbar el servidor Linux, localizado detrás del firewall Check Point del proveedor de internet. El firewall recibe este flujo de tráfico y empieza a dropear los paquetes ilegítimos recibidos en el equipo como se muestra en la figura 4.31

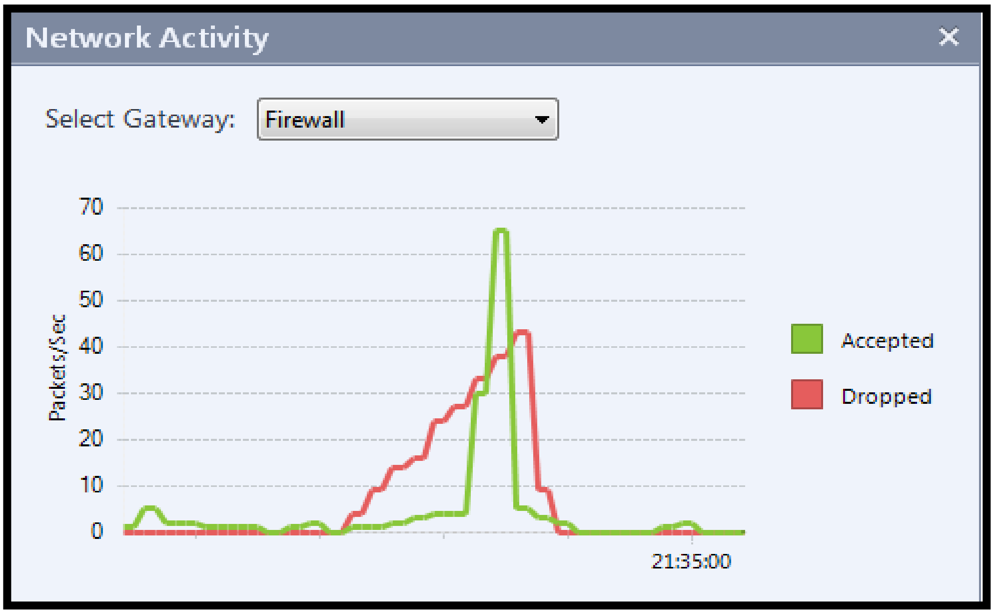


Figura 4. 31: Paquetes dropeados en el firewall Check Point
Elaborada por: El Autor.

En el smart view tracker se aprecia los eventos de dropeo que realiza el gateway al momento del ataque ocasionado por el hacker (ver figura 4.32), el firewall recibe demasiadas peticiones http desde una dirección IP desconocida para las reglas del gateway, por lo que hace un match en la política número 3 ya instalada; desde host legítimos en la red MPLS se puede acceder a las páginas web del servidor del ISP sin problemas durante el ataque, como se resalta en la figura 4.33.

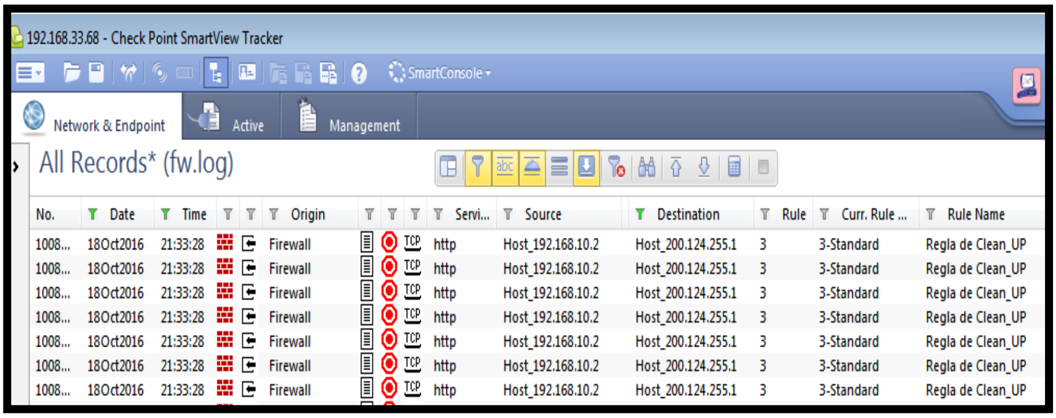


Figura 4. 32: Logs indicando el dropeo del ataque al servidor web
Elaborada por: El Autor.

Figura 4. 33: Acceso al sitio web de pruebas durante el ataque desde una PC legítima
Elaborada por: El Autor.

Luego de los ataques realizados en la red interna del ISP, se realizarán ataques desde la red externa a la red MPLS, es decir, desde un host localizado en la nube de internet, de igual manera el firewall deberá ser capaz de bloquear este tráfico no deseado para los servidores protegidos por el equipo, y habilitar el acceso a los host de clientes legítimos en la red MPLS.

Ataque FTP L7

Se realiza este tipo de ataque externo a la red MPLS, que consiste en levantar demasiadas peticiones desde el puerto TCP 21 al server web destino; desde la máquina virtual PC_Attacker ubicada en la nube de internet (ver figura 4.34); se escoge la opción *service attacks*, *FTP*, *cracking*, se coloca la IP del servidor web destino (200.124.255.1), el cual será el objetivo de los ataques realizados por el hacker desde internet; se realiza la ofensiva desde la PC atacante con el objetivo de derribar el servidor Linux, localizado detrás del firewall Check Point del ISP, el smart view tracker genera logs indicando que existen demasiadas peticiones desde una dirección IP pública 190.30.20.2 (dirección IP de la PC del hacker)

hacia el servidor web del ISP 200.124.255.1, empleando el protocolo FTP, por lo que dropea este tráfico como se indica en la figura 4.35, ya que coincide con la política número 3 instalada en el gateway; el acceso de clientes legítimos al servidor web se da sin problema alguno como resalta la figura 4.36 (se realizó la consulta a la página html de la red social Facebook subida al servidor web Linux).

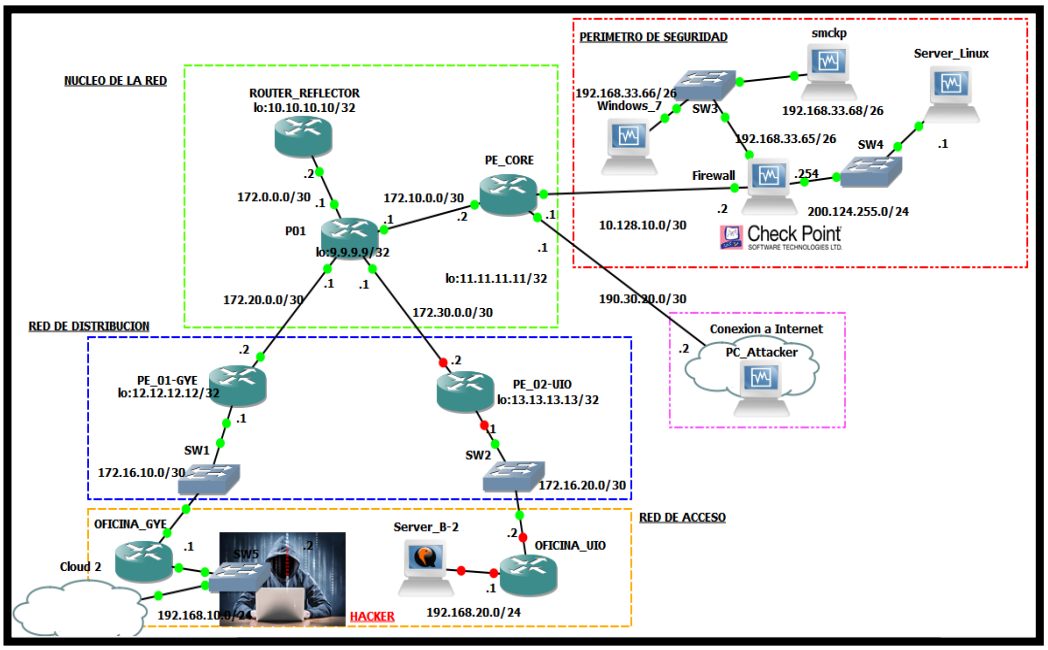


Figura 4. 34: Ubicación de la PC atacante desde la nube de internet en la red IP MPLS del ISP
Elaborada por: El Autor.

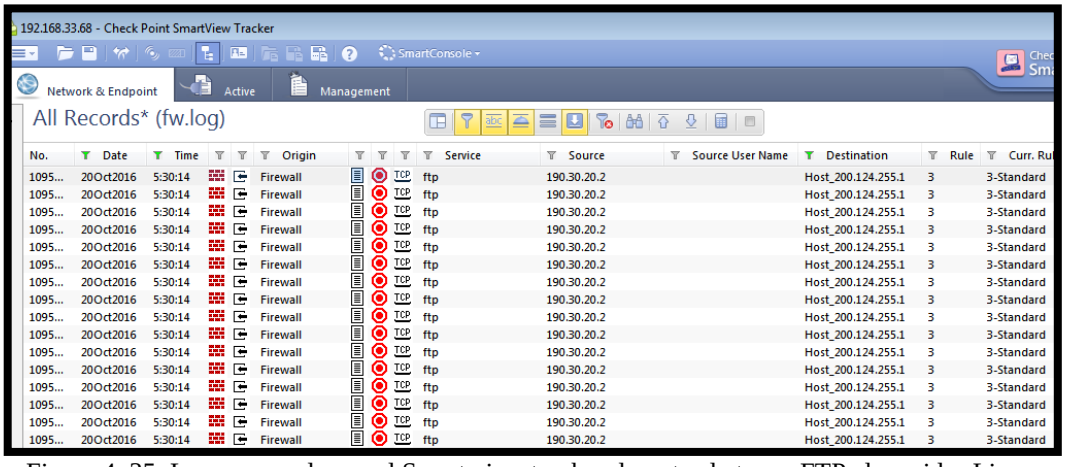
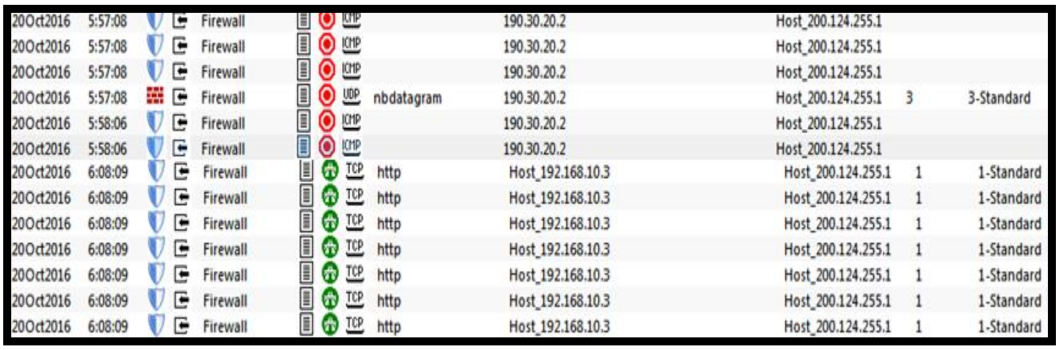


Figura 4. 35: Logs generados en el Smart view tracker durante el ataque FTP al servidor Linux
Elaborada por: El Autor.

Figura 4. 36: Acceso exitoso a la página html de Facebook durante el ataque
Elaborada por: El Autor.

Ataque ICMP-fragmented

Es otro tipo de ataque externo a la red MPLS del proveedor de internet que consiste en enviar paquetes más pequeños al paquete MTU (Maximum Transmission Unit) transmitido; para realizar este tipo de ataques se dirige a la máquina virtual PC_Attacker ubicada en la nube de internet, se configura la dirección IP 190.30.20.2 (dirección IP de la PC del hacker), luego se escoge el tipo de ataque en *Intrusión attack, single, dirección IP del servidor web que será la victima del ataque (200.124.255.1), ICMP as Advanced, ICMP Fragmented;* empieza el ataque, el firewall recibe paquetes anómalos ICMP como muestra la figura 4.37 del smart view tracker y dropea el paquete inmediatamente gracias al escudo de protección IPS activado en el firewall, el acceso web desde clientes legítimos se realiza con absoluta normalidad como indica la figura 4.38 (se cargó la página html de la UCSG en el servidor web de pruebas); en la figura 4.39 se ilustra más detalladamente un log del IPS indicando: día y hora del evento, el tipo de ataque realizado, información del tipo de ataque, dirección IP fuente y destino, y el tipo de protocolo que generaba la PC atacante administrada por el hacker.



20Oct2016	5:57:08	Firewall	ICMP		190.30.20.2	Host_200.124.255.1		
20Oct2016	5:57:08	Firewall	ICMP		190.30.20.2	Host_200.124.255.1		
20Oct2016	5:57:08	Firewall	ICMP		190.30.20.2	Host_200.124.255.1		
20Oct2016	5:57:08	Firewall	UDP	nbdatagram	190.30.20.2	Host_200.124.255.1	3	3-Standard
20Oct2016	5:58:06	Firewall	ICMP		190.30.20.2	Host_200.124.255.1		
20Oct2016	5:58:06	Firewall	ICMP		190.30.20.2	Host_200.124.255.1		
20Oct2016	6:08:09	Firewall	TCP	http	Host_192.168.10.3	Host_200.124.255.1	1	1-Standard
20Oct2016	6:08:09	Firewall	TCP	http	Host_192.168.10.3	Host_200.124.255.1	1	1-Standard
20Oct2016	6:08:09	Firewall	TCP	http	Host_192.168.10.3	Host_200.124.255.1	1	1-Standard
20Oct2016	6:08:09	Firewall	TCP	http	Host_192.168.10.3	Host_200.124.255.1	1	1-Standard
20Oct2016	6:08:09	Firewall	TCP	http	Host_192.168.10.3	Host_200.124.255.1	1	1-Standard
20Oct2016	6:08:09	Firewall	TCP	http	Host_192.168.10.3	Host_200.124.255.1	1	1-Standard
20Oct2016	6:08:09	Firewall	TCP	http	Host_192.168.10.3	Host_200.124.255.1	1	1-Standard

Figura 4. 37: Logs Smart view tracker indicando el dropeo del firewall al ataque ICMP fragmented
Elaborada por: El Autor.

Figura 4. 38: Acceso exitoso a la página html de la UCSG durante el ataque
Elaborada por: El Autor.

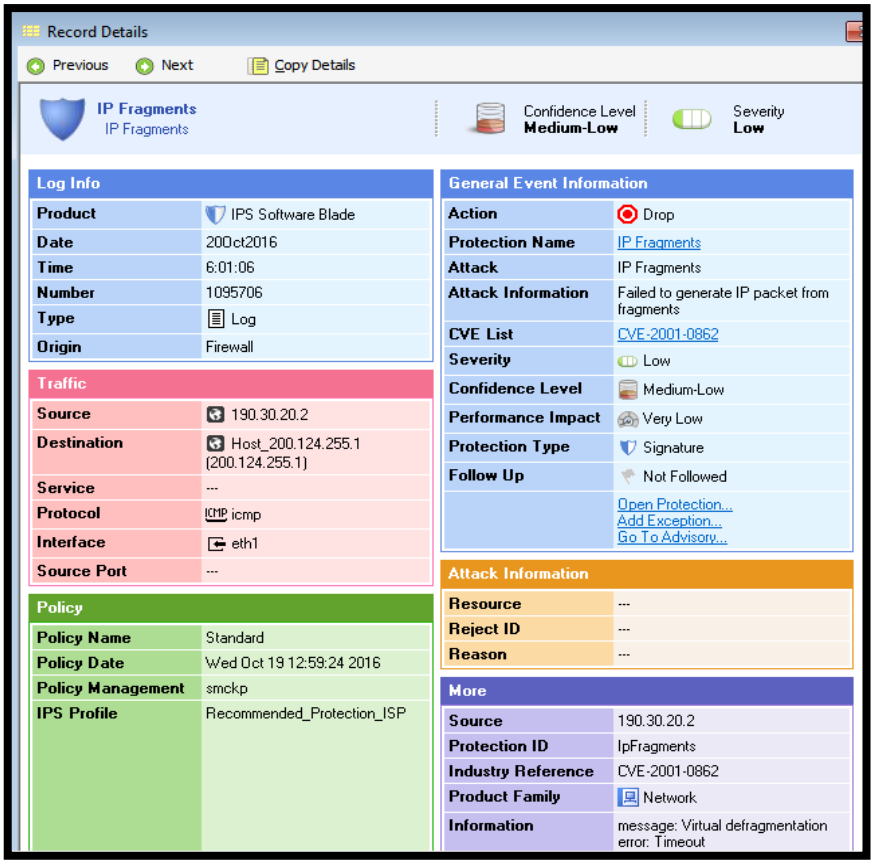


Figura 4. 39: Log generado por el módulo IPS durante el ataque ICMP
Elaborada por: El Autor.

Conclusiones.

1. La tecnología MPLS posee una arquitectura escalable y de fácil administración, gracias a la transmisión de etiquetas de 20 bits que son agregadas al paquete de datos para su transmisión; se considera una red de transporte segura y fiable para enrutar datos a los destinos determinados.

2. Luego de la configuración de los routers y switches que componen la red MPLS, se analizó el correcto aprendizaje de las redes ip del core del proveedor de internet en su respectiva vrf, logrando asi, el adecuado enrutamiento desde las PC's de los clientes hacia los servidores del ISP.

3. En la simulación planteada en este trabajo de titulación, se logró diseñar e implementar un firewall virtual para la protección de los servidores del proveedor de internet, esto se obtuvo mediante el software de simulación GNS3 que permite instalar maquinas virtuales utilizando el software VirtualBox.

4. Al implementar políticas de seguridad en el firewall virtual Check Point, se aseguró que los host de clientes legítimos accedan al servidor Linux mediante puertos específicos; además se implemento la política que dropea el tráfico no deseado, desde cualquier red, hacia el servidor web del ISP.

5. Durante el ataque generado por una PC administrada por el hacker, se observaron logs en el smart view tracker del Check Point indicando la dirección ip fuente, ip destino, puerto y protocolo que busca ingresar a la red de manera ilícita y con un comportamiento anómalo; sin embargo, gracias al firewall virtual, estos ataques fueron rechazados rotundamente.

6. Los objetivos e hipótesis expuestos en este trabajo de titulación fueron cumplidos exitosamente, puesto que se demostró que el firewall Check Point es capaz de proteger la granja de servidores de diferentes ataques ocasionados de manera interna o externa a la red IP-MPLS del ISP.

Recomendaciones.

1. Se sugiere levantar un firewall de respaldo Chek Point, adicional al que esta configurado en la actualidad, con el objetivo de crear un ambiente de cluster entre estos dispositivos, que figurarían como activo/standby; entre ambos equipos debe existir una interfaz de sincronismo donde se transmita las tablas de enrutamiento, rutas y estado de interfaces de ambos gateways, al detectar uno de las interfaces caídas, automáticamente el equipo que se encuentra activo pasa a modo standby y viceversa.

2. La arquitectura SMART de Chek Point permite crear instancias virtuales dentro del firewall, esto permitiría crear firewalls lógicos dentro del mismo hardware físico, asi, en caso de necesitar separar servicios de una instancia virtual actual, se lo haría a una nueva instancia virtual creada, por consiguiente se incrementaría la rentabilidad de la inversión realizada por el proveedor de servicios de internet.

3. El firewall Chek Point posee módulos adicionales de protección que se pueden habilitar como: Application Control, URL Filtering, DLP, Antivirus, VPN, pero requiere licenciamiento adicional; el firewall configurado en la simulación propuesta en este trabajo de titulación posee una licencia demo para el modulo de firewall e IPS.

Glosario de términos

ABR: Area Border Router, Router border de area.

ACK: Acknowledgement, Acuse de recibo.

AES: Advanced Encryption Standard, Encriptación estandar avanzada.

AH: Authentication Header, Autenticación de cabecera

AS: Autonomous System, Sistema autónomo

BGP: Border Gateway Protocol, Protocolo de pasarela de borde

BMA: Broadcast Multiaccess, Difusión por multiacceso.

CE: Costumer Edge, Borde del cliente.

CEF: Cisco Express Forwarding, Reenvío express de Cisco.

CLI: Command Line Interface, Interface de linea de comando.

DBD: Database Description, Descripción de base de datos.

DDoS: Distributed Denial of Service, Denegación de servicio distribuido.

DES: Data Encryption Standard, Encriptación de datos estándar.

DNS: Domain Name System, Sistema de nombre de dominio.

EBGP: External Border Gateway Protocol, Protocolo de frontera de borde externo.

EGP: External Gateway Protocol, Protocolo de frontera externo.

ELSR: Edge Label Switch Router, Router conmutador de etiquetas de borde.

EIGRP: Enhanced Interior Gateway Routing Protocol, Protocolo de enrutamiento interior mejorado.

ESP: Encapsulating Security Payload, Carga útil de seguridad encapsulada.

FEC: Forwading Equivalence Class, Clase equivalente de reenvió.

FIB: Forwarding Information Base, Base de información de reenvío.

HMAC: Hash-based Message Authentication Code, Codigo de autenticación basado en mensajes hash.

HTTP: Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto.

HTTPS: Hypertext Transfer Protocol Secure, Protocolo de transferencia de hipertexto seguro.

IBGP: Internal Border Gateway Protocol, Protocolo de frontera de borde interno.

ICMP: Internet Control Message Protocol, Protocolo de mensajes de control de internet.

IGMP: Internet Group Management Protocol, Protocolo de administración de grupo de internet.

IGP: Interior Gateway Protocol, Protocolo de pasarela interno.

IGRP: Interior Gateway Routing Protocol, Protocolo de enrutamiento de pasarela interior.

IKE: Internet Key Exchange, Intercambio de llaves de internet.

IOS: Internetwork Operating System, Sistema operativo de internet working.

IP: Internet Protocol, Protocolo de internet.

IP-MPLS: Internet Protocol Multiprotocol Label Switching, Multiprotocolo de conmutación de etiquetas, protocolo de internet.

IPS: Intrusion Prevention System, Sistema de prevención de intrusos.

IPSEC: Internet Protocol Security, Seguridad de protocolo de internet.

IS-IS: Intermediate System to Intermediate System, Sistema intermedio a sistema intermedio.

ISO: International Organization for Standardization, Organización internacional de normalización.

ISP: Internet Service Provider, Proveedor de servicio de internet.

IT: Information technology, Tecnologías de información.

LAN: Local Area Network, Red de área local.

LDP: Label Distribution Protocol, Protocolo de distribución de etiquetas.

LFIB: Label Forwarding Information Base, Información base de reenvió de etiquetas.

LSP: Label Switched Path, Ruta de conmutación de etiquetas.

LSR: Label Switch Router, Router de conmutación de etiquetas.

MAC: Media Access Control, Control de acceso al medio.

MP-BGP: Multi-Protocol Border Gateway Protocol, Multi protocolo de pasarela de borde.

MPLS: Multiprotocol Label Switching, Multiprotocolo de conmutación de etiquetas.

MTU: Maximum Transmission Unit, Unidad máxima de transmisión.

NAT: Network Address Translation, Traducción de direcciones de red.

NBMA: Non-Broadcast Multiaccess Network, Red de acceso no difundida.

NGFW: Next Generation Firewall, Firewalls de siguiente generación.

OSI: Open System Interconnection, Interconexión de sistemas abiertos.

OSPF: Open Shortest Path First, Primero la ruta más corta.

P: Provider, Proveedor.

PE: Provider Edge, Proveedor de borde.

PIM-SM: Protocol Independent Multicast - Sparse Mode,

PKI: Public Key Infrastructure, Llave de insfraestructura pública.

QoS: Quality of Service, Calidad de Servicio.

RFC: Request for Comments, Solicitud de comentarios.

RIP: Routing Information Protocol, Protocolo de información de enrutamiento.

RIB: Routing Information Base, Base de información de enrutamiento.

SEO: Search Engine Optimization, Ingeniería de búsqueda de optimización.

SGSI: Sistemas de Gestión de la Seguridad de la Información.

SIC: Secure Internal Communications, Comunicación interna segura.

SMART: Security Management Architecture, Arquitectura de gestión de seguridad.

SNMP: Simple Network Management Protocol, Protocolo de administración de red simple.

SPF: Short Path First, Primer camino corto.

SSH: Secure Shell, Ingreso seguro.

TCP: Transmission Control Protocol, Protocolo de control de transmisión.

TCP/IP: Transmission Control Protocol / Internet Protocol, Protocolo de control de transmisión / Protocolo de internet.

3DES: Triple Data Encryption Standard, Estándar de encriptación de datos triple.

UDP: User Datagram Protocol, Protocolo de datagrama de usuario.

VBA: Visual Basic Applications, Aplicaciones de Visual Basic.

VLSM: Variable Length Subnet Mask, Máscara de subred de longitude variable.

VPN: Virtual Private Networks, Red privada virtual.

VRF: Virtual Routing and Forwarding, Red privada virtual de enrutamiento y reenvío.

WINSCP: Windows Secure Copy, Copia segura de Windows.

Referencias bibliográficas

Akamai Technologies, Inc. (2016). *Informe de seguridad sobre el estado de internet, 1Q del 2016.* Cambridge, Massachusetts; USA .

Ariganello, E., & Barrientos, E. (2010). *Redes Cisco, guia de estudio para la certificacion CCNP.* Madrid, España: RA-MA editorial.

Check Point Company. (2013). *Documentos SC1 Check Point*. Obtenido de https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/89230.htm

Check Point Company. (2015). Obtenido de sitio web de Check Point, datasheet firewalls: http://www.checkpoint.com/downloads/product-related/comparison-chart/appliance-comparison-chart.pdf

Check Point Company. (2015). Check Point Security Report 2014. USA. Obtenido de Check Point Security report 2014.

Check Point Company. (2016). Check Point 12600 appliance Datasheet. Tel Aviv, Israel. Obtenido de https://www.checkpoint.com/downloads/product-related/datasheets/12600-appliance-datasheet.pdf

Check Point Company. (2016). Gaia R77 versions, Administration Guide. USA.

Cisco System, Inc. (2014). Abordar toda la continuidad del ataque: antes durante y despues de un ataque. San José, California, USA.

Cisco Systems, Inc. (2015). Obtenido de sitio web de Cisco, datasheet firewalls Cisco: http://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-736661.html

De Ghein, L. (2007). Mpls Fundamentals. Indianapolis: Cisco Press.

Dordoigne, J. (2011). *Redes Informaticas.* Barcelona: Editoriales ENI.

Eset Company. (2016). Eset Security Report Lationamerica 2016. Buenos Aires, Argentina.

FireEye, Inc. (2016). Obtenido de sitio web de FireEye, datasheet firewall: https://www.fireeye.com/products/nx-network-security-products/nx-network-security-datasheet.html

García-Cervigón Hurtado, A., & Alegre Ramos, M. D. (2011). Seguridad Informática. En A. García-Cervigón Hurtado, & M. D. Alegre Ramos, *Seguridad Informática* (pág. 19). Madrid, España: Paraninfo SA.

Go-Mpls. (2009). Obtenido de sitio web de Go-Mpls: http://www.gompls.net/2009/08/understanding-mpls-header.html

Guichard, J., Pepelhjak, I., & Apcar, J. (2003). *MPLS and VPN Architectures.* Indianapolis: Cisco Press.

Hawkinson, J., & Bates, T. (1996). *sitio web de IETF*. Obtenido de https://tools.ietf.org/html/rfc1930

Hils, A., D'Hoinne, J., Kaur, R., & Young, G. (2016). Obtenido de sitio web de Gartner INC. (ID: G00277994): https://www.gartner.com/doc/reprints?id=1-3800T0M&ct=160525&st=sb

Jiménez, M., & Reuter, A. (2013). Diseño del Backbone de la red óptica metropolitana con tecnología MPLS para un Proveedor de Servicios de Internet dentro del Distrito Metropolitano de Quito. *Revista Politécnica*, 29.

Moran Rivera, L. (2015). Contribucion en el analisis y simulacion de una red IP/MPLS para un proveedor de servicios de telecomunicaciones. Guayaquil, Guayas, Ecuador.

Radware Ltd. (2016). Global Application & Network Security Report 2015-2016. Tel Aviv, Israel .

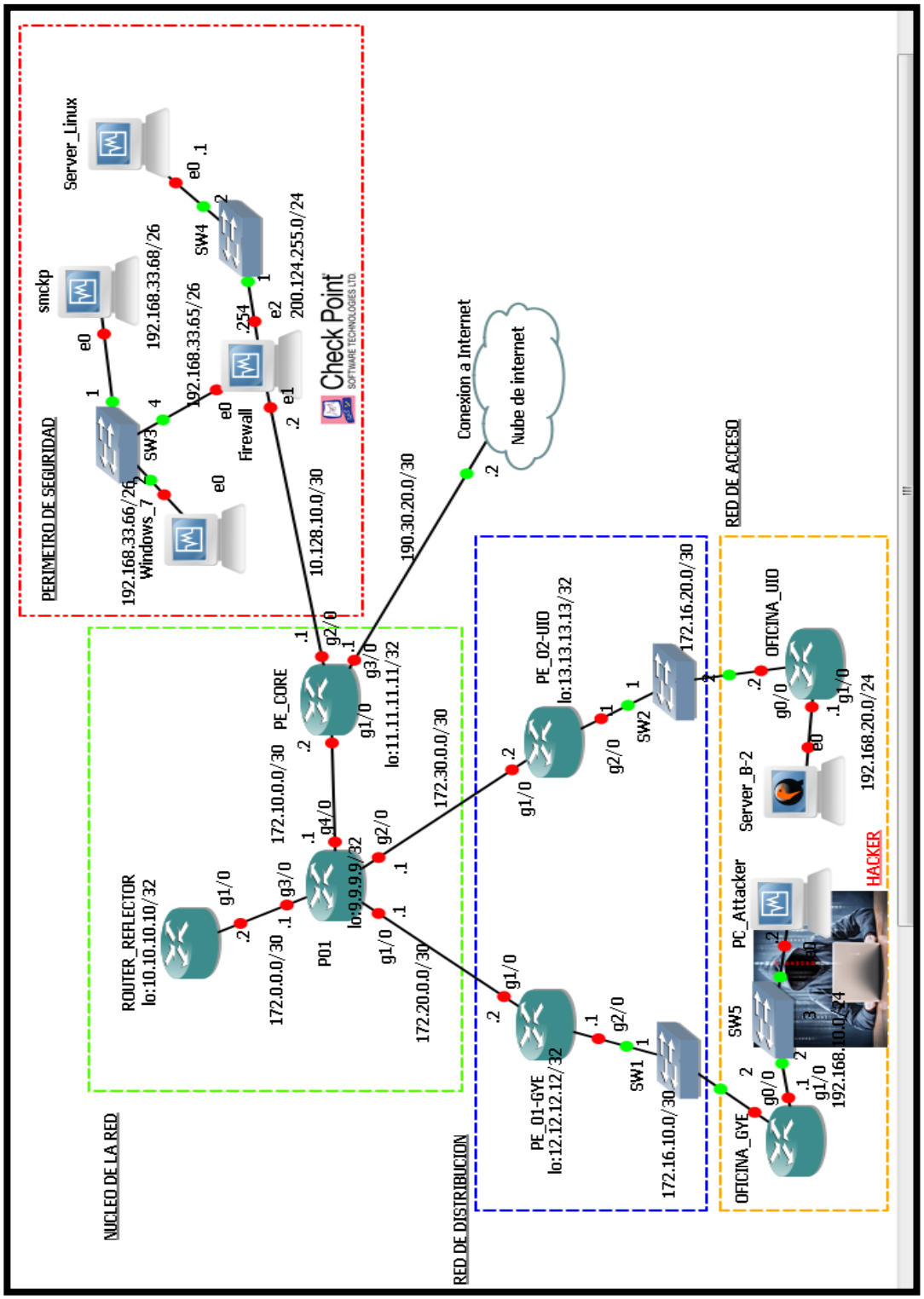
Salcedo, O., Pedraza, L., & Espinosa, M. (2012). Evaluacion de redes MPLS/VPN/BGP con rutas reflejadas. *Tecnura*, 109.

Stephens, R., Stiefel, B., Watkins, S., Desmeules, S., & Faskha, E. (2005). Configuring Checkpoint NGX VPN-1/Firewal-1. En *Configuring Checkpoint NGX VPN-1/Firewal-1* (pág. 13). Rockland - Massachusetts; USA: Syngress Publishing, Inc.

Stephens, R., Stiefel, B., Watkins, S., Desmeules, S., & Faskha, E. (2005). Configuring Checkpoint NGX VPN-1/Firewall-1. En *Configuring Checkpoint NGX VPN-1/Firewall-1* (pág. 14). Rockland - Massachusetts; USA: Syngress Publishing, Inc.

Symantec Corporation. (2016). Website security threat report 2016 (part 1). San José, California, USA.

Anexos

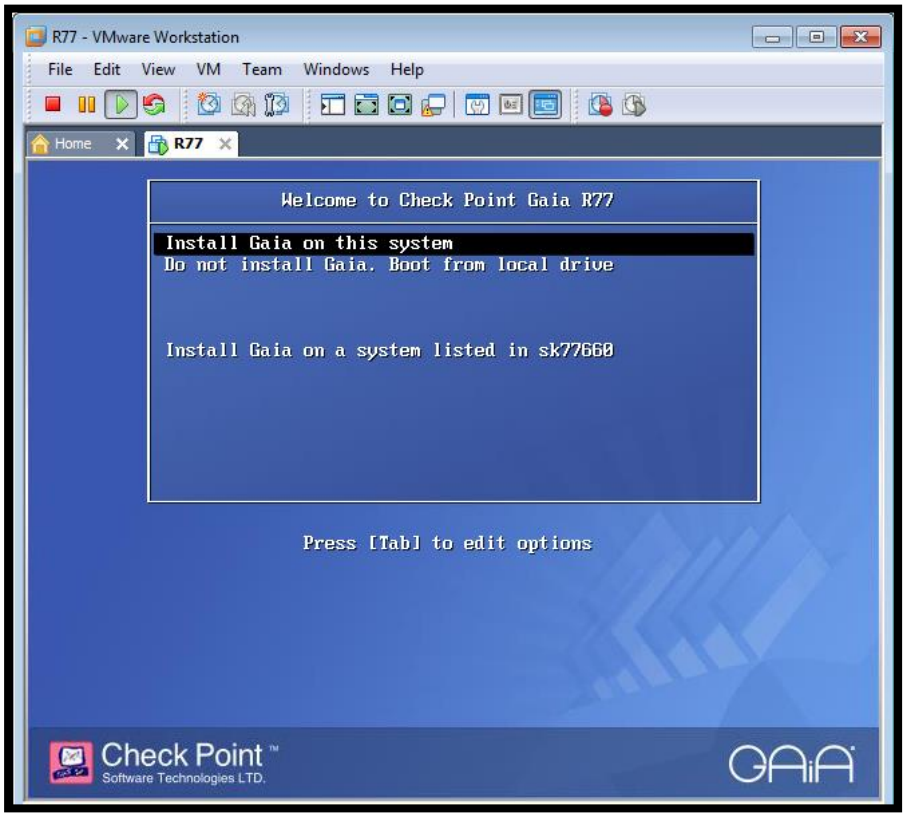


Anexo # 1: Diseño de la red IP MPLS que incluye el perímetro de seguridad con el firewall Check Point y las interfaces aplicadas en las configuraciones

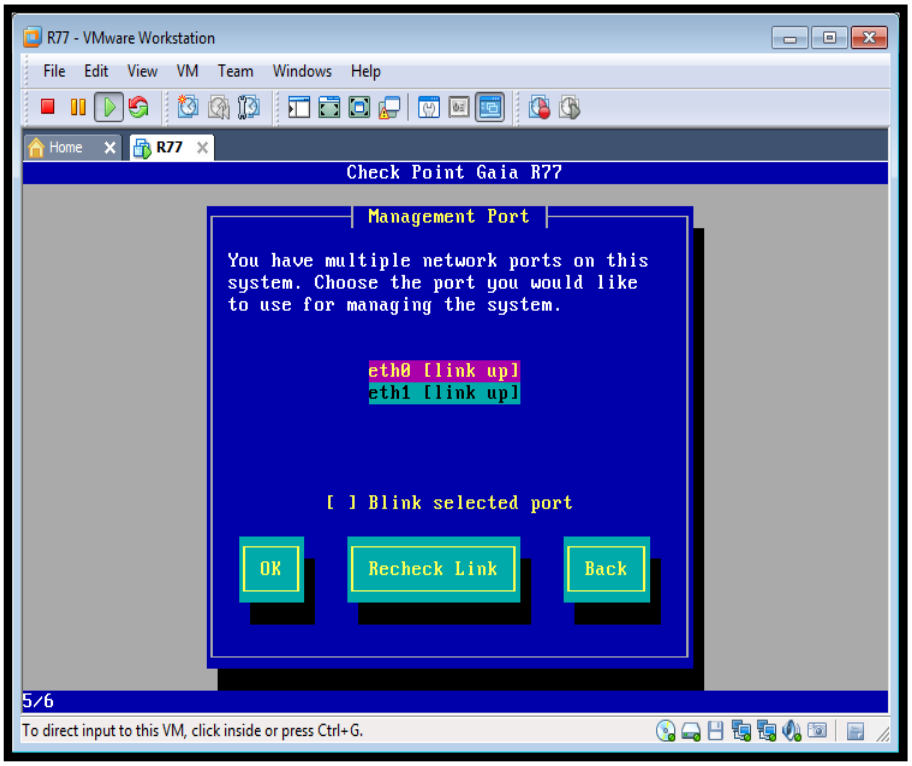
Anexo # 2: Instalación del firewall Check Point, instalación del security manager y la instalación del smart console

Instalacion del firewall Check Point en una maquina virtual (aplica el mismo procedimiento para el security manager)

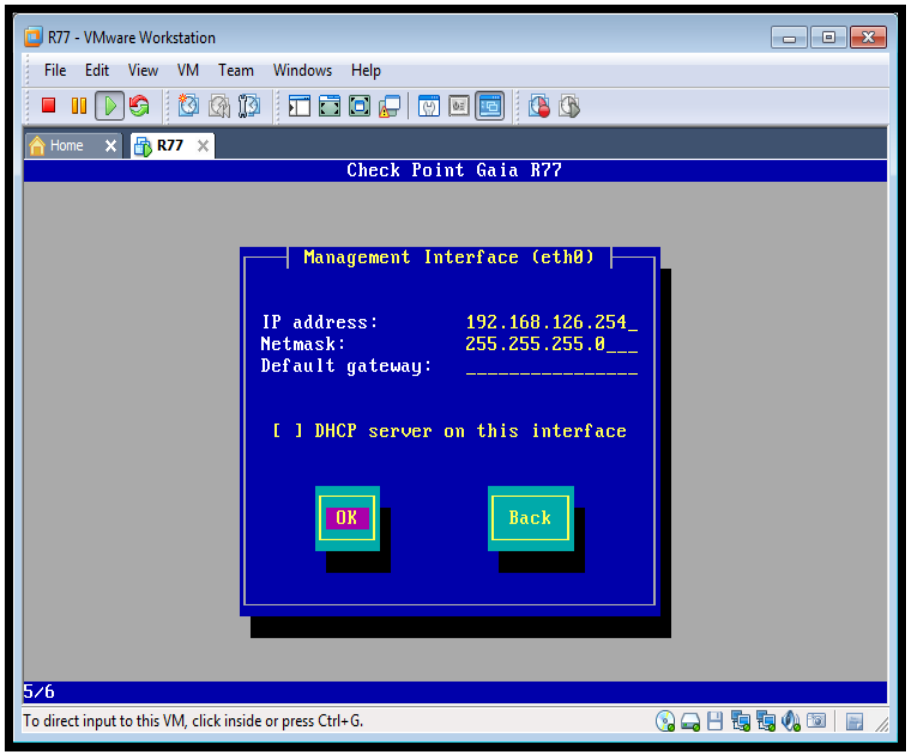
Paso I.- Se selecciona el sistema operativo a instalar:



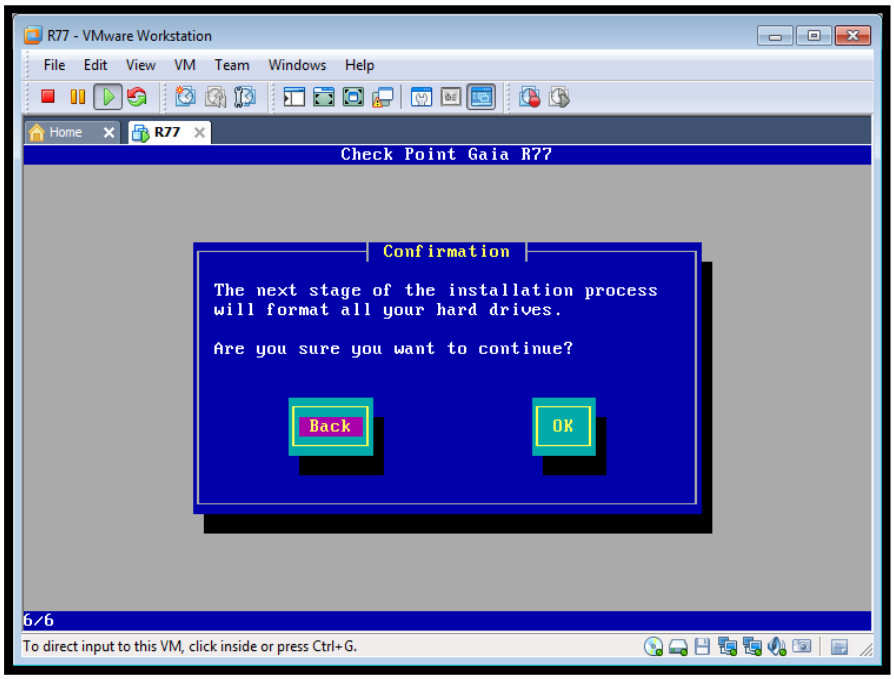
Paso II.- Se selecciona la interfaz de administración del equipo:



Paso III.- Se configura la dirección ip de gestión del equipo:

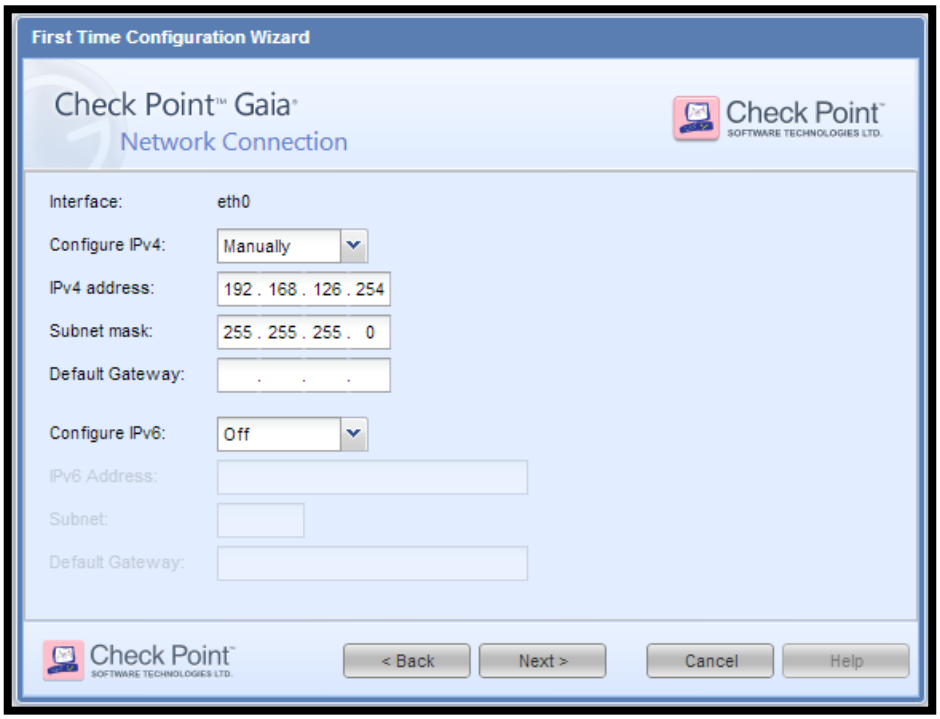


Paso IV.- Se acepta los cambios realizados:

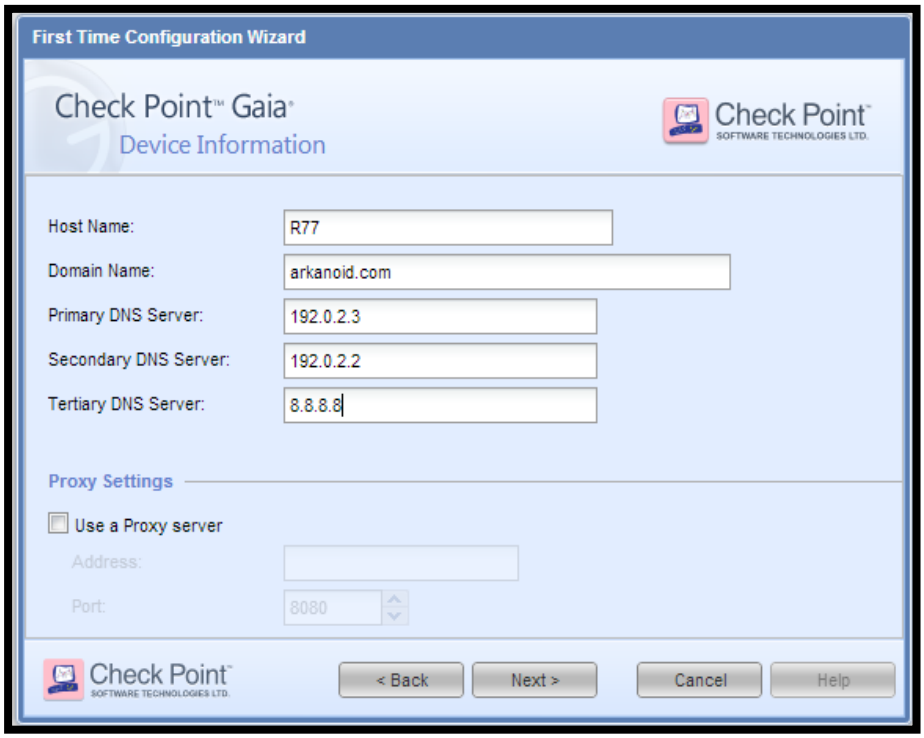


Paso V.- Se ingresa via https al servidor ya levantado:

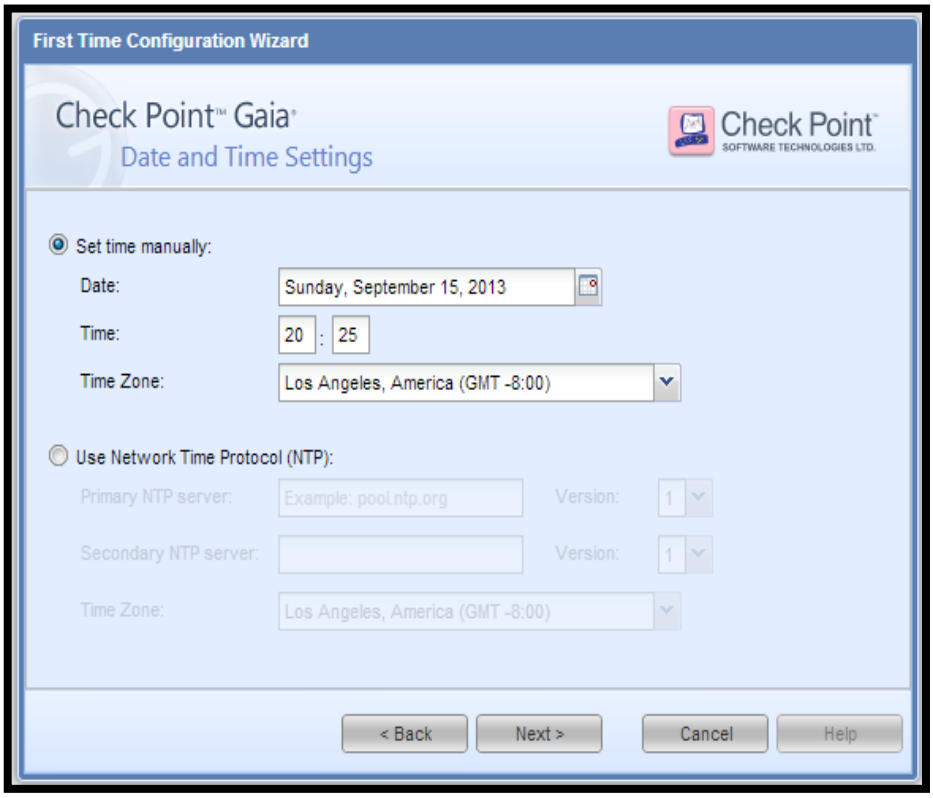
Paso VI.- El equipo muestra la dirección ip previamente configurada



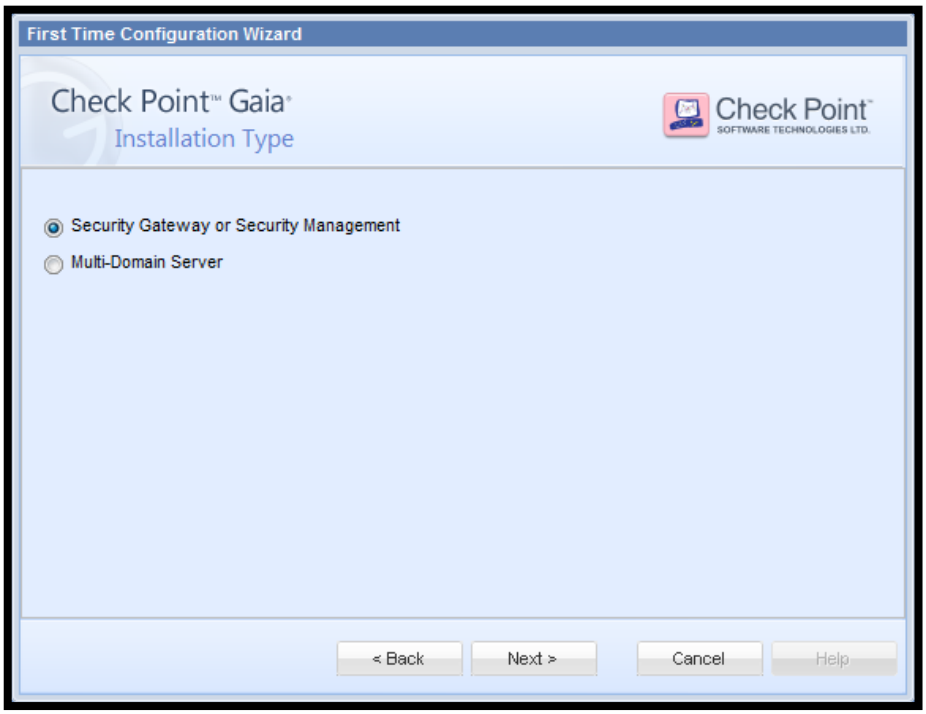
Paso VII.- Se agrega el hostname del equipo, dominio, direcciones ip de los servidores DNS:



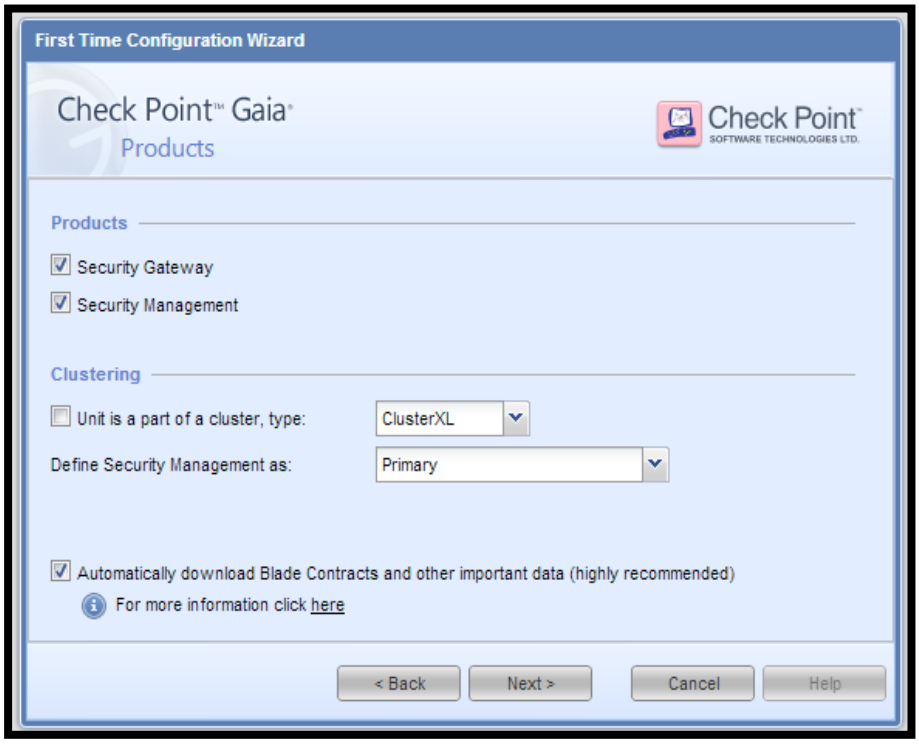
Paso VIII.- Se selecciona la fecha actual, hora y el time zone adecuado:



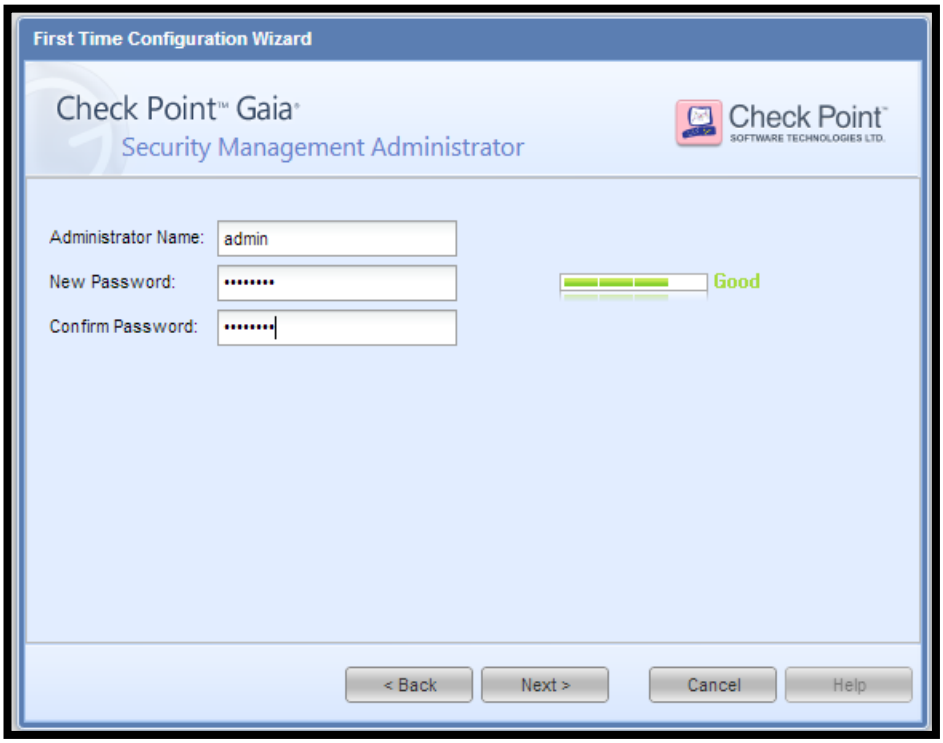
Paso IX.- Se selecciona security Gateway or security manager:



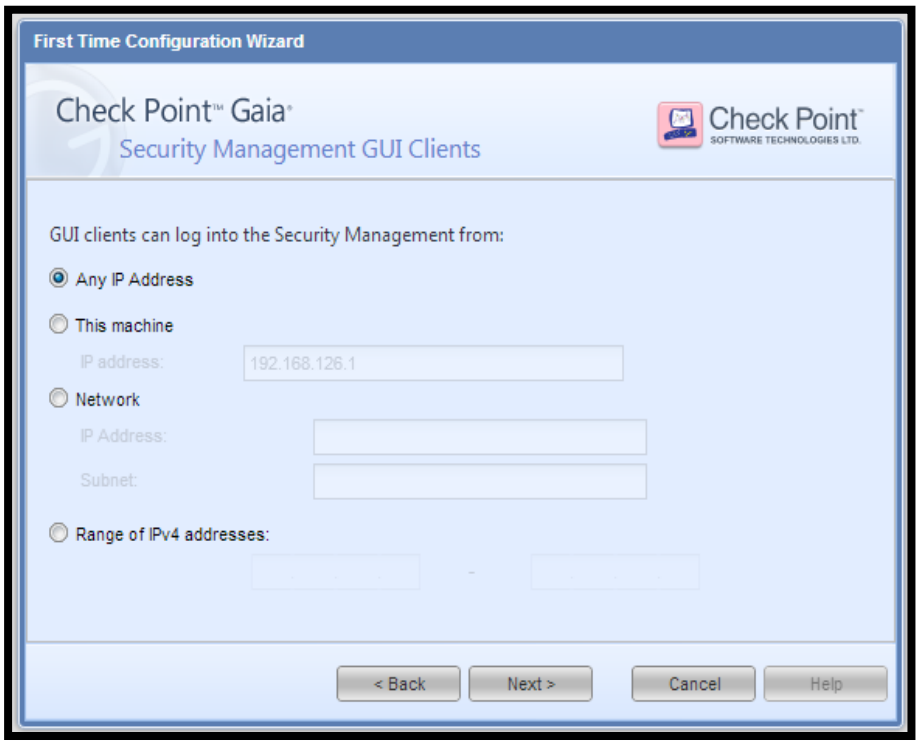
Paso X.- Se selecciona security Gateway o el security manager dependiendo del equipo que desean configurar:



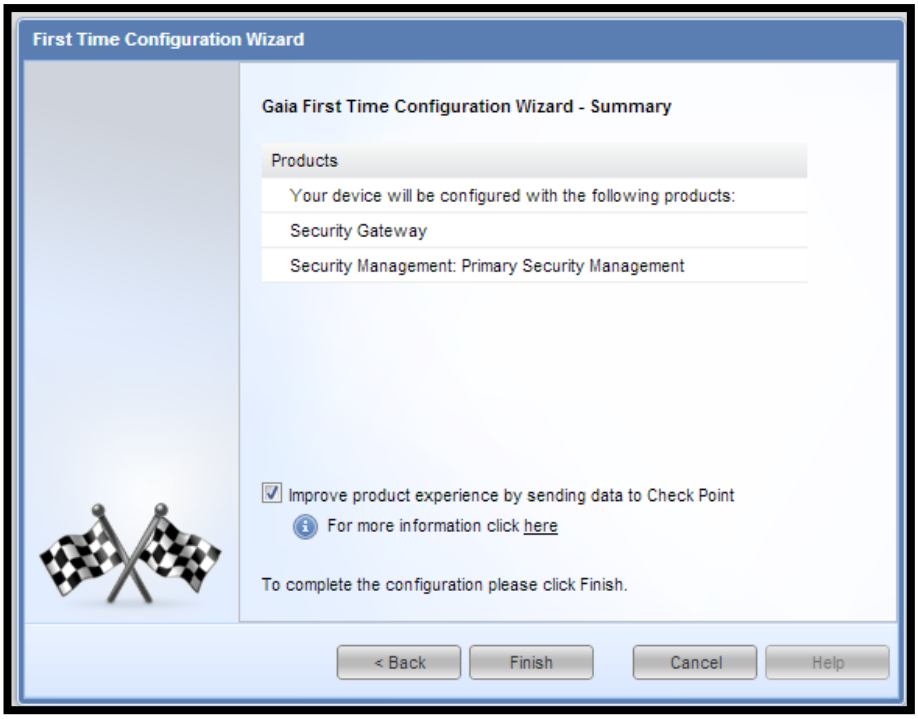
Paso XI.- Se configura la contraseña de acceso del usuario admin:



Paso XII.- Se selecciona el direccionamiento ip de los clientes que accederían al security manager; al colocar any, cualquier ip puede conectarse al equipo:

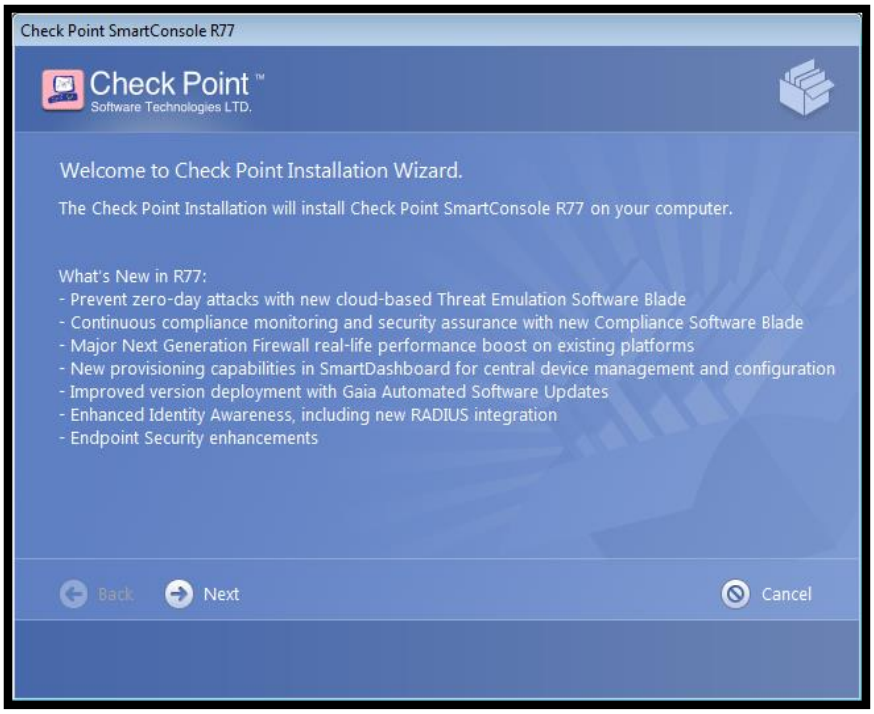


Paso XIII.- La instalación ha finalizado exitosamente, se selecciona finish para guardar los cambios en el equipo:

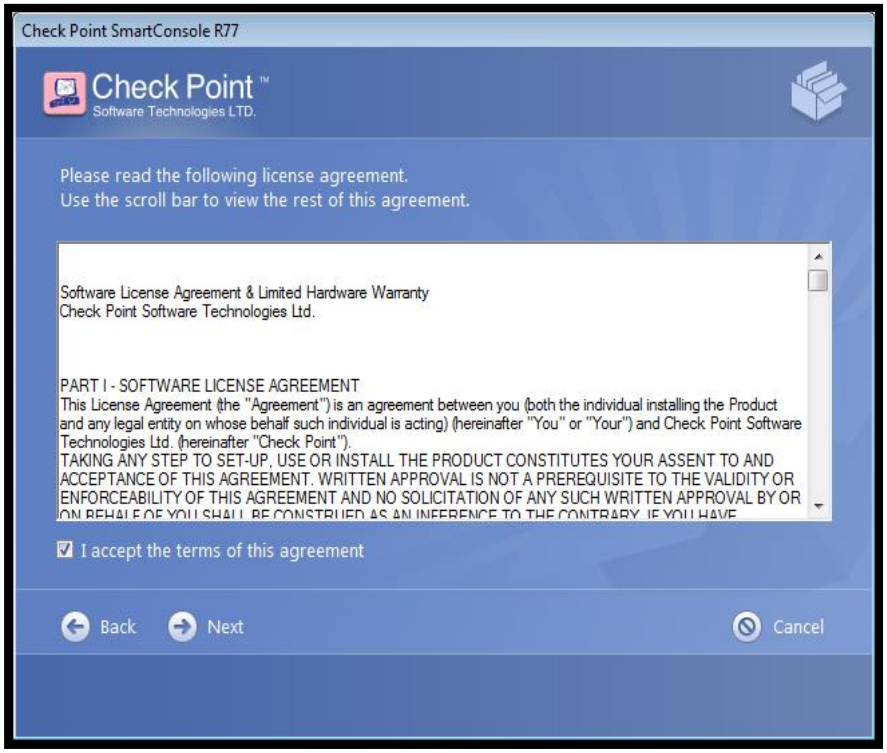


Instalacion del Smart console en una maquina virtual:

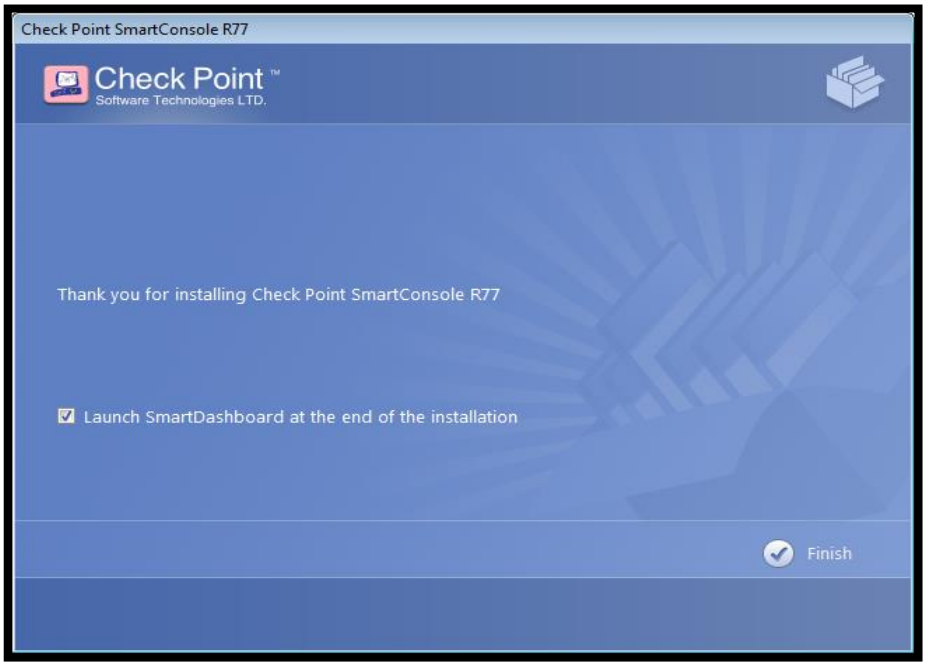
Paso I.- Se instala el software Check Point R77 (Smart console) en el servidor



Paso II.- Aceptamos los términos y condiciones de licenciamiento:



Paso III.- Se inicia el proceso de instalación del Smart console R77, da un clic en finish:



Paso IV.- Inmediatamente aparece el Smart dashboard, esto indica que la instalación del Smart console fue realizado de manera exitosa:

DECLARACIÓN Y AUTORIZACIÓN

Yo, **GORDILLO LÓPEZ PATRICIO LEONARDO** con C.C: # 0923016661 autor del trabajo de titulación: **SIMULACIÓN DE UN PERIMETRO DE SEGURIDAD LOGICA EMPLEANDO NUEVA GENERACION DE FIREWALLS PARA PREVENIR ATAQUES EXTERNOS E INTERNOS A LA GRANJA DE SERVIDORES DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN UNA RED IP-MPLS** previo a la obtención del título de **MAGISTER EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, **29 de noviembre del 2016**

f. _____

Nombre: **GORDILLO LÓPEZ PATRICIO LEONARDO**

C.C: **0923016661**

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

SENESCYT
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	**SIMULACIÓN DE UN PERIMETRO DE SEGURIDAD LOGICA EMPLEANDO NUEVA GENERACION DE FIREWALLS PARA PREVENIR ATAQUES EXTERNOS E INTERNOS A LA GRANJA DE SERVIDORES DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN UNA RED IP-MPLS**		
AUTOR(ES)	Gordillo López Patricio Leonardo		
REVISOR(ES)/TUTOR(ES)	MSc. Orlando Philco Asqui; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
CARRERA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	29 de Noviembre del 2016	**No. DE PÁGINAS:**	142
ÁREAS TEMÁTICAS:	Seguridad informática, Redes de datos, Firewalls de última generación, Granja de servidores, Protocolos, Ataques		
PALABRAS CLAVES/ KEYWORDS:	IP-MPLS, Firewall, Seguridad Informática, Hacker, ISP, gateway		

RESUMEN/ABSTRACT (150-250 palabras):
En el presente trabajo de titulación, se exponen los fundamentos teóricos de la red MPLS, la cual, es considerada como una red de transporte para clientes de un ISP; también se analiza las condiciones necesarias para el respectivo control y acceso hacia los servidores del proveedor de internet mediante la implementación de un firewall de última generación, además, se detallan los diferentes tipos de ataques realizados por los hackers, como el de denegación de servicio DDoS, TCP flood, UDP flood y reconocimiento de puertos, que generan tráfico ilegitimo en la red de datos; finalmente se realiza una simulación de diferentes ataques informáticos ocasionados por cibercriminales localizados en cualquier parte de la red, pretendiendo dejar fuera de servicio los servidores de comunicación localizados detrás del firewall del ISP, sin embargo, el gateway instalado en el core de la red impedirá este tipo de accesos no legítimos, asegurando la operatividad de la red para todos sus clientes.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-9-89795547	E-mail: plgordillo.lopez@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Romero Paz, Manuel de Jesús	
	Teléfono: +593-4-2202935 / 0994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec / mromeropaz@yahoo.com	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	