PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

TRABAJO PREVIO A LA OBTENCION DEL TÍTULO DE

MAGISTER EN REDES DE COMUNICACIONES

TEMA:

"ANÁLISIS Y PROPUESTA DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD PERIMETRAL APLICABLE A INSTITUCIÓN PÚBLICA DE SEGURIDAD SOCIAL"

FREIRE ARAGÓN FREDDY ALEJANDRO

Quito, marzo 2018

AGRADECIMIENTOS

No sería justo iniciar este trabajo sin antes agradecer a Jehová, quien ha estado conmigo en cada instante, muchas veces sin siquiera yo merecerlo. Por fijarte en mí y bendecirme siempre en tus tiempos perfectos… Alabado seas, Padre.

A mi esposa, Adriana Elizabeth. Hermoso privilegio es ser tu esposo, caminar a tu lado, y reír con las ocurrencias de tu corazón alegre y bondadoso. Eres el amor de mi vida, bebé.

A mis padres Cristhian y Patricia, quienes con amor, paciencia, valores y bellos sentimientos me convirtieron en la persona que soy ahora. Nunca podré agradecerles lo suficiente, padrecitos.

A mis hermanas María José y María Carolina por su amor y cariño, pero ante todo, por nunca darse por vencidas… ¡Son un ejemplo!

A mis hermosas sobrinas, Eva Martina y Olivia Sofía, por traer tanta alegría a la familia.

A mis suegros John y Adriana, por estar pendientes de mis avances con el presente trabajo, pero ante todo, por abrirme las puertas de su hogar y familia. Les quiero mucho.

Al Dr. Germán Arévalo, PhD., quien como docente ha hecho un trabajo excelente, y como director de tesis, aún mejor. Es un privilegio ser tu amigo.

A Pablo, Christian y Santiago, por su apoyo y arduo trabajo. Es bueno contar con su amistad.

A quienes con su buena voluntad supieron brindarme ayuda aclarando mis dudas.

A todos en la Pontificia Universidad Católica del Ecuador.

DEDICATORIA

A la memoria de mi amado abuelito, Ángel Virgilio Aragón Castro (1924 – 2018)

No te imaginas cuántas cosas me enseñaste, ni cuánto te extraño…

RESUMEN

En la actualidad, tanto las instituciones públicas como privadas explotan con éxito las llamadas “tecnologías de información y comunicaciones” con objetivos tales como ofrecer nuevos y novedosos servicios a sus usuarios y clientes, lograr presencia en Internet, realizar investigaciones, entre otros; sin embargo, para lograrlo requieren de una infraestructura informática, así como un perímetro de seguridad de red pocas veces identificados.

El presente documento presenta información introductoria a las tecnologías de red y dispositivos asociados, así como contenido referencial acerca de las metodologías desarrolladas para la creación de redes, sistemas de seguridad perimetral y entornos seguros creados por los líderes del mercado en cada uno de sus ámbitos.

Del mismo modo, expone la situación de un ente público, mismo que requiere una nueva arquitectura de seguridad perimetral, para lo cual se ha realizado un análisis de la situación actual, se han establecido criterios de comparación e identificado las necesidades presentes y futuras, lográndose así una nueva arquitectura, creada en base a los requerimientos de la institución.

Contenido

Índice de figuras

Índice de tablas

CAPÍTULO I - INTRODUCCIÓN

INTRODUCCIÓN

El presente trabajo presenta un análisis de la situación actual de un sistema de seguridad perimetral basado en firewalls y la consiguiente propuesta de mejoramiento del mismo, teniendo en cuenta las mejores prácticas aplicables a la seguridad de redes y de la información, así como las metodologías de diseño, rediseño y mejoramiento de redes y los sistemas que involucran las tecnologías de información y telecomunicaciones propuestas por los fabricantes Cisco Systems, Check Point Software Technologies e IBM Corporation.

Aunque éste se halla dirigido hacia una institución pública encargada de los servicios de salud, pensiones y otros correspondientes a los afiliados al sistema de seguridad social, el mismo podrá ser aplicable a las realidades de otras instituciones y/o empresas, tanto del ámbito público como privado, ya que su principal objetivo es el de establecer puntos de referencia fundamentales y sólidos como puntos de partida para el análisis y posterior mejoramiento de sistemas de seguridad perimetral.

Por lo tanto, se establecerá un marco de referencia que otorgará información de primera mano en base a las experiencias obtenidas, y que sirva de apoyo al personal del área de seguridad de redes e información cuando se deban realizar tareas como actualizaciones, mantenimientos programados, preventivos o correctivos, análisis de requerimientos de seguridad informática, repotenciación o reemplazo de equipos, generando a su vez un conjunto de información útil para la institución, sea ésta pública o privada.

La necesidad surge debido a que en las instituciones públicas y privadas las tecnologías de la información y telecomunicaciones y las correspondientes a la seguridad de redes e información, hoy por hoy se han convertido una piedra angular que permite el funcionamiento de las mismas al convertirse en el núcleo de procesamiento de información y comunicación global para el ámbito del negocio; empero, estas son consideradas y manejadas muchas veces aún como entornos separados, sin relación aparente, y mucho menos con la importancia y consideración necesarias, motivo por el cual se tornan un problema al momento de establecer y sustentar sus políticas, procesos

y controles relacionados, ante los entes de control que rigen el negocio, posibles auditorías internas y/o externas, o simplemente al requerirse que la información disponible y ofrecida sea la correcta, de modo que los elementos de protección de la información deben ser eficaces y efectivos.

Por tales motivos nace el interés de efectuar una labor que se convierta en aporte para los profesionales de las áreas de tecnologías de la información, telecomunicaciones y seguridad de redes, en base a un análisis profundo de las características, funcionalidades y operaciones de un sistema de seguridad perimetral, pues ésta es la línea de defensa que debe ser la más robusta y confiable ante los distintos eventos que puedan comprometer la seguridad de la red y por ende, de la información de la institución.

JUSTIFICACIÓN

Actualmente en cualquier institución, sea esta grande o pequeña, existe una conexión y presencia en Internet con el objetivo de formar parte de un mercado globalizado y capaz de brindar muchas oportunidades para ofrecer productos y servicios. Si bien teniendo este tipo de presencia se logran muchos beneficios, se presentan a su vez riesgos no menos importantes, que deben ser minuciosamente evaluados, mitigados o eliminados casi al mismo ritmo de la necesidad de incorporar nuevos procesos que permitan la interacción del cliente beneficiario con entidad por medio del uso de las tecnologías de información y telecomunicaciones. Por lo tanto, hoy en día toda organización necesita administrar los riesgos que conlleva la exposición de los datos críticos del negocio, garantizar y mejorar la continuidad del mismo y reducir el costo de las operaciones de seguridad de las redes e información.

La seguridad de la información se convierte en una consideración mayor en el modo en que los procesos del negocio y los sistemas de información con desarrollados, desplegados y administrados; la necesidad de la seguridad entre las funciones del negocio y las operaciones de la empresa es más patente que nunca.

La mayoría de los proyectos están impulsados por impulsores del negocio como de TI, aunque casi siempre son los primeros quienes conforman el factor iniciador, presentándose a la vez los siguientes factores influyentes:

1. Los factores del negocio miden el valor, riesgos y costos económicos que influencian su enfoque hacia la seguridad de la información y redes. También representan problemas y consecuencias de partes interesadas del sistema empresarial administrado y de diferentes aplicaciones empresariales en la organización.
2. Los factores de valor determinan el valor de los activos del sistema para el negocio y de la propia empresa.
3. Los factores de riesgo implican cumplimiento, estructura corporativa, imagen corporativa y tolerancia al riesgo de la empresa.
4. Los factores económicos determinan la productividad, impacto, ventaja competitiva y costo del sistema.
5. Los factores TI representan limitaciones operacionales en el entorno general de TI, por ejemplo, la complejidad de un sistema, incluyendo su entorno, que es expuesto a amenazas internas y externas, presentando riesgos que la organización debe atender. Representan también consideraciones técnicas que afectan a la confiabilidad del entorno de TI y muy posiblemente los sistemas empresariales administrados como un todo.

De esta manera, puede verse claramente que la combinación de impulsadores y factores tanto del negocio como de Tecnologías de la Información y Comunicaciones y redes representan la clave para la gestión de la seguridad de la información, y por ende de la red.

ANTECEDENTES

Para el presente trabajo se tomará como referencia a una institución pública de seguridad social, organización que se halla en un constante proceso de mejora tecnológica, en la que se hallan involucradas tanto áreas como componentes heterogéneos, que con gran esfuerzo y compromiso, permiten ofrecer tanto al cliente interno como externo servicios de vanguardia, en beneficio de los afiliados al sistema de seguridad social.

Debido a ello, se tomaron como referencia diagramas y documentos de la Dirección Nacional de Tecnología de la Información (DNTI) para llevar a cabo actividades realizadas por esta última. Los componentes tecnológicos (tanto a nivel de hardware y software) deben cumplir especificaciones estrictas definidas por la DNTI, con el objetivo de que una vez implementados y probados, sean capaces de funcionar sin inconvenientes en conjunto con la demás infraestructura tecnológica de la institución.

Si bien se disponen componentes heterogéneos, las especificaciones aplicadas a los mismos permiten un nivel de estandarización de características que en conjunto permiten a la institución disponer de un parque tecnológico robusto. Uno de estos componentes está formado por los equipos de seguridad perimetral, que trabajan en conjunto con los demás, tales como equipos de usuario final, servidores, routers, switches, aplicaciones, entre otros.

El crecimiento de la institución, así como los servicios que se están brindando al afiliado y los que en un futuro se ofrecerán, está teniendo un impacto fuerte en el rendimiento de los sistemas de la institución. Pese a que se ha identificado esta problemática y han existido esfuerzos internos para atacar dicho problema, a la vez que se ha hecho patente la necesidad de revisar y mejorar la información interna correspondiente al diseño de la red de tal modo que se identifiquen y eliminen potenciales cuellos de botella, así como la optimización de los equipos de seguridad perimetral, la inexistencia de un análisis profundo y por ende la indisponibilidad de la documentación resultante, ha permitido que el mejoramiento de dichos sistemas no sea considerado como prioritario.

Es por ello que el autor realizará un análisis del estado de la arquitectura de seguridad perimetral, para en base a una comparativa de las principales metodologías de mejoramiento de red y seguridad, plantear la mejor alternativa y diseñar/elaborar la propuesta correspondiente; todo ello según las mejores prácticas establecidas para el diseño de redes y seguridad de la información.

OBJETIVO GENERAL

Realizar un análisis del sistema de seguridad perimetral en base a las metodologías propuestas por Cisco Systems (PPDIOO, Top-Down), Check Point (SDP), IBM (ISF) que permitan el mejoramiento de la arquitectura de seguridad perimetral.

OBJETIVOS ESPECÍFICOS

- Analizar las metodologías de Cisco (Top-Down Network Design, Bottom-Up, PPDIOO) usadas en el análisis, diseño e implementación de redes.
- Analizar la metodología de Check Point (SDP: Software Defined Protection) usada en el análisis, diseño e implementación de sistemas de seguridad perimetral.
- Analizar la metodología de IBM (IBM Solutions Framework) usadas en el análisis, diseño e implementación de sistemas de seguridad perimetral acorde a la naturaleza del negocio.
- Realizar una comparativa de las metodologías antes mencionadas.
- Identificar los distintos riesgos y amenazas que enfrenta la infraestructura tecnológica la institución.
- Presentar la solución elegida de acuerdo a la situación de la institución.
- Elaboración de la propuesta de mejoramiento correspondiente para el sistema de seguridad perimetral.
- Recomendar políticas de mejora continua y control del sistema de seguridad perimetral.

CAPÍTULO II - DEFINICIONES GENERALES Y TERMINOLOGÍA DE RED

EL MODELO DE REFERENCIA ISO OSI

A fines de la década de los setenta, la Organización Internacional para la Normalización (ISO – International Standards Organization) inició el desarrollo de un modelo conceptual para la conexión en redes de datos, al que nombró Open Systems Interconnection Reference Model o Modelo de Referencia de Interconexión de Sistemas Abiertos (estándar ISO 3309). En los entornos de redes, éste es mejor conocido como modelo OSI (Open Systems Interconnection). En el año de 1984, el modelo pasó a ser el estándar internacional para las comunicaciones de red, al proporcionar un marco de trabajo conceptual que posibilitaba explicar claramente y de un modo relativamente sencillo la manera en que los datos son transportados dentro de una red.

El modelo OSI separa todo el proceso de transmisión de información entre nodos informáticos en siete capas; cada capa es responsable de realizar una tarea específica dentro del proceso total. Este marco de trabajo basado en capas se utiliza para describir y explicar el conjunto de protocolos reales que son empleados para permitir la conexión entre distintos sistemas, e incluso correlacionarlos con otros modelos existentes, tales como TCP/IP y AppleTalk.

Capas del Modelo OSI

El objetivo del modelo OSI es el de posibilitar el trabajo cooperativo entre sistemas abiertos. Un sistema abierto es aquel formado por un conjunto de computadores, periféricos, terminales de datos, material lógico, operadores humanos, entre otros elementos, que conforma un elemento que se encuentra en capacidad de procesar y/o transferir información.

Desde esta óptica, cada sistema abierto se considera está compuesto por siete capas verticales. Asimismo, el modelo prevé una comunicación entre capas de un mismo sistema (capa n+1 con n y n con n-1) llamada “servicio”, y una comunicación horizontal entre sistemas (capa n con n) bautizada como “protocolo”.

FIGURA 2.1 – CAPAS QUE FORMAN EL MODELO OSI

Fuente: El autor

Las tres capas superiores están relacionadas asuntos concernientes a la aplicación, tales como la interfaz de usuario y el formato de datos, en tanto que las cuatro capas inferiores se relacionan con tareas de transporte, como la transmisión de datos y las características físicas de la red.

Es esencial comprender el modelo de referencia OSI desde el punto de vista del diseño debido a su arquitectura modular. El modelo OSI divide las tareas específicas involucradas en mover la información de un dispositivo de red a otro en siete grupos más pequeños y manejables de tareas o acciones.

Los objetivos generales del modelo OSI son mejorar la interoperabilidad y la funcionalidad entre diferentes aplicaciones y proveedores, así como facilitar a los administradores de red enfocarse en el diseño de capas particulares del modelo. Por ejemplo, las aplicaciones se pueden diseñar sin tener que preocuparse por las capas OSI más bajas, ya que si el paquete ha sido analizado ya por las capas inferiores, existe un cierto nivel de confianza de que las capas inferiores procesarán y enviarán el paquete exitosamente a través del medio de transmisión.

Capa de Aplicación

La capa de aplicación (capa 7) es donde el usuario final interactúa efectivamente con una aplicación. Por ejemplo, cuando se tiene información para transmitir (tales como solicitud de datos, imágenes, documentos electrónicos, etc.), la capa de aplicación interactúa directamente con cualquier aplicación software que se comunique con la red.

Dependiendo de la información que el usuario desee enviar a través de la red, se utiliza un protocolo específico, como por ejemplo:

- Los protocolos SMTP o POP3 se usan para enviar un mensaje de correo electrónico
- El protocolo FTP se usa para transmitir un archivo a través de la red
- El protocolo Telnet se usa para controlar un dispositivo remoto

Capa de Presentación

La capa de presentación (capa 6) garantiza que los datos sean comprensibles para el sistema destino. En otras palabras, los datos deben ser preparados, convertidos y formateados de tal modo que el sistema final pueda reconocerlos y sepa cómo manejarlos, de tal manera que la información enviada desde un host origen pueda ser interpretada adecuadamente por el host destino.

Incluye las conversiones necesarias para formatear, estructurar datos, codificar, esquemas de compresión para video y audio (por ejemplo, archivos MPEG, AVI, JPEG, GIF y TIF), esquemas de encriptación y formatos de representación de caracteres (tales como ASCII a Unicode). En pocas palabras, si los paquetes de la capa de aplicación llegan a ésta sin formato, la capa de presentación los traduce y luego los envía hacia adyacente inferior, la capa de sesión.

Capa de Sesión

Desde un punto de vista técnico, los sistemas de comunicaciones están compuestos por diferentes solicitudes de servicio, y las respuestas de servicio entre aplicaciones se encuentran en diferentes dispositivos de red. La capa de sesión (capa 5) establece, gestiona y finaliza estas sesiones de comunicación y conecta las capas inferiores con las capas de presentación y aplicación.

Capa de Transporte

La capa de transporte (capa 4) acepta datos de la capa de sesión y los divide en segmentos transportables. Esta capa es responsable de que la información que llega al dispositivo de destino esté libre de errores y en el orden correcto (es decir, secuencia de paquetes), pero también es responsable de lo siguiente:

- Confiabilidad
- Comprobación de errores de transmisión
- Corrección de errores
- Retransmisión de datos
- Control de flujo
- Secuenciación
- Multiplexación de datos

Desde el punto de vista técnico, todas estas características se implementan mediante el establecimiento de un circuito virtual entre el emisor y los dispositivos receptores. La capa de transporte inicia, mantiene y termina estos circuitos virtuales, y usa segmentos como la unidad de datos de protocolo. Los segmentos son conjuntos de datos definidos que incluyen información de control y se envían entre las capas de transporte de los puntos finales.

Los dos protocolos principales de la capa de transporte utilizados son TCP (Transmission Control Protocol), un protocolo orientado a la conexión y UDP, (User Datagram Protocol), protocolo no confiable, de bajo costo y no orientado a conexión.
Los protocolos orientados a la conexión establecen una conexión lógica y usan números de secuencia para garantizar que todos los datos se reciban en el destino; mientras que los sin conexión sólo envían los datos y dependen de los protocolos de la capa superior para manejar la detección de errores y corregir posibles problemas.

Capa de Red

La capa de red (capa 3) es la responsable de conocer la ruta (enrutamiento) desde el dispositivo emisor hasta el receptor, así como de los esquemas de direccionamiento lógico (como por ejemplo IP) que asignan direcciones lógicas a los hosts de la red en ambos lados de la ruta de comunicación.

Esta capa envía datagramas (o paquetes), que contienen un conjunto definido de datos que incluye información de direccionamiento y control, y se encaminan entre los dispositivos de origen y de destino. Si un datagrama necesita ser enviado a través de una red que puede manejar sólo una cierta cantidad de datos a la vez, el datagrama puede ser fragmentado en múltiples paquetes y reconstruido por el dispositivo receptor. Si no se produce fragmentación, se envía un datagrama como un paquete único.
Es importante tener en cuenta que un datagrama es una unidad de datos, mientras que un paquete se envía físicamente a través de la red.

Además de los esquemas de direccionamiento lógico, la capa de red también es responsable de la selección de enrutadores y el reenvío de paquetes, utilizando los siguientes tipos de protocolos:

- Protocolos enrutados: IP, IPX / SPX, AppleTalk y DECnet
- Protocolos de enrutamiento: RIP, EIGRP, OSPF, IS-IS y BGP

Los protocolos enrutados son responsables de las reglas y procesos reales con respecto a la encapsulación de los paquetes de datos, y finalmente se enrutan a través de la red, en tanto que los protocolos de enrutamiento mueven los paquetes provenientes de los protocolos enrutados (unidades de datos de capa 3) a través de la red, de un enrutador a otro, usando algoritmos de enrutamiento específicos.

Capa de Enlace de datos

La capa de enlace de datos (capa 2) define el formato de los datos que se transmiten a través de la red física. Esta capa tiene dos subcapas: la subcapa LLC (Logical Link Control) y la subcapa MAC (Media Access Control). LLC trata con la capa de red mientras que MAC tiene acceso a la capa física (capa 1).

La subcapa LLC (IEEE 802.2) permite que múltiples protocolos de capa 3 se comuniquen a través del mismo enlace físico al permitir que éstos se especifiquen en los campos LLC.

La subcapa MAC (IEEE 802.3) especifica la dirección MAC física que identifica un dispositivo en una red.

Cada frame enviado a través del cable contiene un campo de dirección MAC, y sólo los dispositivos con una dirección MAC específica pueden procesarlo. Un campo de dirección MAC origen también se incluye en el frame.

La capa de enlace de datos es responsable de la transmisión confiable de datos a través de un enlace físico, empleando especificaciones que proporcionan diferentes características de red y protocolos, incluyendo direccionamiento físico, topologías de red diferentes, notificaciones de errores, secuencias de frames (unidades de datos de capa 2), control de flujo.

La capa 2 está relacionada con una estructura de direccionamiento específica, concretamente el direccionamiento físico, en oposición al esquema de direccionamiento lógico de capa 3. El direccionamiento físico generalmente viene en forma de direcciones MAC que se graban en una tarjeta de interfaz de red (NIC) o en las interfaces de los dispositivos de red.

Capa Física

La capa física (capa 1) se encuentra en la parte inferior de la pila de protocolos OSI y representa el medio físico real en el que viaja la información entre los dispositivos de red. Como se mencionó, esta capa se interconecta con la capa de Enlace de Datos a través de la subcapa MAC, que controla el envío de las señales físicas que codifican los dígitos binarios (0 y 1) en señales adaptadas a las características del medio de transmisión físico (por ejemplo, señales eléctricas sobre un enlace de cobre u óptico-lumínicas si se trata de fibra óptica).

Los siguientes protocolos operan en la capa física:

- Protocolos de red de área local (LAN) (Ethernet, IEEE 802.3, 100Base-T, Token Ring / IEEE 802.5 y FDDI)
- Protocolos de red de área amplia (WAN) (EIA / TIA-232, EIA / TIA-449, V.35 y EIA-530)

La capa 1 define los procedimientos de medios físicos, aspectos eléctricos y mecánicos, codificación y modulación (voltaje) en la línea (es decir, la señal eléctrica es 0 o 1, o está en un estado de transición), así como la activación, el mantenimiento y desactivación del enlace físico real entre múltiples sistemas en redes LAN o WAN.

Encapsulamiento

Tanto en entornos LAN como WAN, la transmisión de paquetes puede analizarse empleando el modelo de OSI de siete capas.

Cuando los datos son transmitidos por el origen hacia un destino específico, éstos pasan a través de las capas Aplicación, Presentación y Sesión, llegando así la PDU (Protocol Datagram Unit) a la capa de Transporte. En esta capa, un encabezado de 20 bytes se coloca delante de los datos.

Independientemente de si el protocolo es confiable, orientado a la conexión (TCP) o uno no confiable y sin conexión (UDP), los datos y el encabezado de capa 4, que juntos forman un segmento, se trasladan a la capa 3, como se ilustra en la figura 2.2, a continuación:

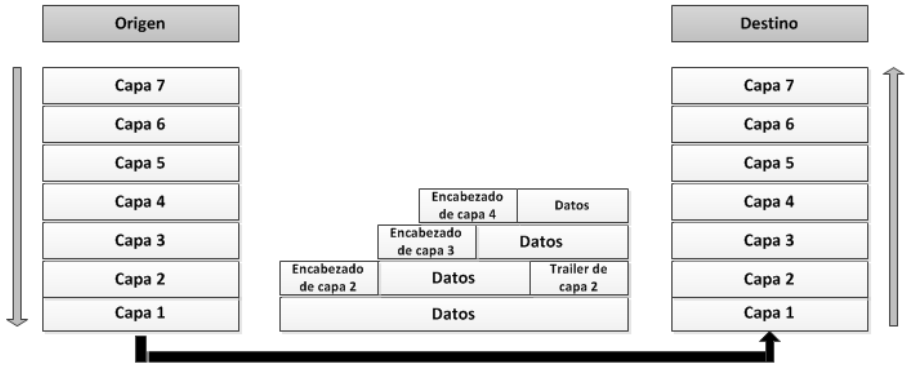


FIGURA 2.2 – ENCAPSULAMIENTO DE PAQUETES

Fuente: El autor

La capa de red coloca su encabezado delante del segmento recibido y este grupo se convierte entonces en un paquete (o un datagrama). El encabezado de capa 3 contiene campos importantes, como la dirección lógica (dirección IP) tanto del dispositivo de origen como el de destino. El paquete recién formado se pasa luego a la capa 2. La capa de enlace de datos crea asimismo una nueva unidad de datos, llamada frame (trama, cuadro), añadiendo el encabezado de la trama y el trailer (carga o cola). La trama se pasa luego a la capa física, que convierte la información en bits que se envían a través del medio físico. Tanto los encabezados y trailers conforman una forma específica de información de control que permite que los datos sean trasladados dentro de la red correctamente. Por lo tanto, los datos en cada capa se encuentran encapsulados en la información apropiada correspondiente a la capa específica, incluido el direccionamiento y la comprobación de errores.

Una unidad de datos de protocolo (PDU – Protocol Datagram Unit) consiste en una agrupación de datos utilizada para intercambiar información en una capa del modelo OSI en particular.

Los tipos de PDU de capa 1 hasta la capa 4, que representan el grupo de datos y los encabezados y trailers específicos, se resumen de la siguiente manera:

Capa	PDU
Física	Bit
Enlace de datos	Marco (frame)
Red	Paquete (datagrama)
Transporte	Segmento

Tabla 2.1 – Capas inferiores del modelo OSI y su PDU

Fuente: El autor

El tamaño total de la información aumenta a medida que los datos viajan a través de las capas inferiores (desde la capa 1 hasta la 4). El dispositivo destino recibe los datos, y esta información adicional es analizada y luego se elimina a medida que los datos pasan a través de las capas superiores, hasta llegar a la capa de aplicación, donde los datos se desencapsulan.

Además de los campos de direccionamiento lógico de capa 3 ubicados en el encabezado, también se aplica una estructura de direccionamiento en el encabezado de capa 2 (es decir, la dirección MAC). Cada dispositivo de red tiene una dirección física grabada en él, misma que se encuentra en un campo especial en el encabezado de la capa de Enlace de datos. Ésta cambia a medida que el paquete pasa de un dispositivo a otro (por ejemplo, desde el computador de origen a un router, de un router a otro router, desde un router a un switch, y finalmente al computador destino)

Sin embargo, las direcciones IP de origen y destino originales no varían al transitar por la red, ya que el paquete carece de su encabezado de capa 3 cuando va más allá de un router. Si permanece dentro de la misma red LAN, únicamente pasa a través de switches, quienes desencapsulan el encabezado de capa 2, mismo que contiene la dirección MAC. Como resultado, el encabezado cambia a medida que el paquete se vuelve a encapsular, al igual que los campos de dirección MAC.

Debido a que diferentes protocolos están disponibles en cada capa (por ejemplo, los paquetes IP son diferentes de los paquetes IPX), la operación adecuada dentro de la red necesita que tanto el origen como el destino se comuniquen utilizando el mismo protocolo.

EL MODELO DE REFERENCIA TCP/IP

El conjunto de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol) (Figura 2.3) es una adaptación moderna del modelo OSI y contiene las siguientes cinco capas:

1. Capa de Aplicación
2. Capa de Transporte
3. Capa de Internet
4. Capa de Enlace de datos
5. Capa Física

En ocasiones, las capas de Enlace de Datos y Física se agrupan como la capa de Acceso a Red o la capa de Interfaz de Red.

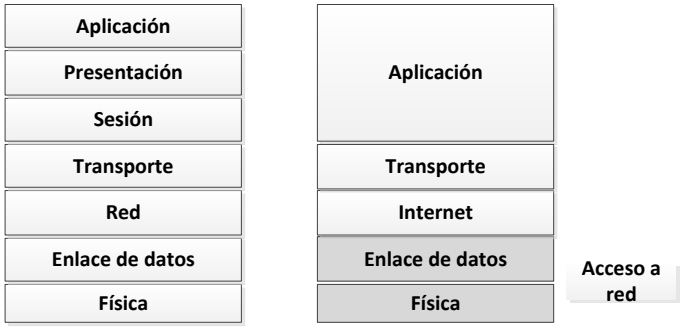


FIGURA 2.3 – MODELO OSI (IZQUIERDA) Y MODELO TCP/IP (DERECHA)

Fuente: El autor

Capa de Aplicación

La capa de Aplicación del modelo TCP/IP engloba la funcionalidad de las capas de Sesión, Presentación y Aplicación correspondientes al modelo de referencia OSI. Se pueden usar varios protocolos en esta capa, entre los que se incluyen los siguientes:

- SMTP y POP3, utilizados para proporcionar servicios de correo electrónico
- HTTP, un protocolo de entrega de contenido de navegador de la World Wide Web
- FTP, utilizado en transferencias de archivos
- DNS, utilizado en la traducción de nombres de dominio
- SNMP, un protocolo de gestión de red
- DHCP, utilizado para asignar direcciones IP a dispositivos de red automáticamente
- Telnet, utilizado para administrar y controlar dispositivos de red

Capa de Transporte

La capa de transporte se basa en dos protocolos:

Transmission Control Protocol (TCP): Brinda una transmisión orientada a conexión, lo cual significa que la ruta en la que se transportan los datos sobre la red es confiable, puesto que los puntos finales establecen una conexión sincronizada antes de enviar los datos. Cada paquete de datos es reconocido por el equipo receptor. Por ejemplo, el protocolo FTP (File Transfer Protocol) usa TCP.

User Datagram Protocol (UDP): Ofrece una transmisión no confiable y sin conexión entre equipos finales. A diferencia de TCP, UDP no garantiza que los segmentos que llegan a un destino sean válidos y lo hagan en el orden correcto, necesitándose verificaciones de integridad y procesos de corrección de errores en la capa de Aplicación. Sin embargo, UDP posee una sobrecarga menor que TCP, ya que el encabezado UDP es mucho más pequeño. Como ejemplo, TFTP (Trivial File Transfer Protocol) emplea UDP.

Las unidades de datos del protocolo TCP y UDP se conocen como segmentos. Cada segmento contiene una cantidad de campos que llevan información diferente sobre los datos, como se muestra en las siguientes figuras:

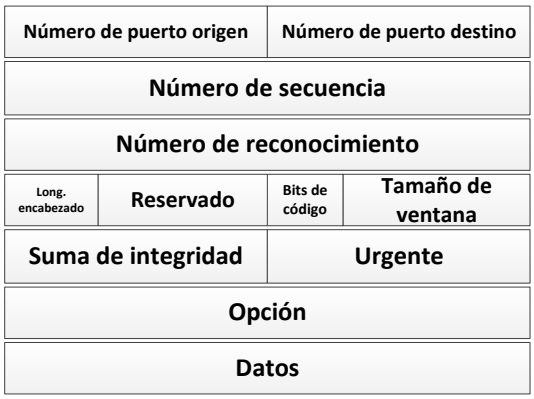


FIGURA 2.4 – CAMPOS DE UN SEGMENTO TCP

Fuente: El autor

Campo	Tamaño	Descripción
Número de puerto origen	16 bits	Identifica a la aplicación usada por el origen
Número de puerto destino	16 bits	Identifica a la aplicación usada por el destino
Número de secuencia	32 bits	Permite verificar el orden correcto de recepción
Número de reconocimiento	32 bits	Permite verificar el orden correcto de recepción
Longitud de encabezado	4 bits	Indica la longitud del encabezado
Reservado	6 bits	No usado
Bits de código	6 bits	Indica el tipo de segmento
Tamaño de la ventana	16 bits	Indica el número de bytes a recibirse antes de enviar un reconocimiento
Suma de integridad	16 bits	Suma de integridad del encabezado y los datos, permite comprobar la integridad del segmento
Urgente	16 bits	Marca el fin de los datos urgentes
Opción	0 hasta 32 bits	Define el tamaño máximo de un segmento TCP
Datos	Variable	Contiene los datos de la capa aplicación

Tabla 2.2 – Descripción de los datos de un segmento TCP

Fuente: El autor

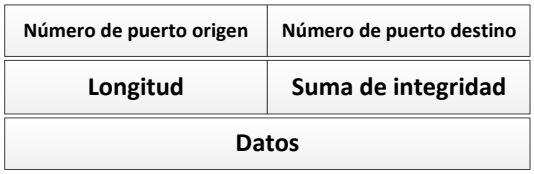


FIGURA 2.5 – CAMPOS DE UN SEGMENTO UDP

Fuente: El autor

Campo	Tamaño	Descripción
Número de puerto origen	16 bits	Identifica a la aplicación usada por el origen
Número de puerto destino	16 bits	Identifica a la aplicación usada por el destino
Longitud	16 bits	Indica la longitud del encabezado y los datos
Suma de integridad	16 bits	Suma de integridad del encabezado y los datos, permite comprobar la integridad del segmento
Datos	Variable	Contiene los datos de la capa aplicación

Tabla 2.3 – Descripción de los datos de un segmento UDP

Fuente: El autor

El encabezado TCP es más grande que el de UDP, ya que todos los campos adicionales son necesarios para garantizar una conexión confiable.

Los números de puerto toman valores de hasta 65535. A la mayoría de las aplicaciones comunes se les asignan números de puerto conocidos en el rango entre 1 a 1023 (el número de puerto 0 está reservado). Los números de puerto desde 1024 hasta 49151 son números de puerto registrados, mientras que los números de puerto 49152 a 65535 definen números de puerto dinámico (asignados automáticamente por dispositivos de red)

Los números de puerto se usan para distinguir entre aplicaciones que se ejecutan en el mismo dispositivo; algunos ejemplos de números de puerto conocidos son los siguientes:

Protocolo	Puerto
TFTP	69 (UDP)
POP3	110 (TCP)
SMTP	25 (TCP)
DNS	53 (TCP y UDP)
SNMP	161 (UDP)
Telnet	23 (TCP)

Tabla 2.4 – Ejemplos de protocolos y sus números de puerto

Fuente: El autor

Cuando se establece una conexión TCP, se sigue un proceso llamado three-way handshake, el cual utiliza bits SYN y ACK en los bits de código de los campos de Segmento, Secuencia y Número de Acuse de Recibo de TCP.

Capa de Internet

La capa de Internet de TCP/IP corresponde a la capa de Red de OSI, e incluye los siguientes protocolos:

Internet Protocol (IP): Este protocolo sin conexión ofrece la mejor entrega de paquetes de la red, confiando en los protocolos de la capa de Transporte (como TCP) para garantizar una conexión confiable.
Las direcciones IP se asignan a cada dispositivo de red o interfaz en la red. Además, el protocolo IP viene en dos “sabores”: IPv4 e IPv6

Internet Control Message Prococol (ICMP): Este protocolo envía mensajes e informes de errores a través de la red. La aplicación más común que depende de ICMP es Ping, la que envía un mensaje de eco ICMP al destino y espera una respuesta también de eco ICMP para garantizar que se pueda alcanzar el destino y para proporcionar información sobre el retraso entre los dos puntos finales.

Capa de Acceso a Red

Esta capa está formada por las capas de Enlace de datos y Física, teniendo la misma funcionalidad que en el modelo de referencia OSI. Un protocolo común utilizado en la capa de Enlace de Datos es el protocolo de resolución de direcciones (ARP – Address Resolution Protocol), el cual solicita las direcciones MAC de un host respecto a una dirección IP conocida. Una vez que se conoce la dirección MAC, ésta se usa como dirección de destino en los marcos (frames) enviados en esa dirección específica.

TIPOS DE REDES

Las redes se clasifican en dos categorías principales: LAN y WAN, basadas en los dispositivos y las áreas que interconectan.

Redes de Área Local (Local Area Networks – LAN)

Una red de tipo LAN es una red computarizada localizada, empleada para permitir la comunicación entre hosts, con el objetivo de compartir información (por ejemplo, documentos, archivos de audio/video, correo electrónico, mensajes de chat) y el uso de una amplia variedad de herramientas de productividad.

Las LAN, como su nombre lo indica, tienen un alcance limitado, abarcando generalmente longitudes que no superan el centenar de metros, por lo que solo pueden conectar dispositivos en el mismo edificio o campus. Las conexiones de área local generalmente pertenecen a las empresas en las que están desplegadas o brindan servicio.

Las diferentes tecnologías LAN disponibles en la actualidad incluyen lo siguiente:

- Ethernet (10 Mbps)
- FastEthernet (100 Mbps)
- GigabitEthernet (1 Gbps)
- LAN inalámbricas (hasta 600 Mbps, según la especificación 802.11n)

Todos los equipos de red en una LAN poseen un esquema de direccionamiento lógico común y asimismo comparten la misma dirección de red (dirección IP). Un ejemplo de una dirección IP es 192.168.10.0, dispositivos individuales pueden tener direcciones lógicas como 192.168.10.1, 192.168.10.2, y así sucesivamente.

Los términos “dirección IP”, router, switch, entre otros, se verán en las siguientes secciones del presente trabajo.

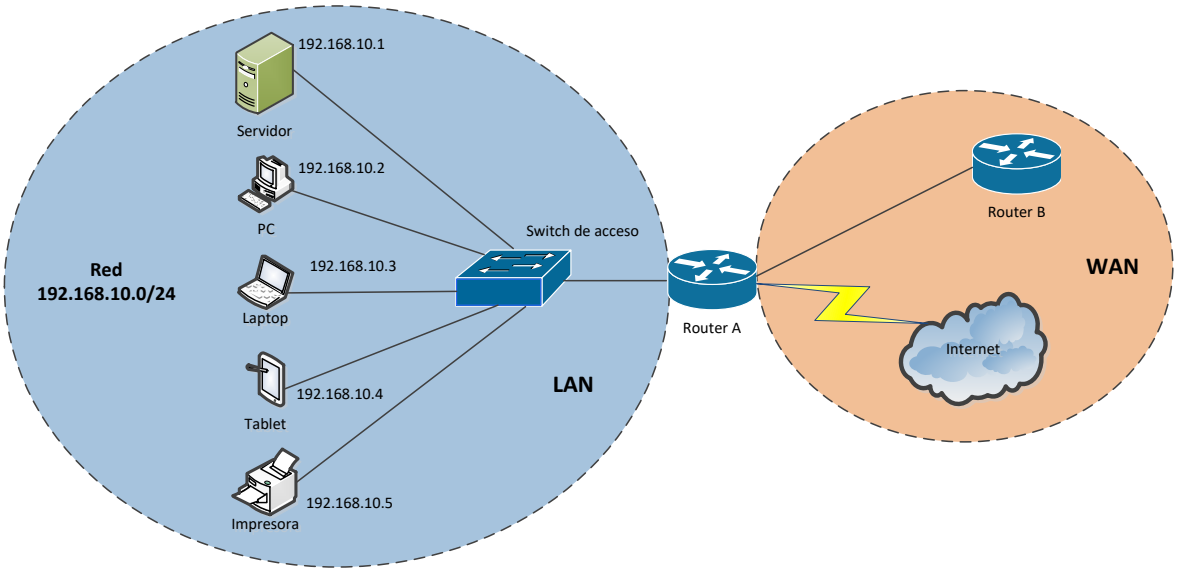


FIGURA 2.6 – EJEMPLOS DE DISPOSITIVOS DENTRO DE UNA RED LAN

Fuente: El autor

De manera general, los dispositivos de red tales como servidores, estaciones de trabajo, laptops, tablets, impresoras, etc. se conectan a un switch de capa acceso por medio de una red cableada o inalámbrica, como se muestra en la Figura 2.6.

El switch de acceso puede tener un enlace de mayor velocidad hacia un router, pudiendo este último estar conectado a otros routers o disponer de una conexión de salida hacia Internet. Todo lo que está detrás del enrutador es parte de la red WAN, por tanto, el router funciona como un dispositivo de borde entre una red LAN y una WAN.

Redes de Área Amplia (Wide Area Networks – WAN)

Una red WAN en pocas palabras conecta múltiples redes LAN o WAN (por ejemplo, Internet es una red WAN muy grande)

Una WAN se encuentra en un área geográfica amplia y dispersa, perteneciendo a un proveedor de servicios de Internet (ISP - Internet Service Provider), el que generalmente cobra una tarifa por usar sus servicios WAN. Debido a su tamaño, una WAN típica es más lenta que una LAN.

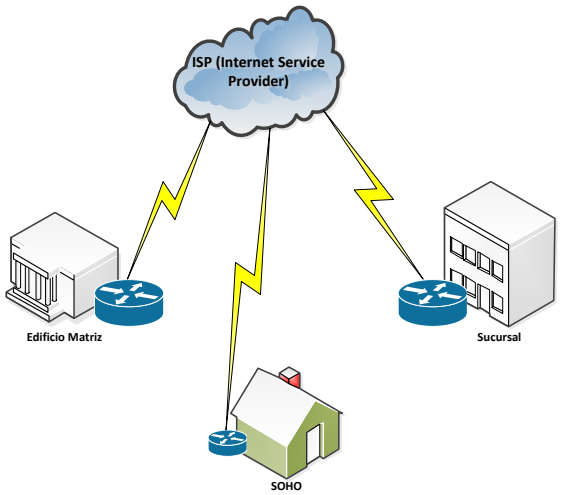


FIGURA 2.7 – EJEMPLO DE UNA RED WAN

Fuente: El autor

Como se muestra en la Figura 2.7, el ISP sirve como una red que cubre un área específica y que conecta distintas redes locales, como por ejemplo una oficina doméstica y una oficina empresarial, o una sucursal y una sede central. Las WAN utilizan una amplia variedad de protocolos y topologías para lograr esta interconexión entre diversas redes LAN.

Las conexiones LAN hacia el ISP pueden tomar muchas formas, dependiendo de la tecnología a usarse, como:

- Redes de conmutación de paquetes (Frame Relay), donde el ISP crea circuitos virtuales permanentes y circuitos virtuales conmutados que transportan datos entre sitios del suscriptor.
- Redes de conmutación de circuitos (RDSI – Red Digital de Servicios Integrados), donde el ISP crea una ruta física reservada durante la duración de la conexión entre dos sitios.
- Líneas T1/E1.
- Líneas arrendadas, empleando protocolos PPP o HDLC.
- Conexiones de acceso telefónico.
- Cable, usando redes de televisión por cable para entregar datos.
- DSL, que utiliza las líneas telefónicas tradicionales de cobre para enviar datos.

Las redes WAN y LAN emplean protocolos de enrutamiento específicos, los cuales se configuran en función de la topología a usarse y otros criterios.

DISPOSITIVOS DE RED Y TECNOLOGÍAS ASOCIADAS

Los tres dispositivos de red más comunes actualmente en uso son los routers (enrutadores), switches (conmutadores) y hubs (concentradores), mismos que se muestran a continuación:

FIGURA 2.8 – ROUTER CISCO MODELO 2821

Fuente: http://routerpictures.blogspot.com/2008/09/cisco-2821-router.html

FIGURA 2.9 – SWITCH HP 5500G

Fuente: https://www.dabware.com.au/hp-a5500-48g-si-switch0235a04v-h3c

FIGURA 2.10 – HUB NETGEAR DS108

Fuente: http://www.listlux.com/dallas/a,32,1827535,Netgear-DS108-10-100-8-Port-Dual-Speed-Hub-RJ-45-w--Uplink-Button----30--Arlington-.htm

Cuando se describen varios dispositivos de red, se utiliza la siguiente terminología:

Dominio: Hace referencia a una parte específica de una red.
Ancho de banda: Indica la cantidad de datos que se pueden transportar en un enlace en un período de tiempo determinado.
Datos de unicast (unidifusión): Corresponden a los datos enviados a un dispositivo
Datos de multicast (multidifusión): Corresponden a los datos enviados a un grupo de dispositivos.
Datos de broadcast (transmisión): Datos enviados a todos los dispositivos.
Dominio de colisión: Incluye a todos los dispositivos que comparten el mismo ancho de banda. Estos dominios son separados por switches.
Dominio de difusión: Incluye a todos los dispositivos que reciben mensajes de difusión. Se encuentran separados por enrutadores routers.

Hub

Es un dispositivo de red que opera en la capa 1 y conecta varios dispositivos que se encuentran en una misma red LAN.
Los hubs se hicieron necesarios cuando surgió la necesidad de conectar más de dos dispositivos, ya que un cable sólo puede conectar dos puntos finales.

Los hubs no tienen inteligencia y no procesan paquetes de manera alguna.

Su función principal es la de enviar todos los datos recibidos en un puerto a todos los demás, de modo que los dispositivos reciban todos los paquetes que atraviesan una red específica, incluso si no están dirigidos a ellos. Por esta razón, los hubs también se llaman repetidores.
Este comportamiento se describe a continuación en la Figura 2.11, donde un paquete enviado por la PC 1 a la PC 3 es emitido por el hub a todos los puertos, obligando a las estaciones de trabajo que no necesitan el paquete (es decir, PC 2 y PC 4) a descartarlo.

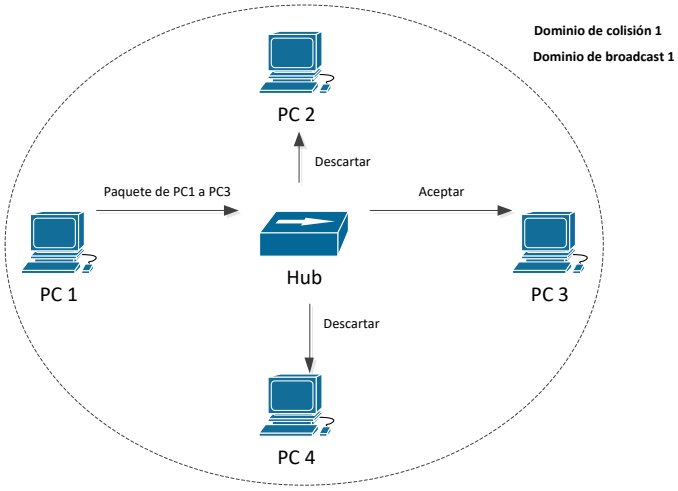


FIGURA 2.11 – MODO DE OPERACIÓN DE UN HUB

Fuente: El autor

Los dispositivos conectados a un hub se encuentran dentro de un mismo dominio de colisión y en el mismo de broadcast.

Switch

El uso de hubs en redes medianas y grandes no es eficiente. Para mejorar el rendimiento, especialmente desde un punto de vista de ancho de banda y seguridad, las redes LAN se dividen en múltiples entornos más pequeños, denominados dominios de colisión, que se encuentran interconectados por un switch LAN.

Cuando se usan switches, solamente el dispositivo de destino en un flujo de comunicación recibe los datos enviados por el dispositivo origen; sin embargo, múltiples transacciones entre los dispositivos conectados a un switch pueden ocurrir de manera simultánea.

A diferencia de los hubs, los switches tienen cierta inteligencia, ya que son capaces de enviar datos a un puerto sólo si los datos necesitan llegar a ese segmento en particular. El cambio de funciones de inteligencia se basa en una tabla de direcciones MAC mantenida en la memoria del switch. Dicha tabla contiene las correspondencias entre direcciones MAC y su puerto asociado, la cual se va llenando cuando un dispositivo envía datos a un dispositivo ubicado en otro puerto del switch, y éste aprende la dirección MAC de origen (dirección de capa 2) y su puerto asociado. A continuación, inunda con

los frames recibidos todos los puertos. Este proceso continúa hasta que la tabla MAC contiene entradas para todos los dispositivos en la red.
Cuando un switch debe reenviar un frame con una dirección MAC de destino que se encuentra en su tabla MAC, lo reenvía sólo al puerto específico al que se refiere.

La Figura 2.12 a continuación ejemplifica este proceso.

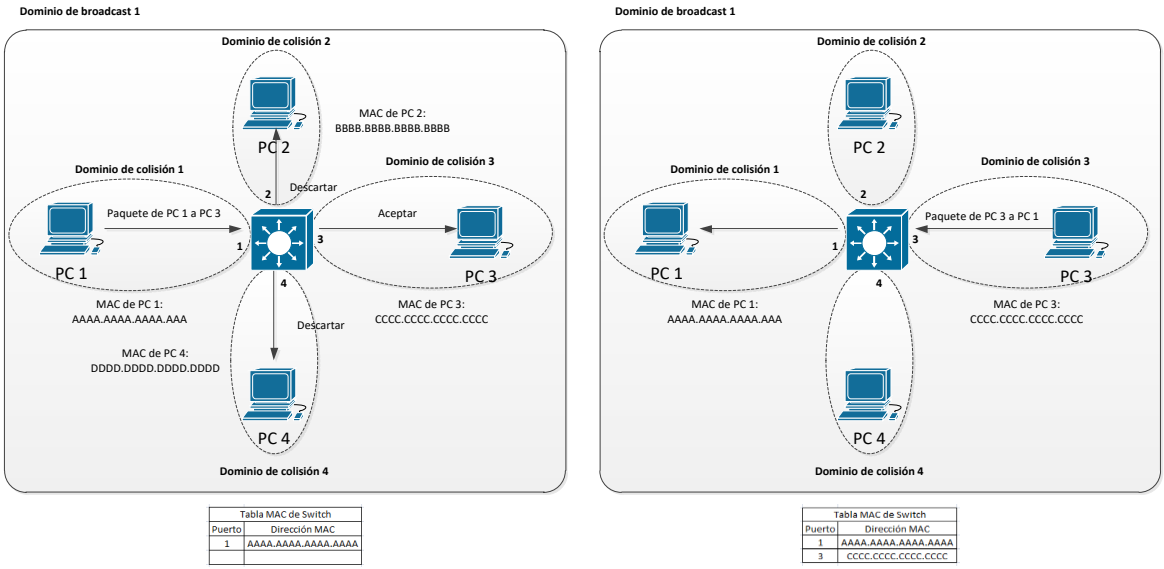


FIGURA 2.12 – MODO DE OPERACIÓN DE UN SWITCH

Fuente: El autor

En el diagrama de la izquierda, PC 1 envía una trama a PC 3, pero el switch desconoce el puerto al que está conectada PC 3, por lo que inunda con esa trama todos los puertos. Al mismo tiempo, registra el puerto de origen y la dirección MAC de esa trama específica (Puerto 1, con una dirección MAC de PC 1)
En el diagrama de la derecha, PC 3 responde y envía un cuadro de regreso a la PC 1, pero el switch no tiene que pasar la trama a todos los puertos, puesto que ahora conoce el puerto de destino asociado a PC 1, que es el puerto 1.
Al mismo tiempo, también registra la asociación puerto-dirección MAC para PC 3, por lo que si PC 1 enviara una trama a PC 3, el switch la reenviará sólo al puerto 3, puesto que sabe ya dónde está conectada.

Los dispositivos conectados a un puerto del switch están en los mismos dominios de colisión. La característica más importante de un switch es precisamente la de separar los dominios de colisión. Asimismo, todos los dispositivos conectados a un switch están en el mismo dominio de difusión.

Existen casos especiales donde el campo destino de capa 2 contiene una dirección de multicast (multidifusión) o de broadcast (difusión). En esos casos, el switch reenvía la trama a múltiples puertos. Además, una categoría especial la conforman los conocidos como switches de capa 3, que tienen capacidades completas de capa 3, incluido el enrutamiento.

Direccionamiento de Capa 2

Como se indicó anteriormente, las direcciones de capa 2 se denominan direcciones MAC o direcciones físicas. Éstas se asignan a las tarjetas de red o interfaces de dispositivos cuando son fabricadas.

Las direcciones MAC (Figura 2.13) tienen un valor de 48 bits, donde los primeros 24 bits comprenden el Identificador Único Organizacional (OUI – Organisational Unique Identifier), el cual representa un código que identifica al proveedor del dispositivo. El segundo bit menos significativo en la parte del OUI identifica si la dirección asignada es local (valor 1) o universal (valor 0), mientras que el bit más significativo identifica a una dirección MAC de tipo unicast (valor 0) o una dirección de multicast (valor 1)
Los últimos 24 bits conforman un valor único asignado a una interfaz específica, permitiendo así que cada interfaz de red sea identificada de una manera única a través de la dirección MAC asociada.

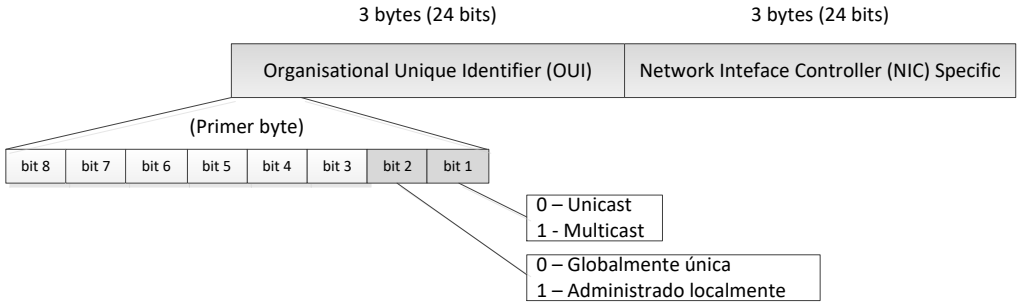


FIGURA 2.13 – ESTRUCTURA DE UNA DIRECCIÓN MAC

Fuente: El autor

Conmutación o Switching

Los switches son dispositivos de red que separan los dominios de colisión y son capaces de procesar datos a altas velocidades gracias a la función de conmutación implementada en hardware por medio de un conjunto de circuitos integrados diseñados para tal fin, conocidos como ASIC (Application Specific Integrated Circuit)

Las redes se segmentan mediante switches para obtener más ancho de banda por usuario al reducir el número de dispositivos que comparten el mismo ancho de banda. Adicionalmente envían tráfico solo en las interfaces que necesitan recibirlo; sin embargo, para el tráfico unicast, el switch envía el frame a un solo puerto, en lugar de hacerlo a todos los puertos.

Cuando un frame ingresa a una interfaz, el switch añade la dirección MAC origen y también el puerto de origen a su tabla de conmutación y después examina la dirección MAC destino. Si se trata de una trama de broadcast, multicast o unicast desconocida, el switch enviará dicho frame a todos los puertos, exceptuando el puerto de origen.

Si las direcciones de origen y destino se hallan en la misma interfaz, el frame se desecha, empero, si conoce la dirección de destino (es decir, el switch contiene una entrada válida en la tabla), lo enviará hacia la interfaz correspondiente.

La operación de un switch puede resumirse de acuerdo a la siguiente ilustración:

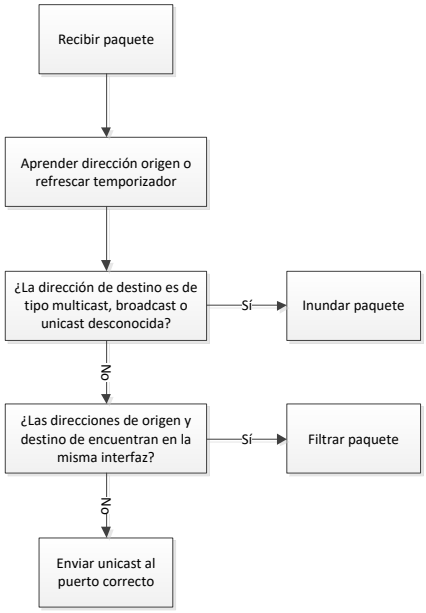


FIGURA 2.14 – DIAGRAMA DE FLUJO DE LA OPERACIÓN BÁSICA DE UN SWITCH

Fuente: El autor

Cuando un switch se enciende, su tabla de conmutación no tiene entrada alguna. La tabla de conmutación (llamada también tabla de direcciones MAC o la tabla CAM (Content Addressable Memory) es una estructura de datos interna que registra todas las direcciones MAC a la par con su interfaz cuando el switch recibe un frame desde un dispositivo. Los switches aprenden las direcciones MAC de origen para enviar datos a los segmentos de destino apropiados.

Un switch, además de inundar las interfaces con tramas unicast desconocidas cuando es necesario, inunda también otros dos tipos de tramas: broadcast y multicast. Muchas y variadas aplicaciones multimedia generan tráfico multicast o broadcast que se propaga a través de una red conmutada (es decir, de un dominio de difusión). Cuando un switch aprende una dirección MAC origen, registra su tiempo de entrada. Cada vez que el switch recibe un frame de la misma fuente, actualiza el tiempo de entrada. Si el switch no recibe otro frame de esa fuente antes de que finalice un temporizador de purgado predefinido, la entrada se elimina de la tabla de conmutación.

Tiempo de entrada	Acción	Puerto	Dirección MAC	Edad (s)
00:00	PC 1 envía frame # 1	Fa0/1	AAAA.AAAA.AAAA.AAAA	0
00:30	Incrementar edad (age)	Fa0/1	AAAA.AAAA.AAAA.AAAA	30
01:15	PC 1 envía frame # 2	Fa0/1	AAAA.AAAA.AAAA.AAAA	0
06:14	Incrementar edad (age)	Fa0/1	AAAA.AAAA.AAAA.AAAA	299
06:16	Entrada eliminada (purgada)	-	-	-
06:30	PC 1 envía frame # 3	Fa0/1	AAAA.AAAA.AAAA.AAAA	0
06:45	Incrementar edad (age)	Fa0/1	AAAA.AAAA.AAAA.AAAA	15

Tabla 2.5 – Ejemplo de una tabla de conmutación de un switch

Fuente: El autor

Las entradas de la tabla de direcciones MAC se eliminan cuando expira el temporizador de purgado, ya que los switches disponen de una cantidad finita de memoria, lo que limita el número de direcciones que pueden almacenar en su tabla de conmutación. Si la tabla de direcciones MAC está llena y el switch recibe un frame desde una fuente desconocida, enviará dicho frame a todas las interfaces hasta que una entrada en la tabla de conmutación se encuentre disponible y le permita aprenda sobre dicha estación. Las entradas se hallarán disponibles cada vez que el temporizador de purgado se agote para una dirección. De esta manera, el temporizador ayuda a limitar las inundaciones de frames al recordar las estaciones más activas de la red. Asimismo, el temporizador de purgado se puede ajustar si la cantidad total de dispositivos de red es inferior a la capacidad de la tabla de conmutación, lo que hace que el switch recuerde la estación por más tiempo y reduzca las inundaciones.

Protocolo Spanning Tree

Definido por el estándar IEEE 802.1D, STP es un protocolo de prevención de bucles que permite a los switches comunicarse entre sí para descubrir bucles físicos en una red. Si se encuentra un bucle, STP especifica un algoritmo que los switches pueden usar para crear una topología lógica sin bucles. Éste crea una estructura en formar de árbol lógico, con ramas libres de bucles, la cual que abarca toda la topología de Capa 2.

Los bucles ocurren con mayor frecuencia como resultado de conexiones redundantes entre switches, como se muestra a continuación en la Figura 2.15:

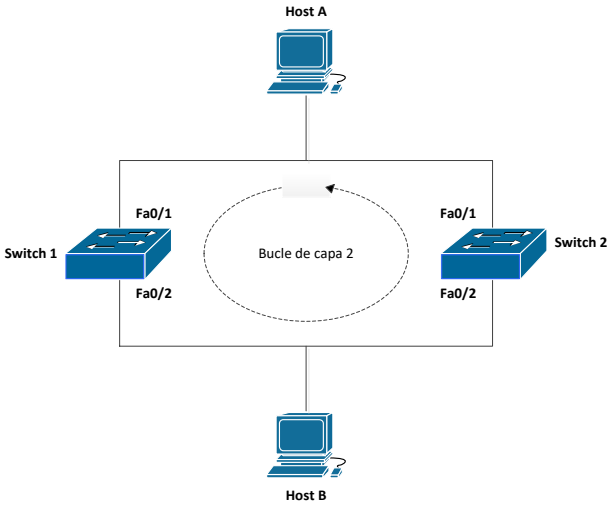


FIGURA 2.15 – ESCENARIO DE UN BUCLE DE CAPA 2 (O DE BROADCAST)

Fuente: El autor

De acuerdo a la ilustración anterior, si ninguno de los switches implementa STP, se ejecutará el siguiente proceso:

El host A envía una trama a la dirección MAC de difusión (FF-FF-FF-FF-FF-FF), la misma que llega tanto a Switch 1 como a Switch 2. Cuando Switch 1 recibe el frame en su interfaz Fa0/1, lo inundará hacia Fa0/2, donde el frame alcanzará a Host B y la interfaz Fa0/2 de Switch 2.

El Switch 2 enviará el frame a su interfaz Fa0/1 y entonces switch 1 recibirá el mismo frame transmitido.

Siguiendo el mismo conjunto de reglas, Switch 1 retransmitirá el frame a su interfaz Fa0/2, lo que dará como resultado un bucle de broadcast o de difusión. Un bucle de broadcast también puede ocurrir en la dirección opuesta (el marco recibido en la interfaz Fa0/1 de Switch 2 se transmitirá a la interfaz Fa0/2, siendo entonces recibido por Switch 1)

Los bucles de puenteo son más peligrosos que los bucles de enrutamiento, ya que como se mencionó anteriormente, un paquete de capa 3 contiene un campo especial llamado TTL (Time To Live), el cual decrece a medida que pasa a través de otros dispositivos de capa 3. En un ciclo de enrutamiento, el campo TTL alcanzará 0 y el paquete será descartado. Un frame de capa 2 que está en un bucle se detendrá solo cuando se apague una interfaz del switch. Los efectos nocivos de los bucles de capa 2 aumentan a medida que crece la complejidad de la red (es decir, el número de switches), puesto

que a medida que el frame se inunda a múltiples puertos, el número total de cuadros se multiplica a una velocidad exponencial.

Las tormentas de difusión (broadcast storms) tienen también un impacto negativo en los hosts de la red, ya que la CPU debe procesar los broadcasts en todos los dispositivos del segmento. En la figura 1.17, tanto el Host A como el Host B intentarán procesar todas las tramas que reciban; esto eventualmente agotará sus recursos a menos que los marcos sean eliminados de la red.

Los cálculos de STP se basan en los siguientes dos conceptos:

ID del puente (Bridge ID)
Costo de ruta (Path cost)

Un Bridge ID (BID) es un campo de 8 bytes compuesto por dos campos secundarios: la prioridad de puente de orden superior (2 bytes) y la dirección MAC de orden inferior (6 bytes). La dirección MAC se expresa en formato hexadecimal, mientras que la prioridad del puente es un valor decimal de 2 bytes con valores de 0 a 65535 y un valor predeterminado de 32768.

Los switches usan el concepto de costo para evaluar qué tan cerca están de otros switches. El estándar 802.1d original definió un costo de 1000 Mbps dividido por el ancho de banda del enlace medido en Megabits por segundo (Mbps). Por ejemplo, a un enlace de 10 Mbps se le asignó un costo de 100 y un enlace FastEthernet tuvo uno de 10. Los costos más bajos de STP son mejores. Sin embargo, como las conexiones de mayor ancho de banda han ganado popularidad, ha surgido un nuevo problema, es decir, que el costo se almacena sólo como un valor entero. La opción de usar un costo de 1 para todos los enlaces de más de 1 Gbps reduciría la precisión de los cálculos de costos de STP, por lo que se considera no válido.

Como solución a este problema, el IEEE decidió modificar los valores de costo en una escala no lineal, como se muestra a continuación:

Ancho de banda	Costo STP
10 Mbps	100
45 Mbps	39
100 Mbps	19
622 Mbps	6
1 Gbps	4
10 Gbps	2

Tabla 2.6 – Valores de costo STP para enlaces de distintas velocidades

Fuente: El autor

Estos valores se eligieron cuidadosamente para permitir que los esquemas antiguos y nuevos interactúen para las velocidades de enlace de uso común en la actualidad.

Virtual LAN (VLAN)

Las VLAN (Virtual Local Area Networks) representan una subred definida administrativamente, conformada por puertos de un switch forman parte de un mismo dominio de broadcast, siendo ésta el área en la que un frame se propaga a través de una red; y permiten crear grupos de usuarios y sistemas, y segmentarlos dentro de una red.

Los routers separan los dominios de broadcast, impidiendo que las transmisiones se propaguen a través de las interfaces del equipo. En cambio, los switches crean dominios de broadcast mediante una configuración específica.
Al definir estos dominios en el switch, se pueden configurar distintos puertos del mismo para reenviar un frame recibido hacia otros a otros puertos establecidos.

Al ser una VLAN una definición lógica, debe tenerse en cuenta que no se la puede observar analizando una topología física, sino mediante la revisión de los parámetros de configuración de la misma en los switches que componen el entorno LAN que la implementan.

Puesto que el tráfico de una VLAN no puede pasar directamente a otra dentro de un switch, es necesario emplear un router para dirigir los paquetes entre ellas. Adicionalmente, los puertos se pueden agrupar en diferentes VLAN en uno o varios switches conectados entre sí, pero las tramas de broadcast enviadas por un dispositivo en una VLAN solo alcanzarán los dispositivos en esa VLAN específica.

Las VLAN representan a un grupo de dispositivos que conforman un mismo dominio de capa 2 y pueden comunicarse sin necesidad de pasar a través de un router, lo que significa que comparten el mismo dominio de broadcast.
Las mejores prácticas de diseño sugieren una relación uno-a-uno entre las VLAN y las subredes IP. Los dispositivos en una sola VLAN por lo general se encuentran también en la misma subred IP.

En la Figura 2.16 se muestran dos VLAN, cada una asociada a una subred IP. La VLAN 10 engloba al Router 1, Host A y a Router 2 configurados en Switch 1 y Switch 3, teniendo asignado el segmento 10.10.10.0/24.La VLAN 20 contiene a Host B, Host C y Host D configurados en Switch 2 y Switch 3 estando asignado el segmento 10.10.20.0/24.

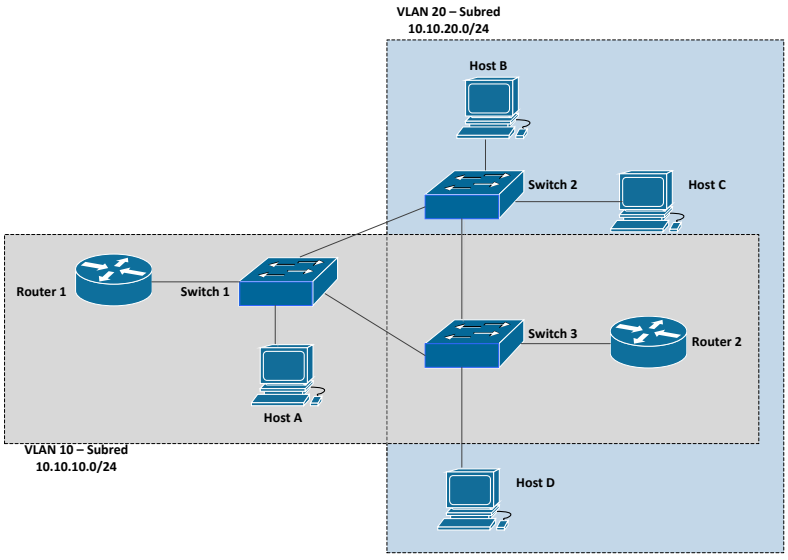


FIGURA 2.16 – ESCENARIO DONDE SE HAN DESPLEGADO 2 VLAN Y LOS EQUIPOS QUE LAS CONFORMAN

Fuente: El autor

Si bien los proveedores emplearon enfoques individuales para crear redes VLAN, una red VLAN conformada por varios proveedores debe planificarse y gestionarse con cuidado, debido a posibles problemas de interoperabilidad.

Por ejemplo, Cisco Systems desarrolló el estándar ISL, que opera agregando un nuevo encabezado de 26 bytes, más un nuevo tráiler, el cual que encapsula al frame original, como se muestra a continuación:

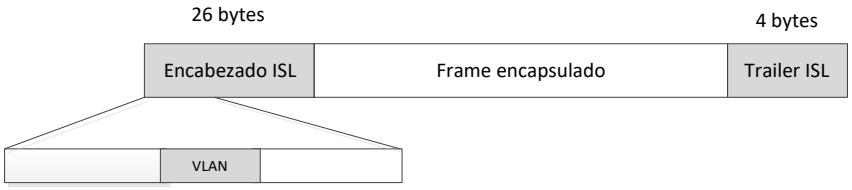


FIGURA 2.17 – ILUSTRACIÓN DE CISCO ISL PARA LA CREACIÓN DE VLAN

Fuente: El autor

Para resolver los problemas de incompatibilidad, IEEE desarrolló el estándar 802.1Q, siendo éste un método que permite implementar VLAN interoperables, independientemente de los proveedores.

A 802.1Q se lo conoce también como “frame tagging”, ya que inserta un encabezado de 32 bits, llamado etiqueta, en el frame original después del campo Dirección origen, sin modificar otros campos.

Los siguientes 2 bytes después del campo Dirección origen poseen un valor registrado tipo Ethernet de 0x8100, lo cual significa que el frame contiene un encabezado 802.1Q. Los siguientes 3 bits representan el campo Prioridad de usuario 802.1P, los que se utilizan como bits de Class of Service (CoS) en técnicas de Quality of Service (QoS).

El siguiente subcampo es llamado Indicador de Formato Canónico de 1 bit, seguido del campo VLAN ID (de 12 bits), dando un resultado de hasta 4.096 VLAN cuando se emplea 802.1Q.

El método de marcado 802.1Q se ilustra en la Figura 2.18 a continuación:

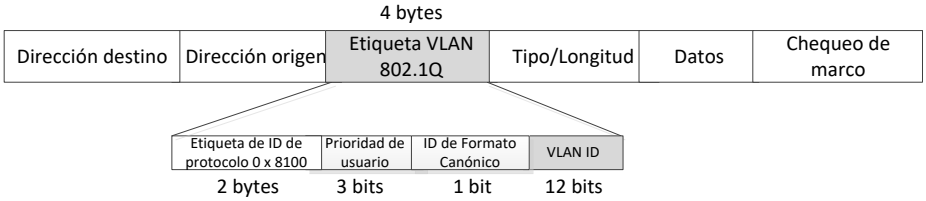


FIGURA 2.18 – MÉTODO DE MARCADO 802.1Q

Fuente: El autor

Un puerto que transporta datos de múltiples VLAN se conoce como trunk (troncal), pudiendo usar los protocolos ISL o 802.1Q.

Un concepto especial en 802.1Q es el de VLAN nativa, la cual es un tipo particular de VLAN en la que los frames no se encuentran etiquetados.
Su propósito es permitir que un switch use un enlace troncal 802.1Q (es decir, varias VLAN en un solo enlace) en una interfaz; pero si el otro dispositivo no es compatible con el enlace troncal, el tráfico de la VLAN nativa aún pueda ser enviado través del enlace.

Entre las razones para usar VLAN, las más importantes incluyen las siguientes:

1. Seguridad de red
2. Distribución de broadcasts
3. Mejor utilización del ancho de banda

Un beneficio importante del uso de VLAN es la seguridad de la red. Al crear VLAN en dispositivos de red conmutados, se establece un nivel lógico de protección.
Esto puede ser útil por ejemplo, en situaciones en las que un grupo de hosts no debe recibir datos destinados a otro grupo de hosts (a saber, departamentos dentro de una misma empresa, como se muestra a continuación)

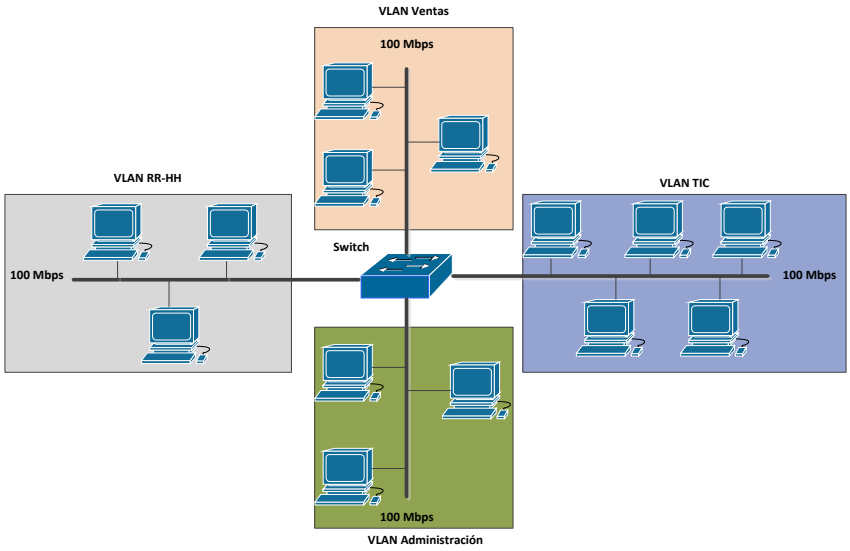


FIGURA 2.19 – EJEMPLO DE SEGMENTACIÓN DEPARTAMENTAL MEDIANTE VLAN

Fuente: El autor

Las VLAN pueden mitigar situaciones en las que los broadcasts representan un problema en una red. La creación de VLAN adicionales y la conexión de menos dispositivos a cada una los aísla en sectores más pequeños y manejables.
Sin embargo, la efectividad de esta acción depende de la ubicación de la fuente de los broadcasts; si los frames provienen de un servidor localizado, dicho servidor podría necesitar estar aislado en otro dominio, en cambio, si las transmisiones provienen de estaciones de trabajo, la creación de múltiples dominios ayuda a reducir el número de broadcasts en cada dominio.

En la Figura 2.19, la VLAN de cada departamento tiene un ancho de banda de 100 Mbps compartido entre las estaciones de trabajo, creando así un dominio de difusión independiente. Los usuarios conectados al mismo segmento de red comparten el ancho de banda de ese segmento en particular. A medida que crece el número de usuarios conectados al segmento, disminuye el ancho de banda promedio asignado a cada usuario, lo que afecta a sus aplicaciones. Por lo tanto, la implementación de VLAN permite ofrecer más ancho de banda a los usuarios.

Router

El dispositivo más inteligente de una red es el router. Es un dispositivo de capa 3 que usa direcciones de capa de Red y permite que los dispositivos ubicados en diferentes redes LAN se comuniquen entre sí. De forma predeterminada, no reenvían ninguna información entre dispositivos conectados a diferentes puertos.

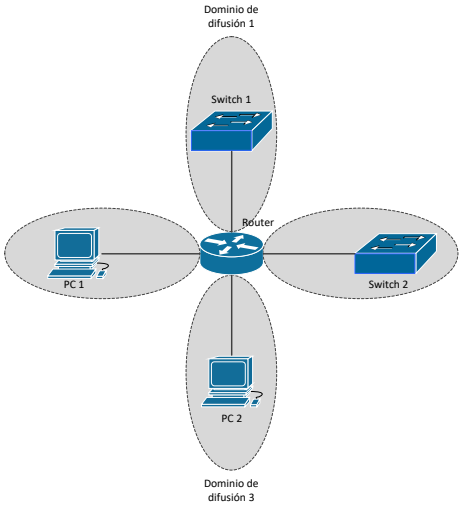


FIGURA 2.20 – SEPARACIÓN DE DOMINIOS DE DIFUSIÓN MEDIANTE UN ROUTER

Fuente: El autor

La figura anterior ilustra cómo funciona un router. Primero, lee las direcciones IP de origen y destino en los paquetes y luego realiza un seguimiento de qué dispositivos se conectan a qué puertos y qué dispositivos necesitan comunicarse con los dispositivos en otros puertos. Un router separa los dominios de difusión (broadcast), por lo que los dispositivos conectados a diferentes puertos se encuentran en diferentes dominios de difusión. El proceso de mover un paquete a través de diferentes dominios de difusión se denomina enrutamiento, y funciona implementando diferentes protocolos de enrutamiento en el router.

Los routers bloquean el tráfico multicast y transmiten paquetes de forma predeterminada. Esta es una diferencia significativa entre un router y un switch, ayudando a controlar la utilización del ancho de banda en una red. Adicionalmente, los dispositivos conectados a un mismo puerto del router se encuentran en los mismos dominios de colisión y difusión, pero los dispositivos conectados a diferentes puertos del equipo se hallan en diferentes dominios de colisión y difusión.

Direccionamiento de Capa 3

Aunque cada interfaz de red tiene una dirección MAC única, esto no especifica la ubicación de un dispositivo específico y tampoco a qué red está conectada, lo cual significa que un enrutador no puede determinar la mejor ruta para ese dispositivo. Para resolver este problema, se utiliza el direccionamiento de Capa 3, o de Red.

Las direcciones de red son direcciones lógicas asignadas cuando un dispositivo se ubica dentro de una red, y cambian cuando se mueve el dispositivo. Las direcciones de capa de red tienen una estructura jerárquica compuesta de dos partes: la dirección de red y la dirección de host. El administrador puede asignar direcciones lógicas de modo manual o dinámico a través de un protocolo dedicado, como el protocolo DHCP (Dynamic Host Configuration Protocol). Todos los dispositivos en una misma red tienen la misma porción de red en la dirección y distintos identificadores de host.

La estructura de direccionamiento se ilustra en la Figura 2.21 a continuación, tanto para IPv4 como para IPv6:

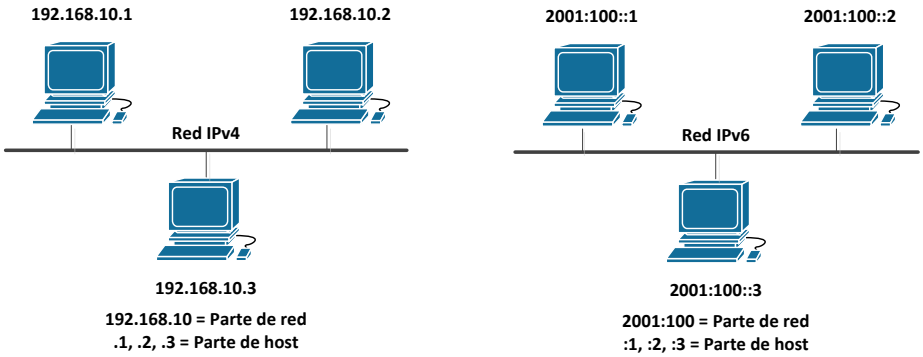


FIGURA 2.21 – ESTRUCTURA DE DIRECCIONAMIENTO DE RED

Fuente: El autor

Los routers analizan la porción de red de las direcciones IP y las comparan con las entradas de su tabla de enrutamiento. Si se encuentra una coincidencia, el paquete se envía a la interfaz adecuada. Si los dispositivos están conectados directamente, los enrutadores examinan también la parte del host de la dirección, para enviar el paquete al dispositivo apropiado. El router emplea el protocolo ARP (Address Resolution Protocol) para determinar la dirección MAC del dispositivo con una dirección IP específica y encapsula el paquete con un encabezado que contiene dicha dirección MAC específica antes de enviarlo por el medio de transmisión.

Direccionamiento IPv4

Las direcciones IPv4 son números de 32 bits representados como cadenas de 0 y 1. Como se mencionó anteriormente, el encabezado de Capa 3 contiene un campo de dirección IP de origen y uno de dirección IP de destino. Cada campo tiene 32 bits de longitud. Para una representación más intuitiva de las direcciones IPv4, los 32 bits se dividen en cuatro grupos de 4 octetos cada uno (1 octeto o byte = 8 bits) separadas por puntos, lo que se denomina notación decimal con puntos. Los octetos se convierten en números decimales por mediante la transformación de base 2 a base 10.

Por ejemplo, considérese la siguiente cadena de 32 bits:

11000000101010001000001110101101

Al separarla por puntos en grupos de 8 bits (1 octeto), se tendrá:

11000000.10101000.10000011.10101101

Lo que en notación decimal, equivale a: 192.128.131.173

El valor máximo de un octeto es 255, el cual se obtiene cuando sus ocho bits equivalen a 1 (por tanto, 255 = 11111111)

Las direcciones IPv4 se clasifican en cinco clases. Las clases A, B y C se utilizan para dispositivos de direccionamiento, la clase D es para grupos de multidifusión (multicast) y la clase E está reservada para uso experimental.

Los primeros bits de una dirección definen a qué clase pertenece:

Clase	Bits iniciales	Tamaño porción de red	Tamaño porción de host	Número redes	Dirección inicial	Dirección final
A	0	24	128	16777216	0.0.0.0	127.255.255.255
B	10	16	16384	65535	128.0.0.0	191.255.255.255
C	110	8	2097152	256	192.0.0.0	223.255.255.255
D	1110	-	-	-	224.0.0.0	239.255.255.255
E	1111	-	-	-	240.0.0.0	255.255.255.255

Tabla 2.7 – Clases de direcciones IPv4

Fuente: El autor

Saber la clase de una dirección IPv4 ayuda a determinar qué parte de la dirección representa a la red y qué parte representan los bits del host.

Las direcciones IPv4 se pueden clasificar en las siguientes categorías:

1. Direcciones públicas: usadas para comunicación externa.
2. Direcciones privadas: están reservadas y se usan solo internamente en una organización.

Los rangos de direcciones privadas, según lo definido en el RFC 1918, son:

10.0.0.0 hasta 10.255.255.255
172.16.0.0 hasta 172.31.255.255
192.168.0.0 hasta 192.168.255.255

Al reservar clases completas de direcciones, es decir usar direccionamiento con clase (classful addressing) para ciertas redes, aparecen ciertas limitaciones debido a la gran cantidad de direcciones por red y al espacio limitado de direcciones IPv4. Por tal motivo, se introdujo el concepto de subredes o direccionamiento sin clases (classless addressing), definido en el RFC 950.

El direccionamiento sin clases permite que las direcciones clase A, B y C se dividan en redes más pequeñas llamadas subredes, lo que permite tener una mayor cantidad de redes posibles, cada una con menos direcciones de host. Las subredes se crean tomando prestados bits de la porción de host y usándolos como bits de subred.
Un aspecto importante en el direccionamiento IPv4 es la de separar la red y la parte del host de la cadena de direccionamiento. Esto se logra mediante el uso de una máscara de subred, también representada como un número de 32 bits.
La máscara de subred comienza con una cadena continua de bits con el valor de 1 y termina con una cadena de 0. El número de bits con el valor de 1 representa el número de bits en la dirección IP que se debe considerar para calcular la dirección de red. Un bit de máscara de subred 0 indica que el bit correspondiente en la dirección IPv4 es un bit de host.

Usando el mismo ejemplo anterior empleando una máscara 255.255.255.0, da como resultado la siguiente situación:

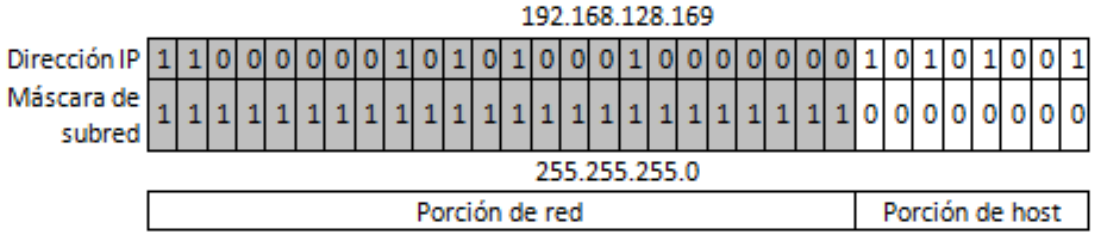


FIGURA 2.22 – PORCIÓN DE RED Y DE HOST EN UNA DIRECCIÓN IPV4

Fuente: El autor

Con una cadena de 24 bits de valor 1 en la máscara de subred, se consideran solamente los primeros 24 bits en la dirección IP como la porción de red, dando como resultado una dirección de red de 192.168.128.0 con una máscara de subred de 255.255.255.0.

Los últimos 8 bits en la dirección IP, llamados porción de host, pueden asignarse a los dispositivos de red. Con 8 bits libres, es posible asignar una dirección IP a 28 hosts, lo que implica un total de 256 direcciones de host en el espacio de red 192.168.128.0.

Cada máquina en una red particular tendrá la misma dirección de red y máscara de subred; sin embargo, la parte del host de la dirección IP será diferente.

Cuando se utiliza el direccionamiento sin clases, la máscara de subred indica qué bits se han tomado prestados del campo de host. El uso de máscaras de subred crea una jerarquía de tres niveles: red, subred y host. Otra forma de representar la máscara de subred es usar una barra (/) para indicar cuántos bits de red contiene la dirección.

Por ejemplo, 192.168.10.0/24 significa que los primeros 24 bits de la dirección 192.168.10.0 son bits de red, por lo tanto, corresponde a una máscara de subred 255.255.255.0.

Un paquete IPv4 contiene los siguientes campos:

FIGURA 2.23 – CAMPOS QUE CONFORMAN UN PAQUETE IPV4

Fuente: El autor

Campo	Tamaño	Descripción
Versión	4 bits	Identifica la versión de IP
Longitud de encabezado	4 bits	Tamaño del encabezado
Tipo de servicio	8 bits	Para QoS, especifica cómo debe ser manejado el paquete a través de la red
Longitud total	16 bits	Longitud total del encabezado y los datos
Identificación	16 bits	Se usa cuando el paquete está fragmentado
Banderas	3 bits	Se usa cuando el paquete está fragmentado
Desplazamiento de fragmentos	13 bits	Se usa cuando el paquete está fragmentado
Tiempo de vida	8 bits	Protección en contra de bucles infinitos, se decrementa en 1 cada vez que el paquete atraviesa un router
Protocolo	8 bits	Identifica el protocolo de capa 4 (TCP, UDP)
Suma de comprobación de encabezado	16 bits	Permite verificar la integridad del encabezado
Dirección IP origen	32 bits	Dirección IP lógica de origen
Dirección IP destino	32 bits	Dirección IP lógica de destino
Opciones IP y relleno	Variable	Usada para depuración
Datos	Variable	Datos de capa Transporte

Tabla 2.8 – Descripción de los campos que conforman un paquete IPv4

Fuente: El autor

Direccionamiento IPv6

El número limitado de direcciones IPv4 y el constante aumento del número de dispositivos de red direccionables alrededor del globo ha acelerado la implementación de la versión IPv6.

Las direcciones IPv6 tienen una composición distinta a las de IPv4. Poseen una longitud de 128 bits, lo que significa que existe un conjunto más grande de direcciones IPv6. Asimismo, su notación es diferente, puesto que una dirección IPv4 se puede escribir en formato decimal, una dirección IPv6 se anota en un formato hexadecimal (es decir, 16 bits separados por dos puntos), así:

2001:43aa:0000:0000:11b4:0031:0000:c110

Considerando el formato complejo de las direcciones IPv6, se desarrollaron las siguientes técnicas para acortar su notación:

- Uno o más grupos sucesivos de 16 bits que constan de todos los 0 pueden omitirse y representarse mediante dos puntos (:)
- Si un grupo de 16 bits comienza con uno o más ceros, los 0 iniciales pueden omitirse.

Para el ejemplo anterior (2001:43aa:0000:0000:11b4:0031:0000:c110), las representaciones abreviadas son las siguientes:

2001: 43aa :: 11b4: 0031: 0000: c110
2001: 43aa :: 11b4: 0031: 0: c110
2001: 43aa :: 11b4: 31: 0: c110

Se requieren varios tipos de direcciones IPv6 para varias aplicaciones, como se detalla a continuación. En comparación con los tipos de direcciones IPv4 (es decir, unicast, multicast y broadcast), IPv6 es diferente en el sentido de que se emplean direcciones de multicast especiales en lugar del direccionamiento de broadcast, e incluye un nuevo tipo de dirección llamado “anycast” (de difusión ilimitada)

Tipo de dirección	Rango	Descripción
Aggregatable Global Unicast	2000::/3	Direcciones públicas, comunicaciones host a host (equivalente a unicast IPV4)
Multicast	FF00::/8	Comunicación uno a varios y varios a varios (equivalente a multicast IPv4)
Anycast	El mismo que Unicast	Puede asignarse a las interfaces de un grupo de dispositivos (responderá el dispositivo más cercano al origen)
Link-local Unicast	FE80::/10	Asignada a todas las interfaces de un dispositivo y usada solamente para tráfico de enlace local
Solicited-node Multicast	FF02::1:FF00:0/104	Solicitud de vecino

Tabla 2.9 – Tipos de direcciones multicast usadas en IPv6

Fuente: El autor

Un paquete IPv6 contiene los siguientes campos:

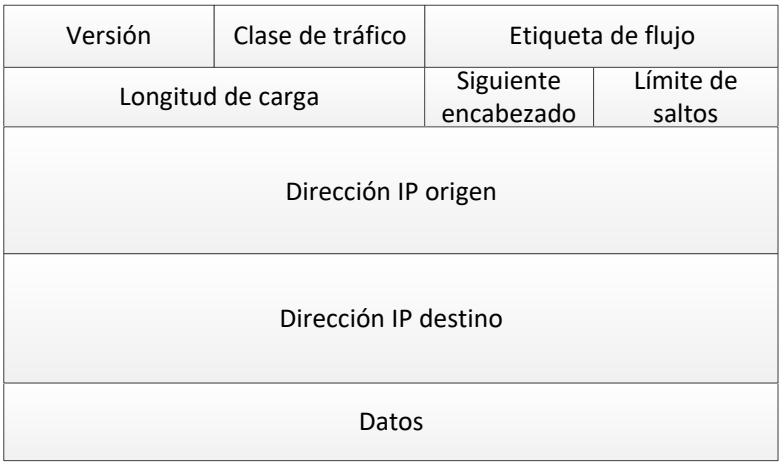


FIGURA 2.24 – CAMPOS QUE CONFORMAN UN PAQUETE IPV6

Fuente: El autor

Campo	Tamaño	Descripción
Versión	4 bits	Identifica la versión de IP
Clase de tráfico	8 bits	Similar al bit ToS (Tipo de servicio) en IPv4, usado para marcado QoS
Etiqueta de flujo	20 bits	Permite identificar y clasificar flujos de paquetes
Longitud de carga	16 bits	Indica el tamaño de la carga del paquete
Siguiente encabezado	8 bits	Similar al campo Protocolo de IPv4. Define el tipo de tráfico contenido en la carga y el tipo de encabezado a esperarse
Límite de saltos	8 bits	Similar al campo TTL (Tiempo de vida) en IPv4, previene bucles infinitos
Dirección IP origen	128 bits	Dirección IP lógica de origen
Dirección IP destino	128 bits	Dirección IP lógica de destino
Datos	Variable	Datos de capa Transporte

Tabla 2.10 - Descripción de los campos que conforman un paquete IPv6

Fuente: El autor

Enrutamiento IP

Los routers son dispositivos que operan en la capa 3 del modelo OSI. Son los responsables de determinar la mejor ruta para el envío de una hacia un destino específico. Una vez que ha elegido la mejor ruta, encapsula el paquete con un nuevo marco (frame), y el router lo coloca en la interfaz que tiene un enlace al siguiente salto correspondiente a la ruta.

El proceso de elegir la mejor ruta se denomina enrutamiento o ruteo, mientras que el de enviar el paquete hacia la interfaz correcta se conoce como conmutación.
Aunque los routers son los equipos de red más populares en tomar decisiones de enrutamiento, otros dispositivos de red pueden tener esta funcionalidad, tales como switches de capa 3 o dispositivos de seguridad (cortafuegos o firewalls)

Un router es responsable de enviar el paquete de la manera correcta, sin importar lo que esté sucediendo en la capa de red. Sin embargo, sí se preocupa por lo que está sucediendo tanto en la capa física como enlace de datos, ya que podría necesitar recibir datos de ciertos medios y enviarlos a través de un tipo de medio diferente. Esto se realiza desencapsulando el paquete recibido hasta la capa de red, y encapsulándolo nuevamente con el encabezado específico para el nuevo tipo de medio.

La Figura 2.25 muestra este proceso. Router A recibe el paquete a través de una conexión Ethernet, lo vuelve a encapsular con un encabezado Frame Relay y lo envía a Router B, el cual que procesa el paquete en el orden inverso, retirando el encabezado de Frame Relay y encapsulándolo en el formato Ethernet antes de enviarlo el paquete al punto final del receptor. Se debe tener en cuenta que los routers solo están interesados en las últimas tres capas del modelo OSI.

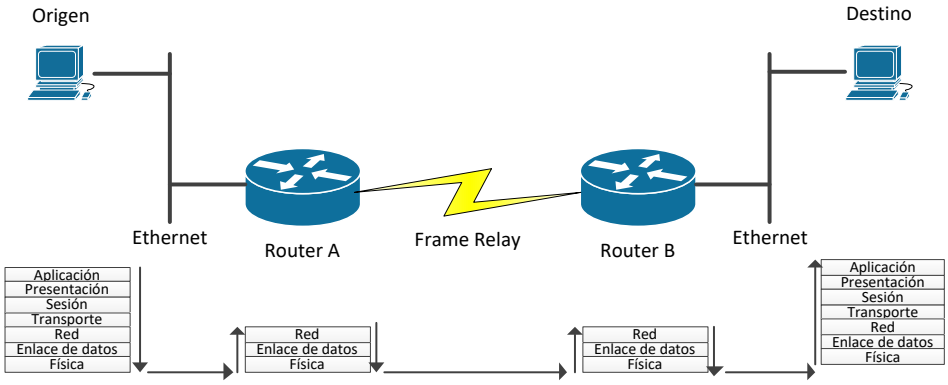


FIGURA 2.25 – ENCAPSULAMIENTO Y DESENCAPSULAMIENTO DE PAQUETES IP

Fuente: El autor

Un router analiza la dirección de destino del paquete para determinar hacia dónde se dirige, a fin de seleccionar la mejor ruta que permita enviarlo a su destino. Para calcular la mejor ruta, debe saber qué interfaz tiene que usarse para llegar a la red de destino indicada en el paquete. Aprende acerca de la red al conectarse físicamente a ella, al recibir información de otros routers o según la configuración introducida por un administrador de red. El proceso de aprendizaje sobre las redes a partir de los anuncios de otros routers se conoce como enrutamiento dinámico y se pueden utilizar diferentes protocolos de enrutamiento para lograrlo. Diferentes protocolos de enrutamiento pueden lograr esta tarea, como por ejemplo:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)
- Border Gateway Protocol (BGP)

El proceso según el cual un administrador de red define manualmente las reglas de enrutamiento en el dispositivo se conoce como enrutamiento estático. Finalmente, las rutas a las cuales un router está conectado físicamente se conocen como rutas conectadas directamente. Los routers mantienen la mejor ruta hacia los destinos aprendidos a través de conexiones directas, enrutamiento estático o enrutamiento dinámico en estructuras de datos internas denominadas tablas de enrutamiento; entonces, una tabla de enrutamiento contiene una lista de redes que el router ha aprendido y la información sobre cómo llegar a ellas.

La información más importante que contiene una tabla de enrutamiento incluye los siguientes elementos:

- Cómo se aprendió la ruta (es decir, por vía estática, dinámica o se encuentra directamente conectada)
- La dirección del router vecino desde el cual se aprendió la red
- La interfaz a través de la cual se puede llegar a la red
- La métrica de ruta, que corresponda a una medida que proporciona a los routers información sobre qué tan lejos o qué tan preferida es una red (tener en cuenta que el significado exacto del valor de la métrica depende del protocolo de enrutamiento utilizado)

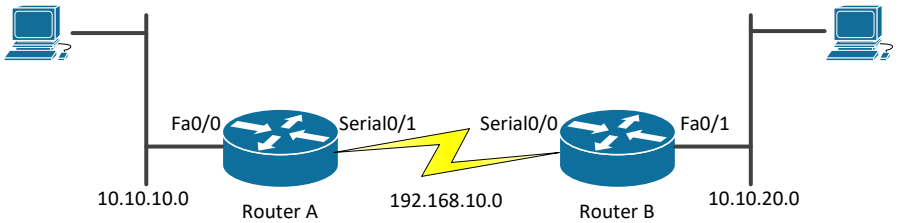


Tabla de enrutamiento Router A		
Red	Interfaz	Métrica
10.10.10.0	Fa0/0	0
192.168.10.0	Serial0/1	0
10.10.20.0	Serial0/1	1

Tabla de enrutamiento Router B		
Red	Interfaz	Métrica
10.10.10.0	Serial0/0	1
192.168.10.0	Serial0/0	0
10.10.20.0	Fa0/1	0

FIGURA 2.26 – TABLAS DE ENRUTAMIENTO DE LOS ROUTERS A Y B

Fuente: El autor

La Figura 2.26 ilustra un escenario con dos enrutadores que usan el recuento de saltos como métrica. La topología contiene tres redes conocidas por ambos enrutadores. El conteo de saltos representa la cantidad de enrutadores por los que se envía un paquete para llegar a un destino específico.

El enrutador A tiene dos redes conectadas directamente, 10.10.10.0 y 192.168.10.0; por lo tanto, la métrica para cada uno de ellos es 0. El enrutador A conoce la red 10.10.20.0 del enrutador B, por lo que la métrica para esta red es 1, porque un paquete enviado por el enrutador A debe atravesar el enrutador B para alcanzar el 10.10.20.0 red. El enrutador B tiene dos redes conectadas directamente, 10.10.20.0 y 192.168.10.0, y una red remota aprendió del enrutador A, 10.10.10.0, con una métrica de 1.

DISPOSITIVOS DE SEGURIDAD DE RED

En la actualidad, los dispositivos de seguridad de redes más utilizados son los firewalls (cortafuegos), IPS e IDS, mostrados a continuación:

FIGURA 2.27 – FIREWALL CHECK POINT MODELO 21400

Fuente: http://www.checkfirewalls.com/21400.asp

FIGURA 2.28 – IDS IBM PROVENTIA GX6116

Fuente: https://issthai.wordpress.com/2009/03/24/ids/

FIGURA 2.29 – IPS TIPPINGPOINT S2500N

Fuente: http://www.esaitech.com/hewlett-packard-jc021a-tippingpoint-s2500n-ips-3gbps-5-gt-1-10ge-2-gb-security-appliance.html

Firewall

Es un dispositivo de seguridad de red que permite o niega el acceso a la red a los distintos flujos de tráfico entre una zona no confiable (por ejemplo, Internet) y una zona confiable (a saber, una red privada o corporativa); de este modo, un firewall actúa como un punto de demarcación en la red, puesto que todas las comunicaciones deben fluir a través de él, siendo quien autoriza o prohíbe el acceso al tráfico. Un firewall impone controles de acceso por medio de un modelo de control positivo, el que establece que sólo el tráfico definido en la política de seguridad sea permitido en la red; todo el restante es denegado (lo que se conoce como "denegación implícita")

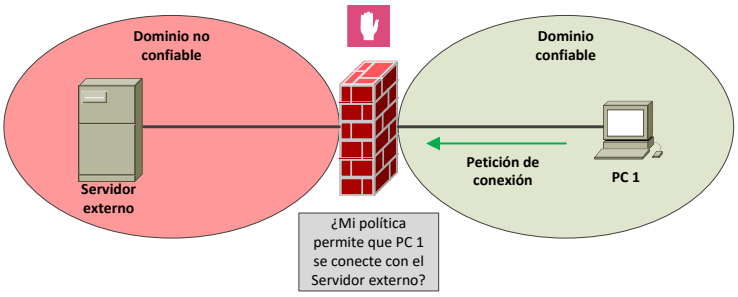


Figura 2.30 – Un firewall y dominios de seguridad
Fuente: El autor

De esta manera, un firewall protege dominios o zonas confiables de los no confiables, y permitirá el tráfico desde un dominio confiable a uno no confiable sin configuración explícita alguna, sin embargo, el tráfico desde uno no confiable hacia uno confiable debe ser explícitamente permitido. De la misma manera, cualquier tráfico que no está explícitamente permitido desde un dominio no confiable a uno confiable será implícitamente denegado.

Un firewall no está limitado a tener 2 interfaces como en la ilustración (una de tráfico entrante y otra para el tráfico saliente), por lo general dispone de un conjunto interfaces “menos confiables”, conocidas como “zonas desmilitarizadas” (DMZ – Demilitarized Zones)

Así, para establecer el valor de confianza de las interfaces, se debe colocar en el firewall un nivel de seguridad a cada interfaz del mismo, normalmente en base a un valor numérico que va desde 0 hasta 100, siendo el valor más alto el indicador de mayor confianza de una interfaz.

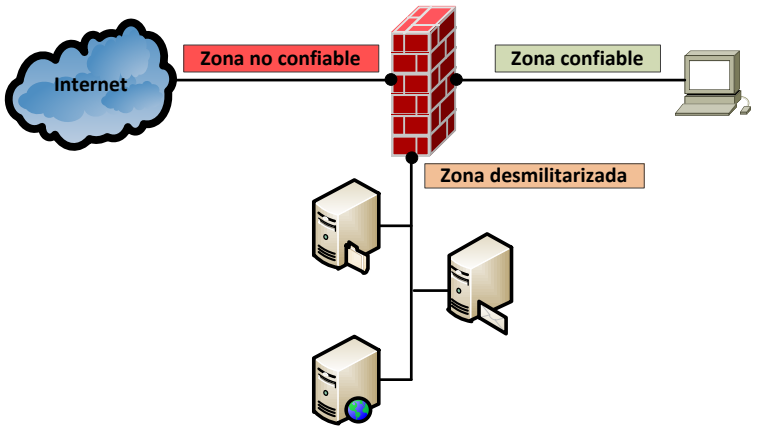


FIGURA 2.31 – ZONAS DE SEGURIDAD EN UN FIREWALL

Fuente: El autor

Para hacer cumplir las políticas de control de acceso entre dominios, un firewall debe ser primero ubicado dentro de la topología de red. Existen dos modos de hacerlo: el modo enrutado y el modo transparente.

Modo enrutado

En este modo, desde la perspectiva de los hosts que se conectan al firewall, éste funciona como un dispositivo de capa 3 (router). Cada una de sus interfaces está asignada a una subred diferente, y los paquetes son enrutados condicionalmente entre ellas.

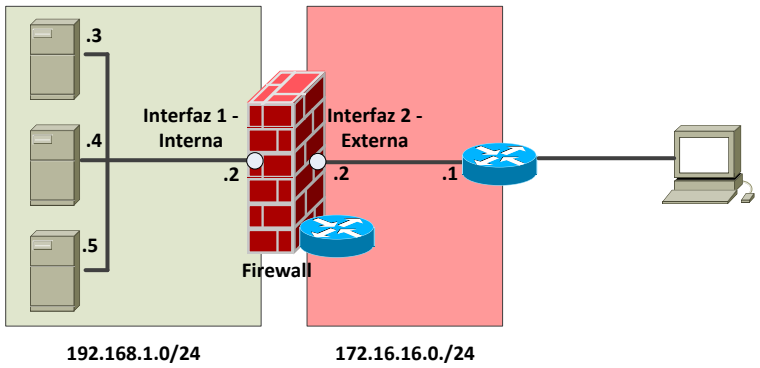


FIGURA 2.32 – FIREWALL EN MODO ENRUTADO

Fuente: El autor

En el ejemplo mostrado en la Figura 2.32, la Interfaz1 (Interna) tiene la dirección IP 192.168.1.2, mientras que la Interfaz 2 (Externa) usa la dirección 172.16.16.2. Puesto que los hosts se encuentran interconectados por el firewall, los equipos en el interior necesitan configurar la dirección 192.168.1.2 como su puerta de enlace de capa 3 para poder alcanzar destinos externos.

Modo transparente

Aquí el firewall actúa como un bridge (puente) condicional, reenviando tramas entre interfaces basadas en información de capa 2. En este caso, las dos interfaces mostradas en la Figura 2.33 se conectan a la misma subred, y los hosts internos utilizan el router externo (192.168.2.1) como su puerta de enlace para llegar a destinos externos.

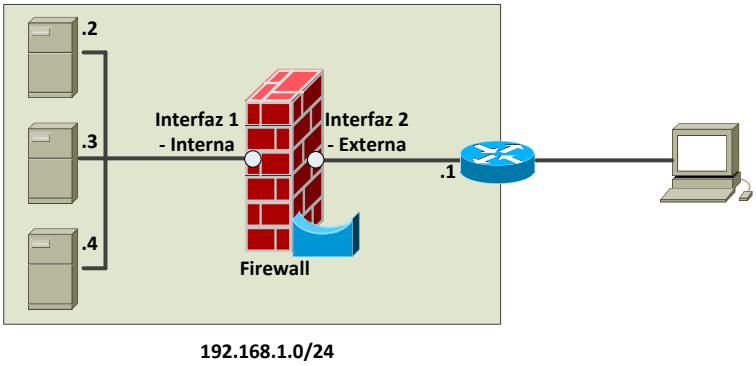


FIGURA 2.33 – FIREWALL EN MODO TRANSPARENTE

Fuente: El autor

Pese a que el modo enrutado es el modo más común en que se ubica un firewall dentro de una red, el modo transparente es la opción conveniente en escenarios en los que una mínima reconfiguración de red es menester.

Tipos de firewalls

Filtrador de paquetes: Compone la primera generación de firewalls; concentra sus tareas de control de acceso en algunos parámetros tanto de la capa de red como de transporte incluidos en los paquetes. Por su naturaleza, se lo conoce como “stateless”, ya que no tiene una noción de una tabla de estado o de conexiones.

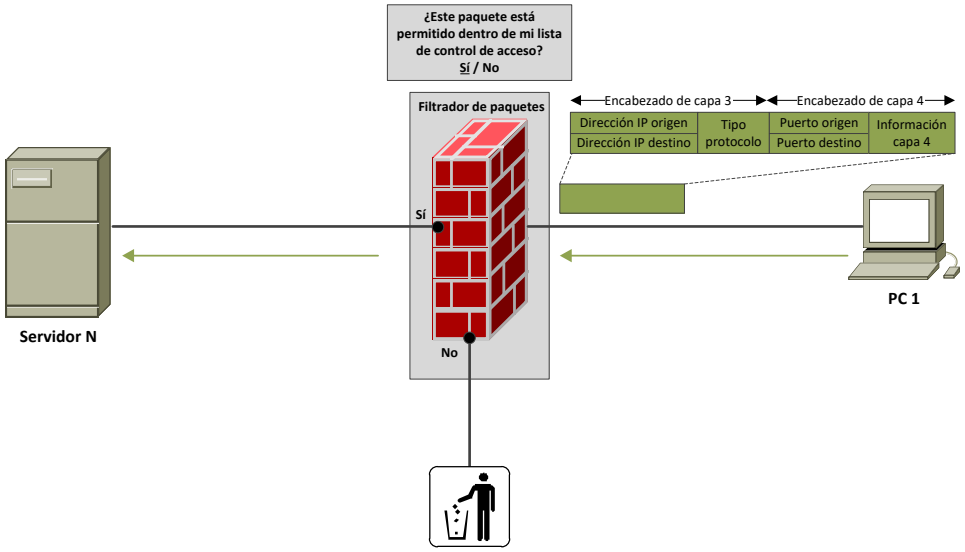


FIGURA 2.34 – FILTRADOR DE PAQUETES

Fuente: El autor

Si existe una regla que permita el tránsito del tipo de paquete, éste pasará a través del firewall hacia su destino, caso contrario el paquete será desechado.

Un router puede convertirse en un firewall filtrador de paquetes al implementar listas de control de acceso.

Proxy a nivel circuito: Un firewall de este tipo establece sesiones hacia el destino requerido en lugar del host solicitante. El término “sesión” hace referencia a la capa 5 del modelo OSI, que es la responsable de crear, gestionar y finalizar conexiones lógicas entre procesos de aplicaciones que residen en distintos equipos.

Este firewall es conocido también como proxy genérico, puesto que no requiere un software proxy de aplicación específica en el lado del cliente; ello brinda flexibilidad, ya que no es necesario desarrollar una aplicación cliente determinada para cada aplicación, sin embargo, no está en capacidad de comprender la forma en la que funcionan las aplicaciones.

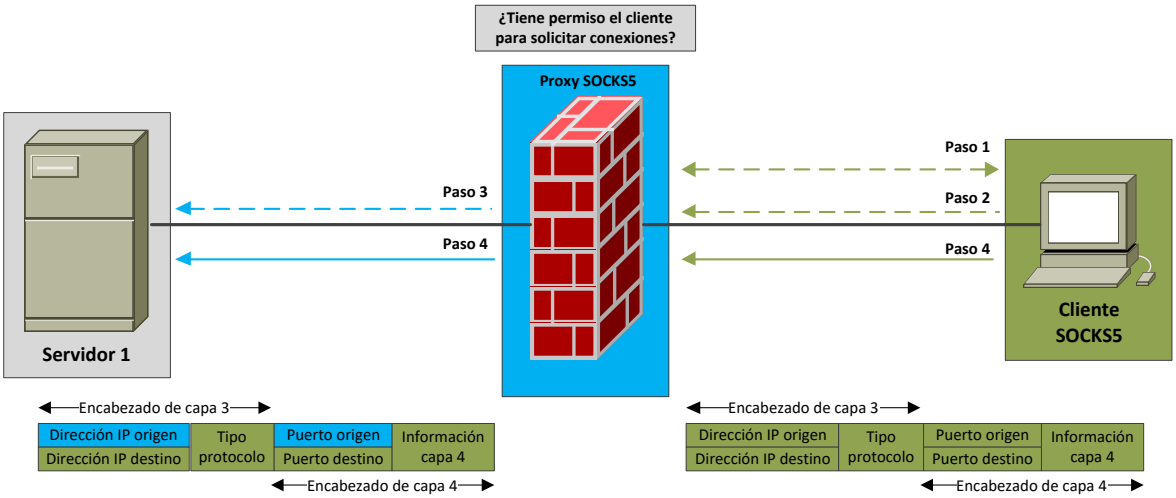


FIGURA 2.35 – PROXY A NIVEL CIRCUITO

Fuente: El autor

La Figura 2.35 resume la operación de un proxy de circuito SOCKS5.

En el paso 1, el cliente SOCKS5 abre una conexión con Proxy SOCKS5 en un puerto TCP reservado y negocia el tipo de autenticación a usarse.
En el paso 2 el cliente se autentica según el método establecido y envía un "relay request" a Proxy SOCKS5. Esta petición contiene el puerto destino de capa 4 y la dirección IP del host remoto alcanzable a través del firewall.
En el paso 3, Proxy SOCKS5 establece una conexión con Servidor 1 en representación de Cliente SOCKS5.
En el paso 4, los paquetes enviados por Cliente SOCKS5 hacia el Proxy SOCKS5 son reenviados a Servidor 1.

En este tipo de implementación, Servidor 1 creerá que todo el tráfico está siendo generado por Proxy SOCKS5.

Proxy a nivel aplicación: Este tipo de firewall está en capacidad de comprender e interpretar los comandos del protocolo de aplicación para el cual está proporcionado servicios proxy. Ya que se requiere un software proxy específico del lado del cliente, también se lo conoce como proxy dedicado.

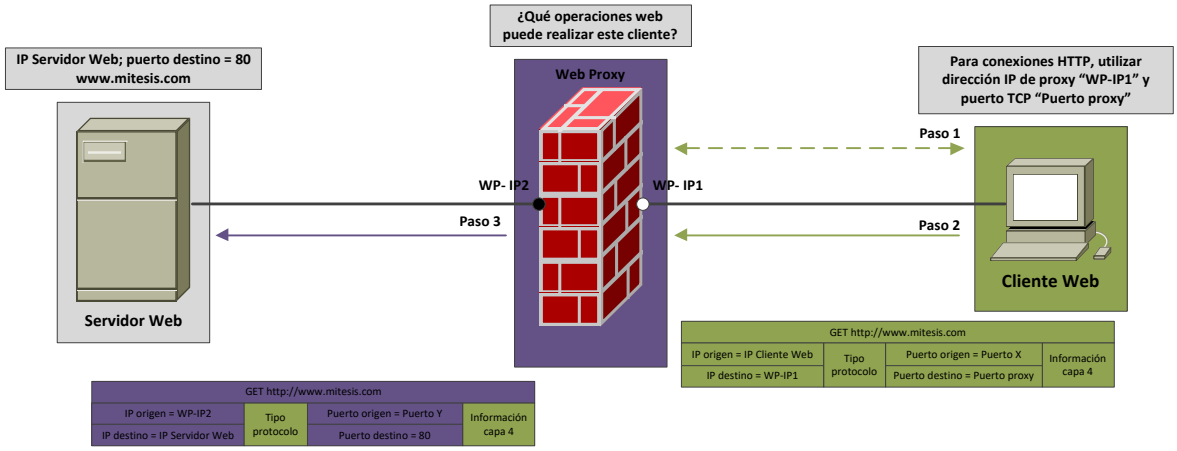


FIGURA 2.36 – PROXY A NIVEL APLICACIÓN

Fuente: El autor

La Figura 2.36 ilustra la operación de un proxy dedicado al protocolo HTTP.

En el paso 1, el explorador (browser) de Cliente Web configurado para usar servicios proxy, se autentica contra Web Proxy. De acuerdo al perfil de usuario, Web Proxy brinda filtrado de contenido a nivel aplicación.

En el paso 2, todo el tráfico web dirigido hacia Servidor Web, se reenvía hacia Web Proxy, quien cambia la información del encabezado.

En el paso 3, Web Proxy envía los paquetes con su nuevo encabezado hacia Servidor Web, de tal manera que los paquetes parecerán ser originados por éste. Todos los paquetes de Servidor Web regresan al Cliente Web a través de Web Proxy.

Debido a su naturaleza, este tipo de firewall puede brindar servicios detallados de registro (logging), autenticación y caché, sin embargo, necesita software cliente específico para cada aplicación y el funcionamiento de estas características consumen recursos de procesamiento.

Stateful firewall: Este tipo de firewall incorpora los conceptos de conexiones y estado para implementar el filtrado de paquetes. En lugar de ejecutar control sobre paquetes individuales, lo hace sobre grupos de paquetes que pertenecen a una misma conexión (o flujo)

La Figura 2.37 ilustra un entorno en el que Cliente 1 necesita iniciar una conexión a través de un firewall tipo stateful para acceder al servicio TCP/Y1 en Servidor 1.

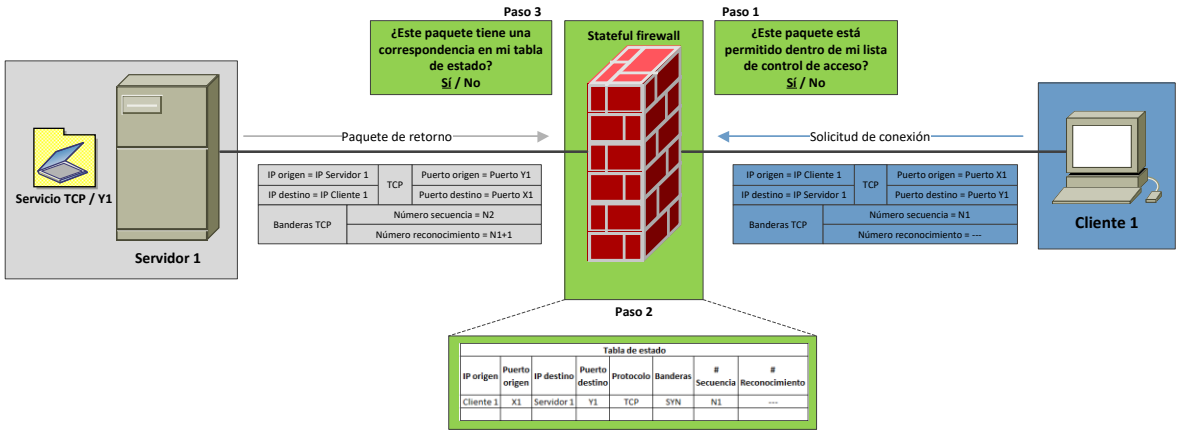


FIGURA 2.37 – STATEFUL FIREWALL

Fuente: El autor

En el paso 1 el firewall chequea sus listas de control de acceso (al igual que un filtrador de paquetes) para verificar si el tipo de conexión está permitida.
En el paso 2, en el firewall se crea una entrada de estado para conexiones aceptadas, la que contiene parámetros tales como dirección IP origen, dirección IP destino, puerto TCP origen, puerto TCP destino, banderas TCP, números de secuencia y de reconocimiento.
En el paso 3, los paquetes que retornan desde Servidor 1 se comparan con la tabla de estado y se los permite atravesar el firewall si sus parámetros son coherentes con la definición de la máquina TCP de estado finito.

Es importante considerar que los conceptos de estado y conexión originalmente se refieren a TCP, un protocolo de capa Transporte orientado a conexión.

Sin embargo, el término conexión se emplea también con protocolos tales como UDP e ICMP, ya que un stateful firewall mantiene un registro de parámetros como números de puerto UDP y tipos de mensajes ICMP dentro de su tabla de estado. Un modo dinámico de finalizar conexiones no TCP es la aplicación de purgadores por inactividad.

UTM: Acrónimo de Unified Threat Management, corresponde a un equipo de seguridad consolidado, el cual integra un firewall de inspección de estado (stateful), antivirus e IPS en un único dispositivo.

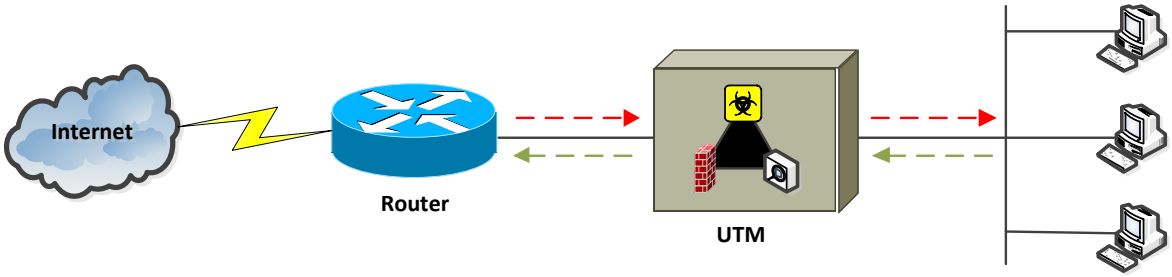


FIGURA 2.38 – UBICACIÓN DE UN UTM DENTRO DE LA RED

Fuente: El autor

Es importante considerar que el éxito de un UTM está basado en la efectividad del motor de decisión del firewall, pues esta funcionalidad precede a la de los demás componentes, ya que los elementos del UTM brindan servicios de seguridad en sentido descendente. De este modo, la carga de trabajo de todos los componentes de seguridad dentro de la red estará determinada por la potencia del control de acceso. Pese a que un UTM proporciona varias funciones de seguridad en un solo producto, la tecnología de control de acceso fundamental permanece inalterada.

NGFW: Acrónimo de Next Generation Firewall, fue creado como respuesta a la evolución y sofisticación de las aplicaciones y malware, puesto que los desarrolladores de aplicaciones y malware han sido capaces de burlar la clasificación de tráfico basada en puertos mediante la creación y construcción de técnicas de evasión de puertos en sus programas.

Hoy en día, el malware es capaz de conectar estas aplicaciones para ingresar a las redes y enlazarse entre ellas (por ejemplo, unido por medio de las computadoras que fueron infectadas de manera individual)

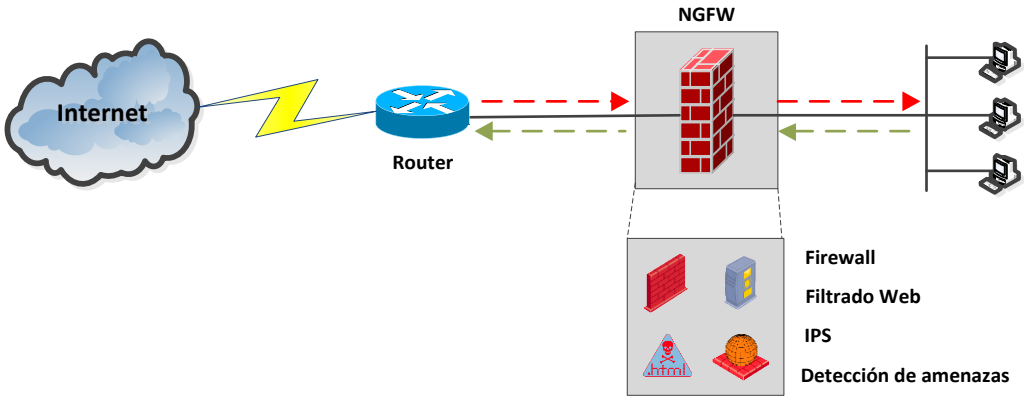


FIGURA 2.39 – UBICACIÓN DE UN NGFW EN LA RED

Fuente: El autor

Un NGFW trabaja como una plataforma para la aplicación de políticas de seguridad de red y la inspección de tráfico de red. Para que un equipo de seguridad pueda ser definido como un NGFW, debe cumplir los siguientes requisitos:

1. Poseer capacidades estándar de un firewall de primera generación (filtrador de paquetes), además de inspeccionar protocolos con estado, efectuar traducción de direcciones de red (NAT), brindar conectividad VPN.
2. Implementar prevención de intrusiones verdaderamente integrada, incluyendo soporte para reconocimiento y aplicación firmas orientadas a vulnerabilidad y a amenazas, poseer la inteligencia suficiente para y sugerir reglas o tomar acciones basadas en la actividad de su módulo de prevención de intrusiones; de tal manera que la suma de estas dos funciones que trabajan conjunta y colaborativamente a través del NGFW sea mayor que las partes individuales.
3. Brindar visibilidad completa de la pila de protocolos e identificación de aplicaciones, estar en capacidad de aplicar políticas en la capa de Aplicación independientemente del puerto y el protocolo.

4. Poseer inteligencia adicional capaz de tomar información de fuentes externas y tomar las mejores decisiones en base a éstas, como por ejemplo la creación de listas negras o listas blancas, capacidad de asignar el tráfico a usuarios y grupos que utilizan servicios de directorio (Active Directory)
5. Debe ser adaptable y flexible respecto al panorama de amenazas actual, aceptando rutas de actualización para la integración con nuevas fuentes de información y nuevas técnicas para abordar amenazas futuras.
6. Permitir soporte en línea con una mínima degradación del rendimiento y sin interrumpir las operaciones de red.

IDS

Un Sistema de Detección de Intrusiones (IDS – Intrusion Detection System) es una tecnología de seguridad de red creada originalmente para detectar exploits de vulnerabilidades contra una aplicación o computador de destino.

Un IDS necesita solamente detectar las amenazas, y por lo tanto, se coloca fuera de banda (out of band) en la infraestructura de red, lo cual significa que no se encuentra en la verdadera ruta de comunicación en tiempo real entre el emisor y el receptor de la información; por el contrario un IDS aprovecha un puerto TAP (Test Access Point) o SPAN (Switch Port Analyzer) para analizar una copia de la secuencia de tráfico en línea, garantizando así que el IDS no afecte el rendimiento de la red.

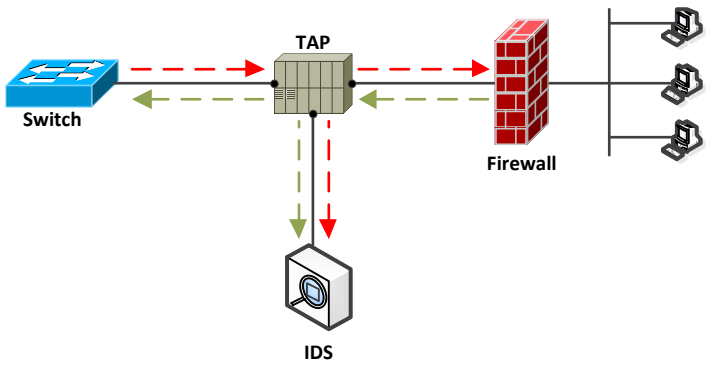


FIGURA 2.40 – IDS EN MODO TAP

Fuente: El autor

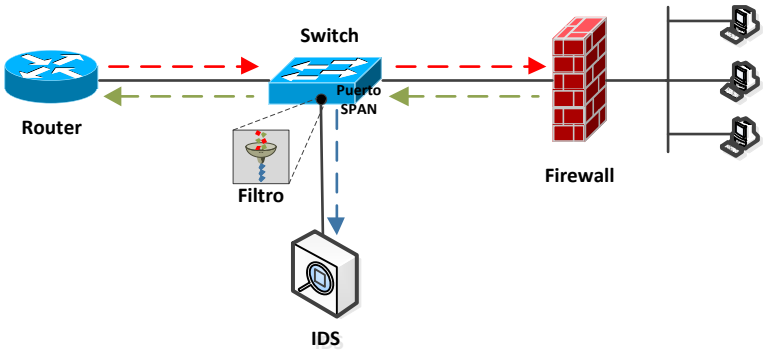


FIGURA 2.41 – IDS EN MODO SPAN

Fuente: El autor

El IDS fue desarrollado de este modo debido a que en el momento la profundidad de análisis requerida para la detección de intrusión no podía realizarse a una velocidad que pudiera seguir el ritmo de los componentes en la ruta de comunicaciones directas de la infraestructura de red.

Clasificación

De acuerdo a su naturaleza de detección, un IDS puede clasificarse como:

Basado en firmas (signature-based): Supervisa los paquetes en la red y los compara contra una base de datos de firmas o atributos de amenazas maliciosas conocidas. En esto es similar al modo en que la mayoría de los programas antivirus detectan malware. Sin embargo, el problema es que existirá un desfase entre la detección de una nueva amenaza en la naturaleza y la liberación de la firma requerida para detectar dicha amenaza, durante ese tiempo de retraso, el IDS no estará en capacidad de detectarla.

Basado en anomalías (anomaly-based): Supervisa el tráfico de red y lo compara con una línea base definida, siendo esta línea la que identificará qué se considera normal para la red (por ejemplo, qué tipo de ancho de banda se usa generalmente, qué protocolos y puertos, qué dispositivos normalmente se conectan, etc.) y alerta al administrador o usuario cuando se detecta tráfico anómalo, o significativamente diferente de la línea de base.

Respecto a su nivel de proactividad, un IDS puede clasificarse como:

Pasivo: Simplemente detecta intrusiones y emite avisos. Cuando detecta tráfico sospechoso o malicioso, genera una alerta y la envía al administrador, dependiendo de este último tomar medidas para bloquear la actividad o responder de alguna manera.

Reactivo: Este no sólo detectará tráfico sospechoso o malicioso y alertará al administrador, sino que tomará medidas proactivas predefinidas para responder a la amenaza. Por lo general, esto significa bloquear cualquier tráfico de red adicional desde la dirección IP de origen o usuario, rechazar paquetes maliciosos o resetear las conexiones involucradas.

IPS

Un Sistema de Prevención de Intrusiones (IPS – Intrusion Prevention System) es una tecnología de seguridad de red y prevención de amenazas que examina los flujos de tráfico de red para detectar y prevenir vulnerabilidades.

Los exploits de vulnerabilidades suelen presentarse en forma de entradas maliciosas hacia una aplicación o servicio de destino que los atacantes usan para interrumpir y obtener el control de una aplicación o máquina. Después de una explotación exitosa, el atacante puede deshabilitar la aplicación objetivo (dando como resultado un estado de denegación de servicio), o puede acceder a todos los derechos y permisos disponibles para la aplicación comprometida.

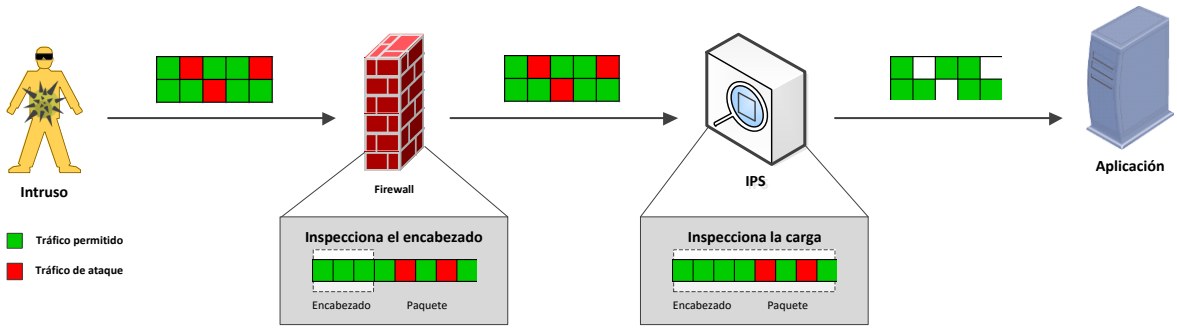


FIGURA 2.42 – DIFERENCIA ENTRE LOS OBJETOS DE INSPECCIÓN DE UN FIREWALL Y UN IPS

Fuente: El autor

Un IPS comúnmente se ubica directamente detrás de un firewall y brinda una capa complementaria de análisis que selecciona negativamente el contenido peligroso. A diferencia de un IDS, el IPS se coloca en línea (en la ruta de comunicación directa entre el origen y el destino), analizando activamente y tomando acciones automáticas en todos flujos de tráfico que ingresan a la red.

Como componente de seguridad en línea, un IPS debe funcionar de manera eficiente para evitar la degradación del rendimiento de la red, también debe hacerlo rápido, ya que las exploraciones deben ocurrir casi en tiempo real. El IPS también debe detectar y responder con precisión, a fin de eliminar las amenazas y los falsos positivos (cuando paquetes legítimos se malinterpretan como amenazas)

Clasificación

De acuerdo a la naturaleza de detección, al igual que un IDS, un IPS se clasifica en basado en firmas o basado en anomalías.

La detección basada en firmas se origina en un diccionario de patrones identificables (firmas) únicas en el código de cada exploit. A medida que se descubre un exploit, su firma se registra y se almacena en un diccionario de firmas en continuo crecimiento.

Las firmas para IPS se dividen en dos tipos:

Orientadas a exploits: Identifican explotaciones individuales activando los patrones únicos de un intento de explotación particular. El IPS puede identificar exploits específicos al encontrar una coincidencia con una firma de exploit en la corriente de tráfico

Orientadas a las vulnerabilidades: Son firmas más amplias que se dirigen a la vulnerabilidad subyacente en el sistema al que se apunta. Estas firmas permiten que las redes estén protegidas contra variantes de un exploit que no se hayan observado directamente en la naturaleza, pero también aumentan el riesgo de falsos positivos.

La detección de anomalías estadísticas toma muestras de tráfico de red al azar y las compara con un nivel de rendimiento de referencia calculado previamente. Cuando la muestra de actividad de tráfico de red está fuera de los parámetros del rendimiento de referencia, el IPS toma medidas para gestionar la situación.

METODOLOGÍAS DE DISEÑO DE REDES

Puesto que el diseño de redes se está volviendo cada vez más complejo debido al creciente desarrollo de la tecnología y los diferentes tipos de tráfico agregados a la red troncal, es necesario contar con metodologías, procesos y arquitecturas que soporten los planes de diseño de red.

Los siguientes problemas han dado lugar a nuevas arquitecturas de red:

- El crecimiento en diferentes tipos de aplicaciones
- La evolución de las TI, desde la conectividad de red básica hasta los sistemas inteligentes convergentes
- Mayores expectativas comerciales de las redes

Al construir, mantener o rediseñar una red, la elección de los componentes de hardware y software de red debe completarse con un diseño, planificación, implementación y soporte cuidadosos.

Los modelos organizativos modernos actuales intentan aprovechar el poder de la interconexión y los beneficios de Internet global. El enfoque moderno es diferente en muchos aspectos del modelo organizacional tradicionalmente empleado, el que muchas veces generó un diseño de red vertical.

Las empresas y organizaciones tradicionales tienen una estructura cerrada y una capacidad limitada para integrarse con otras organizaciones y otras compañías desde el punto de vista de TI, lo que da como resultado un acceso limitado a la información.

Estas instituciones son difíciles de asociar e interactuar, ya que la mayoría de los procesos y aplicaciones se realizan internamente. Por tanto, las empresas que adoptan este modelo no pueden adaptarse y aprovechar las nuevas tecnologías.

Es difícil también para ellas crear y mantener relaciones óptimas con sus partes interesadas (por ejemplo, socios, clientes e inversionistas)

Estas desventajas crearon la necesidad de un nuevo modelo organizativo de redes moderno basado en un diseño de red horizontal que permita la asociación y la colaboración con otras entidades. Proporciona también una experiencia más centrada sobre los productos y servicios vitales para el modelo de negocio de una organización.

El problema clave en el diseño de redes es la capacidad de compartir información, tanto interna como externamente. Internet ofrece una forma de lograr esto al brindar a las empresas acceso a recursos ilimitados que aportan valor; lo cual hace que las relaciones con grupos de interés sean tan importantes como los productos o servicios reales ofrecidos por una institución, lo que es clave para el éxito de la misma.

El poder de las relaciones es un aspecto clave del intercambio de información institucional y la integración de sistemas.

El proceso de construir un sistema capaz de integrar todas las partes interesadas se conoce como “ecosistema”. El diseño de un ecosistema debe incluir una infraestructura de red escalable y flexible que pueda aprovechar las redes empresariales e Internet.

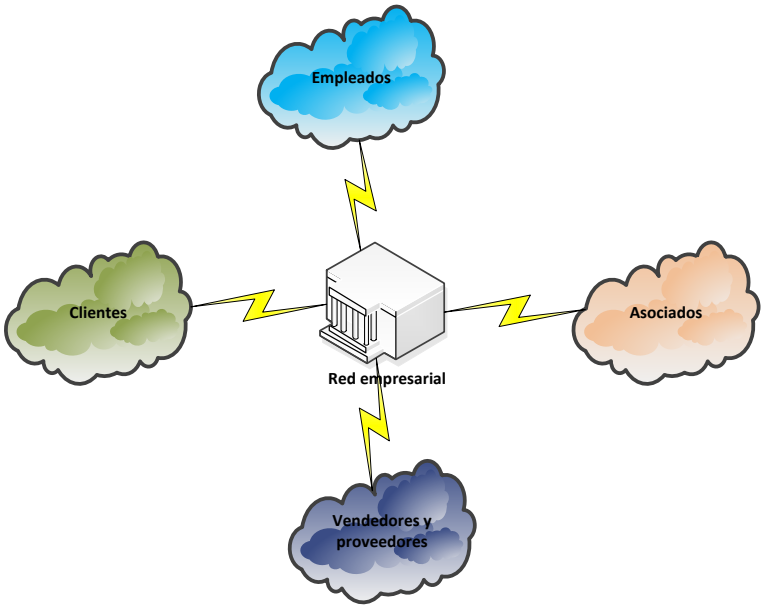


FIGURA 2.43 – EJEMPLO DE UN ECOSISTEMA DE RED EMPRESARIAL

Fuente: El autor

Crear un entorno que sea accesible, colaborativo, y que pueda romper las fronteras geográficas, promoverá un entorno eficiente integración de todas las partes interesadas.

Aspectos básicos de la infraestructura de red

Como se mencionó anteriormente, una infraestructura de red flexible ayuda a la organización y sus clientes a satisfacer las necesidades, políticas y procedimientos para ayudar a facilitar los flujos de información.

Diseñar y mantener la infraestructura de red implica considerar las siguientes características esenciales:

Disponibilidad: Las aplicaciones críticas deben tener acceso completo a los recursos de la red las 24 horas del día, los 7 días de la semana. Todos los componentes de la infraestructura de red deben ser redundantes y resistentes.

Eficiencia: Se debe proporcionar el mejor equipo y software para obtener resultados óptimos, lo cual debe lograrse con costos e inversiones razonables (la red más eficiente al menor costo), mediante la implementación de características tales como calidad de servicio (QoS); Autenticación, Autorización y Contabilidad (AAA); y filtrado.

Funcionalidad: La infraestructura de red debe admitir las aplicaciones y servicios de negocios en términos de eficiencia y disponibilidad.

Capacidad de administración: Las herramientas de administración deben incluir tecnologías que mejoren el control de la red (administración de la configuración, monitoreo del rendimiento y detección de fallas)

Rendimiento: Las aplicaciones importantes deberían obtener todo el ancho de banda que necesitan. Se debe usar hardware escalable y modular, los sistemas operativos de los equipos de red deben estar configurados correctamente y emplear tecnologías especiales cuando sea necesario (como por ejemplo, QoS)

Escalabilidad: Esto incluye la capacidad de crecer y expandirse de acuerdo con los objetivos organizacionales, políticas y procedimientos. Es posible que se requieran estudios de escalabilidad, por ejemplo cuando se planifican adquisiciones de empresas e integración de infraestructuras y servicios.

Introducción a Cisco SONA Framework

Cisco SONA (Software-Oriented Network Architecture) consiste en un marco arquitectónico que ilustra cómo construir sistemas integrados y guiar la evolución de empresas y organizaciones hacia redes más inteligentes. Al usarlo, las instituciones tendrán la capacidad de mejorar la flexibilidad e incrementar la eficiencia mediante la optimización de las aplicaciones, procesos de negocios, y recursos para habilitar que las TI tengan un gran impacto y efecto en el negocio.

Este marco, el cual se muestra en la figura a continuación, indica cómo los sistemas integrados pueden permitir una arquitectura flexible y proveer virtualización y estandarización con eficiencia operativa. Debe tenerse en cuenta que en el marco arquitectónico SONA, la red es el elemento común, y habilita todos los componentes de la infraestructura de las TI.

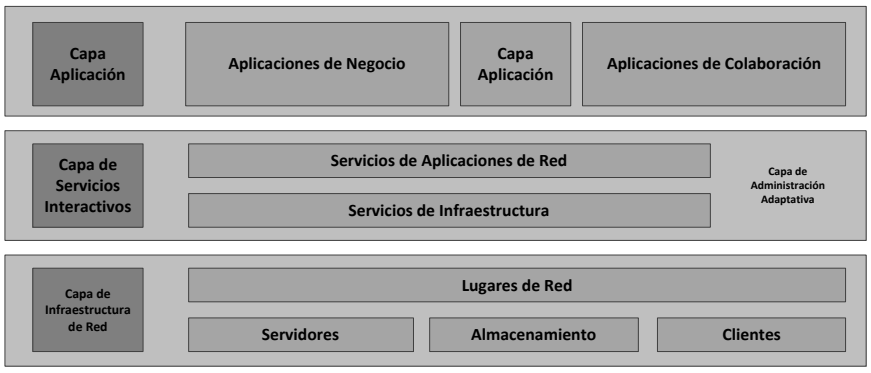


FIGURA 2.44 – MARCO ARQUITECTÓNICO DE CISCO SONA

Fuente: El autor

La capa inferior está compuesta por la infraestructura física, que también se conoce como capa de infraestructura de red; aquí es donde se encuentran los servidores, el almacenamiento y los clientes e incluye diferentes áreas de diseño modular (por ejemplo, WAN, borde empresarial, sucursal, campus, centro de datos y teletrabajo)

La capa intermedia comprende a los servicios centrales comunes; éstos se integran en una capa de servicios interactivos junto con la gestión de servicios e incluyen lo siguiente: comunicaciones en tiempo real, servicios de movilidad, servicios de almacenamiento, entrega de aplicaciones, servicios de gestión, tecnología de virtualización, servicios de transporte.

La capa superior comprende la plataforma de aplicaciones, que incluye aplicaciones comerciales, aplicaciones desarrolladas internamente, software como servicio (Software as a Service (SaaS)), aplicaciones compuestas (Product Lifecycle Management (PLM), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Supply Chain Management (SCM)), aplicaciones de colaboración (mensajería instantánea, centro de contacto IP, entrega de video, etc.)

Una red basada en SONA estará construida desde cero con redundancia y resistencia para evitar el tiempo de inactividad de la red.

El objetivo de SONA es proporcionar tiempos de respuesta y rendimiento rápidos y de alto rendimiento asegurando QoS según la aplicación.
Una red SONA estará configurada para maximizar el rendimiento de todas las aplicaciones críticas, como voz y video, brindando capacidad de administración incorporada, administración de configuración, monitoreo de rendimiento, detección de fallas, herramientas de análisis; proporciona un diseño eficiente con el objetivo de reducir el costo total de propiedad (TCO – Total Cost of Ownership) y aumentar al máximo los recursos existentes de la organización cuando aumenta la demanda de aplicaciones.

Metodología de Diseño PPDIOO

La metodología de diseño Cisco PPDIOO (Preparación, Planeación, Diseño, Implementación, Operación, Optimización), refleja el ciclo de vida de una red, teniendo al diseño como parte integral de esta metodología.

El ciclo de vida PPDIOO de una red, que se muestra en la siguiente figura, refleja las fases del ciclo de vida de una red en general; que si bien se hallan separadas, están cercanamente relacionadas entre sí.

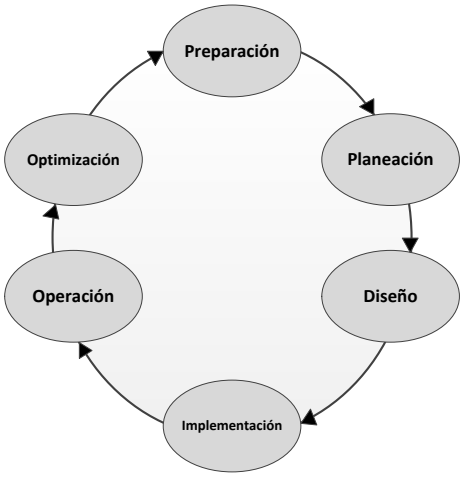


FIGURA 2.45 – FASES DE LA METODOLOGÍA CISCO PPDIOO

Fuente: El autor

A continuación se describen cada una de las fases de la metodología PPDIOO:

Fase de preparación: Involucra el establecimiento de los requerimientos tanto de la organización como del negocio, el desarrollo de una estrategia de red y proposición de una arquitectura conceptual de alto nivel, así como la identificación de tecnologías que puedan soportar de la mejor manera dicha arquitectura. Los justificativos económicos basados en la estrategia de red son establecidos mediante la evaluación del caso del negocio relacionado con la arquitectura propuesta

Fase de planeación: Involucra la identificación de los requerimientos de la red, que se basan en los objetivos establecidos para la misma, tales como dónde será instalada, qué servicios proporcionará y a quiénes, etc.
Esta fase envuelve además la evaluación de los sitios en los que la red se instalará, así como en los que ya se halla instalada una red preexistente, la realización de un análisis para determinar si la infraestructura de sistemas existente, ubicación y entorno operativo podrán soportar el sistema propuesto.

Un plan proyecto ayuda a administrar tareas, responsabilidades, puntos críticos y recursos necesarios para llevar a cabo los cambios en la red. Éste debe alinearse con los parámetros de alcance, costo y recursos establecidos en los requerimientos iniciales del negocio. Por tanto, el resultado de llevar a cabo esta fase será la obtención de un conjunto de requisitos y requerimientos para la red

Fase de diseño: Los requisitos iniciales determinados en la fase de planeación dirigirán las actividades de los especialistas en diseño de redes. Dichos especialistas diseñarán la red de acuerdo a estos últimos, incorporando cualquier dato adicional reunido durante el análisis y la auditoria de la red (si es que existe una, la cual se está mejorando) y a través de discusiones con los administradores y usuarios de la red.
La especificación del diseño de red es detallada y comprensible, reúne los requerimientos tanto técnicos como del negocio, e incorpora especificaciones para brindar disponibilidad, confiabilidad, seguridad, escalabilidad y desempeño. Esta especificación de diseño proporciona las bases para las actividades de implementación

Fase de implementación: La implementación y verificación empieza luego que el diseño ha sido aprobado. La red y cualquier componente adicional se construyen en concordancia con las especificaciones de diseño, teniendo como objetivo integrar los dispositivos sin romper la red preexistente o crear puntos vulnerables

Fase de operación: Es la prueba final sobre la adecuación del diseño. Esta fase envuelve el mantenimiento de la salud de la red mediante operaciones diarias, que pueden incluir el mantenimiento de alta disponibilidad y reducción de costos.
La detección de fallos y su corrección así como la supervisión del desempeño por medio de las operaciones diarias antes mencionadas, proporcionan datos iniciales para la fase de optimización

Fase de optimización: Esta fase se fundamenta en la administración y manejo proactivo de la red, cuyo objetivo es identificar y resolver inconvenientes antes que verdaderos problemas surjan y la organización se vea afectada.
Tanto la detección y corrección reactiva de problemas (troubleshooting) son necesarias cuando el manejo proactivo no puede predecir y mitigar los fallos.

En el proceso PPDIOO, la fase de optimización puede apuntar a un completo rediseño de la red si es que se presentan demasiados problemas o errores en la red, si la red no cumple con las expectativas o si es que nuevas aplicaciones de soporte institucional o requisitos técnicos han sido identificados

Aunque el diseño es una de las seis fases de la metodología PPDIOO, todas las otras fases influencian las decisiones de diseño, por tanto, la fase de diseño interactúa cercanamente con las restantes, como se muestra a continuación:

- Los requerimientos y requisitos derivados de las fases de preparación y planeación son las bases del diseño de la red
- La fase de implementación incluye la comprobación inicial del diseño en la red real
- Durante las fases de operación y optimización, la decisión definitiva se relaciona con la adecuación del diseño, basada en el análisis de la red y cualquier problema que pueda surgir. La red podría tener que ser rediseñada con el objeto de corregir cualquier error descubierto

Pasos de Diseño

La metodología de diseño presentada aquí incluye tres pasos básicos, algunos de los cuales son intrínsecos a la fase de diseño de la metodología PPDIOO, mientras que otros lo estarán con otras fases de la misma metodología:

Paso 1 - Identificar los requerimientos del cliente

En este paso, el cual es generalmente completado durante la fase de preparación de la metodología PPDIOO, los diseñadores identifican los requerimientos iniciales. En base a ellos, se presentará una arquitectura conceptual de alto nivel.

Paso 2 - Describir la red existente y sitios

La fase de planeación involucra una descripción de los sitios, evaluación de cualquier red existente, y la realización de un análisis para determinar si la infraestructura disponible, los sitios y el entorno operacional podrán apoyar el sistema propuesto. La descripción de la red existente y sitios incluye tanto una auditoria como el análisis de la red. Durante la auditoria de la red, se la verifica completamente para comprobar la integridad y calidad; mientras que cuando se efectúe el análisis de la red, el comportamiento de la red (tráfico, congestión, etc.) será analizado.

Paso 3 - Diseño de la topología y soluciones de red

Se crea el diseño detallado de la red. Se toman decisiones acerca de las infraestructuras de red, servicios y las aplicaciones. La información y datos reunidos gracias a las decisiones tomadas recolectados durante los pasos descritos anteriormente. Una red piloto o prototipo podría tener que ser construida para verificar la exactitud del diseño e para identificar y corregir cualquier problema como una prueba conceptual antes de implementar la red completa. Se redacta un diseño detallado, que incluirá la información documentada en los pasos previos.

Paso 4 - Planear la implementación

Durante este paso, se establecen los procedimientos de implementación. La valoración de costos también se lleva a cabo en este momento. Este paso se realiza durante la fase de planeación correspondiente a la metodología PPDIOO.

Paso 5 - Implementar y verificar el diseño

La implementación y verificación del diseño toman lugar durante este paso al construir la red; éste nos lleva directamente a la fase de Implementación correspondiente a la metodología PPDIOO.

Paso 6 - Supervisar, y opcionalmente, rediseñar: La red es puesta en operación después de su construcción. Durante la operación, ésta es supervisada constantemente en busca de posibles errores. Si los problemas son muy frecuentes o incluso imposibles de gestionar, se requerirá un rediseño de la red; lo cual puede ser evitado si todos los pasos previos han sido realizados correcta y completamente.

Este paso es, de hecho, una parte de las fases de operación y optimización de la metodología PPDIOO.

Luego de establecer los requerimientos organizacionales y de documentar la red existente (si es que la hay), los diseñadores estarán listos para establecer y diseñar una solución de red.

Metodología de Diseño Top-Down

Como puede verse, el diseño de una red mediana o grande puede ser un proyecto bastante complejo, es por ello que se han desarrollado procedimientos para facilitar el proceso de diseño al dividirlo en pasos más pequeños y manejables. La identificación de estos pasos o tareas por separado asegura un proceso uniforme, que ayuda a reducir riesgos potenciales.

La metodología Top-Down permite a los diseñadores ver el cuadro en su totalidad antes de adentrarse en los detalles. Un diseño basado en Top-Down aclara los objetivos del diseño y permite iniciar el proceso de diseño desde la perspectiva de las aplicaciones requeridas.

Esta aproximación permite adaptar la infraestructura física a las necesidades de las aplicaciones. Los dispositivos de red se elegirán luego de un profundo y meticuloso análisis de requerimientos. Se deberán integrar prácticas estructuradas de diseño a la aproximación Top-Down, especialmente en redes muy complejas.

Las guías para desarrollar un diseño basado en Top-Down incluyen lo siguiente:

1. Analizar cuidadosamente los requerimientos del cliente.
2. Iniciar el diseño desde la capa más superior del modelo OSI. En otras palabras, primero definir las capas superiores (aplicación, presentación y sesión), después las inferiores (transporte, red, enlace de datos y física), finalmente la infraestructura requerida (routers, switches y medios de transmisión)
3. Reunir información adicional relacionada con la red (protocolos, requisitos de escalabilidad, requerimientos adicionales, etc.) que podrían influenciar tanto el diseño lógico como físico. Asimismo, adaptar el diseño a los nuevos requerimientos, si es necesario.

Metodología de Diseño Bottom-Up

La contraparte de un diseño basado en Top-Down, en la que los dispositivos de red y las tecnologías se eligen primero se conoce como Bottom-Up.

En ésta, en lugar de centrarse en las aplicaciones que impulsan la necesidad de crear una red nueva o rediseñar una pre-existente, se empieza en la capa más baja del modelo OSI (física), centrándose en cuestiones tales como tecnologías específicas, protocolos, medios de red, etc.

En términos generales, este es el contenido con el que los profesionales de redes están más familiarizados; teniendo una tendencia a comenzar el proceso de diseño en este nivel, dejando las aplicaciones y servicios como una idea de último momento para ser considerados más adelante, ya que después de todo, la red no funcionará sin contar con el equipo necesario (routers, switches, firewalls…)

En la mayoría de los casos, tomar un enfoque ascendente tiende a requerir un análisis inicial menos minucioso, y es más fácil de implementar como una solución rápida.

Empero, el enfoque Bottom-Up pocas veces es realmente exitoso, ya que tiende a depender de una serie de soluciones ideadas e implementadas sobre la marcha, con el fin de tratar los problemas que inicialmente no fueron considerados.

Esta aproximación a menudo da como resultado una red inapropiada para los servicios requeridos, usándose principalmente cuando se solicita una respuesta rápida a una solicitud de diseño de red o una red pequeña. Sin embargo, al usar esta metodología, se corre un alto riesgo de tener que rediseñar completamente la red.

Comparación entre las Técnicas Top-Down y Bottom-Up

La metodología de diseño Top-Down tiene varios beneficios al compararla con la aproximación Bottom-Up, incluyendo los siguientes:

- Incorpora los requerimientos y necesidades del cliente
- Provee tanto a los diseñadores como al cliente de una perspectiva global del diseño deseado
- Proporciona un diseño que es apropiado tanto para los requerimientos actuales como para un despliegue futuro

La principal desventaja que presenta un diseño basado en Top-Down es que requiere más tiempo que uno basado en Bottom-Up; puesto que se necesita un análisis de requerimientos meticuloso, de tal manera que el diseño pueda adaptarse a las necesidades identificadas y establecidas.

Una ventaja de un diseño basado en Bottom-Up (elegir los dispositivos y tecnologías y luego moverlos hacia los servicios y aplicaciones) es que permite brindar una pronta respuesta a una solicitud de diseño, lo que facilita los diseños basados en la experiencia previa de los diseñadores.

La mayor desventaja es, sin embargo, que puede dar como resultado un diseño inapropiado, lo que apuntaría a un costoso rediseño; Bottom-Up es la metodología de diseño más común, pero se encuentra lejos de ser óptima.

Metodología SAFE

Cisco SAFE brinda una metodología para el diseño e implementación de redes empresariales seguras, mediante una arquitectura modular en base a los siguientes requisitos de diseño:

- Seguridad y defensa contra ataques basada en normativas
- Implementación de seguridad a través de toda la infraestructura
- Gestión de informes y reportes seguros
- Autenticación y autorización de usuarios
- Detección de intrusos
- Compatibilidad y soporte con las aplicaciones de red actuales y futuras

Las redes actuales abren su infraestructura con el objeto de poder brindar acceso a Internet, conectividad y soporte remoto, servicios en la web, lo que si bien es conveniente, es también inseguro. SAFE proporciona una guía para el diseño de redes seguras mediante módulos, cada uno de los cuales puede incluir firewalls, IPS, antivirus, sistemas de encriptación, entre otros.

SAFE está compuesto por los siguientes módulos:

1. Campus Empresarial
2. Perímetro Empresarial
3. Proveedor de Servicios

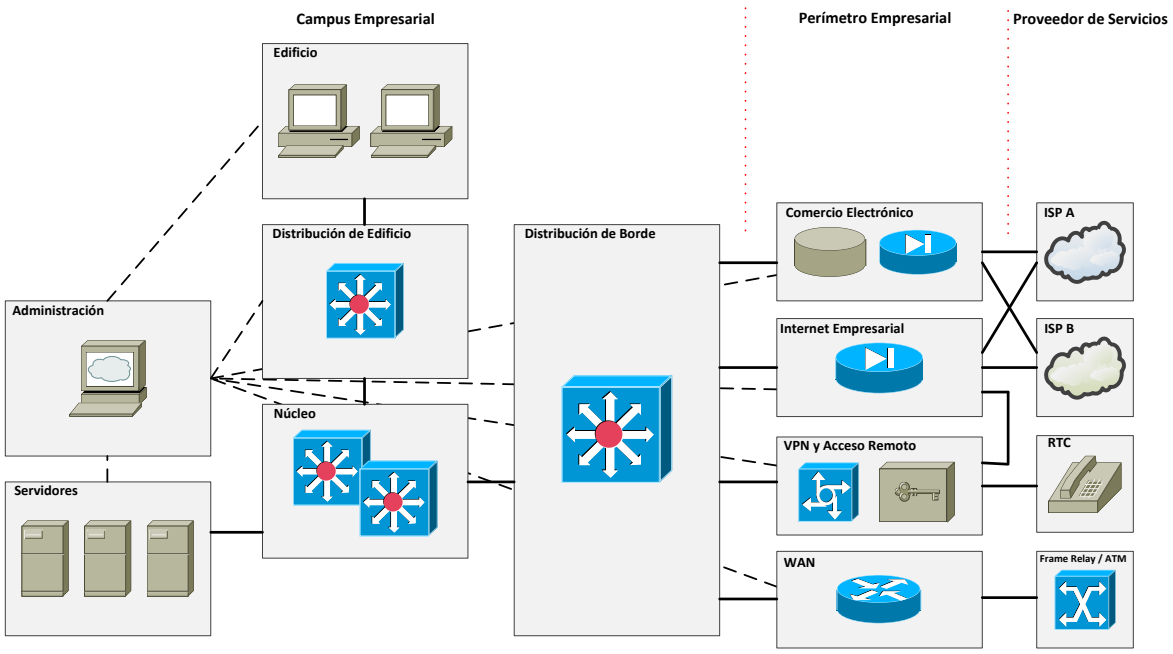


FIGURA 2.46 – MÓDULOS DE CISCO SAFE

Fuente: El autor

Campus Empresarial

Está formado por los siguientes módulos:

Módulo de Administración

Proporciona una administración segura de los dispositivos y hosts en el entorno empresarial.

Dentro de este módulo se consideran dos segmentos de red separados por un router; el primero contiene todos los hosts de administración, entre los que se pueden considerar servidores de control de acceso, monitoreo de red, sistemas de detección de intrusiones, es decir, equipos que se encargan de la administración de configuraciones,

actualizaciones de software, autenticación de usuarios, monitoreo y registros (logs), mientras que en el segundo segmento brinda conectividad a todos los dispositivos que requieren administración.

Módulo de Núcleo (Core)

En un módulo virtualmente idéntico al módulo core (núcleo) de cualquier otra arquitectura de red.

Este módulo está formado por routers y switches encargados del envío de la información tan rápido como sea posible entre redes, y establece la comunicación hacia los módulos de distribución de edificio y de servidores.

Módulo de Distribución

Está dividido en el Módulo de Distribución de Edificio el Módulo de Distribución Perimetral.

El primero brinda servicios de capa distribución hacia los switches de acceso, empleados para otorgar conexión de usuarios finales, incluyendo ruteo, calidad de servicio (QoS) y control de acceso. Este módulo provee la primera línea de defensa contraataques originados internamente, restringiendo el acceso a ciertos departamentos de acuerdo a las políticas establecidas por la empresa.

El Módulo de Distribución Perimetral, permite aumentar la conectividad los elementos en el perímetro, filtra el tráfico y lo enruta desde los módulos de la periferia hacia el módulo de Core.

Este módulo provee la última línea de defensa contra ataques, ofreciendo también conectividad con otros módulos contenidos en el perímetro empresarial, tales como comercio electrónico, Internet corporativo, acceso remoto vía VPN, acceso WAN.

Módulo de Edificio

Llamado también Módulo de Acceso, está definido por los componentes de la red que contienen las estaciones de trabajo, teléfonos y todos los puntos de acceso asociados a la Capa 2 de usuario final.

Proporciona servicio de datos a los usuarios autorizados dentro de la red. Implementa seguridad a nivel de estaciones finales (endpoints) con aplicaciones antivirus o antimalware.

Módulo de Servidores

Brinda servicios de aplicaciones tanto para usuarios finales como dispositivos. Controla el flujo de tráfico por medio de switches de capa 3 y sistemas de detección de intrusos. Este módulo puede contener servidores de correo electrónico interno, servidores departamentales y corporativos, equipos de telefonía central (call management)

Perímetro empresarial

Está formado por:

Módulo de Internet Empresarial

Proporciona conectividad a servicios de Internet tanto a usuarios internos.
El tráfico también fluye desde este módulo hacia el Módulo de VPN y de acceso remoto.

Módulo de VPN y Acceso Remoto

Gestiona tráfico generado desde usuarios remotos hacia las VPN, haciendo caer en desuso las técnicas antiguas de conexión remota (como por ejemplo, dial-up)

Módulo WAN

Este módulo enfatiza la seguridad en la parte que encara a la WAN, enrutando el tráfico entre los distintos sitios remotos en el sitio central.

Proveedor de servicios

Este módulo no es implementado por la institución, sino que se lo incluye hasta el punto de que, para combatir ciertos ataques, habrá que pedir determinadas características de seguridad al ISP.

Metodología SDP de Check Point

SDP (Software Defined Protection) es una arquitectura y metodología de seguridad desarrollada por Check Point Software Technologies en base a la experiencia de dicha empresa en el desarrollo, implementación y mantenimiento de infraestructuras de seguridad modular.

La arquitectura SDP caracteriza la seguridad de una organización en base a tres capas interconectadas y capaces de funcionar en conjunto con el objeto de brindar una seguridad adaptativa y administración centralizada.

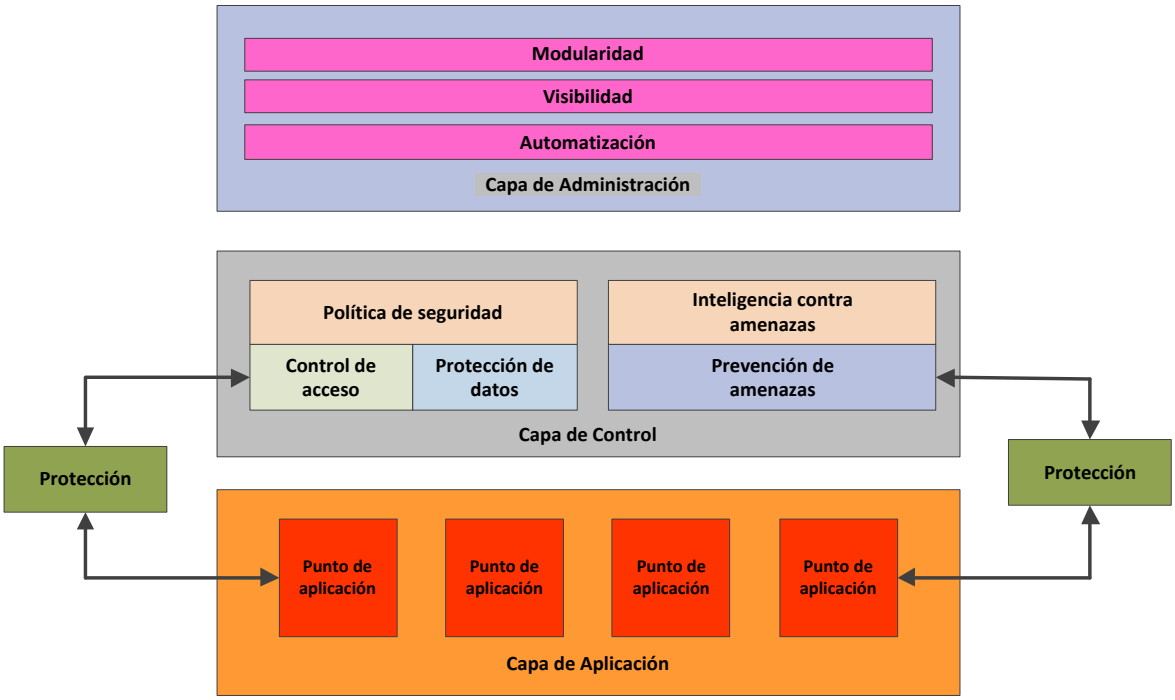


FIGURA 2.47 – CAPAS DE LA ARQUITECTURA CHECK POINT SDP

Fuente: El autor

Las capas que forman parte de la arquitectura son:

1. Capa de Aplicación: Se basa en puntos físicos y virtuales de aplicación de seguridad de red, siendo la encargada de ejecutar la lógica de protección para ambientes de alta demanda.
2. Capa de Control: Analiza distintas fuentes de información sobre amenazas, y es capaz de generar protecciones y políticas que serán ejecutadas por la capa de aplicación.
3. Capa de Administración: Se encarga de gestionar y brindar agilidad a la infraestructura de protección.

SDP es una arquitectura diseñada para apoyar los requerimientos tradicionales de seguridad de red y políticas de accesos, así como la prevención de amenazas que conlleva la implementación de nuevas tecnologías, tales como la computación móvil, redes SDN, computación en la nube, entre otros.

Capa de Aplicación

Esta capa permite identificar y definir los puntos de aplicación tanto a nivel de hosts como de red con el objeto de proteger las interacciones entre los usuarios y los sistemas que éstos emplean. En SDP, este proceso se conoce como “segmentación”, y es el principio fundamental detrás de la capa de Aplicación.

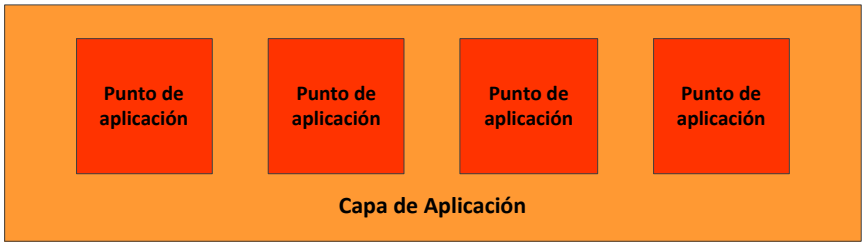


FIGURA 2.48 – CAPA DE APLICACIÓN SDP

Fuente: El autor

Esta segmentación evita que una amenaza (ataque) se reproduzca dentro de la red, por lo que un ataque dirigido a un componente único de la red no estará en capacidad de minar toda la infraestructura de seguridad de la institución.

De esta manera, la segmentación se convierte en la piedra angular de la aplicación de seguridad, teniendo los siguientes objetivos:

- Impulsar una política de seguridad más simple y modular aplicable a varios segmentos de red.
- Permitir la creación de plantillas de arquitectura de seguridad adaptables a los diferentes segmentos de red.
- Hacer cumplir las políticas de contención en los equipos comprometidos dentro de un segmento de red.
- Definir las interacciones internas al segmento de red que no requieren supervisión de los controles de seguridad implementados.

Segmentación

La implementación de la segmentación se inicia con la definición de segmentos atómicos en la red.

Un segmento está definido como un conjunto lógico de elementos informáticos y de redes protegidas por un punto de aplicación; de esta manera, un segmento puede ser tan pequeño como una única aplicación o programa ejecutable en un host, o tan grande como toda la institución.

Un segmento atómico contiene elementos que comparten la misma política y características de protección. Los puntos de aplicación se introducen en la frontera de cada segmento para aplicar una lógica de protección definida, y los segmentos pueden ser agrupados para permitir la protección modular.

Luego de que el modelo de segmentación ha sido creado, se lo integra en el diseño de la red. Por último se definen canales de confianza con el objetivo de proteger las interacciones y el flujo de datos existente entre los distintos segmentos de la red.

Según la arquitectura SDP, los cuatro pasos requeridos para la segmentación son los que siguen:

Paso 1 - Identificación de segmentos atómicos

Un segmento atómico está formado por un conjunto de elementos de cómputo y de redes que comparten un perfil de seguridad común, no puede ser dividido en segmentos más pequeños, y puede protegerse empleando controles de seguridad que regulen todas las interacciones entre el segmento y entidades externas.

La definición de los segmentos atómicos y la identificación de las entidades que comparten un perfil de seguridad común es el primer paso para la implementación de la arquitectura SDP. Se asignará un perfil de seguridad a cada segmento en base al valor de los activos de la organización dentro de un segmento y el nivel de confianza dado a los usuarios del mismo y los controles de seguridad.

Ejemplos de un segmento atómico podrían incluir un elemento de cómputo único en el cual está instalado un software de seguridad o un grupo de servidores en una red compartida, protegida por un equipo (gateway) de seguridad.

Es importante considerar que pueden existir amenazas cuando dos segmentos con distintos perfiles de seguridad interactúan. Adicionalmente, el nivel potencial de amenazas aumentará en paralelo con el diferencial entre el perfil de seguridad de dos segmentos. Para evitarlo, muchas instituciones hacen uso de un sistema de clasificación empresarial global para datos, hosts, aplicaciones y redes que esté en capacidad de soportar esta metodología de segmentación.

Según los objetivos de negocio, uno de los requisitos de seguridad siguientes se elige como principio rector para la clasificación: confidencialidad, integridad o disponibilidad, por ejemplo:

Público: Sistemas y datos que están libres para el acceso por parte del público en general.
Cliente: Sistemas y datos que contienen información confidencial de los clientes, típicamente libres para el acceso de los clientes autenticados y un reducido número de usuarios internos.
Interno: Puede ser accedida por los empleados desde cualquier lugar.
Sensible: Sistemas internos y datos que necesitan mayores protecciones.
Departamental: Restringido sólo para los colaboradores elegidos según su función departamental.

Este tipo de clasificación es útil en la definición de segmentos y sus perfiles de seguridad. El nivel y alcance de la segmentación necesaria para cada organización depende de sus necesidades de negocio y sus requisitos de seguridad; por ejemplo, varias organizaciones hacen cumplir estrictamente las políticas de “privilegios mínimos” y “separación de privilegios”, en tanto que otras contemplan que todos los usuarios y sistemas son equivalentes en términos de niveles de acceso y criticidad de su misión.

Paso 2 – Agrupación de segmentos

Una vez identificados los segmentos, deben agruparse en segmentos jerárquicos (como ejemplo, aplicaciones pueden ser agrupadas dentro de la frontera del host, múltiples hosts dentro de un segmento de red, y múltiples redes de manera jerárquica)

Pese a que cada sub-segmento gestiona su propia protección, la agrupación brinda soporte para:

1. Tener modularidad mejorada mediante la abstracción y el ocultamiento de información.
2. Una confianza mayor y protección más completa en la frontera de segmento superior que dentro de los sub-segmentos.
3. Tener control centralizado en la entrega de servicios de infraestructura de seguridad.
4. Escenarios de infección, contención y recuperación.

Obsérvese la Figura 2.49. En el ejemplo, una organización está formada por varios sitios enlazados por una red de proveedores MPLS. En cada localidad se tiene un hosting de acceso a red, usuarios internos en una red local y segmentos de servidores. Los servidores internos sensibles se encuentran ubicados en segmentos separados, alejados de los usuarios mediante un gateway o punto de aplicación.
Varios segmentos funcionales brindan servicios autónomos a los usuarios finales de los departamentos. Finalmente, una zona desmilitarizada (DMZ) en su propio segmento, proporciona servicios públicos. En el ejemplo, los segmentos de servidores y uno independiente de usuario autorizan control preciso sobre las interacciones realizadas entre segmentos. De este modo, el control hace cumplir las políticas de seguridad en base a clasificación y ejecuta la contención de equipos comprometidos. Todos los segmentos internos reciben servicios de seguridad de un sistema centralizado y una infraestructura de gestión de red dentro de los segmentos de servidores. Tanto el acceso a Internet y como WAN se encuentran controlados por los puntos de aplicación dedicados; el punto de aplicación de Internet controla también el acceso hacia y desde la zona desmilitarizada.

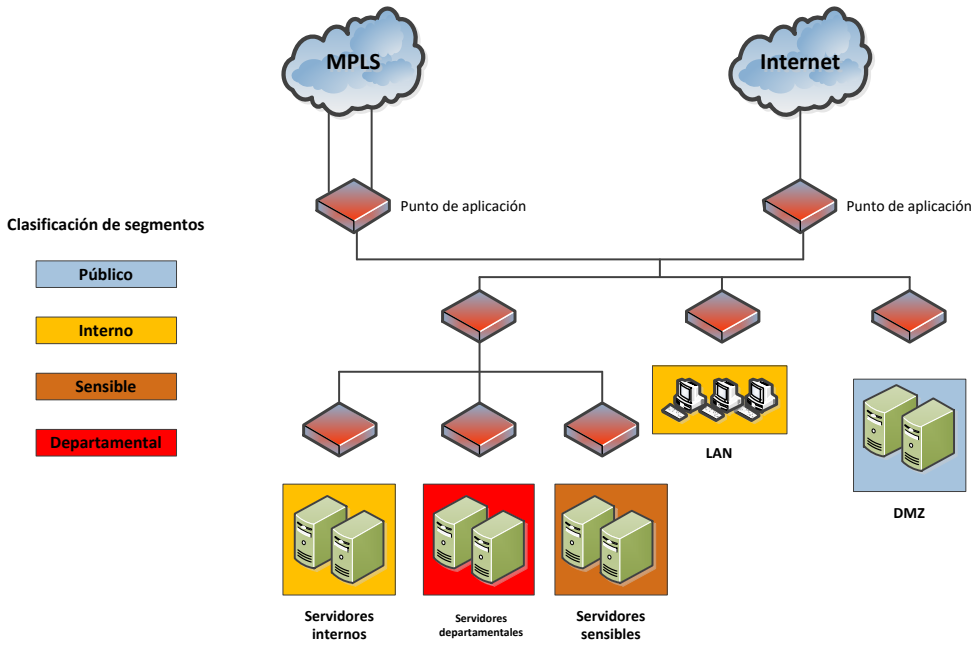


FIGURA 2.49 – EJEMPLO DE AGRUPACIÓN DE SEGMENTOS

Fuente: El autor

En una agrupación jerárquica, es posible que las interacciones deban atravesar varios puntos de aplicación; así, un servidor dentro del segmento de "Servidores Internos" que se conecta a un recurso en Internet (por ejemplo, un servicio de actualización de contenido) podría estar bajo control de los siguientes puntos de aplicación, de manera secuencial:

1. El software de seguridad disponible dentro del segmento "Servidores Internos".
2. El punto de aplicación de frontera del segmento "Servidores internos".
3. El punto de aplicación ubicado en la frontera del Centro de Datos.
4. El punto de aplicación de entrada y salida a Internet.

Las interacciones por medio de servidores tipo proxy del segmento de la DMZ atravesarían rutas adicionales de control, incluyendo el punto de aplicación del segmento desde y hacia el segmento DMZ. Mediante la repetición del proceso de agrupación de segmentos en las partes más grandes de la red, las organizaciones pueden asegurar que todos los activos han sido incluidos en un segmento protegido. Las líneas de defensa jerárquica definidas en base a la agrupación de segmentos compartimentan la red interna y brindan protección superior.

Paso 3 – Consolidación de la aplicación

Una vez creado el modelo de segmentación, deben implementarse los puntos de aplicación a manera de gateways de seguridad de red o como software basado en host.

En la Figura 2.50 se presenta la segmentación de una red que incluye estaciones de trabajo, servidores (de CRM, R&D y Finanzas), un Centro de Operaciones de Seguridad (SOC) y servidores que ven al exterior en un segmento de DMZ. Los perfiles de seguridad se asocian con los segmentos atómicos y los puntos de aplicación se ubican en la frontera de cada segmento. Luego los segmentos se agrupan respecto a sus perfiles de seguridad.

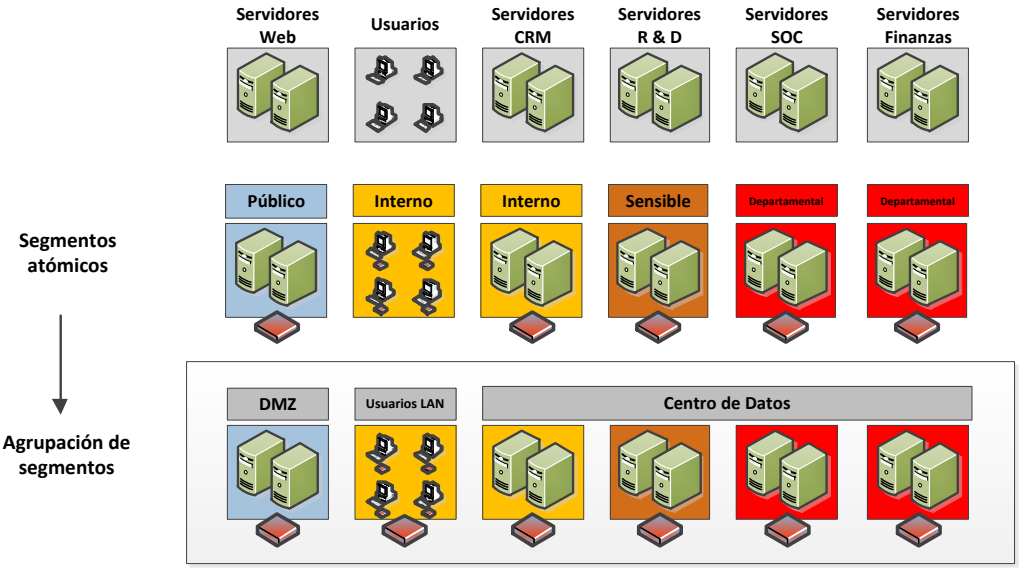


FIGURA 2.50 – PROCESO DE SEGMENTACIÓN EMPRESARIAL

Fuente: El autor

El modelado desde abajo hacia arriba, brinda tanto la flexibilidad como la modularidad requeridas para poder determinar los puntos de aplicación necesarios para cualquier caso, desde una sola aplicación institucional hasta el total de la organización. Los encargados de la seguridad establecen dónde empezar (por ejemplo, el proceso, el host y la red) y dónde acabar.

A continuación, los puntos de aplicación definen líneas de defensa jerárquicas que ofrecen protección para los datos y sistemas ubicados dentro de la frontera de los segmentos correspondientes.

Las tecnologías de consolidación y virtualización abarcan gateways multipuerto, virtualización de gateways, VLAN, SDN y virtualización de la red; las cuales pueden emplearse para obtener un rendimiento óptimo, lograr capacidad de administración y disminuir el costo de propiedad.

Paso 4 – Canales confiables

Los puntos de aplicación del segmento previenen el establecimiento de interacciones no autorizadas entre segmentos; pero las interacciones autorizadas también deben ser protegidas.

Cuando dos segmentos de red tienen elementos comunes, un gateway de seguridad puede instalarse físicamente a los dos segmentos para supervisar las interacciones entre ellos. En cambio, cuando se encuentran separados físicamente, dichas interacciones deben asegurarse mientras viajan a través de la infraestructura de red.

Si las interacciones entre segmentos se establecen por medio de un segmento jerárquico ubicado dentro de una red de confianza, entonces dicho segmento jerárquico es el responsable de asegurar los datos en tránsito; pero, si la red no es confiable respecto a los perfiles de seguridad de los dos segmentos, los atacantes tendrían la oportunidad de acceder o modificar los datos que corren a través de los dos segmentos.

Entonces, debe establecerse un canal de confianza entre los segmentos y utilizar cifrado para sus interacciones; de este modo, dicho canal impediría el acceso no autorizado a los datos que lo atraviesan, al mismo tiempo que detectaría y bloquearía los intentos de modificación de la información.

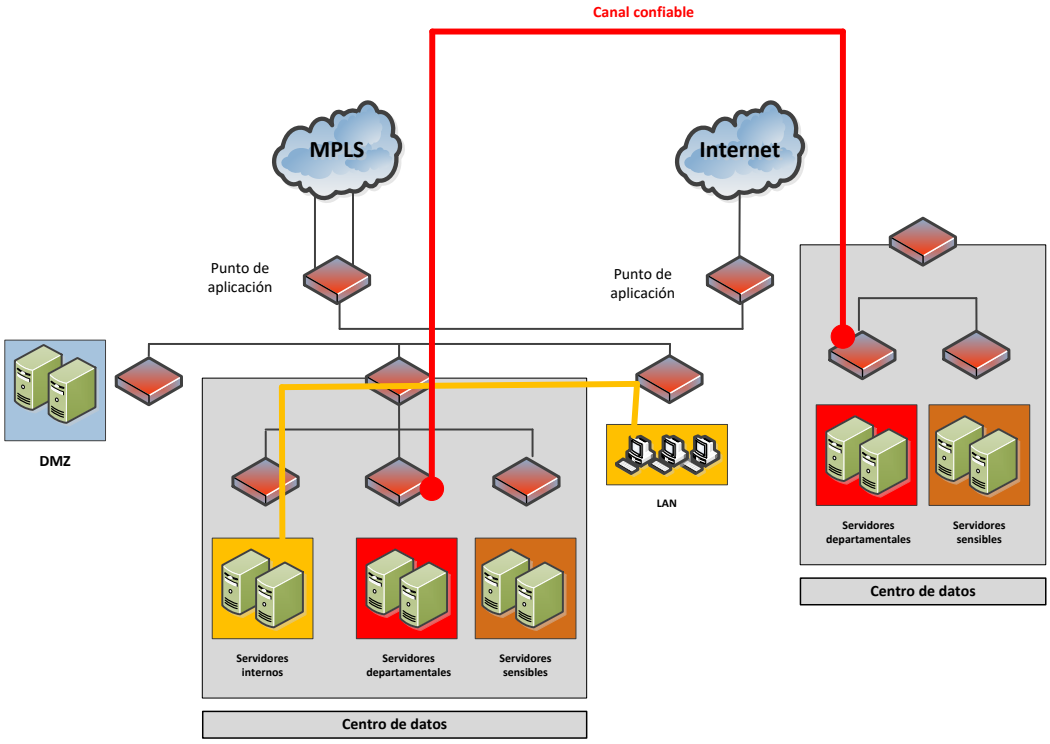


FIGURA 2.51 – EJEMPLO DE UN CANAL CONFIABLE

Fuente: El autor

Capa de Control

Esta capa es el núcleo de la arquitectura SDP; su trabajo es generar protecciones definidas por software y extenderlas para su ejecución en los puntos de aplicación apropiados previamente definidos en la capa de Aplicación, sea que se la implemente usando equipamiento dedicado de alto rendimiento o como un software basado en host en la red, en dispositivos móviles o en la nube.

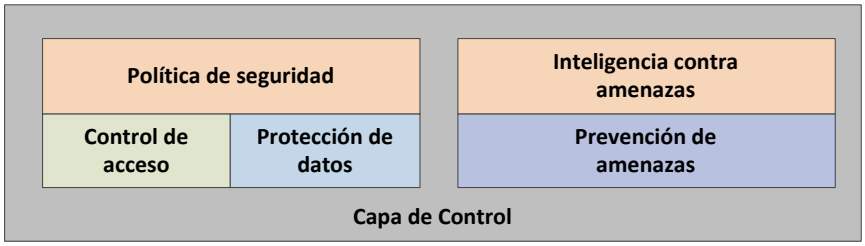


FIGURA 2.52 – CAPA DE CONTROL SDP

Fuente: El autor

La capa de control provee una plataforma robusta, capaz de ejecutar las protecciones en los puntos de aplicación de toda una organización.

Ya que las protecciones son controladas por software, el equipamiento (hardware) subyacente desplegado en dichos puntos no necesita ser reemplazado cuando se descubre un nuevo método de amenaza o ataque, o se introducen nuevas tecnologías en la organización.

Las protecciones deben ser capaces de adaptarse de manera automática al entorno de amenazas sin ser necesario el seguimiento manual para la revisión de los avisos y recomendaciones; lo cual se logra empleando controles de prevención de amenazas automáticos que sean capaces de interactuar con la capa de administración únicamente cuando sea necesaria la toma de decisiones por parte del personal técnico (por ejemplo, cuando los indicadores de una amenaza solamente brindan baja confianza respecto a la identificación de una amenaza o ataque)

Prevención de Amenazas

Las protecciones de prevención de amenazas deben estar en capacidad de bloquear atacantes y evitan la explotación de vulnerabilidades y entrega de cargas malignas.

Aquí, la premisa es simple y directa: todas las amenazas deben prevenirse.

Esta premisa necesita poca personalización a nivel de la organización, pues es genérica y debe ser aplicada en todas las instituciones.

Las protecciones de prevención de amenazas pueden dividirse en dos grupos: pre-infección y post-infección. Las protecciones pre-infección proveen de detección proactiva y prevención de amenazas que tratan de aprovecharse de vulnerabilidades en aplicaciones y protocolos internos o de querer denegar servicios a las aplicaciones autorizadas, mientras que las protecciones post-infección proporcionan defensas ágiles que permiten la detección, contención y neutralización de amenazas después de que han alterado exitosamente una o más entidades de la red.

Estas protecciones limitan la expansión de malware y bloquean las conexiones bot a servidores de comando y control.

En ocasiones, un solo hallazgo de seguridad brinda poca confianza respecto a la existencia de una amenaza, El componente de prevención de amenazas de la capa de Control es capaz de correlacionar los hallazgos en base a varios motores (firmas, reputación, comportamiento, emulación de malware y validación humana) para proporcionar un nivel de confianza mayor. Adicionalmente, esta capaz es capaz de utilizar recursos externos para componer una protección de seguridad significativa.
Para lograr que los distintos controles de prevención de amenazas sean eficaces, éstos tienen que ser alimentados por una inteligencia contra amenazas vasta y confiable; las organizaciones deben contar con un flujo de información constante contra amenazas para difundirla dentro de su entorno seguridad sin que sea necesaria la intervención manual alguna.

Control de Acceso

La función de la capa de control es la de seleccionar la lógica de control de seguridad requerida, misma que se ejecutará en cada uno de los puntos de aplicación ubicados en las fronteras de los segmentos, con el objeto de hacer cumplir la política de protección de datos y control de acceso, además de contrarrestar las amenazas identificadas.

Del mismo modos, habilita los procesos de negocio gracias a la definición de interacciones entre usuarios y los datos dentro de la red corporativa, aplica el nivel mínimo necesario para apoyar el negocio y hace cumplir la directiva de seguridad de “mínimo privilegio", de este modo, las interacciones no autorizadas de manera expresa, simplemente se considerarán como no autorizadas y deberán bloquearse.
Las diversas protecciones de control de acceso dependen de repositorios que describen las reglas de negocio, aplicaciones, activos, usuarios y roles de la organización, definen también las políticas de seguridad para el conjunto de interacciones autorizadas entre los activos, usuarios y aplicaciones antes mencionadas; por ejemplo, el control de acceso determinará si se autoriza a un usuario acceder a los servicios sensibles de la institución y podría evaluar y calificar autorizaciones en base a parámetros como la ubicación del usuario, el estado del host, la hora del día, entre otros.

Los controles de protección usualmente se dividen en grupos de control de entrada y salida.

A nivel de entrada, cada segmento debe proteger sus activos contra ataques externos. La estricta aplicación de mínimos privilegios mínimos disminuye la superficie de ataque, así por ejemplo, si una aplicación dentro del segmento contiene alguna brecha de seguridad, pero debido a que el acceso a la aplicación está prohibido por la política de control de acceso, la vulnerabilidad no podrá ser explotada.
El principio de mínimos privilegios indica también que los clientes ubicados dentro del segmento protegido deben tener acceso sólo a los servicios externos que directa o indirectamente apoyen al negocio, entonces serán necesarios controles de salida para el cumplimiento de este principio.

El análisis y control del tráfico se hacen de manera adaptativa en base al contexto, por ejemplo, en el caso del tráfico de Internet, la capa de control consultará con una base de datos ubicada en la nube sobre los últimos protocolos y aplicaciones autorizadas; mientras que en el caso del tráfico interno se podrá autorizar el uso de una aplicación propietaria o protocolo utilizado por la organización.

Adicionalmente, la capa de control se encuentra al corriente de los cambios de red y definiciones aplicadas en otros sistemas de tecnologías de la información; tales ejemplos pueden ser los cambios del repositorio de usuarios, aplicación automática de seguridad de una nueva máquina virtual o permitir el acceso a un host nuevo definido en un servidor de nombres de dominio (DNS). En el caso de SDN, la capa de control orquesta también el flujo de tráfico de la red a través de los puntos de aplicación apropiados, modelando así la red para adaptarse al modelo de segmentación de la empresa y a la política de seguridad requerida.

Protección de Datos

Para poder resguardar y asegurar la información de modo adecuado, las protecciones deben seguir a los datos en reposo (almacenados) y en movimiento.

Para denegar acceso a usuarios no autorizados, se deben aplicar controles criptográficos para garantizar la protección de los datos tanto dentro como fuera de la institución. Al realizar la clasificación de los datos mediante la categorización de la información de la institución, es posible examinar los flujos de datos para identificar y prevenir la pérdida de los mismos.

Por tanto, la protección de datos depende de la política de seguridad para la categorización de datos

Los datos se clasifican en función de sus propiedades, atributos y contenido. Las firmas de datos son creadas de acuerdo al grado de sensibilidad de los datos, y se usan para prevenir la fuga de datos hacia usuarios no autorizados, estén en cualquier host o ubicación. Adicionalmente, los mecanismos de cifrado, tales como el cifrado de datos y aplicación firmas digitales, deben aplicarse a los datos en almacenamiento, para evitar el acceso y la modificación no autorizada.

Estos mecanismos brindan protección persistente, inclusive cuando los datos son copiados fuera del entorno controlado. Por ejemplo, la aplicación de cifrado es particularmente valiosa para los dispositivos móviles, el almacenamiento en medios extraíbles, los entornos de almacenamiento compartido y el cómputo en la nube; necesitándose una infraestructura de gestión de llaves local o en la nube para poder gestionar las llaves y el acceso a los datos cifrados con eficacia.
Del mismo modo, el cifrado puede usarse también para garantizar la eliminación segura de datos mediante la revocación de llaves.

Puesto que en una organización se tienen distintos tipos de activos valiosos, se necesitan distintas protecciones aplicables en diferentes puntos de aplicación.
La selección de los tipos de protección depende de los activos del segmento, así como las autorizaciones a nivel de usuario y el entorno de las amenazas, tomándose en cuenta también el rendimiento del sistema y las limitaciones operacionales.

Para la selección de los controles de seguridad proactivos, se necesita aplicar una estrategia de identificación de riesgos.

El primer paso es realizar un análisis de riesgo en cada segmento o grupo de segmentos. Se define como riesgo al nivel de impacto y potencial de ocurrencia de incidentes de seguridad en las operaciones o los activos de una organización.
Los tipos de eventos de seguridad incluyen violaciones de la política de seguridad, manifestación de amenazas y flujos de datos inapropiados o no autorizados. La comprensión del riesgo brinda un marco de prioridades para los controles de seguridad.

Deben considerarse distintas categorías de riesgo para cada interacción que atraviesa una frontera de segmento. Un nivel de riesgo puede codificarse en base a la ocurrencia, las posibilidades de éxito y el daño potencial; por ejemplo, una petición HTTP saliente puede analizarse respecto a un esquema de clasificación de riesgo, como se indica a continuación:

Riesgo	Descripción del riesgo	Análisis para una petición HTTP saliente
Interno	Un usuario autorizado realiza una interacción que viola la política de seguridad	¿Está el usuario dentro de un segmento autorizado para acceder al servicio externo?
Ataque externo	Un ente externo intenta lograr acceso restringido a bienes o servicios	¿El servicio externo podría haber sido falsificado por el atacante?
Acceso a datos	Un atacante lee o modifica datos en tránsito o en reposo mediante el acceso a la red o la infraestructura de almacenamiento	¿La ruta de acceso de red para dicha interacción es vulnerable a la intercepción?
Fuga de datos	Transmisión de datos sensibles a usuarios no autorizados, o se almacenan en un medio extraíble	¿Cantidades significativas de datos podrían ser almacenadas en lugares no autorizados?
Exploit	Un atacante lleva a cabo una violación del protocolo, causando un fallo del sistema	¿Cuál es la probabilidad de que una violación del protocolo pueda disparar un exploit de cliente y malware en el segmento al que pertenece?
Malware	El código malicioso diseminado en la red o por un dispositivo extraíble, afecta los activos institucionales	¿La petición podría ser un indicativo de comportamiento sospechoso?
Negación de servicio	Una interacción consume excesivas cantidades de procesamiento, almacenamiento o capacidades de red, negando el servicio a las interacciones autorizadas	¿Podrían la tasa, duración del evento o consumo de ancho de banda afectar el nivel de servicio para interacciones autorizadas?

Tabla 2.11 - Ejemplo de tabla de riesgos versus petición de servicio HTTP

Fuente: El autor

Los riesgos también pueden ser detallados respecto a los métodos de ataque potenciales, a diferencia del modo general mostrado anteriormente; en este caso se define un conjunto de controles de seguridad para mitigar cada riesgo, reduciendo la exposición a un nivel que sea aceptable para la institución. Obsérvese a continuación una vista simplificada del mapeo de los riesgos versus las protecciones:

Riesgo	Control de acceso		Prevención de amenazas		Protección de datos
	Entrada	Salida	Pre	Post	
Interno	Sí	Sí		Sí	Sí
Ataque externo	Sí		Sí	Sí	Sí
Acceso a datos					Sí
Fuga de datos		Sí		Sí	Sí
Exploit	Sí		Sí		
Malware	Sí	Sí	Sí	Sí	
Negación de servicio	Sí		Sí		

Tabla 2.12 - Mapeo de riesgos versus protecciones

Fuente: El autor

Cada una de las filas describe un riesgo de nivel general o un método detallado de ataque (por ejemplo, el malware entregado como un adjunto a un correo electrónico), mientras que cada columna identifica un módulo de protección y mitigación (por ejemplo, prevención de amenazas pre-infección) o de protección específica (a saber, filtrado de URL basado en la reputación)

El mapeo de protecciones respecto a los riesgos ayuda a determinar en qué puntos de aplicación deben ejecutarse que controles de seguridad considerando las interacciones atraviesan varios puntos de aplicación, permiten identificar el riesgo residual y ajustar los controles de seguridad en el caso de que un control determinado resulta ser ineficaz, muy costoso o requiere recursos excesivos, y para asegurar que todos los riesgos están suficientemente mitigados.

Como se hizo notar durante la agrupación de segmentos, la agrupación jerárquica implica que una sola interacción es capaz de atravesar múltiples puntos de aplicación; lo cual significa que los controles deben ser aplicados en múltiples puntos a lo largo de la ruta de interacción, con el objeto de mitigar los riesgos correspondientes.
Por ejemplo, los controles anti-malware que responden a los mensajes de correo electrónico entrantes contra firmas de malware conocidas, pueden aplicarse en un punto de aplicación de gateway de seguridad dentro de una DMZ que contiene al servidor de correo interno, en el host cliente o incluso en el mail relay.

La Figura 2.53 muestra una implementación aplicada al ejemplo del apartado anterior, la que incluye distintos controles de seguridad establecidos en los diferentes puntos de aplicación.

Los controles de frontera de segmento se implementan y consolidan en dos dispositivos físicos; el primero es el responsable de controlar el acceso entre Internet y la DMZ, del mismo modo entre la DMZ y la red interna.

El segundo gateway de seguridad incluye cinco sistemas virtuales que brindan controles para la WAN basada en MPLS, la LAN y los segmentos de servidores Internos, Sensibles y Departamentales.

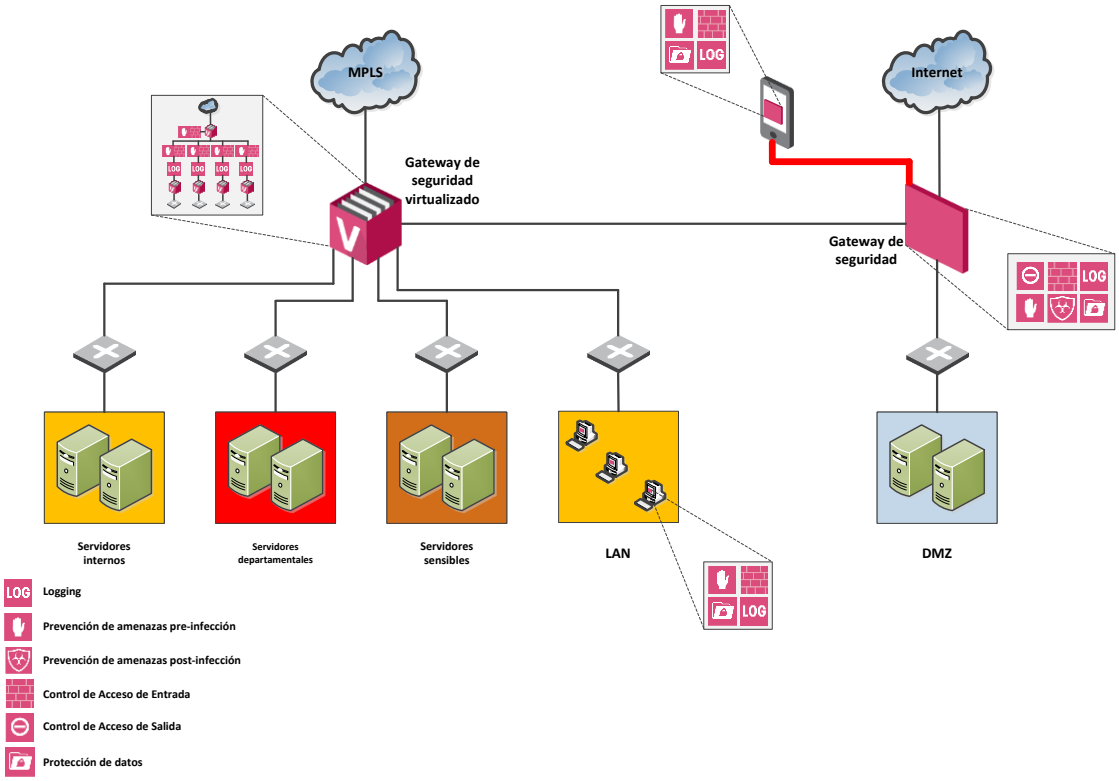


FIGURA 2.53 – APLICACIÓN DE CONTROLES DE SEGURIDAD EN PUNTOS DE APLICACIÓN

Fuente: El autor

En este ejemplo, lo distintos hosts ubicados en el segmento de Servidores Internos incluyen controles de software de seguridad tales como firewall, anti-malware, cifrado completo del disco y registro centralizado.

Los dispositivos móviles implementan firewall, cifrado, registro de datos y controles VPN. Un canal de confianza VPN se emplea para brindar conectividad dispositivos móviles a la institución por medio de Internet.

El gateway de seguridad que encara a Internet implementa el conjunto más amplio de controles, puesto que el diferencial entre el Internet de acceso público y los perfiles de seguridad perimetral de la institución es más significativo.

De esta manera conforma un diseño robusto, el cual incluye:

1. Control de acceso de entrada: Firewall, IPS y protección DDoS.
2. Prevención de amenazas pre-infección: Anti-malware.
3. Prevención de amenazas post-infección: Anti-bot.
4. Control de acceso de salida: Control de aplicaciones y filtrado URL.
5. Protección de datos: Prevención de pérdida de datos (DLP) y VPN.

Para los servidores internos, los sistemas virtuales implementan control de acceso de entrada y prevención de amenazas (firewall e IPS), ya que el diferencial en los perfiles de seguridad es menor.

Capa de Administración

Esta capa otorga visibilidad para saber qué está sucediendo en la red y brinda la respuesta proactiva ante incidentes, así como la inteligencia necesaria para adaptar los controles de seguridad de la institución, permitiendo además la integración de la seguridad en los procesos de negocio de la institución.

FIGURA 2.54 – CAPA DE ADMINISTRACIÓN SDP

Fuente: El autor

En los nuevos entornos de red, los cuales implementan virtualización y arquitecturas orientadas a servicios, es común que las aplicaciones se muevan entre hosts, los hosts virtuales lo hagan de un servidor físico a otro, y las redes mismas sean capaces de auto-

configurarse dinámicamente a través de SDN (Software Defined Networking) y otras API (Application Programming Interface), los usuarios móviles y los servicios en la nube amplían el alcance de la red de la institución; siendo estos cambios una carga grande que recae sobre los administradores de seguridad, personal que es necesario para gestionar los controles de acceso a la red en función de las direcciones y distintos servicios de red.

Del mismo modo, un entorno de amenazas que se vuelve más hostil a cada momento, tanto dentro como fuera de la organización, requiere que los administradores gestionen una política de mínimo privilegio más granular, pero capaz de tener en cuenta atributos adicionales tales como la identidad del usuario, asignaciones de funciones, estado de cumplimiento del host, identidad de los datos, identidad de la aplicación y los parámetros de la petición.

En este entorno de rápida evolución de los procesos del negocio, la capa de administración de la metodología SDP brinda un marco de referencia que es modular, abierto y resiliente.

Modularidad

Facilita la distribución de las tareas de administración de seguridad en los diferentes equipos que trabajan de forma simultánea para abordar los retos de la organización. Cada administrador está en contacto con un subconjunto de la política de seguridad global y simple, el cual se relaciona con su área de responsabilidad.

Con el objeto de estar en capacidad de escalar a organizaciones muy grandes, la capa de administración debe soportar múltiples administradores trabajando de manera simultánea en el proceso de gestión de la política de seguridad, permitiendo así modificaciones concurrentes a las políticas y brindando capacidad de combinación, de ser necesario.

A fin de lograr el objetivo de la política modular, la política de seguridad debe seguir las fronteras de los segmentos lógicos, tal y como se define en la capa de aplicación; de este modo, la definición de políticas se simplifica en gran manera, ya que se centran en las necesidades de cada segmento y en las interacciones necesarias.

A modo de ejemplo en la Figura 2.55, el segmento de Servidores Internos alberga un servidor de base de datos, en tanto que un servidor web usado para acceder a la base de datos se encuentra alojado en el segmento DMZ. Los administradores de red del centro de datos podrían establecer una política de seguridad de red global que:

1. Permita ciertos protocolos en la red interna
2. Una subcapa que especifique las aplicaciones web autorizadas podría ser controlada por un administrador de DMZ
3. Un administrador a cargo de los Servidores Internos, será capaz de gestionar una capa independiente que define los objetos de datos autorizados a salir del segmento

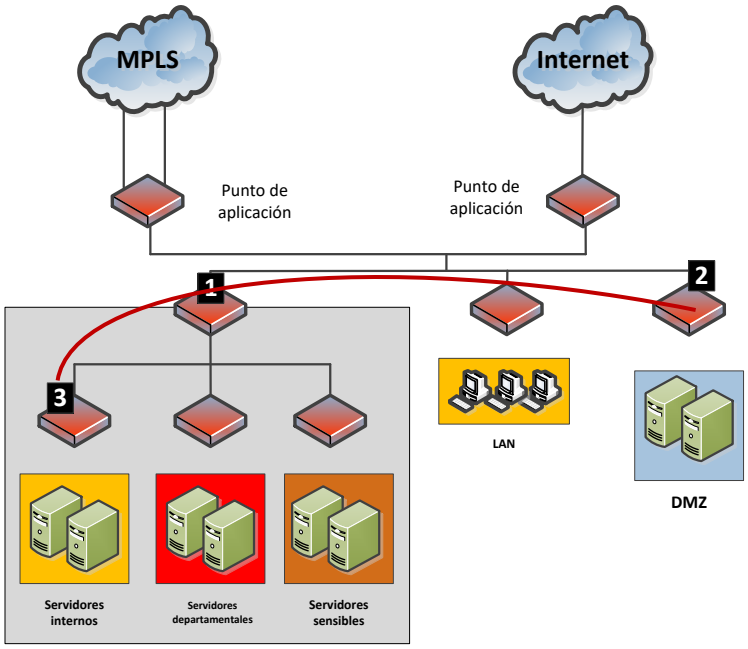


FIGURA 2.55 – MODULARIDAD DE LA POLÍTICA

Fuente: El autor

La capa de administración debe aplicar los principios de mínimo privilegio y segregación de funciones tanto para las acciones del administrador como para secuencias de comandos de automatización de la capa de administración; esto ayuda a reducir la complejidad de las políticas, el riesgo debido a una configuración errónea y las amenazas internas.

Automatización y Sincronización

La automatización brinda interfaces de automatización abiertas que permiten a la organización el automatizar la administración de políticas de seguridad y organizarlas junto con otros sistemas de la institución.

La capa de aplicación sincroniza la política de seguridad de la capa de control con entornos dinámicos empresariales, incluyendo bases de datos de configuración, sistemas de inventario de activos e infraestructura de gestión de identidad, por medio de la actualización automática de objetos y sus atributos a través de las API de capa de administración de SDP, CLI (Command Line Interface) y otras.

De manera general, la automatización se basa en un modelo de “Control de Acceso Basado en Atributo” (Attribute Based Access Control), el cual transmite las políticas de seguridad como funciones de atributos lógicos y contextuales tales como aplicaciones, funciones, clasificación de datos y tipos de cliente y servidor, en lugar de utilizar los identificadores estáticos, como por ejemplo, las direcciones IP y los puertos de red.

La automatización de políticas puede emplearse para llevar un control de las reglas, acción que se conoce como “higiene de reglas”, con el fin de asegurar una política de seguridad precisa, alertando a los administradores de errores comunes, ajustando y afinando automáticamente las políticas de seguridad.

Visibilidad

La visibilidad permite tener conocimiento de la situación y responder ante incidentes.

La capa de administración de la arquitectura SDP establece la respuesta a los incidentes como una interacción entre las distintas protecciones de la capa de control y el equipo técnico de respuesta. Pese a que los controles automatizados son muy efectivos al evaluar y discernir enormes cantidades de datos y detectar comportamientos considerados anómalos, la inteligencia humana es superior en cuanto la identificación de patrones de comportamiento no autorizado, eliminación de falsos positivos,

categorización de los eventos. Adicionalmente, en ocasiones se emplean mecanismos de reacción automatizada para bloquear comportamientos maliciosos que coinciden con los indicadores de confianza.

La capa de administración acopia, consolida y correlaciona eventos de los puntos de aplicación desplegados en la red de la organización. Para apoyar la visibilidad, brinda acciones de respuesta a incidentes con capacidad de visualización en tiempo real de las cadenas de eventos, lo cual permite la identificación de los vectores de ataque iniciales, además de los hosts y datos comprometidos. Posteriormente, la investigación de eventos permitirá generar nuevos indicadores de amenazas de malware, comportamientos de amenazas y direcciones de red asociados con cada ataque identificado; estos indicadores alimentan de manera automática a la capa de control y son distribuidos desde allí a la capa de aplicación, con el objeto de proteger a la institución.

Un incidente puede ser un evento independiente, como por ejemplo una infección por virus sin objetivo específico o intento de hackeo; cuando se lo detecta, se debe ejecutar un procedimiento de respuesta capaz de clasificar los síntomas detectados y que permita tomar una decisión al respecto de que si se requiere o no una respuesta. Se deben tomar y analizar datos forenses, prestando atención a la detección de un ataque, la investigación de posibles daños y detener cualquier intento repetido de ataque.

Metodología IBM ISF

Esta metodología ha sido desarrollada por IBM para afrontar la brecha de comunicación tanto entre las perspectivas del negocio como las técnicas de seguridad, cuyo fin es permitir la simplificación de ideas y procesos.

La mayoría de los proyectos relacionados con tecnología desarrollados en la actualidad están impulsados por los ejes de TI y de negocios, siendo estos últimos por lo general el factor desencadenante. Los ejes de negocios miden el valor, riesgo y costos económicos que influyen en el enfoque de la seguridad de TI; dentro de éstos se consideran: operación correcta y confiable, acuerdos de niveles de servicio, valor de los activos de TI, valores del negocio e imagen de la marca, acuerdos contractuales, marco regulatorio, pérdidas financieras, infraestructura crítica, responsabilidad legal.

Los ejes de TI representan consideraciones técnicas y restricciones operacionales en el entorno general de TI, tales como agentes de amenazas internas y externas, gestión de servicios tecnológicos, complejidad del entorno de TI, complejidad del entorno de negocios, vulnerabilidades por fallos, configuraciones, exploits.

A medida que una institución asegura sus procesos de negocio, el enfoque comercial basado en el negocio debe transformarse en una influencia directa que permita garantizar que todos los dominios de seguridad trabajen juntos, estando alineados con los objetivos comerciales; caso contrario, la postura de riesgo de la organización se vuelve vulnerable debido a una desalineación de prioridades entre el departamento de TI y la estrategia de negocios.

Con el objetivo de ayudar a garantizar que todos los dominios de seguridad de TI necesarios se aborden correctamente, IBM creó el marco de seguridad de TI llamado ISF (IBM Security Framework)

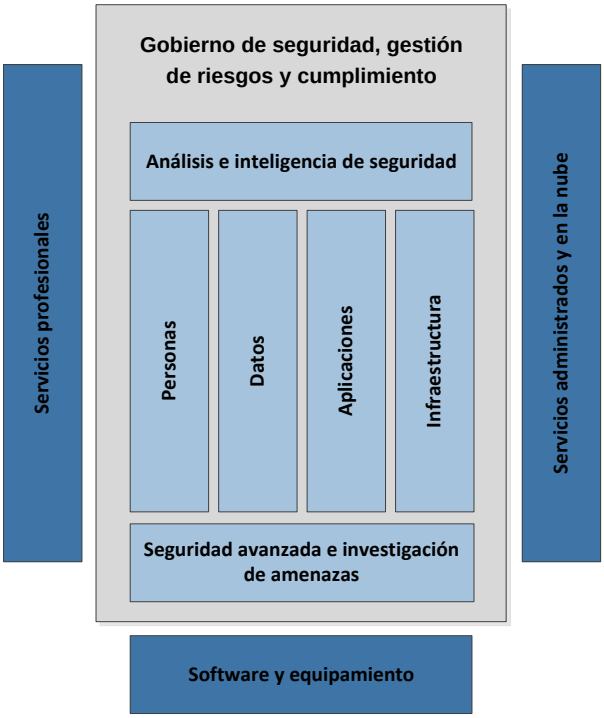


FIGURA 2.56 – IBM SECURITY FRAMEWORK

Fuente: El autor

Gobierno de seguridad, gestión de riesgos y cumplimiento

Este modelo organizacional engloba los principios, políticas, plan de seguridad y el proceso de mejoramiento de calidad.

Toda institución necesita definir y comunicar los principios y políticas que guían su estrategia comercial operativa. Asimismo, cada organización debe evaluar los riesgos comerciales y operativos a los que se encuentra expuesta, y desarrollar un plan de seguridad institucional que sirva como punto de referencia para la ejecución y validación de las actividades de gestión de seguridad que sean apropiadas para la misma.

El modelo cubre los siguientes dominios de seguridad, cada uno de los cuales tiene sus propios requisitos y criterios de cumplimiento:

1. Análisis e inteligencia de seguridad: Proporciona una capa de descubrimiento, información y reportería de los dominios de seguridad, un centro de control para análisis de sesiones, alertas y eventos en dominios
2. Personas: Cubre los aspectos que deben asegurar que sólo las personas correctas tengan acceso a los recursos correctos en el momento correcto, para lo cual se requiere una administración de identidad y control de acceso
3. Datos: Hace referencia a la mejora de los aspectos sobre cómo proteger los datos críticos tanto en tránsito como en reposo (almacenados) en toda la institución
4. Aplicaciones: Cubre aspectos sobre cómo garantizar la seguridad de las aplicaciones y los servicios comerciales
5. Infraestructura: Cubre aspectos sobre cómo mantenerse un paso adelante de amenazas emergentes en todos los componentes del sistema de TI
6. Seguridad avanzada e investigación de amenazas: Aborda las necesidades del mercado respecto a la seguridad y brinda una base para comprender las amenazas, sus fuentes y cómo responder de manera efectiva ante ellas.

Este modelo brinda un marco de referencia para los dominios de seguridad por medio del cual una organización podrá proteger a su personal, datos, aplicaciones e infraestructura

Introducción a IBM Security Blueprint

Como se vio anteriormente, la metodología IBM Security Framework divide al área de seguridad de TI orientada a los negocios en cuatro dominios de seguridad principales y tres capas de soporte.

IBM Security Blueprint fue creado luego de investigar múltiples escenarios relacionados con clientes que se centraban en cómo crear soluciones de TI, siendo la intención apoyar y ayudar al diseño e implementación de soluciones de seguridad de las organizaciones, empleando un enfoque neutral para la categorización y definición de las capacidades de seguridad y servicios necesarios para responder las inquietudes comerciales de la organización o institución.

Proporciona capacidades básicas de seguridad y permite dividir los dominios y capas con más detalle, con el objetivo de trabajar hacia un conjunto común de capacidades básicas de seguridad básicas que son necesarias para ayudar a una organización a cumplir con sus objetivos de negocios de manera segura.

Debe tenerse en cuenta que la creación de una solución requiere una arquitectura, diseño e implementación específicos, elementos que pueden ser evaluados mediante IBM Security Blueprint, pero no los reemplaza. Sin embargo, IBM Security Blueprint puede brindar un enfoque sólido que permita considerar las capacidades de seguridad en una arquitectura o solución particular.

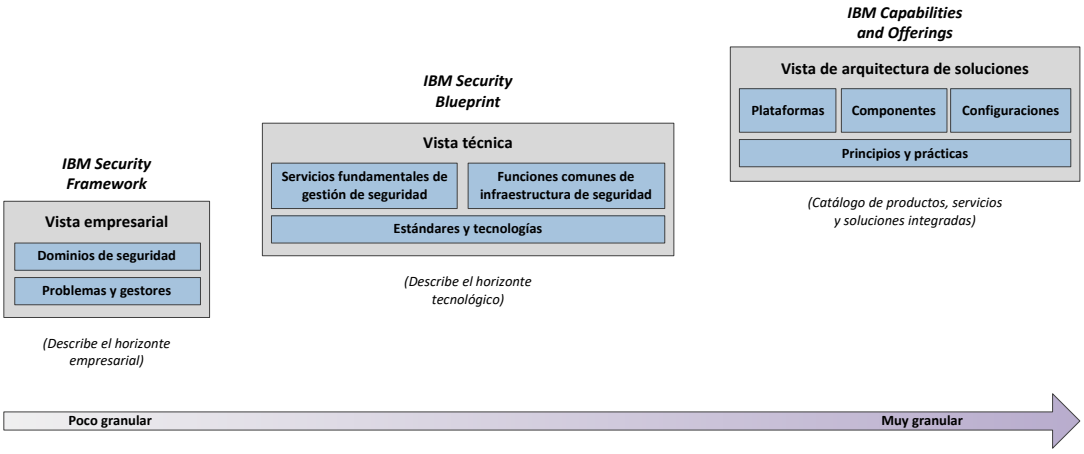


FIGURA 2.57 – POSICIONAMIENTO DE IBM SECURITY BLUEPRINT

Fuente: El autor

En la figura, la parte izquierda representa a IBM Security Framework, la cual define los dominios de seguridad desde una perspectiva comercial, mientras que la parte central a IBM Security Blueprint, que muestra la gestión de seguridad y las capacidades de la infraestructura de seguridad de TI necesarias dentro de una organización, y como se indicó anteriormente, IBM Security Blueprint describe estas capacidades en términos de productos y de proveedores neutrales.

Finalmente, la parte derecha representa las vistas de la arquitectura de la solución, las que describen una guía de implementación específica para un entorno de TI y la madurez actual de la organización dentro de los dominios de seguridad respectivos; de este modo, las vistas de arquitectura de la solución brindan detalles sobre productos específicos, soluciones y las interacciones entre ellos.

La Figura 2.58 muestra completamente el entorno de IBM Security Blueprint, con cada capa y componente:

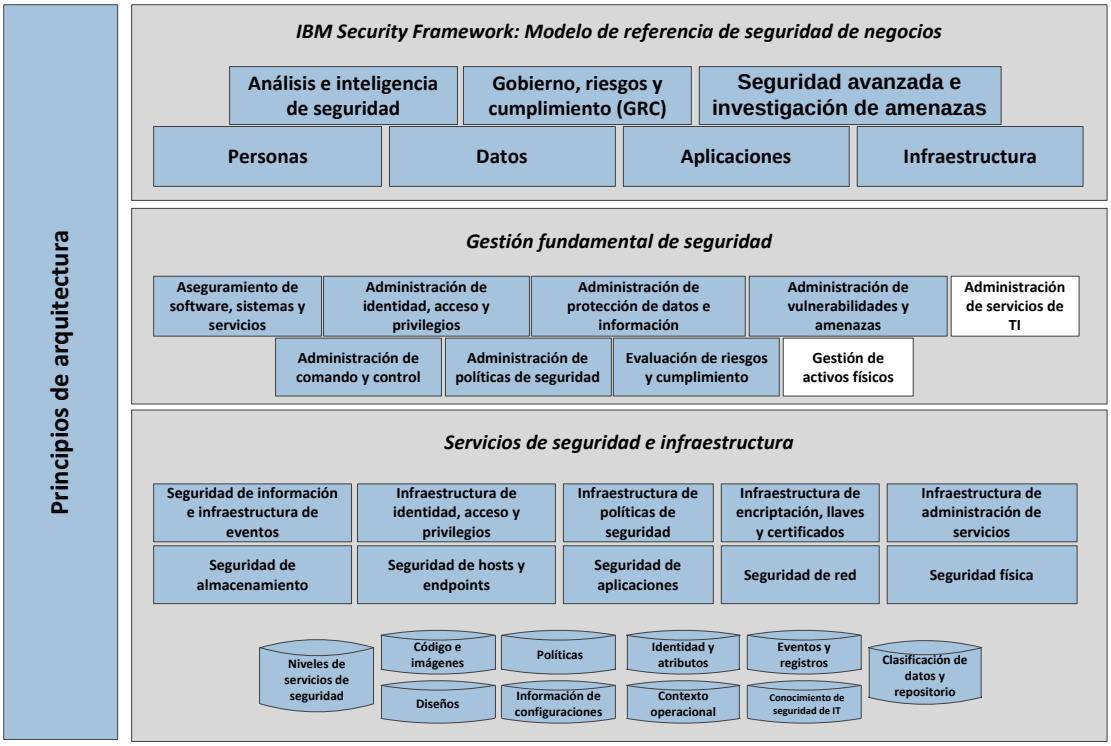


FIGURA 2.58 – ENTORNO TOTAL DE IBM SECURITY BLUEPRINT

Fuente: El autor

Principios de arquitectura

IBM ha definido los siguientes principios que acompañan a la descomposición del servicio. Estos principios se pueden aplicar a todos los niveles del modelo, y diseño de soluciones, convirtiéndose también en pautas para productos y soluciones de fabricante.

Apertura

La apertura es de primordial importancia en un entorno institucional. Incluye soporte para todas las principales plataformas, tiempos de ejecución e lenguajes, soporte para los principales estándares de la industria, interfaces y algoritmos publicados, evitando la "seguridad por oscuridad", confianza documentada y modelos de amenazas y soporte, y programas de validación de seguridad.

Seguridad por defecto

La seguridad no debe ser una ocurrencia tardía en las soluciones de TI; las políticas de seguridad deben ser seguras de inmediato.

Esta situación se ve favorecida tanto por una definición y una administración coherentes de las configuraciones, un conjunto afín de funciones de seguridad en todos los productos, así como una interfaz de usuario de administración de seguridad funcional.

Diseño para auditoría

Teniendo muchos requisitos en el área de cumplimiento, es importante que todas las acciones relevantes para la seguridad puedan registrarse y auditarse, que la infraestructura de auditoría sea escalable y capaz de manejar estos eventos y la información de auditoría sea inmutable.

Diseño para regulaciones

Las regulaciones determinan muchos requisitos en proyectos de seguridad de TI y éstas cambian con el tiempo. El manejo de esta situación necesita un soporte flexible para las restricciones establecidas por las regulaciones gubernamentales y los estándares de la industria, trazabilidad entre las regulaciones, estándares y políticas comerciales, y de las políticas de seguridad que se usan para implementarlas.

Diseño para la privacidad

En la actualidad, el intercambio de datos y la privacidad se vuelve cada vez más importante. Las soluciones deben destacar el uso de la información de identificación personal y los mecanismos de protección de datos correspondientes y habilitar los principios de aviso, elección y acceso.

Diseño para extensibilidad

Las buenas soluciones se basan en componentes que separan la gestión de los mecanismos de los propios mecanismos ubicados en un mismo entorno. Los sistemas implementados deben ser capaces de permitir la adición y extensión de nuevos mecanismos dentro del marco de gestión existente.

Diseño para compartir

Varias soluciones pueden compartir un único entorno de TI, como en un centro de servicios compartido. Para lograr este objetivo, los servicios de seguridad y la administración deben poder abarcar varios dominios, cada uno de los cuales puede proporcionar su propia política de seguridad, identidad, modelos, etc. Las arquitecturas deben documentar explícitamente las suposiciones y limitaciones que se realizan en términos de alcance de control.

Diseño para el consumo

Todos los servicios de seguridad deben ser utilizados fácilmente por sus audiencias. Estas audiencias incluyen programadores que desarrollan e integran aplicaciones con los servicios de seguridad, sistemas de gestión que crean, actualizan y administran políticas de seguridad y otros artefactos de seguridad, personas que administran, auditan actividades de seguridad, y solicitan acceso a recursos protegidos.

Protección multinivel

La defensa en profundidad es un principio general que puede lograrse por medio de múltiples niveles de aplicación y detección. Los recursos deben estar diseñados para protegerse a sí mismos como una primera capa de defensa. Las intrusiones se pueden contener a través del aislamiento y la zonificación. La existencia de múltiples niveles también minimiza la superficie de ataque a la capa externa más accesible.

Separación de administración

Los servicios de administración de seguridad (identidad, autorización, auditoría, etc.) se brindan a través de una infraestructura de seguridad dedicada y compartida, lo que permite un monitoreo y cumplimiento consistentes. La aplicación misma (a través de la criptografía, la aplicación de políticas o el aislamiento físico) se distribuye normalmente y se mantiene cerca de los recursos.

Recursos críticos para la seguridad

Los recursos y los actores se mantienen al tanto de su entorno (incluida la ubicación física y la ubicación lógica) y su estado y contexto de seguridad.

Seguridad basada en modelo

Refleja el entorno operativo, modelos comunes y los formatos coherentes de identidad y confianza, datos, políticas, aplicaciones, información y eventos de seguridad y claves criptográficas. Los modelos se interpretan sistemáticamente en una pila (por ejemplo, las identidades de red están vinculadas a identidades de nivel de aplicación) y en todas las unidades (por ejemplo, las políticas y la confianza se negocian y entienden dentro de una federación). Los modelos son consistentemente validados contra la realidad (retroalimentación de políticas y descubrimiento de modelos)

Capas de IBM Security Framework

Capa de gestión fundamental de seguridad

Esta capa contiene los componentes de nivel superior empleados para dirigir y controlar la seguridad de TI desde una perspectiva de gestión de riesgos basada en políticas.

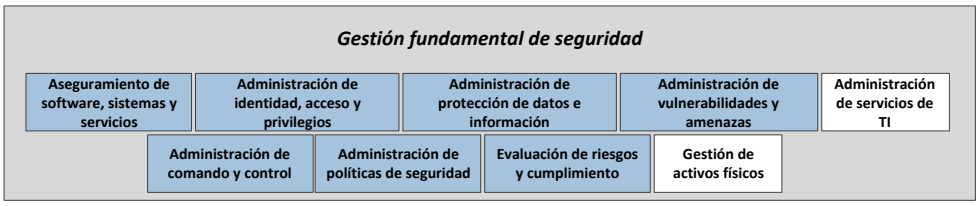


FIGURA 2.59 – CAPA DE GESTIÓN FUNDAMENTAL DE SEGURIDAD

Fuente: El autor

Sus componentes son:

Aseguramiento de sistemas, software y servicios: Aborda cómo los sistemas, software y servicios están diseñados, desarrollados, probados, operados y mantenidos durante todo el ciclo de vida del software, para crear un software predecible y seguro.

Este componente cubre los siguientes elementos:

1. Diseño estructurado
2. Modelado de amenazas
3. Evaluación de riesgos de software
4. Revisiones de diseño para seguridad
5. Análisis y análisis del código fuente
6. Análisis dinámico de aplicaciones
7. Control de código fuente y monitoreo de acceso
8. Firma y verificación de códigos y paquetes
9. Prueba de aseguramiento de calidad
10. Validación de código de proveedor y de terceros

Administración de identidad, acceso y privilegios: Proporciona capacidades relacionadas con roles e identidades y derechos de acceso.
El correcto uso de estas capacidades puede garantizar que se brinde acceso a los recursos a las identidades/individuos correctos, en el momento correcto, y para el propósito correcto. Estos servicios pueden también asegurar que el acceso a los recursos sea monitoreado y auditado para la detección de uso no autorizado.

Administración de protección de datos e información: Otorga capacidades para proteger el acceso a datos tanto no estructurados como estructurados de acuerdo con la naturaleza y el valor comercial de la información.
También proporciona servicios de monitoreo y auditoría de uso y acceso.

Administración de vulnerabilidades y amenazas: Proporciona capacidades para identificación de vulnerabilidades en los sistemas implementados y para recibir informes de vulnerabilidades fuera de las fuentes, determinar la respuesta adecuada y realizar

cambios proactivos en los sistemas implementados con el objetivo de mantener la seguridad de los sistemas desplegados. Otras capacidades recopilan eventos de seguridad e información de un amplio rango de fuentes para obtener información y detectar posibles amenazas a través del evento, correlación e inteligencia y análisis de seguridad.

Administración de servicios de TI: Brinda la automatización del proceso y el flujo de trabajo base para la gestión de seguridad, en particular cambiar y liberarlos procesos de gestión juegan un papel importante en la administración de la seguridad.

Administración de comando y control: Proporciona una plataforma de comando para la gestión de seguridad y las capacidades de seguridad operacional para TI también como activos y servicios no informáticos para garantizar la protección, respuesta, continuidad y recuperación ante eventos que puedan interferir en la normal labor de la institución.
La administración de comando y control cumple tanto un papel estratégico como táctico. El rol estratégico implica la definición de políticas de seguridad, mientras que el rol táctico involucra una coordinación de las operaciones de seguridad.
Cubre temas tales como:

- Asegurar que la seguridad física y operativa se mantenga para las ubicaciones, activos, humanos, medio ambiente y utilidades
- Proporcionar vigilancia y monitoreo de ubicaciones, perímetros y áreas
- Proporcionar incidentes de nivel superior entregados por inteligencia de seguridad para una mayor investigación
- Aplicación de controles de entrada
- Proporcionar posicionamiento, seguimiento e identificación de humanos y activos
- Proporcionar un punto focal para las operaciones de continuidad y recuperación

Administración de políticas de seguridad: Brinda todas las capacidades y repositorios para crear, descubrir, analizar, transformar, distribuir, evaluar y hacer cumplir las políticas de seguridad. La gestión de la política de seguridad involucra la definición de las políticas de seguridad alineadas con los objetivos institucionales capaces de alcanzar niveles de cumplimiento y estar en capacidad de mitigar los riesgos a un nivel aceptable.

Se trata entonces de establecer un marco rector para definir y hacer cumplir las políticas y medir su efectividad, informando a la unidad de Gobernanza, Riesgo y Cumplimiento.

Evaluación de riesgos y cumplimiento: Permite que la organización de TI recolecte y analice información y eventos de seguridad para poder identificar, cuantificar, evaluar e informar sobre los riesgos de TI que pueden contribuir al riesgo operacional de la organización. El establecimiento de tableros de seguridad (dashboards) proporcionan conciencia situacional que permitirá la gestión diaria de riesgo. Este componente cubre la recopilación de riesgos en información sobre los mismos, procesos de riesgo de seguridad de TI, controles comerciales, resiliencia y gestión de la continuidad, informes de cumplimiento, servicios.

Gestión de activos físicos: Permite tener conocimiento de la ubicación y el estado de activos físicos, así como la conciencia de los controles de seguridad física y coordina la información de seguridad para sistemas físicos.

Capa de Servicios de seguridad e infraestructura

Esta capa contiene componentes y subcomponentes que son utilizados por la Gestión de Seguridad Fundamental en sus respectivos contextos:

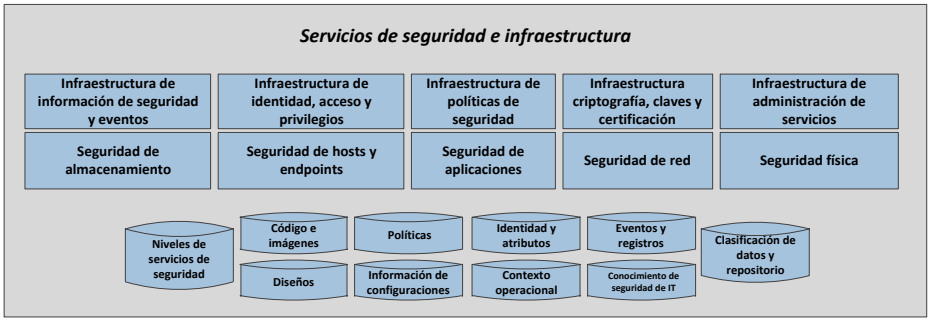


FIGURA 2.60 – CAPA DE SERVICIOS DE SEGURIDAD E INFRAESTRUCTURA

Fuente: El autor

Infraestructura de información de seguridad y eventos: Proporciona la infraestructura para automatizar la agregación, correlación y análisis de registros. Permite también que una organización reconozca, investigue y responda a los incidentes de manera automática, y agilite el seguimiento y gestión de incidentes, con el objetivo de mejorar las operaciones de seguridad y la gestión del riesgo de la información.

Infraestructura de identidad, acceso y privilegios: Brinda servicios para administrar el aprovisionamiento de usuarios, contraseñas, inicio de sesión único, control de acceso y sincronización de la información del usuario en todos los directorios.

Infraestructura de políticas de seguridad: Proporciona servicios para administrar el desarrollo e implementación de políticas de seguridad de manera consistente y automatizar la implementación de esas políticas en los sistemas de TI.

Infraestructura de criptografía, claves y certificación: Proporciona servicios para realizar operaciones criptográficas de manera eficiente y otorga procesos operativos y capacidades para administrar claves criptográficas.

Infraestructura de administración de servicios: Consiste en servicios de infraestructura para manejar los procesos de administración de servicios, tales como gestión de incidentes, problemas, cambios y configuración

Seguridad de almacenamiento: Brinda capacidades de seguridad centradas en datos para proteger tanto los datos que se encuentran en uso, tránsito y reposo a través de capacidades de aislamiento y cifrado. También proporciona servicios para catalogar y clasificar activos de almacenamiento y asociar políticas de control sobre los mismos.

Seguridad de hosts y endpoints: Proporciona protección para servidores y dispositivos de usuario tales como teléfonos móviles, computadoras de escritorio y portátiles que utilizan tecnologías basadas en host y redes. Esta protección se integra en la infraestructura de virtualización para proporcionar seguridad para entornos virtuales. Incluye una certificación basada en hardware de sistemas operativos host y recursos del sistema para proteger contra ataques maliciosos.

Seguridad de aplicaciones: Brinda la infraestructura para probar, supervisar y auditar las aplicaciones implementadas.

Seguridad de red: Consta de seguridad de red multicapa capaz de proporcionar defensa en profundidad, una inspección profunda y análisis de protocolos, cargas útiles a nivel de aplicación y contenido del usuario, para proteger todos los niveles de la pila de red; se extiende a redes virtuales para seguridad en entornos modernos y altamente virtualizados.

Seguridad física: Es un servicio de infraestructura de TI para crear conciencia sobre la seguridad física y coordinarla con la seguridad de TI. Este servicio puede incluir insignias de empleados, lectores de RFID, sistemas de vigilancia y tecnología o activos asociados. La seguridad física puede incluir automatización relacionada con vigilancia, detección de movimiento, identificación y seguimiento de objetos y personas, control de entrada, supervisión del sistema ambiental, control del perímetro y supervisión del sistema de energía y servicios públicos.

Comparativa de las Metodologías de Redes

Una vez expuestas las características, enfoque y elementos o capas que corresponden a las metodologías Cisco SONA, Check Point SDP e IBM ISF, se puede realizar una comparación entre las mismas.

Cisco SONA es una metodología de diseño de sistemas integrados basados en red, siendo ésta el elemento común, y el que permite ligar la infraestructura de las tecnologías de información y comunicación.

Comprende a su vez una arquitectura basada en tres capas, cada una de las cuales engloba elementos comunes que interactúan entre sí:

1. Capa de Aplicación: Corresponde a las aplicaciones desarrolladas internamente o de terceros, aplicaciones comerciales, CRM, ERP, y de colaboración.
2. Capa de Servicios Interactivos: Corresponde a servicios comunes más que aplicaciones, siendo estos servicios de movilidad, de almacenamiento, de transporte y virtualización, entre otros.
3. Capa de Infraestructura de Red: Corresponde a la infraestructura física, y alberga servidores de almacenamiento, lugares de red (sucursales, redes de campus, borde WAN, centro de datos)

Una red SONA debe ser construida desde cero, implementando redundancia de componentes esenciales, por lo tanto, no es aplicable a situaciones en las que no es requerido un rediseño completo de la red o la construcción de una red nueva.

Respecto al diseño de redes, la metodología más común en PPDIOO, la cual refleja las distintas fases del ciclo de vida de la misma:

1. Preparación: Establece un caso de negocio y la justificación financiera que permitirá crear una estrategia de red, así como la identificación de tecnologías sobre las que se soportará la arquitectura de red.
2. Planeación: Identifica los requerimientos de la red mediante caracterización y evaluación, análisis de deficiencias, así como elaborar un plan de proyecto, mismo que será seguido durante las fases restantes.
3. Diseño: Se desarrolla en base a los requerimientos técnicos y de negocios obtenidos en las fases precedentes, aquí se elaboran diagramas de red y listados de equipos.
4. Implementación: Se instala y configura el equipamiento establecido, incluyendo documentación de instalación, tiempos, referencias adicionales y planes de “roll back”.
5. Operación: Implica la administración y monitoreo de la red día a día, tales como manejo de enrutamiento, administración de actualizaciones, revisión de rendimiento, entre otros.
6. Optimización: Es una fase proactiva que permite identificar y resolver problemas que afecten a la red respecto a la administración, rendimiento y operación. Si existen muchos problemas que resolver, puede desembocar en un rediseño de la red.

PPDIOO permite reducir el costo total de propiedad gracias a la validación de los requerimientos de tecnología y planeamiento previo de cambios en la infraestructura y recursos, aumenta la disponibilidad de la red gracias a la implementación de un diseño de red razonado, y mejora la disponibilidad, fiabilidad, seguridad, escalabilidad y rendimiento de la red a través de la operación y optimización de la misma en el tiempo.

Top-Down permite crear una red con énfasis en las aplicaciones, es decir, se diseña la red empezando por las capas superiores del modelo OSI.
Brinda una visión global del entorno de red desde la vista de los desarrolladores y arquitectos de aplicaciones, pues éstos intervienen junto con el grupo técnico y administrativo en la creación de la red. Si bien es la metodología más fiable, conlleva tiempo y un profundo y razonado análisis de requerimientos, por lo que su uso es recomendable para redes medianas o grandes.

Bottom-Up al contrario, permite crear una red tomando como punto de partida la capa más baja del modelo OSI (Física), considerando primeramente en cuenta medios de transmisión, equipos, protocolos antes que las aplicaciones.
Es el método más empleado por los profesionales de redes, puesto que requiere un análisis menos granular y un tiempo de implementación más corto; pero no es aplicable a redes medianas o grandes, sino para redes LAN pequeñas (por ejemplo, sucursales, agencias), es decir, para sitios en los que el uso de aplicaciones no sea intensivo, y que no se encuentren albergadas dentro de la misma red local.

Cisco SAFE brinda principalmente información sobre las mejores prácticas para el diseño e implementación de redes seguras, sirviendo se guía a los diseñadores de red que están planteándose los requisitos de seguridad de su red; adoptando un enfoque de defensa en profundidad para el diseño de la seguridad de las redes.

Sus módulos son:

1. Campus Empresarial
2. Perímetro Empresarial
3. Proveedor de Servicios

Pese a que en las redes existentes en la mayoría de las instituciones no es posible separar con facilidad dichos módulos, esta visión brinda una guía para la implementación de distintas funciones de seguridad en la red.

Check Point SDP brinda una metodología modular centrada en la seguridad, adaptable y probada, desarrollada en base a la experiencia de la marca respecto a la implementación de sistemas de seguridad y maneja la infraestructura de seguridad mediante tres capas interconectadas:

1. Capa de Aplicación: Basa su funcionamiento en el despliegue de puntos de aplicación de seguridad, tanto físicos como virtuales, lo cual se logra mediante lo que se conoce como “segmentación”, primera línea de defensa contra infecciones de red.
2. Capa de Control: Se encarga de analizar amenazas descritas y caracterizadas desde distintas fuentes de información, generando protecciones que serán ejecutadas desde la capa de Aplicación, mediante control de acceso, prevención de amenazas y protección de datos, así como mapeo de controles.
3. Capa de Administración: Es la encargada de gestionar la arquitectura gracias a la modularidad y visibilidad.

La interconexión de estas capas permite tener conciencia de la seguridad de la red, así como la capacidad de prevenir proactivamente las amenazas dentro de un horizonte de amenazas variable.

IBM ISF ofrece un modelo que integra a los ejes del negocio con los de seguridad en base a un modelo de Gobierno de seguridad, gestión de riesgos y cumplimiento, compuesto por los siguientes dominios de seguridad, que permiten una vez definidos, describir el horizonte empresarial:

1. Análisis e inteligencia de seguridad
2. Personas
3. Datos
4. Aplicaciones
5. Infraestructura
6. Seguridad avanzada e investigación de amenazas

El siguiente paso lo compone IBM Security Blueprint, mismo que brinda capacidades básicas de seguridad y una separación de dominios con más detalle, capaz de ofrecer una sólida visión de las capacidades de seguridad de una arquitectura o solución en particular, y lo más importante, en término de productos y proveedores neutrales, en base a un conjunto de principios arquitectónicos aplicables al modelo de servicio y desarrollo de soluciones, que garantizan la aplicabilidad y usabilidad del modelo para todos quienes lo conforman y están involucrados (desde usuarios finales, pasando por desarrolladores y administradores de bienes)

Una vez expuestas las metodologías de diseño de redes, es posible hacer una comparación entre las mismas:

	Metodología		
	Cisco SONA	**Check Point SDP**	**IBM ISF**
Probada en el tiempo	Sí	Sí	Sí
Énfasis en…	Diseño de redes, seguridad de redes	Seguridad perimetral	Integración, seguridad de infraestructura, seguridad de aplicaciones, seguridad de redes, seguridad perimetral
Estructura en capas	Sí	Sí	Sí
Metodologías relacionadas	Sí	No	Sí
(¿Cuáles?)	PPDIOO, Top-Down, Bottom-Up, Cisco SAFE	No aplica	IBM ISB
Neutral	No	No	Sí
Nivel de complejidad	Alto	Medio	Alto

Tabla 2.13 - Comparativa entre las metodologías expuestas

Fuente: El autor

La metodología de seguridad que será empleada para la realización de la propuesta de mejoramiento del sistema de seguridad perimetral, debido a la naturaleza de los servicios y aplicaciones disponibles, estructura de la red desplegada, crecimiento esperado y necesidades de protección es Check Point Software-Defined Protection, puesto que la misma se encuentra centrada en la seguridad perimetral, es la que mejor se ajusta a las necesidades de la institución, siendo una solución probada en el tiempo, eficiente y de fácil administración.

CAPÍTULO III - INFORMACIÓN DE LA INSTITUCIÓN

LA INSTITUCIÓN

El Instituto Ecuatoriano de Seguridad Social (IESS) es una entidad, cuya organización y funcionamiento se fundamenta en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia. Se encarga de aplicar el Sistema del Seguro General Obligatorio que forma parte del sistema nacional de Seguridad Social.

HISTORIA

Como parte del proceso de reforma del Estado, impulsado por el llamado régimen juliano y como consecuencia de las grandes luchas sociales y políticas de los años veinte y treinta, el Seguro Social Ecuatoriano surge en marzo de 1928, en el gobierno del doctor Isidro Ayora. Con el Decreto Ejecutivo Nº 18, publicado en el Registro Oficial Nº 590 del 13 de marzo de 1928, se crea la "Caja de Jubilaciones, Montepío Civil, Retiro y Montepío Militar, Ahorro y Cooperativa", que se denominó "Caja de Pensiones", la cual protegía a funcionarios del magisterio público, empleados públicos, bancarios y a militares.

La seguridad social en el Ecuador ha tenido una compleja evolución institucional, con una variedad de denominaciones que adoptaron a lo largo del tiempo, las entidades encargadas de su ejecución: Caja de Pensiones, Caja del Seguro, Caja Nacional del Seguro Social, Instituto Nacional de Previsión e Instituto Ecuatoriano de Seguridad Social. El 2 de octubre de 1935, mediante Decreto Supremo Nº 12 se dicta la Ley de Seguro Social Obligatorio, estableciendo su aplicación en los trabajadores del sector público y privado y la contribución de aportes bipartita: patronal y personal para la cobertura de los riesgos con beneficios de jubilación, montepío y mortuoria.
La Caja de Pensiones se mantiene como institución ejecutora y bajo la dependencia jurídica del creado Instituto Nacional de Previsión.

En el año 1937, con la Ley del Seguro Social Obligatorio se crea la "Caja del Seguro de Empleados Privados y Obreros y el Departamento Médico" ligado a ella.

El 14 de julio de 1942, se expide la nueva Ley de Seguro Social Obligatorio, en la que se establecen nuevas condiciones de aseguramiento, el financiamiento de todas las

pensiones delante seguro general, con la contribución del Estado del 40%; y se incorpora el seguro de enfermedad y maternidad entre algunos beneficios para los afiliados.

El 19 de septiembre de 1963, mediante el Decreto Supremo Nº 517, se fusionan la Caja de Pensiones y la Caja del Seguro para crear la "Caja Nacional del Seguro y del Departamento Médico".
Mediante Decreto Supremo Nº 40, del 25 de julio de 1970, publicado en el Registro Oficial Nº 15 del 10 de julio de 1970 la Caja Nacional del Seguro Social se transforma en el "Instituto Ecuatoriano de Seguridad Social" (IESS)

En 1988, la Asamblea Nacional reforma la Constitución Política de la República y establece la permanencia del IESS como única Institución autónoma, responsable de la aplicación del Seguro General Obligatorio.
El 30 de noviembre de 2001, en el Registro Oficial Nº 465 se publica la "Ley de Seguridad Social".

El IESS, según lo determina la Constitución de la República del Ecuador aprobada en referendo el 28 de septiembre de 2008, se mantiene como entidad autónoma, con personería jurídica, recursos propios distintos a los del Fisco; y con una estructura orgánica que ha ido modificándose en el transcurso de los años. Asimismo, se establecen modificaciones para separar el financiamiento y administración de las contingencias cubiertas por el seguro general obligatorio que administra el IESS.

En el transcurso de su existencia, el IESS como la institución social más grande del país que brinda seguridad social, ha ido transformándose en el ámbito legal, social y de prestaciones. Tuvo varias etapas de evolución, hasta convertirse en una entidad, cuya organización y trabajo se fundamenta en los principios de: solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia.
Los ingresos al IESS por aportes personales y patronales, fondos de reserva, descuentos, multas, intereses, utilidades de inversiones, contribución financiera obligatoria del Estado y los demás señalados en esta Ley, no pueden destinarse a otros fines que a los de su creación y funciones.

Las prestaciones de la seguridad social se financian con el aporte de las personas aseguradas en relación de dependencia y de sus empleadores; con los aportes de las personas independientes aseguradas; con los aportes voluntarios de las ecuatorianas y los ecuatorianos domiciliados en el exterior; y con los aportes y contribuciones del Estado.

DESCRIPCIÓN DE LA ARQUITECTURA ACTUAL

La infraestructura principal se encuentra distribuida en dos Centros de Datos (Data Centers), uno primario ubicado tanto en el subsuelo como en el segundo piso del edificio "Riesgos del Trabajo del IESS", en la ciudad de Quito, y un sitio de respaldo, ubicado en el edificio de la Dirección Provincial del IESS en la ciudad de Guayaquil.

Todas las operaciones de Producción se realizan en el Centro de Datos Principal, mientras que el Centro de Datos de Respaldo está planeado para emplearse en caso de recuperación de desastres, y en un futuro mediato, para brindar servicios con redundancia geográfica.

Toda la información relacionada con clientes (asegurados, pensionistas, entidades externas públicas y privadas) se encuentra almacenada en bases de datos separadas, mismas que se encuentran agrupadas y administradas para cumplir con parámetros de alta disponibilidad.

La mayoría de las aplicaciones web críticas se encuentran desplegadas en una configuración de alta disponibilidad.

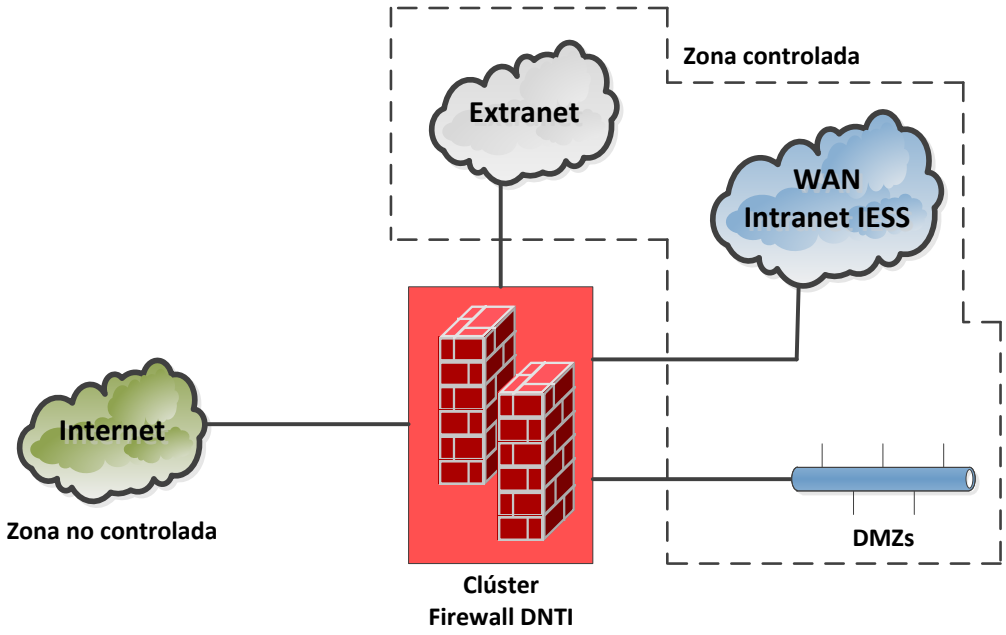


FIGURA 3.1 – PRINCIPALES ZONAS CONECTADAS AL CLÚSTER DE FIREWALL DE LA DNTI

Fuente: El autor

Los principales componentes de la infraestructura de comunicaciones (tales como firewalls, switches y routers) están implementados en una configuración de alta disponibilidad.

Los servidores de aplicaciones y de bases de datos y web, así como otros elementos sensibles se encuentran separados aislados entre sí mediante el clúster de firewalls de la institución.

Los estándares de TI de la institución requieren que todos los servidores usen un sistema operativo basado en tecnología UNIX (en el caso de ciertos servidores del entorno de bases de datos) o Linux (servidores de red)

Las zonas desmilitarizadas tienen un identificador numérico (por ejemplo, DMZ 90), puesto que éste indica el nivel de seguridad (confianza) definido y heredado de cuando aún estaba implementado un firewall Cisco PIX, posteriormente reemplazado por la actual solución.

Zona	Nombre	Agrupa a…
DMZ 90	Producción	Equipos del área de Producción (área de Redes, Bases de Datos, Servidores, Plataforma, Operaciones, Mesa de Servicios…)
DMZ 80	Servidores Web	Servidores web y aplicaciones
DMZ 50	Preproducción	Servidores de aplicaciones y desarrollos propios en período de prueba, entorno de capacitación
DMZ 25	Riesgos del Trabajo	Red de los equipos y servidores del edificio "IESS Riesgos del Trabajo" (Quito)
DMZ 20	Desarrollo	Red de desarrollo de aplicaciones y control de calidad
DMZ 15	Intranet	Red general del IESS
Externa	Extranet	Conexiones desde entidades externas
Externa	Internet	Conexión desde y hacia Internet

Tabla 3.1 – Zonas en el entorno de TI

Fuente: El autor

Se tienen las siguientes zonas:

Producción: Se encuentra conformada por el área de Redes, Plataforma y Servidores, Bases de Datos, Operaciones y Mesa de Servicios, desde los cuales se efectúa el control de la infraestructura tecnológica de la institución, se ejecutan tareas de soporte de primer y segundo nivel.

En esta zona desmilitarizada se encuentran también los equipos de administración de seguridad, como por ejemplo el servidor de administración del clúster de firewalls, del IPS, balanceador de carga y aplicaciones, gestión de servidores físicos y virtuales, equipos de control de las bases de datos, servidores de registros y reportes.

Servidores Web: Formada por servidores web que permiten atender peticiones de servicio sin comprometer la seguridad de otras áreas, y sirven tanto a usuarios internos como externos que acceden a aplicaciones web. Se encuentran algunos servidores de seguridad web que realizan autenticación y autorización centralizada antes de permitir el acceso a las aplicaciones. El contenido web público se encuentra aislado en servidores web protegidos con SSL.

Preproducción: Gestionada principalmente por el grupo de planificadores y desarrolladores de aplicaciones, aquí se encuentra un entorno de servidores, sobre los que se despliegan aplicaciones que deben pasar varios conjuntos de pruebas de funcionamiento y controles de calidad. Se hallan también repositorios propios del área, necesarios para las labores de desarrollo de aplicaciones, investigación, capacitación, y tutoriales.

Riesgos del Trabajo: Comprende los equipos y servidores de la dependencia de Riesgos del Trabajo, exceptuando los de la DNTI, que se encuentran en el mismo edificio, conformando entonces zonas separadas. Se hallan aquí los equipos de cómputo, redes y servidores de Riesgos del Trabajo, Seguro de Pensiones, entre otros.

Desarrollo: Está conformada por el grupo de desarrollo de la institución, encargado de la ejecución de tareas de planificación, creación, despliegue y mantenimiento de aplicaciones propias de la institución. El personal técnico realiza también pruebas de control de calidad del software desarrollado. Trabaja estrechamente con el área de Producción (Servidores y Plataforma, Operaciones)

Intranet: Está conformada por los equipos desplegados en las distintas dependencias de la institución a nivel nacional, desde pequeños dispensarios y centros de atención ambulatoria hasta los hospitales de tercer nivel, incluyendo dependencias administrativas tales como el edificio Matriz IESS, Parque de Mayo, Seguro de Salud Individual y Familiar, las direcciones provinciales, entre otras.
Es la zona más extensa de la institución, y en ella se encuentra un número reducido de aplicaciones legadas basadas en desarrollos anteriores, pero aún en servicio.

Extranet: Comprende los objetos que interactúan con las entidades externas con las que la institución, tales como bancos (BIESS, Banco de Guayaquil, Banco Internacional, otros), dependencias del Estado (ministerios, agencias), y dependencias privadas (recaudadoras…) con las que la institución tiene convenios de prestación de servicio.

Internet: Es una zona no controlada y la menos confiable con la que interactúan las otras definidas dentro de la institución. Se emplea para brindar navegación, publicación de servicios, y brindar presencia web, lográndose esto a través de dos proveedores distintos.

Zona	Interactúa con…
Producción	Servidores Web
	Preproducción
	Riesgos del Trabajo
	Desarrollo
	Intranet
	Extranet
	Internet
Servidores Web	Riesgos del Trabajo
	Intranet
	Extranet
	Internet
Preproducción	Desarrollo
	Intranet
	Extranet
Riesgos del Trabajo	Intranet
Desarrollo	Preproducción
	Extranet
Intranet	Riesgos del Trabajo
Extranet	Producción
	Servidores Web
	Preproducción
	Desarrollo
Internet	Producción
	Servidores Web

Tabla 3.2 – Principales interacciones entre zonas

Fuente: El autor

SITUACIÓN ACTUAL

Hardware del Centro de Datos Principal (Quito)

En el Centro de Datos Principal, ubicado en Quito y administrado por la Dirección Nacional de Tecnologías de la Información, se encuentra una solución de firewalls en modo de alta disponibilidad, instalada y en explotación desde 2010, brindando protección tanto a la red interna como al equipamiento del núcleo (core) informático del IESS, el cual permite el acceso vía VPN a los prestadores externos, así como el acceso encriptado a las instituciones públicas o privadas que mediante convenios, mantienen comunicación y pueden acceder a ciertos recursos e información por medio de canales seguros para la transmisión de la información, misma que debe ser protegida.

La solución firewall se encuentra desplegada en el siguiente hardware:

Hardware	Cantidad	Elemento en la solución
HP Proliant DL360 G7	1	Manager (Administrador)
HP Proliant DL360 G7	1	FireMon (Auditoría)
HP Proliant DL380 G7	1	Firewall Internet Principal
HP Proliant DL380 G7	1	Firewall Internet Failover
HP Proliant DL380 G7	1	Firewall Intranet Principal
HP Proliant DL380 G7	1	Firewall Intranet Failover

Tabla 3.3 – Hardware sobre el cual está instalada la solución firewall en el Centro de Datos Principal

Fuente: El autor

En su sitio web (h17007.www1.hpe.com/us/en/enterprise/servers/retired/index.aspx), el fabricante ha anunciado la salida del mercado del servidor Proliant DL380 G7, y adicionalmente informó el fin de vida de servicio para el servidor Proliant DL360 G6, equipos que estarán en vigencia hasta el día 30 de abril de 2018, como se muestra a continuación:

FIGURA 3.2 – RETIRO DEL MERCADO DE SERVIDORES PROLIANT DL380 G7 Y DL360 G7

Fuente: h17007.www1.hpe.com/us/en/enterprise/servers/retired/index.aspx

FIGURA 3.3 – FIN DE VIDA DE SERVICIO PARA SERVIDORES PROLIANT DL380 G7

Fuente: https://www.parkplacetechnologies.con/end-of-service-life/hp/hp-proliant-dl380-g7/

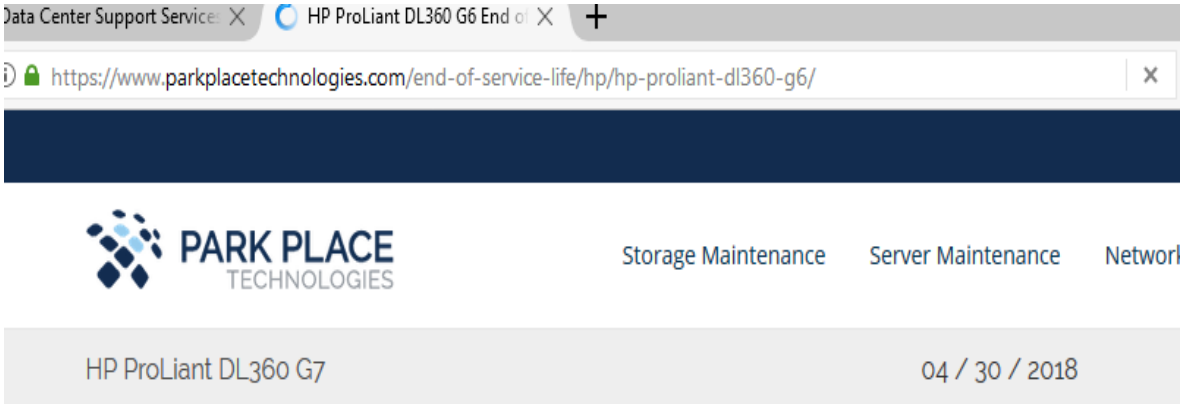


FIGURA 3.4 – FIN DE VIDA DE SERVICIO PARA SERVIDORES PROLIANT DL360 G7

Fuente: https://www.parkplacetechnologies.con/end-of-service-life/hp/hp-proliant-dl360-g6/

Arquitectura de la solución instalada en la actualidad

Cuenta con gestión centralizada para la administración de la plataforma de firewalls desplegada en el Centro de Datos Principal (Quito), la que está formada por un componente de Administración (Management), componente de Eventos (Event) y un componente de Auditoría (desarrollado por FireMon y compatible con Check Point, pero no desarrollado por esta última). Se encuentran instalados dos clústeres de firewalls; uno se emplea para proteger el acceso a los servicios que se prestan a los usuarios externos mientras que el otro protege el acceso a los servicios que se brindan a los usuarios internos.

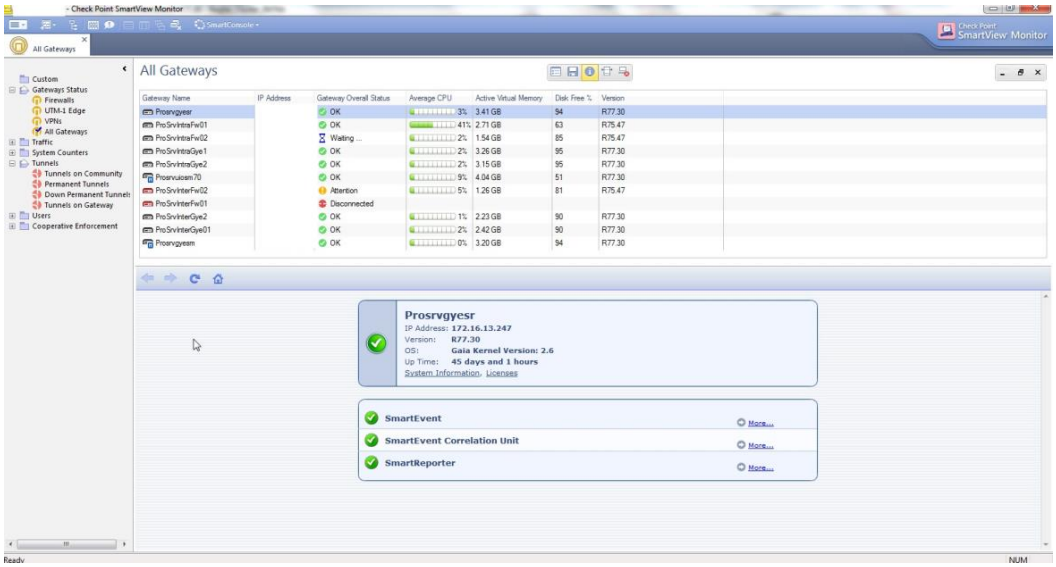


FIGURA 3.5 – CAPTURA DE PANTALLA DE LA HERRAMIENTA SMARTVIEW MONITOR

Fuente: El autor

El estado de los componentes antes mencionados se enuncia a continuación:

Firewall Internet Quito

El clúster está implementado sobre servidores HP Proliant DL 380 G7, con capacidad de 1 TB de almacenamiento en disco, 8 núcleos y 18 GB en RAM. El sistema operativo instalado es Check Point versión R75.47, que cuenta con licenciamiento instalado tanto en hardware como en software, pero que carece de soporte del fabricante.

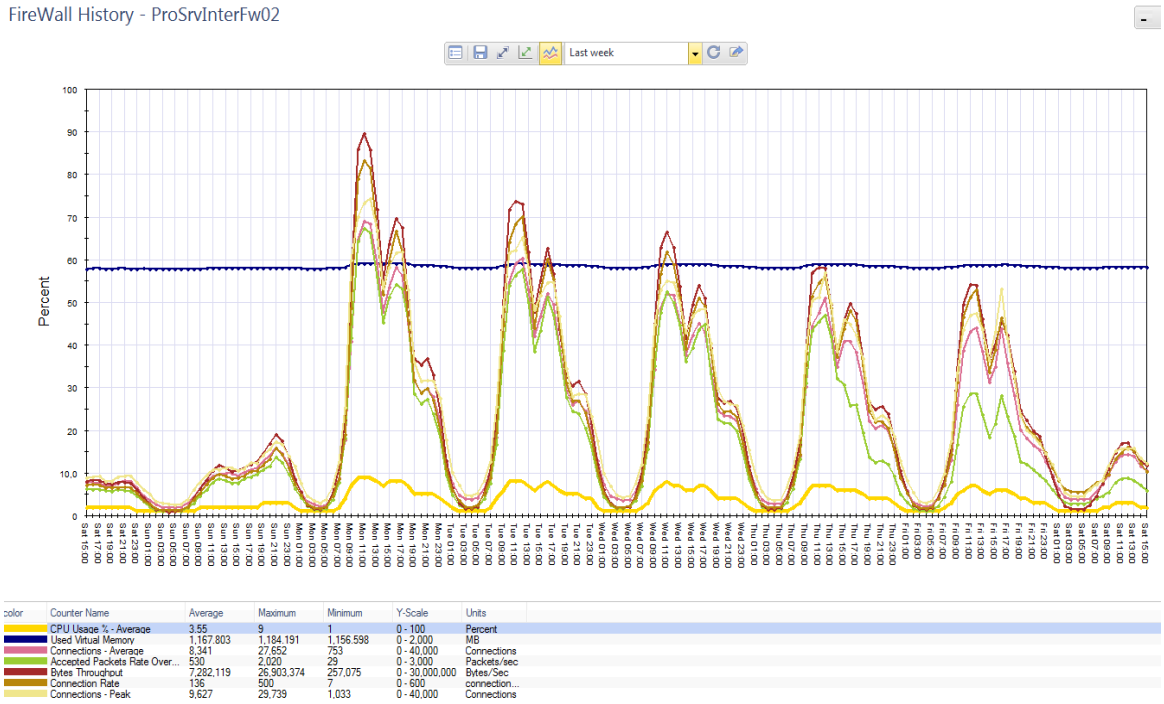


FIGURA 3.6 – CAPTURA DE PANTALLA DEL CONSUMO DE RECURSOS EN EL FIREWALL DE INTERNET QUITO

Fuente: El autor

El consumo de recursos en el firewall activo, correspondiente al de Internet, se puede evidenciar en las siguientes capturas de pantalla, ya que la información presentada en la figura anterior muestra valores promedio.

```
Connections:
        793433340 total, 748249193 TCP, 44774823 UDP, 359508 ICMP,
        49816 other, 314 anticipated, 100439 recovered, 18735 concurrent,
        32193 peak concurrent
```

FIGURA 3.7 – NÚMERO DE CONEXIONES EN FIREWALL DE INTERNET QUITO

Fuente: El autor

```
top - 09:07:45 up 89 days, 13 min,  1 user,  load average: 1.49, 1.21, 0.94
Tasks: 159 total,   2 running, 157 sleeping,   0 stopped,   0 zombie
Cpu(s):  3.7%us,  1.5%sy,  0.0%ni, 88.1%id,  0.4%wa,  2.0%hi,  4.4%si,  0.0%st
Mem:   6221172k total,  3168972k used,  3052200k free,   396192k buffers
Swap: 13631272k total,        0k used, 13631272k free,  1554076k cached
```

FIGURA 3.8 – RECURSOS EN FIREWALL DE INTERNET QUITO

Fuente: El autor

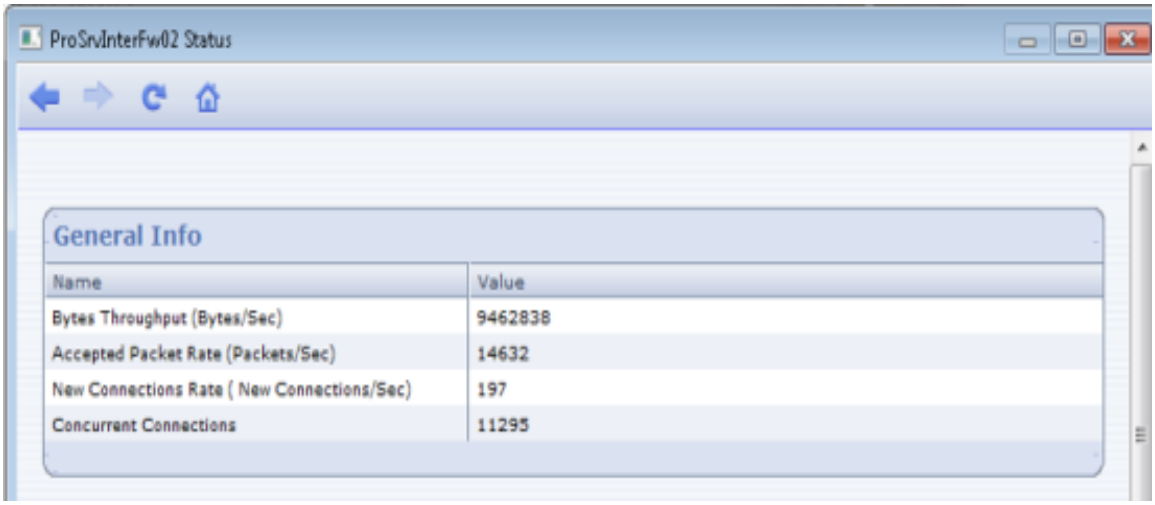


FIGURA 3.9 – THROUGHPUT DE FIREWALL DE INTERNET QUITO

Fuente: El autor

Componentes	Consumo
Memoria RAM	4 GB
Procesador	70%
Throughput	216 Mbps
Tasa de sesiones	500 sesiones/s
Sesiones concurrentes	30K

Tabla 3.4 – Capacidad de clúster de Internet Quito

Fuente: El autor

Firewall Intranet Quito

Implementado sobre servidores HP Proliant DL380 G7 con 1 TB almacenamiento en disco, 8 núcleos y 18 GB en RAM. El sistema operativo instalado es Check Point versión R75.47, que cuenta con licenciamiento instalado tanto en hardware como en software, pero que carece de soporte del fabricante.

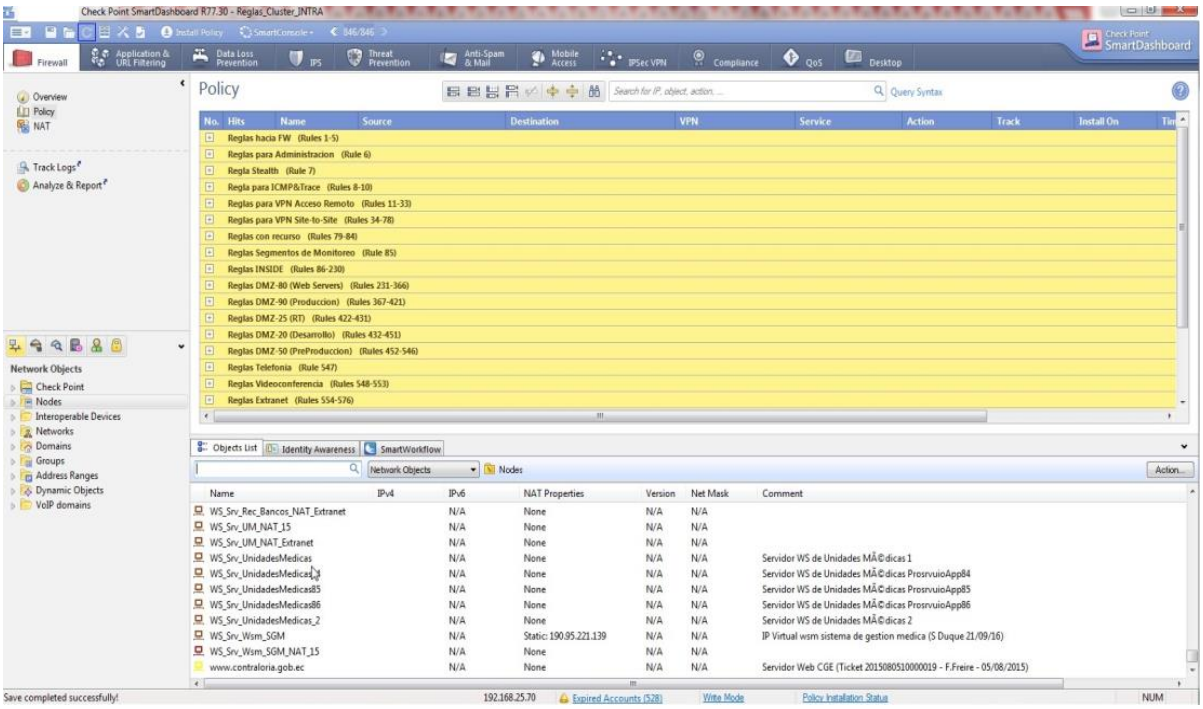


FIGURA 3.10 – CAPTURA DE PANTALLA DE SMARDASHBOARD PARA EL CLÚSTER DE INTRANET QUITO

Fuente: El autor

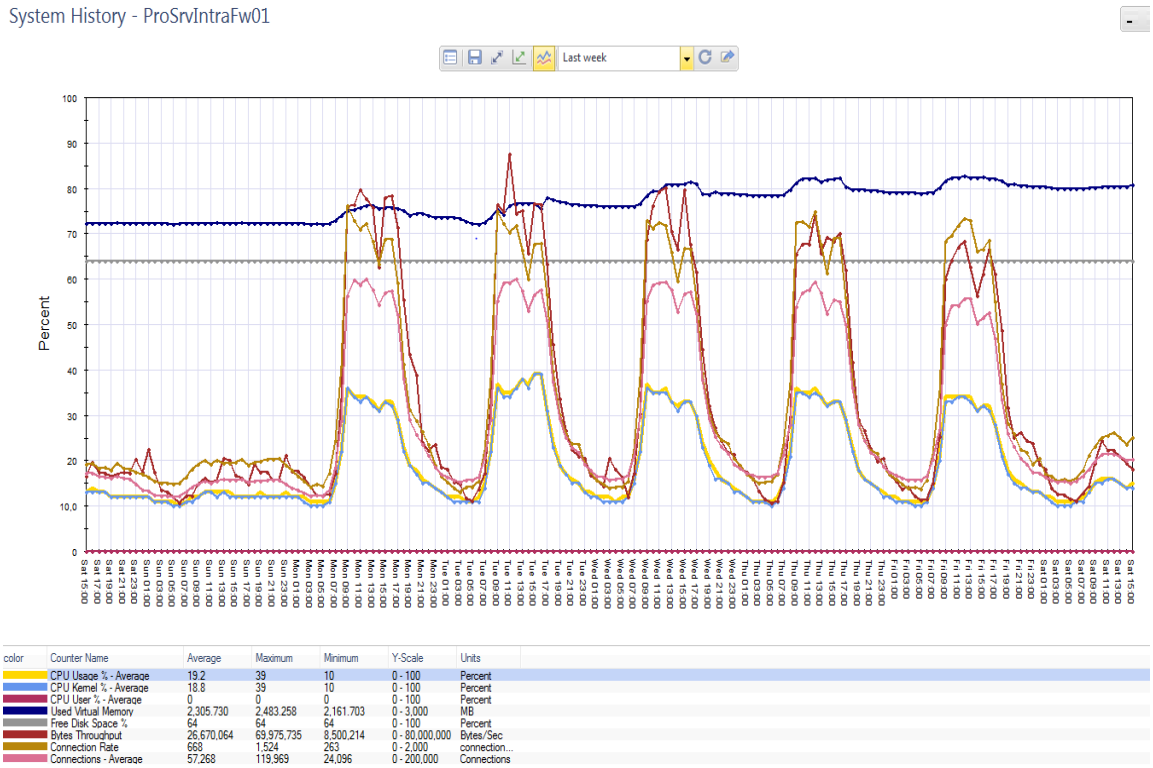


FIGURA 3.11 – HISTÓRICO DE CONSUMO DE RECURSOS EN EL FIREWALL DE INTRANET QUITO

Fuente: El autor

El consumo de recursos en el firewall activo correspondiente al de Intranet , y se puede observar en las siguientes capturas de pantalla, ya que la información presentada en la figura anterior muestra valores promedio.

```
Connections:
        375674417 total, 188572020 TCP, 158686886 UDP, 28415323 ICMP,
        188 other, 95678 anticipated, 0 recovered, 133945 concurrent,
        139364 peak concurrent
```

FIGURA 3.12 – NÚMERO DE CONEXIONES EN FIREWALL DE INTRANET QUITO

Fuente: El autor

```
top - 10:29:34 up 6 days, 17:13,  1 user,  load average: 3.25, 3.08, 3.00
Tasks: 147 total,   3 running, 144 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.4%us,  1.7%sy,  0.0%ni, 63.6%id,  0.9%wa,  2.0%hi, 31.3%si,  0.0%st
Mem:   6221172k total,  2838452k used,  3382720k free,   280404k buffers
Swap: 13631272k total,        0k used, 13631272k free,   568748k cached
```

FIGURA 3.13 – RECURSOS EN FIREWALL DE INTRANET QUITO

Fuente: El autor

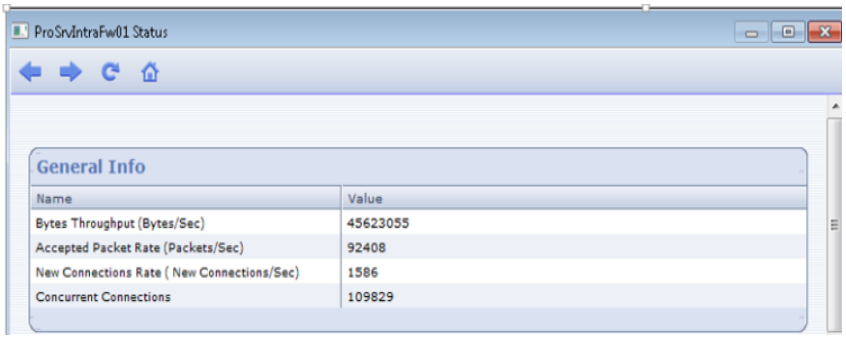


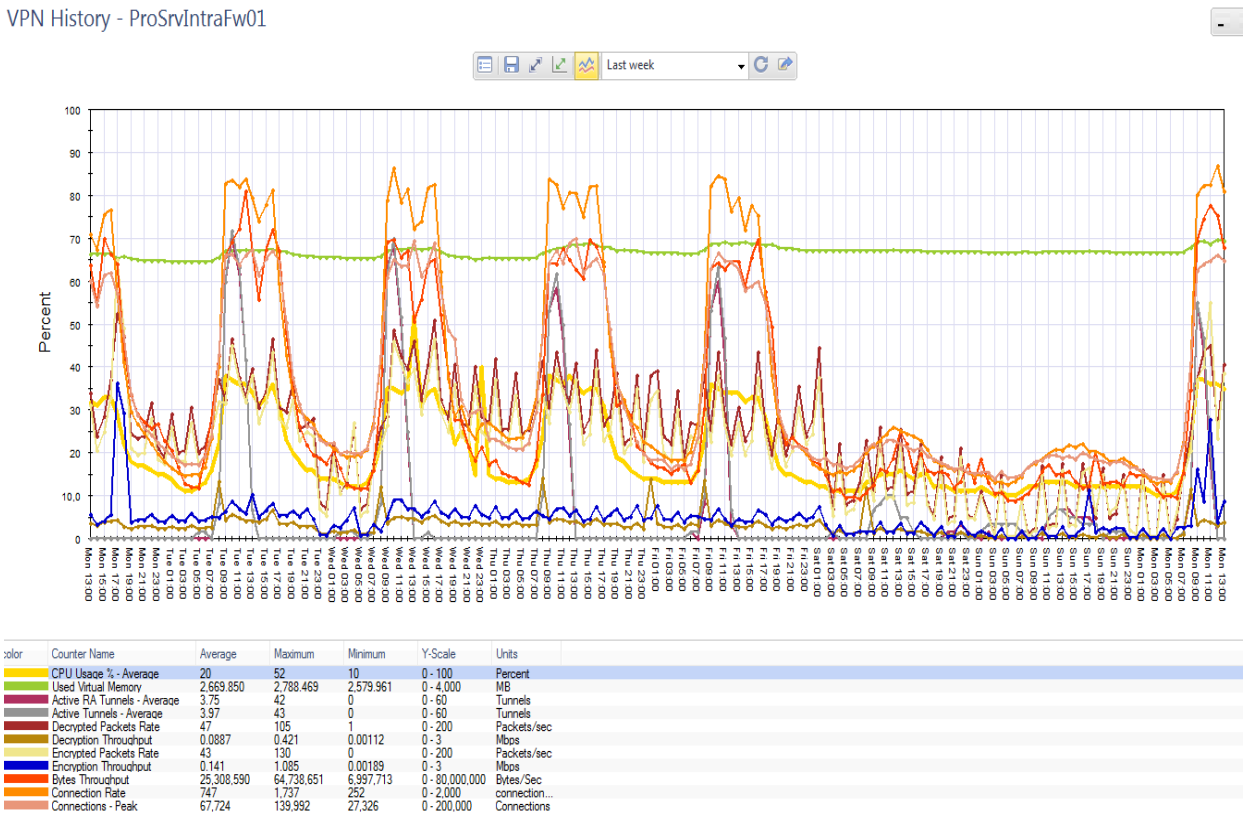
FIGURA 3.14 – THROUGHPUT DE FIREWALL DE INTRANET QUITO

Fuente: El autor

Componentes	Consumo
Memoria	4 GB
Procesador	40%
Throughput	540.24 Mbps
Throughput VPN	648 Mbps
Tasa de sesiones	1703 sesiones/s
Sesiones concurrentes	140 K

Tabla 3.5 – Capacidad de clúster de Intranet Quito

Fuente: El autor



olor	Counter Name	Average	Maximum	Minimum	Y-Scale	Units
	CPU Usage % - Average	20	52	10	0 - 100	Percent
	Used Virtual Memory	2,669.850	2,788.469	2,579.961	0 - 4,000	MB
	Active RA Tunnels - Average	3.75	42	0	0 - 60	Tunnels
	Active Tunnels - Average	3.97	43	0	0 - 60	Tunnels
	Decrypted Packets Rate	47	105	1	0 - 200	Packets/sec
	Decryption Throughput	0.0887	0.421	0.00112	0 - 3	Mbps
	Encrypted Packets Rate	43	130	0	0 - 200	Packets/sec
	Encryption Throughput	0.141	1.085	0.00189	0 - 3	Mbps
	Bytes Throughput	25,308,590	64,738,651	6,997,713	0 - 80,000,000	Bytes/Sec
	Connection Rate	747	1,737	252	0 - 2,000	connection...
	Connections - Peak	67,724	139,992	27,326	0 - 200,000	Connections

FIGURA 3.15 – HISTÓRICO DE RECURSOS VPN EN FIREWALL DE INTRANET QUITO

Fuente: El autor

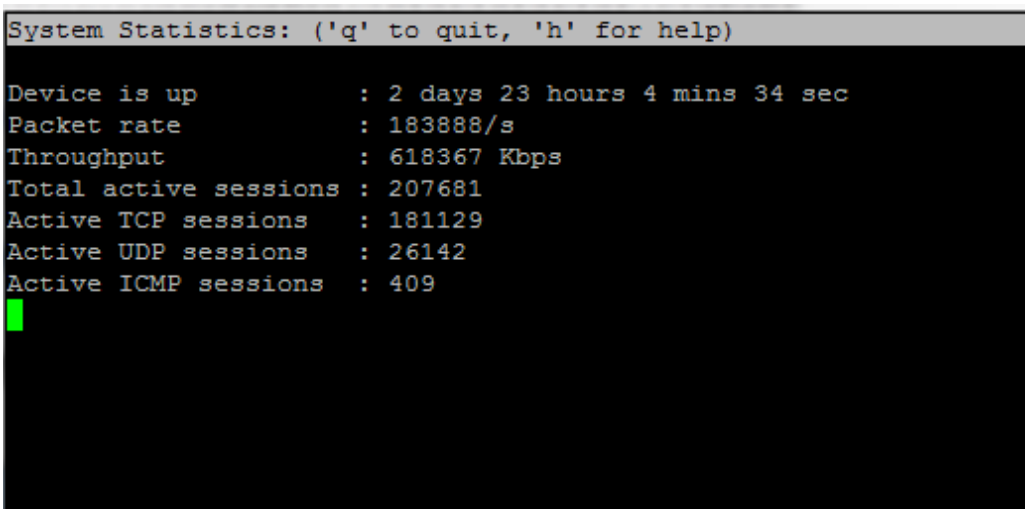


FIGURA 3.16 – ESTADÍSTICAS VARIAS DE FIREWALL DE INTRANET QUITO

Fuente: El autor

FireMon

Es un componente de auditoría implementado en un servidor Proliant DL360 G7, con un sistema operativo propietario FM versión 5.1.5.57. La herramienta presenta un daño desde el mes de marzo de 2016, motivo por el cual no es posible obtener métricas o estadísticas de la misma. El licenciamiento instalado soporta hasta 6 gateways. No dispone de soporte del fabricante.

Componente	Características	Observaciones
FireMon	Sistema operativo FM versión 5.1.5.57, 1 consola de Administración (ASM), 1 licencia (SMM) para consola de gestión de Check Point, 6 licencias SMLO para supervisión de gateways	Licenciamiento perpetuo

Tabla 3.6 – Características principales del componente FireMon

Fuente: El autor

Dependencias que cuentan con conexión directa hacia Internet

Las siguientes dependencias cuentan con conexión directa hacia Internet y no se encuentran protegidas adecuadamente: hospitales “Carlos Andrade Marín” (Quito), “Teodoro Maldonado Carbo” (Guayaquil) y “José Carrasco Arteaga” (Cuenca). Respecto a éstos, sus firewalls pertenecen a distintas marcas y su administración en puramente local. Adicionalmente, tanto en el Centro Médico “La Mariscal” como en el edificio de Procesos Gobernantes (conocido como edificio “Zarzuela”), ambos ubicados en la ciudad de Quito, no disponen de una solución de firewall instalada.

A continuación se detalla la situación actual de los diferentes firewalls en cada una de las unidades médicas mencionadas anteriormente.

Hospital “Carlos Andrade Marín”

Como establecimiento médico de tercer nivel, requiere el uso de Internet ya que este servicio ha permitido mantener funcionales y en operación los sistemas consumidos, tales como el Sistema Quirúrgico Da Vinci (cirugía robótica), “gamma knife”, radioterapia, capacitación en línea, bibliotecas médicas, videoconferencias, así como el acceso a

sitios web y portales gubernamentales tales como SRI, SERCOP, Gestión Documental, Socio Empleo y accesos especiales a redes sociales para las área de Comunicación Social (YouTube, Facebook, WhatsApp, Dropbox…)

En base al número actual de usuarios de la red del HCAM (tanto cableada como inalámbrica) y luego de haberse realizado un estudio interno sobre el posible incremento de la red, se estima que en dos años, la cantidad de usuarios aumente al menos en un 25%, con el consiguiente aumento del consumo de recursos de red y servicios.

Sitio	Firewall instalado	Detalles
HCAM	Untangle	Versión licenciada instalada en un servidor blade, con 24 GB en RAM y procesador de 12 núcleos

Tabla 3.7 – Datos técnicos básicos de firewall instalado en el HCAM

Fuente: El autor

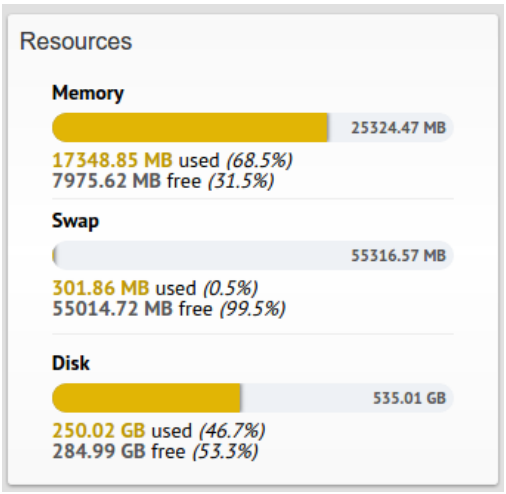


FIGURA 3.17 – USO DE RECURSOS DE FIREWALL UNTANGLE

Fuente: El autor

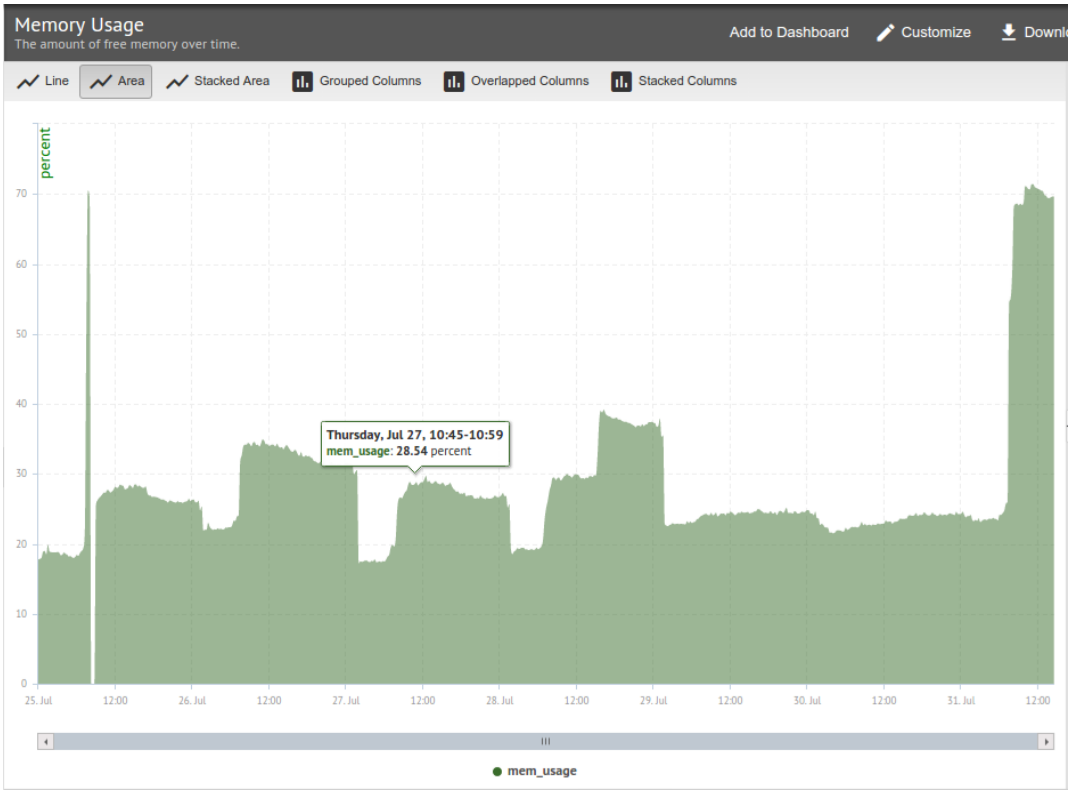


FIGURA 3.18 – CAPTURA DE USO DE MEMORIA DE FIREWALL UNTANGLE

Fuente: El autor

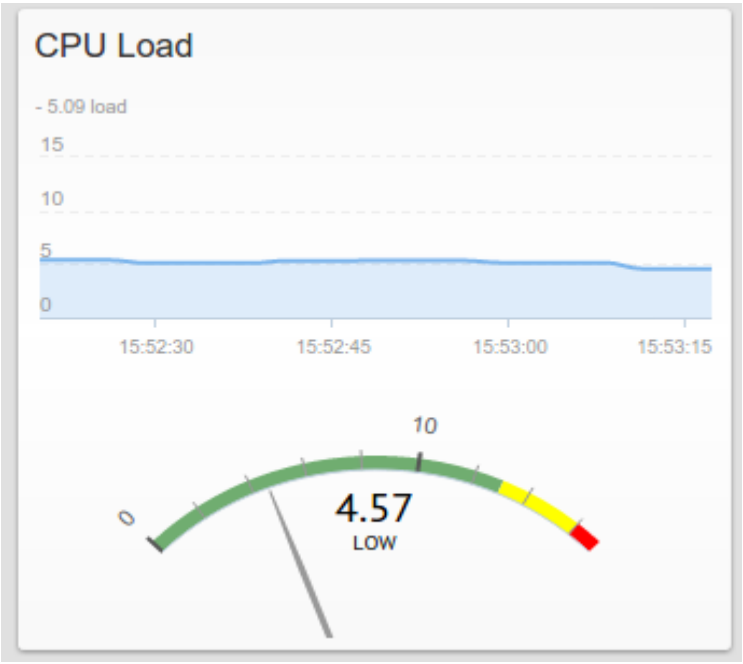


FIGURA 3.19 – MEDIDOR DE CARGA DE CPU DE UNTANGLE

Fuente: El autor

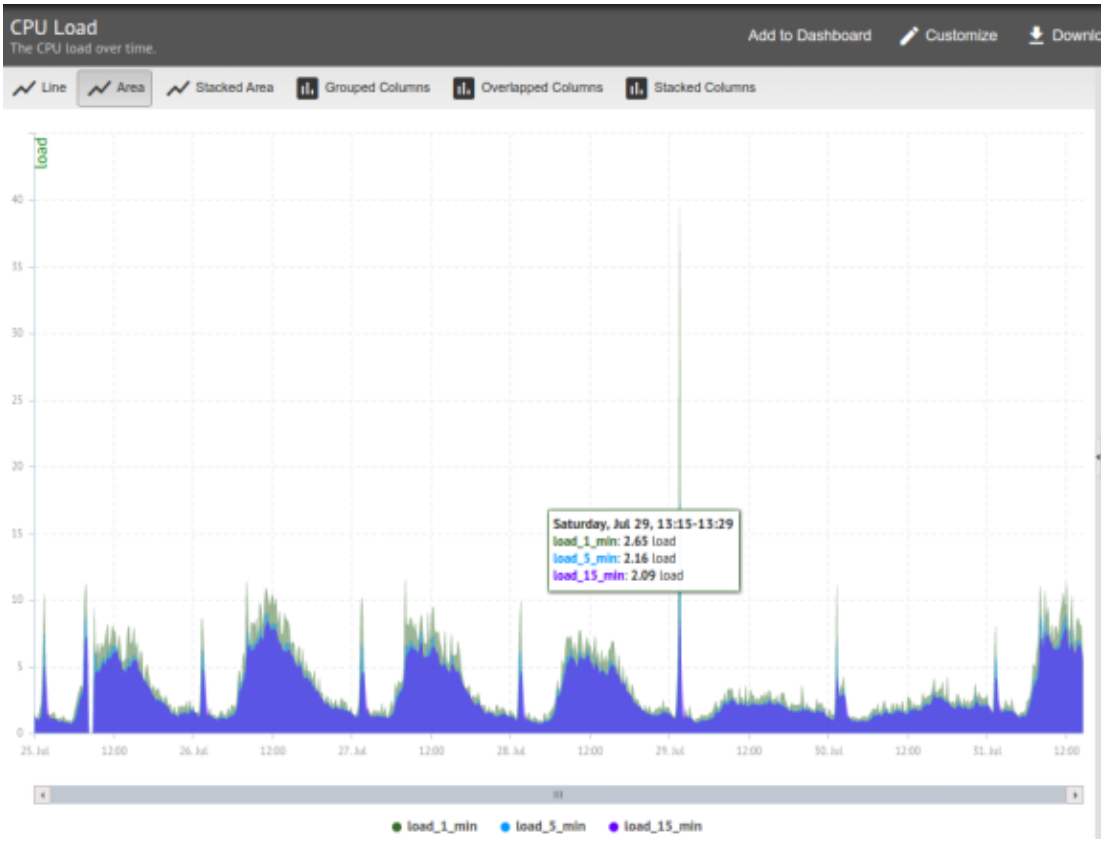


FIGURA 3.20 – GRÁFICO HISTÓRICO DE NIVEL DE CARGA DE CPU DE FIREWALL UNTANGLE

Fuente: El autor

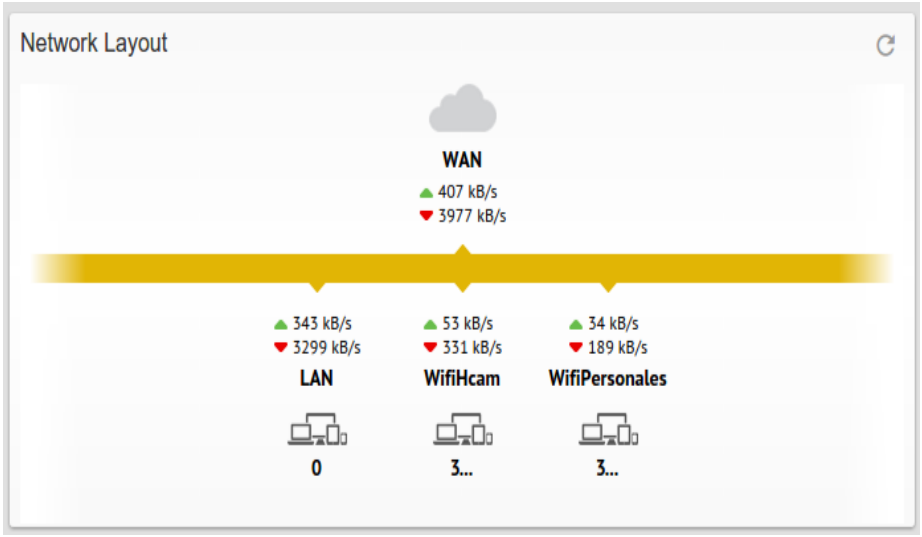


FIGURA 3.21 - DISTRIBUCIÓN DE LOS SEGMENTOS DE RED DEFINIDOS EN FIREWALL UNTANGLE

Fuente: El autor

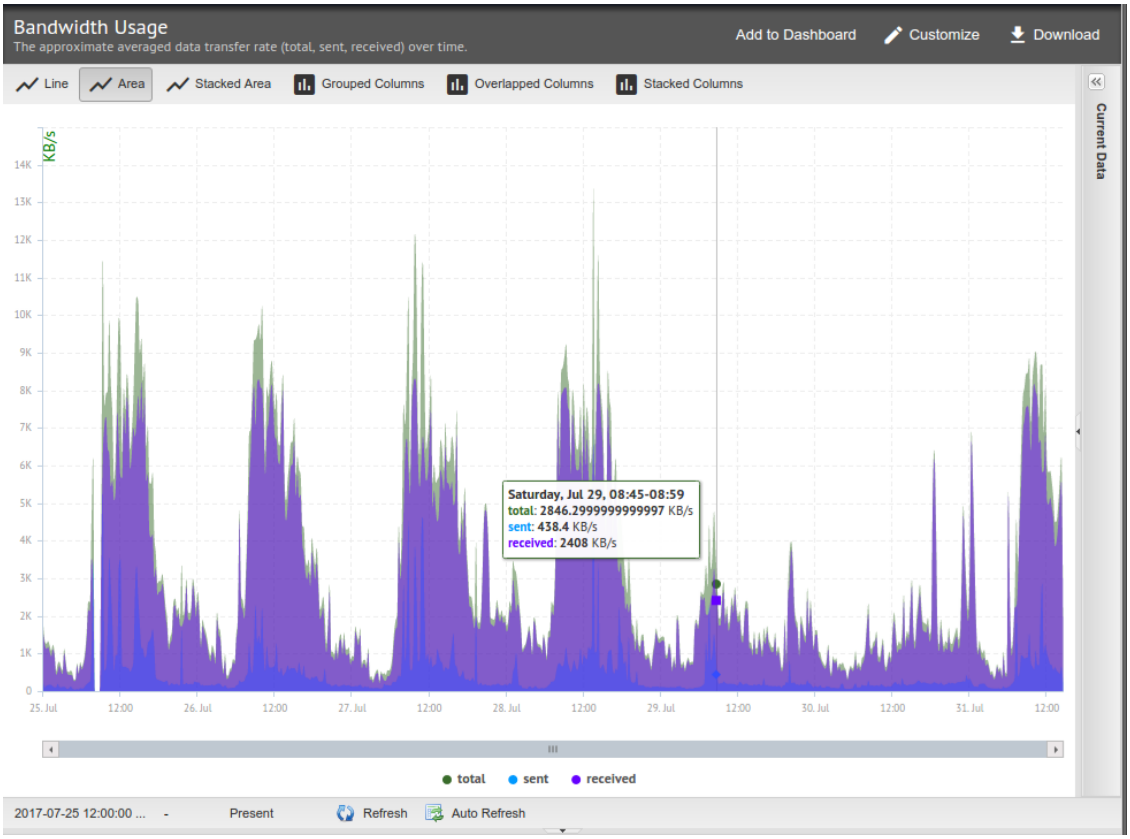


FIGURA 3.22 – HISTÓRICO DE CONSUMO DE DATOS DEL ENLACE DEL HCAM

Fuente: El autor

Hospital "Teodoro Maldonado Carbo"

El consumo de Internet actualmente se ofrece tanto al personal administrativo como médico, quienes acceden a diferentes aplicaciones y sitios web estatales, tales como Gestión Documental, SRI, SERCOP, entidades bancarias, redes sociales, capacitación en línea, videoconferencia, entre otras.

Sitio	Firewall instalado	Detalles
HTMC	pfSense	Versión libre instalada en un servidor basado en procesador Intel Xeon E5 con 64 GB en RAM y procesador de 14 núcleos

Tabla 3.8 – Datos técnicos básicos de firewall instalado en el HTMC

Fuente: El autor

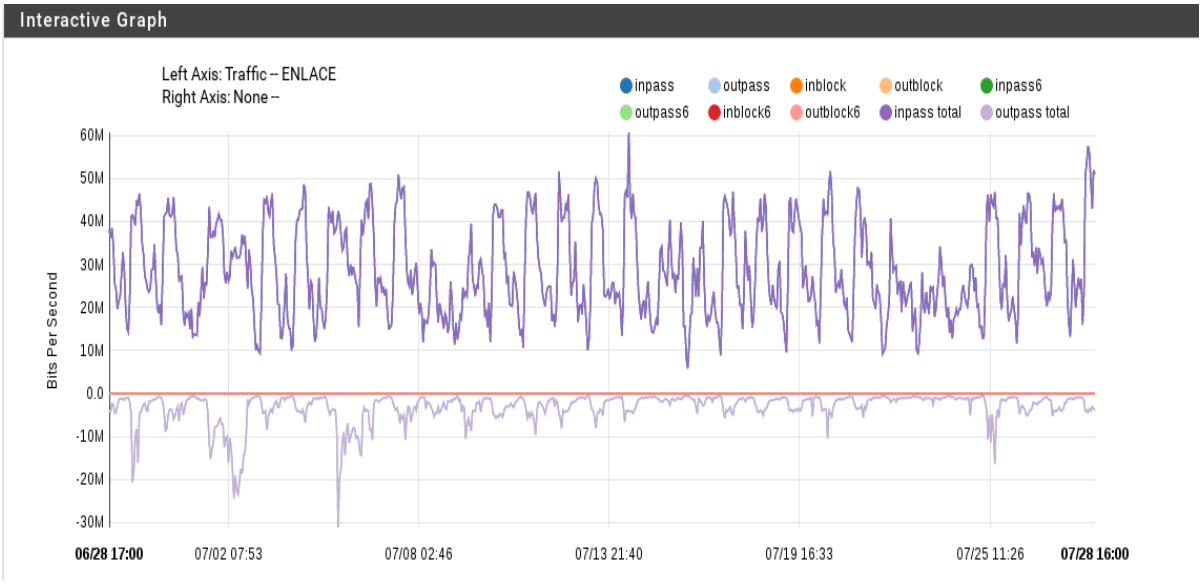


FIGURA 3.23– MUESTRA HISTÓRICA DE CONSUMO DE ENLACE DE INTERNET EN FIREWALL DEL HTMC

Fuente: El autor

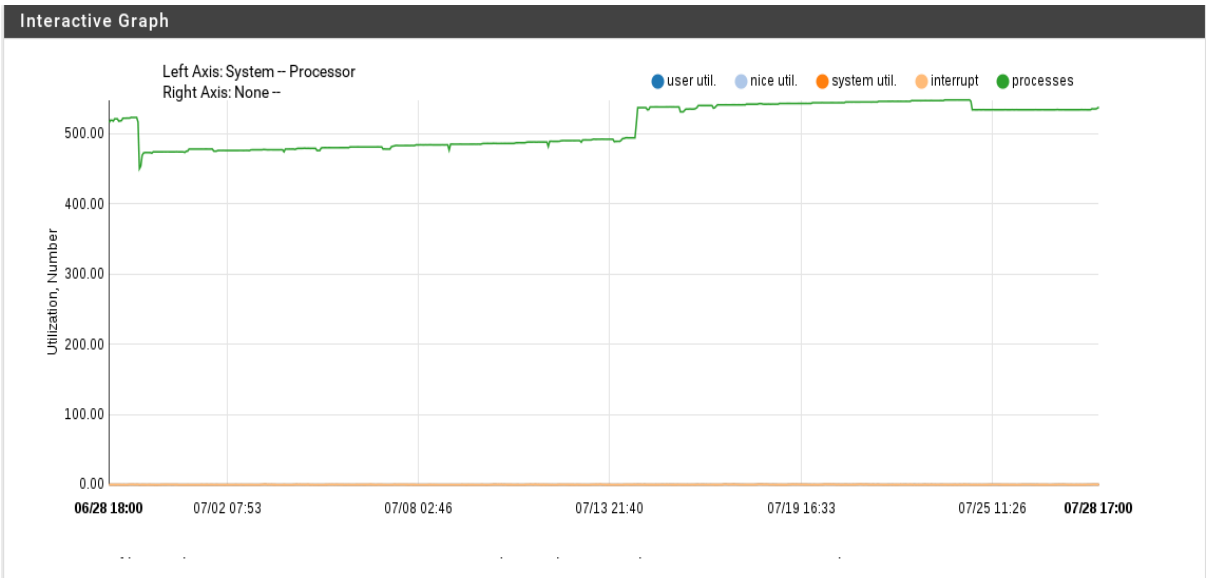


FIGURA 3.24 – MUESTRA HISTÓRICA DE USO DE PROCESADOR DE FIREWALL INSTALADO EN EL HTMC

Fuente: El autor

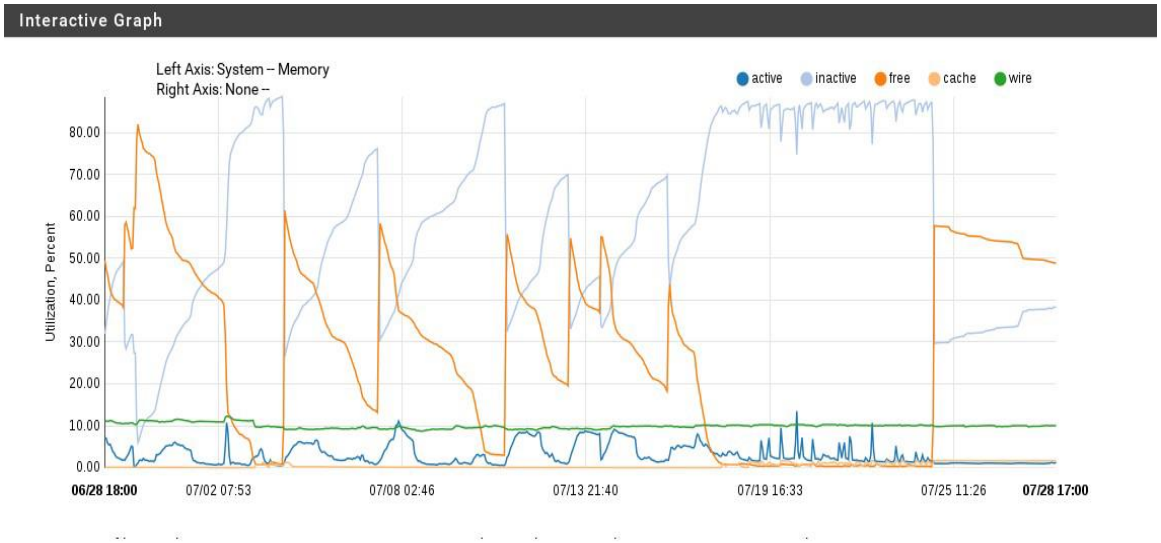


FIGURA 3.25 – MUESTRA HISTÓRICA DEL CONSUMO DE MEMORIA DE FIREWALL INSTALADO EN EL HTMC

Fuente: El autor

Hospital "José Carrasco Arteaga"

En esta casa de salud, el crecimiento que se visto en los últimos años en la parte informática, ha creado nuevas necesidades respecto a la demanda de ancho de banda hacia Internet, motivo por el cual es indispensable contar con la continuidad del servicio actualmente disponible y su ampliar el ancho de banda, con el objetivo de fin de brindar servicios como asistencia remota y actualizaciones de equipamiento especial desplegado en sitio (como por ejemplo, su acelerador lineal, el cual requiere conexión directa del fabricante para soporte y actualizaciones)

Según personal técnico en sitio, se ha podido notar un incremento apreciable de usuarios y estudiantes que se conectan al segmento de red de docencia.

Aquí, al igual que en los hospitales de tercer nivel anteriores, acceden también a aplicaciones y sitios web estatales, como Gestión Documental, SRI, SERCOP, entidades bancarias, redes sociales, capacitación en línea.

Sitio	Firewall instalado	Detalles
HJCA	Mikrotik CCR1036	Equipo propietario con CPU a 1.2 GHz, 16 GB en RAM y 1 GB de almacenamiento

Tabla 3.9 – Datos técnicos básicos de firewall instalado en el HJCA

Fuente: El autor

Hospital "Los Ceibos"

Es desde su inauguración, el hospital del IESS más grande del país.

Sus usuarios requieren del uso de Internet para el acceso a páginas gubernamentales, servicios de correo electrónico, financieros, motores de búsqueda y acceso a boletines médicos tanto para la actualización de conocimientos médicos como para docencia; de igual manera, periódicamente requieren acceso a servicios de videoconferencia.

Adicionalmente, áreas específicas necesitan acceso a redes sociales, para verificación de perfiles de empleados y comunicación social.

Sitio	Firewall instalado	Detalles
Hospital "Los Ceibos"	Cisco ASA 5545	Equipo propietario con CPU a 2.6 GHz (8 núcleos) y 12 GB en RAM

Tabla 3.10 – Datos técnicos básicos de firewall instalado en el Hospital "Los Ceibos"

Fuente: El autor

Al momento de su inauguración, contaba con 1115 usuarios en la red LAN cableada, y 143 en su inalámbrica, esperándose según estimaciones, un crecimiento del 30%.

Hospital “San Francisco de Quito”

Es un hospital de tercer nivel ubicado en el sector de Carcelén, en la ciudad de Quito, de naturaleza mayormente docente que, desde sus inicios, se encuentra a la vanguardia respecto a tecnología y profesionales altamente capacitados.

Pese a que el acceso a Internet se ha vuelto indispensable para su normal funcionamiento, no cuenta con enlace a Internet propio, estando protegido por el firewall gestionado por la DNTI.

Centro Médico “La Mariscal”

Es un hospital especializado en diálisis y enfermedades renales.

Dispone de un enlace propio hacia Internet, sin embargo pese a que su ancho de banda es mínimo, debido al crecimiento esperado, tanto de usuarios como de pacientes, justifica la implementación de un firewall.

“Edificio de Procesos Gobernantes”

Conocido popularmente como edificio “Zarzuela”, aquí funcionan los procesos gobernantes (Consejo Directivo y Dirección General) del IESS. Debido a la naturaleza de sus actividades cuentan con conexión directa hacia Internet, pero no disponen de un firewall para la protección perimetral.

MODOS DISPONIBLES PARA NAVEGACIÓN HACIA INTERNET

De acuerdo tanto a la arquitectura de seguridad, como a la red de la institución, actualmente la navegación hacia Internet se realiza a través de servidores tipo proxy, por firewall o enlaces contratados por las unidades médicas o administrativas.

Servidores Proxy

La institución dispone de servidores de red local mayormente basados en el sistema operativo Linux (distribuciones Red Hat Enterprise Linux y CentOS, principalmente) los cuales brindan servicios de direccionamiento, resolución de nombres, acceso compartido y de proxy, implementado a través de Squid.

DIAGRAMA DE LA ARQUITECTURA ACTUAL

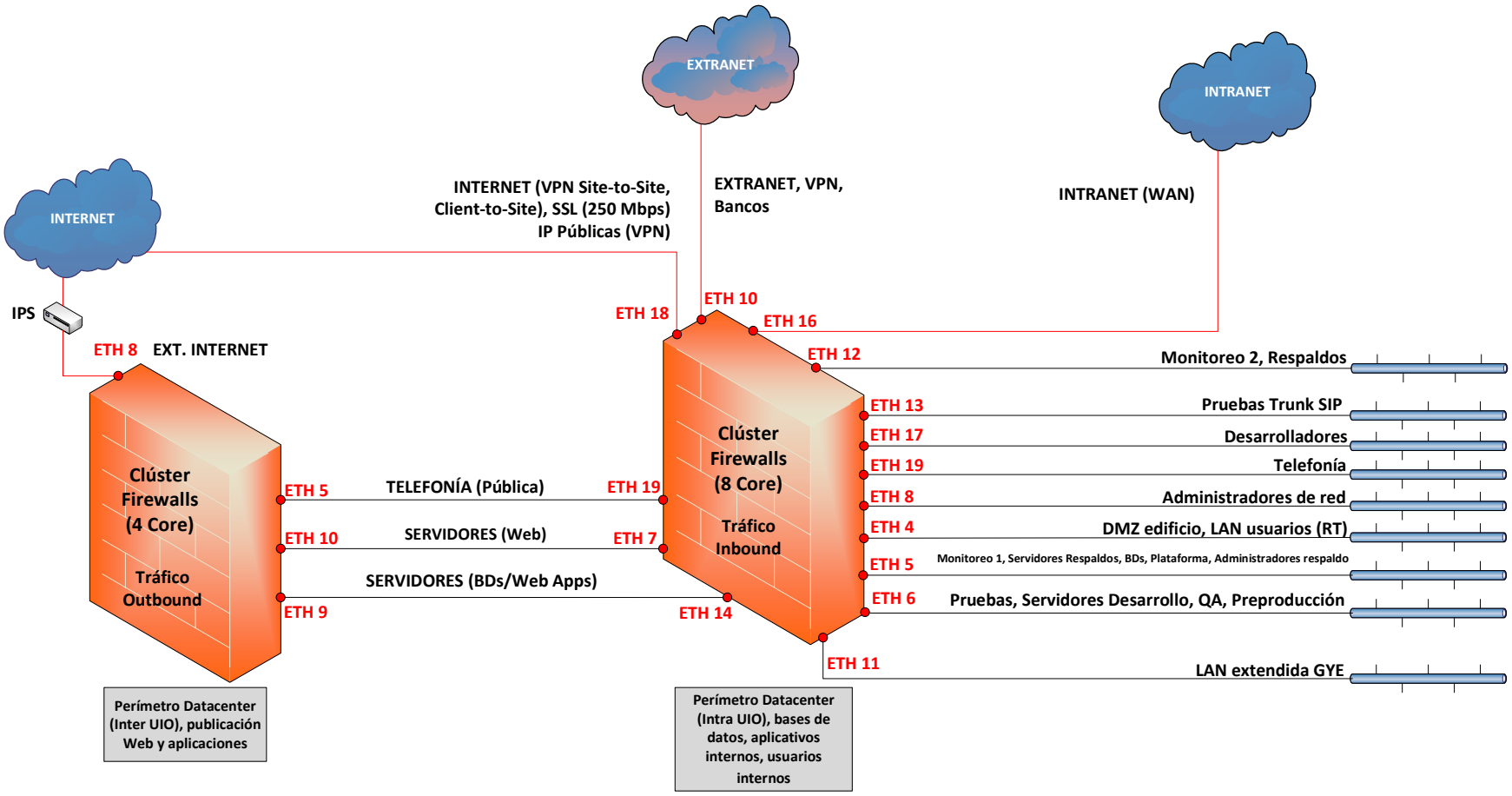


FIGURA 3.26 – DIAGRAMA DE LA ARQUITECTURA DE FIREWALLS ACTUALMENTE INSTALADA

Fuente: El autor

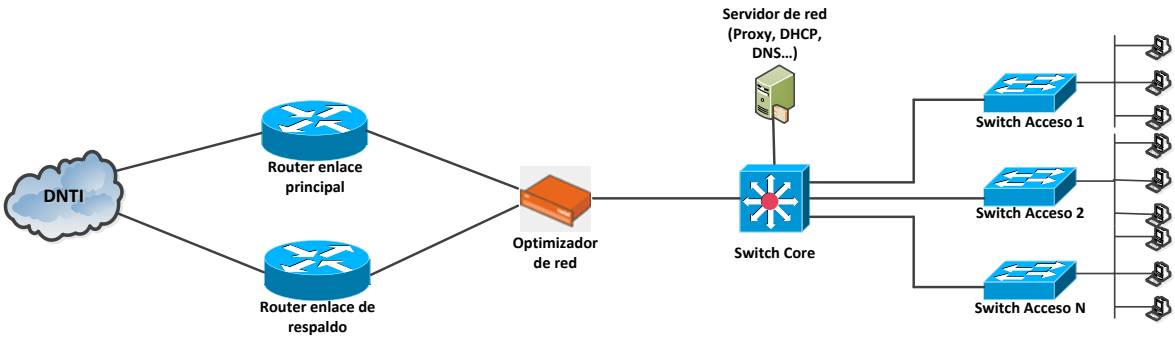


FIGURA 3.27 – DIAGRAMA DE RED LAN TÍPICA PARA LOS SITIOS DE LA INSTITUCIÓN

Fuente: El autor

Todos los servidores locales se conectan a 4 servidores principales configurados con balanceo de carga instalados en el Centro de Datos Principal, con el objeto de controlar y administrar el acceso hacia Internet. Tanto los servidores principales como los locales tienen ciertas limitaciones que impiden controlar el abastecimiento de Internet de una manera rápida y eficaz, debido principalmente a que la actualización de listas de categorización, así como la creación de nuevos permisos es completamente manual, y tampoco es posible la visualización de accesos por usuario, la obtención de reportes globales y/o correlacionados con el uso de Internet.

En la figura 3.28 mostrada a continuación, puede verse la cantidad de consumo de los proxies principales (nacionales). Al momento de la captura, el número de conexiones concurrentes fue de 22600.

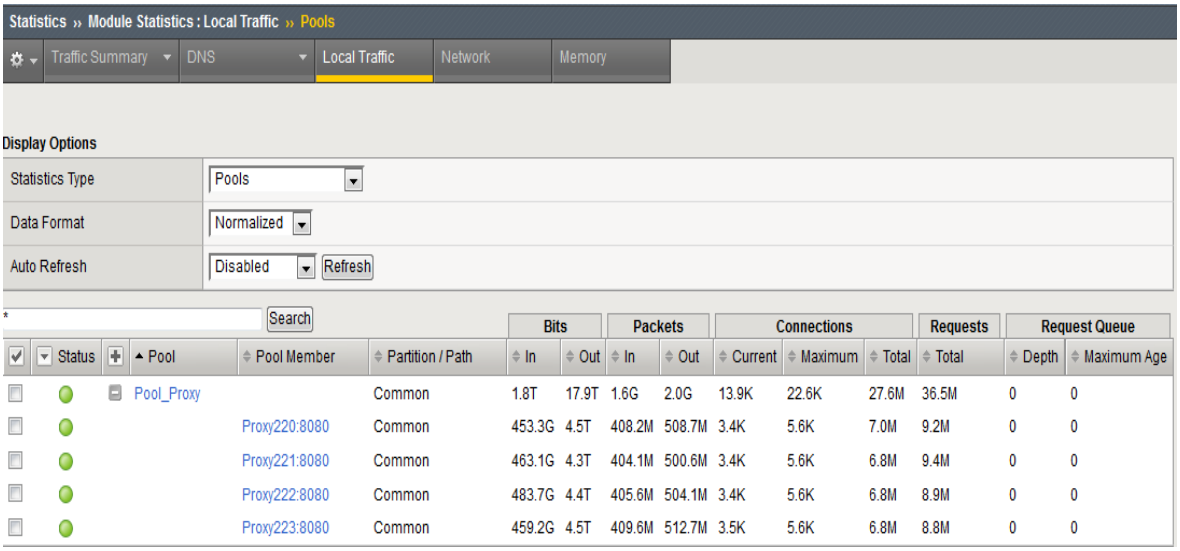


FIGURA 3.28 – CONEXIONES EN PROXIES NACIONALES

Fuente: El autor

De la misma manera, puede verse que el consumo de ancho de banda más alto de los proxies nacionales al momento de la toma de muestra fue de 152.6 Mbps.

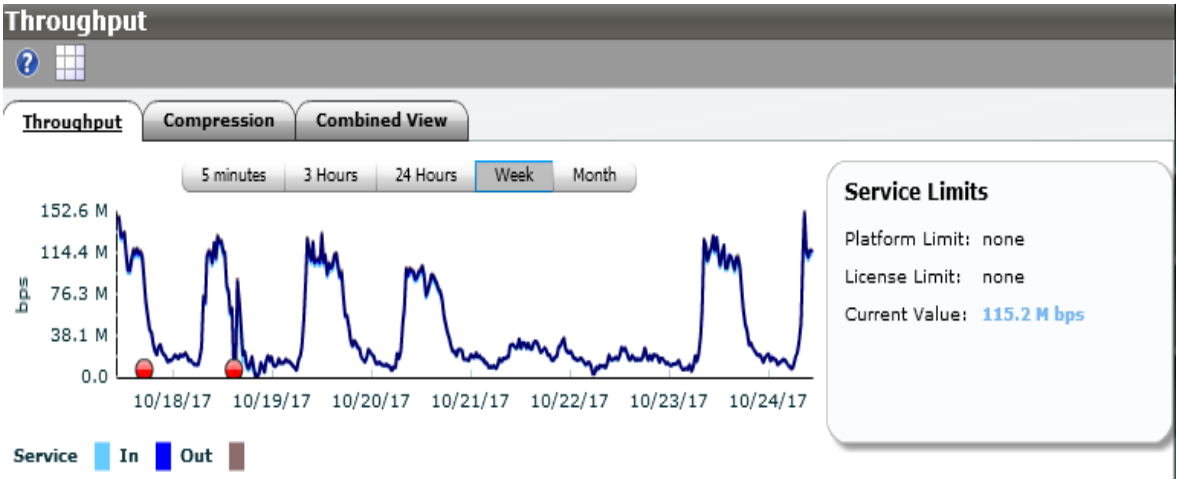


FIGURA 3.29 – MUESTRA DE CONSUMO DE ANCHO DE BANDA EN PROXIES NACIONALES

Fuente: El autor

Firewall

En el firewall se encuentran registrados para navegación libre alrededor de 3000 usuarios internos, los cuales navegan directamente a Internet a través del firewall mediante un proceso de enmascaramiento vía NAT (Network Address Translation) hacia direcciones públicas facilitadas por el proveedor de enlace de comunicaciones.

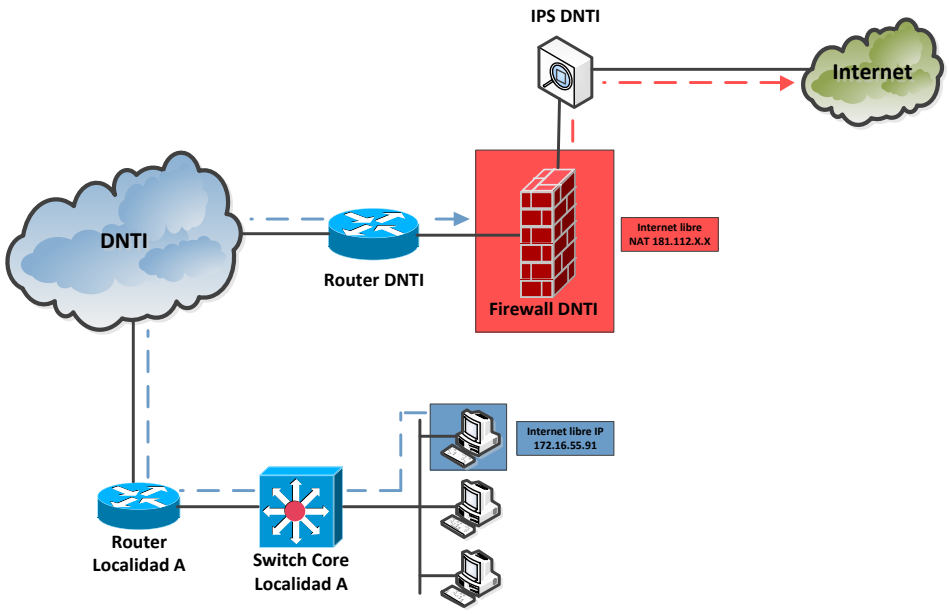


FIGURA 3.30 – PROCESO DE NAT HACIA INTERNET DESDE EL FIREWALL DE LA INSTITUCIÓN

Fuente: El autor

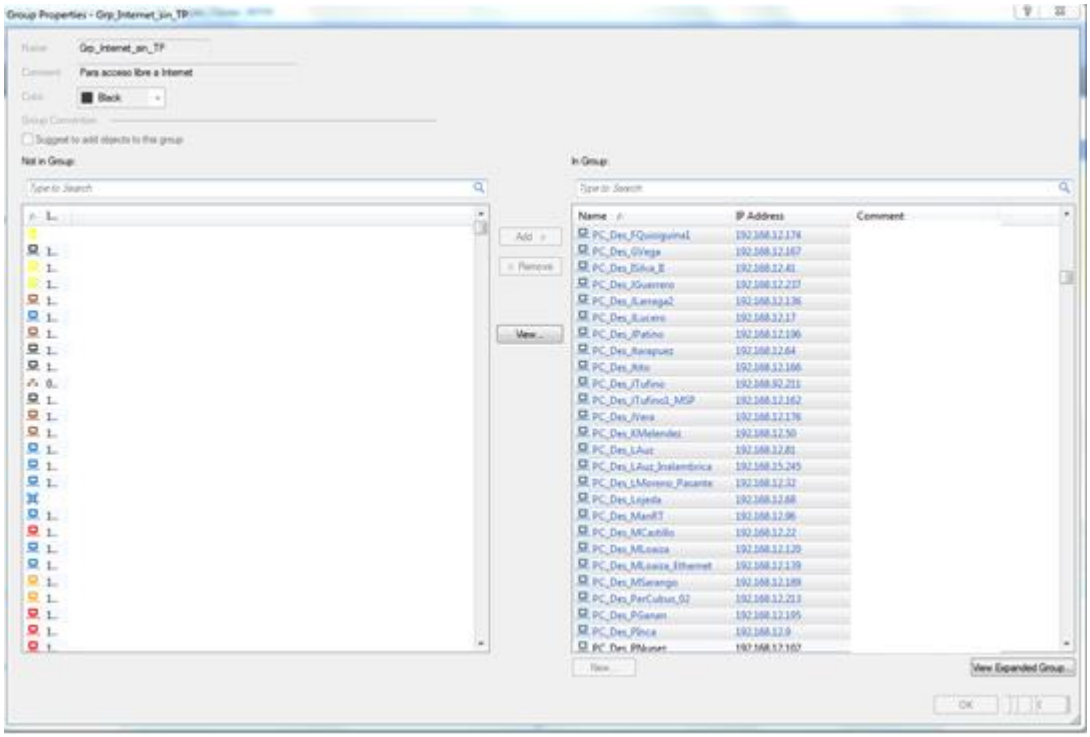


FIGURA 3.31 – VISTA PARCIAL DEL GRUPO DE NAVEGACIÓN LIBRE HACIA INTERNET

Fuente: El autor

Enlaces localmente contratados

Existen ciertas unidades administrativas o médicas tiene disponen de una conexión directa, navegando hacia Internet a través de su canal contratado.

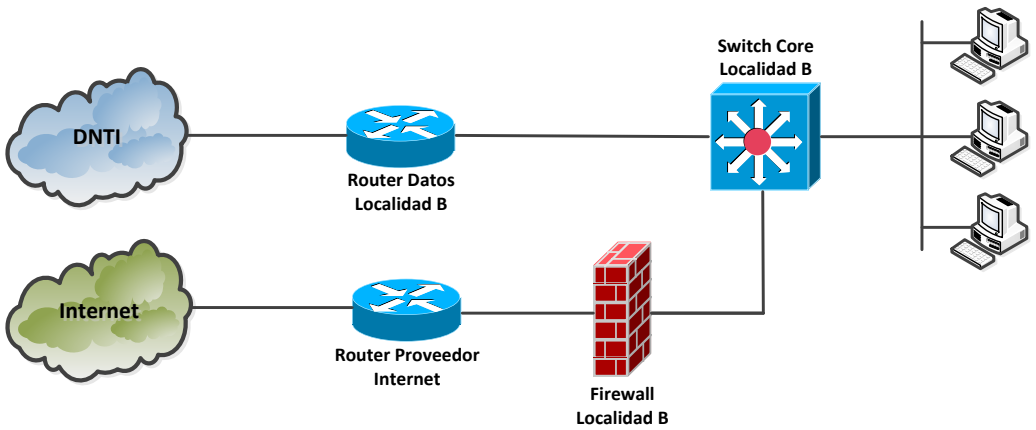


FIGURA 3.32 – NAVEGACIÓN HACIA INTERNET MEDIANTE UN ENLACE LOCALMENTE CONTRATADO

Fuente: El autor

Como se mencionó anteriormente, la protección y control de navegación hacia Internet es realizada de manera local, disponiéndose de un grupo heterogéneo de firewalls, no gestionados directamente por la DNTI.

Este es el caso con:

1. Hospital “Carlos Andrade Marín” (Untangle)
2. Hospital “Teodoro Maldonado Carbo” (pfSense)
3. Hospital “José Carrasco Arteaga” (Mikrotik)
4. Hospital “Los Ceibos” (Cisco)
5. Hospital General de Quevedo (Palo Alto)
6. Hospital General de Machala (Palo Alto)

RIESGOS, AMENAZAS Y NECESIDADES

Actualmente, la solución perimetral basada en firewall no dispone de una administración centralizada que permita gestionar la seguridad de red de las unidades médicas de tercer nivel, mismas que hoy implementan firewalls de diferentes proveedores, imposibilitando así tener control estricto o aplicar políticas globales establecidas y controladas según las directrices de la institución, y asimismo, tampoco es posible la obtención de reportes ni correlación de eventos.

La actual solución perimetral basada en firewall no dispone de soporte y tampoco de mantenimiento respecto al hardware (HP) y software (Check Point) que la conforman, adicionalmente, los servidores sobre los que se encuentra instalada han llegado al fin de su vida útil, careciendo ya incluso de partes y piezas de repuesto.

Se requiere controlar los accesos hacia Internet ante la posibilidad de nuevos ataques de amenazas actuales y futuras, por lo que es menester contar con nuevos componentes de protección, y debido a la necesidad de ejecutar un control del acceso hacia Internet a través de una nueva solución, y aplicar la separación de los segmentos de usuarios de los del core de aplicaciones, se ha diseñado y planteado una nueva arquitectura de seguridad.

El que ciertas unidades médicas de tercer nivel dispongan de enlaces hacia Internet contratados y gestionados localmente, es un punto problemático, puesto que la gestión y administración del mismo no se la efectúa desde la DNTI, sino que es realizada por personal técnico en sitio. Esto ha permitido que se publiquen portales web, aplicaciones y servicios al mundo exterior, a espaldas de la institución y a sabiendas de que esto no está permitido bajo ningún motivo; sin embargo, se han transformado en plataformas de riesgo para la institución, puesto que en ocasiones anteriores, algunos servidores que las alojan han sido intervenidos, infectados y atacados exitosamente, en desmedro de la institución.

De acuerdo a lo antes expuesto se puede concluir que si bien la solución de firewalls actualmente disponible ha permitido que la plataforma de core institucional no se vea comprometida o afectada por ataques y/o accesos no autorizados a la red de la institución, permitiendo mantener la integridad de los datos e información, activo vital para la organización, su arquitectura de seguridad perimetral actual no satisface las exigencias respecto a la seguridad de la red, esto aunado a la creación de dependencias administrativas y médicas a nivel nacional, algunas de las cuales poseen soluciones de control de acceso a Internet no óptimas y ante la aparición de nuevas formas de ataque y amenazas a la seguridad informática, es menester reestructurar la arquitectura actualmente disponible, con el objetivo de contar con una solución de seguridad perimetral centralizada capaz de satisfacer las necesidades actuales respecto al aseguramiento de la integridad de la información.

Al haber sido implementada en el año 2010, la solución no contemplaba brindar servicios de Internet en forma específica, por lo que no cuenta con herramientas tales como antivirus, antibot, filtrado URL o control de aplicaciones. Ante el incremento y la necesidad de brindar servicio de Internet a través de los firewalls, se requiere la separación de dicho servicio y asignar dicha tarea a un gateway especializado, que permita separar físicamente el segmento de usuarios de los segmentos del core de aplicaciones.

La nueva arquitectura deberá estar en capacidad de ser operada por el personal técnico que gestiona la solución actual, aprovechando sus conocimientos en el manejo de la misma, características y peculiaridades de la red, así como permitir una actualización de conocimientos y transición a una nueva plataforma en un tiempo mínimo, sin mayor interrupción de los servicios que proporciona la institución.

Las unidades médicas de tercer nivel que cuentan con un número elevado de usuarios internos, necesitan mantener una conexión directa hacia Internet, con el objetivo de tener mayor disponibilidad de accesos a los aplicativos publicados y otros servicios tales como investigación científica y docencia, sistema de cirugía robótica, soporte específico, entre otros.

La evaluación del proyecto de mejoramiento de la arquitectura de seguridad perimetral es primordial para la Institución, puesto que la actualización del licenciamiento, mantenimiento y soporte técnico de los firewalls permitirá tener operativos todos los servicios de red y contar con la seguridad que éstos brindan.

CAPÍTULO IV - PROPUESTA DE MEJORAMIENTO

INTRODUCCIÓN

En el capítulo anterior se hizo una descripción del estado de la institución respecto a la infraestructura de TI, zonas establecidas, arquitectura del sistema de seguridad perimetral, hardware y otros equipos sobre la que ésta se encuentra desplegada, así como sus bondades y limitaciones respecto a las necesidades actuales.

Del mismo modo, se expuso el escenario actual respecto a las necesidades de los hospitales de tercer nivel y dependencias administrativas que, debido a la naturaleza de sus labores, requieren comunicación hacia Internet propia, la cual al día de hoy disponen, pero que sin embargo ha traído complicaciones respecto a su administración y control.

Si bien al momento el clúster de firewalls desplegado actualmente disponible ha posibilitado que la plataforma de núcleo (core) institucional no se haya visto comprometida y afectada por ataques o accesos no autorizados, siendo capaz de salvaguardar la integridad de los activos lógicos de la institución, su arquitectura actual ya no es suficiente para soportar las necesidades presentes, hecho agravado por la creación de dependencias administrativas y médicas en todo el país, que como se explicó anteriormente, disponen de soluciones de acceso y protección hacia Internet no confiables, aumento de necesidades de protección, entre otros factores.

Es por ello que en el presente capítulo se expondrá la nueva arquitectura propuesta, la cual estará en capacidad de cubrir las necesidades de control centralizado, protección de zonas, navegación segura, control de acceso y filtrado de contenido, así como otras protecciones, lo cual permitirá cumplir con el objetivo estratégico institucional de reducir los riesgos tecnológicos, por medio de la seguridad informática y el uso de esquemas de continuidad tecnológica.

CONSIDERACIONES RESPECTO A LA POSIBILIDAD DE REPOTENCIACIÓN

La repotenciación se aplicaría previa disponibilidad de equipos de cómputo (hardware), donde sea posible la instalación para el despliegue, administración, control y reportes de la solución de firewalls.

Como se explicó en el capítulo anterior, la administración de los clústeres de firewalls se ejecuta mediante un clúster de administración (Management), que proporciona redundancia respecto a la gestión y registros, un componente de reportería (Reporter), y para las tareas de auditoría, la institución disponía de un servidor FireMon, el cual sufrió un daño en el año 2016, cuya restauración y puesta en funcionamiento nuevamente no fue posible, debido a la falta de renovación del soporte por parte del fabricante.

Teniendo en cuenta el escenario de la repotenciación, los costos respecto a la compra de nuevo hardware (servidores tipo blade) disminuirían, debido a que la institución dispone de un banco apreciable de dichos equipos, pero éstos deberían cumplir con las especificaciones técnicas y marco de compatibilidad indicados por el fabricante.

Suponiendo que los equipos disponibles cumplan con los parámetros técnicos y de compatibilidad requeridos, se suma el hecho de que los distintos componentes de software como las licencias de los elementos actualmente instalados deberán aprovecharse.

A continuación, se muestra un detalle del software que forma parte de la solución actual:

Elemento	Código SKU
Security Bundle (SG805 y SMU007)	CPSG-P805-CPSM-PU007
Security Gateway Container - 4 Cores and 4 Blades	CPSG-P405
Security Gateway Container - 4 Cores and 4 Blades	CPSG-P405
Security Gateway Container-4 Cores and 5 Blades –HA	CPSG-P405-HA
Security Gateway Container-4 Cores and 5 Blades –HA	CPSG-P405-HA
Security Gateway Container-8 Cores and 5 Blades –HA	CPSG-P405-HA

Tabla 4.1 – Lista parcial del software con el que cuenta la institución para la administración de la arquitectura actual

Fuente: El autor

Respecto a la solución actualmente desplegada, cabe indicar que las licencias adquiridas por la institución son de naturaleza perpetua, por lo tanto, en el caso de una repotenciación, lo que deberá ser renovado sería el soporte, acceso a las actualizaciones del fabricante, junto con el mantenimiento del software.
He aquí un detalle de las licencias:

Nombre Blade	Código SKU
Identity Awareness Software Blade	CPSB-IA-F
Identity Awareness Software Blade	CPSB-IA-F
Identity Awareness Software Blade	CPSB-IA-HA-F
Identity Awareness Software Blade	CPSB-IA-HA-F
Security Gateway - IPS Blade	CPSB-IPS
IPS Blade - HA	CPSB-IPS-HA
IPS Blade for 1 year (L)	CPSB-IPS-L
IPS Blade 1 Year (L) HA	CPSB-IPS-L-HA
Mobile Access Blade - 50	CPSB-MOB-50
Mobile Access Blade - Unlimited	CPSB-MOB-U
Mobile Access Blade - Unlimited HA	CPSB-MOB-U-HA
SmartWorkflow Blade	CPSB-WKFL-10
Web Security Blade	CPSB-WS
Web Security Blade	CPSB-WS
Web Security Blade- HA	CPSB-WS-HA
Web Security Blade- HA	CPSB-WS-HA
Anti-Bot Blade for 3 years (M)	CPSB-ABOT-M-3Y
Anti-Bot Blade for 3 years - HA (M)	CPSB-ABOT-M-3Y-HA
Acceleration and Clustering Blade	CPSB-ACCL
Acceleration and Clustering Blade	CPSB-ACCL
Acceleration and Clustering Blade	CPSB-ACCL
Acceleration & Clustering Blade	CPSB-ACCL-HA
Acceleration & Clustering Blade	CPSB-ACCL-HA
Acceleration & Clustering Blade	CPSB-ACCL-HA
Advanced Networking Blade	CPSB-ADN
Advanced Networking Blade	CPSB-ADN
Advanced Networking Blade	CPSB-ADN
Advanced Networking Blade	CPSB-ADN-HA
Advanced Networking Blade	CPSB-ADN-HA
Advanced Networking Blade	CPSB-ADN-HA

Tabla 4.2 – Lista parcial de licencias adquiridas por la institución

Fuente: El autor

Nombre Blade	Código SKU
Anti-Virus Blade for 3 years (M)	CPSB-AV-M-3Y
Anti-Virus Blade for 3 years (M) - HA	CPSB-AV-M-3Y-HA
Endpoint Policy Management Software Blade	CPSB-EPM
SmartEvent Intro Blade	CPSB-EVNT-INT
Firewall Software Blade	CPSB-FW
Firewall Software Blade	CPSB-FW
Firewall Software Blade	CPSB-FW
Firewall Software Blade - HA	CPSB-FW-HA
Firewall Software Blade - HA	CPSB-FW-HA
Firewall Software Blade - HA	CPSB-FW-HA
Logging and status Software Blade	CPSB-LOGS
Security Management - Monitoring Blade (MNTR)	CPSB-MNTR
Network Policy Management Software Blade	CPSB-NPM
Provisioning Blade	CPSB-PRVS
User Directory Blade	CPSB-UDIR
IPSEC VPN Software Blade	CPSB-VPN
IPSEC VPN Software Blade	CPSB-VPN
IPSEC VPN Software Blade	CPSB-VPN
IPSEC VPN Software Blade - HA	CPSB-VPN-HA
IPSEC VPN Software Blade - HA	CPSB-VPN-HA
IPSEC VPN Software Blade - HA	CPSB-VPN-HA

Tabla 4.3 – Lista parcial de licencias adquiridas por la institución (continuación)

Fuente: El autor

Estas licencias serían entonces reutilizadas, y los componentes, instalados en los equipos proporcionados por la institución. Se contaría nuevamente con componentes actualizados (blades) de antivirus, antibot, control de identidad, IPS, entre otros.

Sin embargo, la arquitectura actual permanecería mayores cambios, y pese a estar implementada en equipos más modernos (no necesariamente nuevos), continuaría prácticamente proporcionando el mismo nivel de protección, que si bien es funcional, no permitiría establecer una administración global centralizada de las reglas y permisos aplicados en los hospitales de tercer nivel que cuentan con salida propia hacia Internet (situación que ha generado inconvenientes en el pasado), y no se estaría asignando el control del servicio de Internet a un equipo especializado, siendo éste un requisito de seguridad actualmente necesario, que permita separar físicamente el segmento de usuarios de los segmentos del núcleo de aplicaciones.

TABLA DE NECESIDADES

A continuación se muestra un resumen de las necesidades que fueron expuestas en el capítulo anterior, y que servirán como base para el planteamiento de la solución:

	Necesidad	Criticidad
1	Implementar una arquitectura de seguridad perimetral, acorde a los escenarios actuales y futuros	Alta
2	Capacidad de gestión centralizada y administración distribuida de sitios remotos	Alta
3	Disponer de nuevos componentes de protección (antivirus, antibot, IPS, filtrado URL, otros)	Alta
4	Disponer de un componente administrable de reportería general centralizado	Alta
5	Separar los segmentos de aplicaciones, servicios web, bases de datos, entre otros y colocarlos en una nueva capa de protección exclusiva vía firewall	Alta
6	Implementación de un nuevo clúster para segmentos de usuarios, gestión del servicio de Internet y demás servicios	Alta
7	Contar con un equipo que ejecute control de accesos a Internet en dependencias que reciben el servicio desde la DNTI, contando además del firewall con filtrado de contenido	Alta
8	Disponer de una herramienta capaz de proteger el acceso a Internet desde las dependencias que cuentan directamente con este servicio, y otras unidades que se unirán a la red institucional	Alta
9	Contar con soporte del fabricante respecto a componentes de hardware, software, tareas de implementación, afinamiento y troubleshooting relacionadas con la nueva arquitectura	Alta
10	Capacidad de soportar un crecimiento de al menos un 30% a nivel central y un 10% a nivel local en los próximos 3 años	Alta
11	Aprovechar la nueva arquitectura de seguridad perimetral para asegurar el cumplimiento de los objetivos institucionales	Alta

Tabla 4.4 – Tabla de necesidades básicas respecto a la arquitectura de seguridad perimetral

Fuente: El autor

PLANTEAMIENTO DE LA SOLUCIÓN ELEGIDA

Ante lo expuesto en la tabla de necesidades, se plantea:

1. La implementación de una nueva arquitectura de seguridad perimetral, capaz de brindar mayores niveles de protección comparada a la actualmente disponible, mediante la una herramienta que permita la administración centralizada de políticas de seguridad, filtrado de contenido y elementos de protección.

2. El mejoramiento de la arquitectura de firewalls instalada en el core del Centro de Datos (plataforma de seguridad perimetral de la institución), reduciendo los riesgos a los que están expuestos los aplicativos y servicios de la organización, respecto a los criterios básicos de integridad, confidencialidad y disponibilidad.

3. Ejecutar el retiro de los equipos de seguridad perimetral actualmente instalados en sitios considerados como críticos (hospitales de tercer nivel y unidades administrativas), mismos que al día de hoy disponen de distintos firewalls, y según los análisis realizados en el área de Redes de la institución, constituyen un riesgo de seguridad ya que no han sido capaces de mitigar todos los ataques, su licenciamiento está pronto a caducar, o se encuentran ya obsoletos.

PROPUESTA DE MEJORAMIENTO Y COMPONENTES DE LA SOLUCIÓN

Una vez planteada la solución, se tendrán entonces los siguientes elementos:

Elemento	Descripción
Arquitectura	Separación para la protección de servicios en 3 capas: 1) Servicios de Internet, 2) Publicación de servicios, 3) Protección del core
Firewall	Protección perimetral según criterios de aceptación o bloqueo de tráfico de acuerdo a dirección IP de origen, IP de destino, puerto y/o aplicación
VPN	Creación de VPN site-to-site, client-to-site, utilizando protocolos de encriptación

Tabla 4.5 – Descripción de los elementos básicos de la propuesta de mejoramiento

Fuente: El autor

Elemento	Descripción
Antivirus	Protección perimetral ante virus, capaz de proteger en tiempo real las conexiones contra archivos maliciosos entrantes y salientes mediante la verificación de firmas de virus
Filtrado URL y Control de Aplicaciones	Control de acceso a páginas y sitios web por categorización de las URL, permitir la creación de listas negras propias, control granular de acceso a sitios web 2.0 (web social)
Antibot y antiC&C	Protección perimetral contra comando y control, capaz de bloquear equipos infectados que intentan comunicarse con servidores de C&C
Auditoría	Capacidad de visualización del uso de reglas y objetos y auditoría de gestión de equipos e higiene de reglas
Administración	Administración centralizada, mantenimiento de políticas y lineamientos, control de instalación, y capacidad para brindar privilegios controlados a administradores locales de otras dependencias
Generación de reportes	Control central de registros, generación de reportes unificados y capacidad de correlación de eventos

Tabla 4.6 – Descripción de los elementos básicos de la propuesta de mejoramiento (continuación)

Fuente: El autor

COMPONENTES

Data Center Principal (DNTI - Quito)

Clúster de Core			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección de la capa interna de los servidores de la institución (por la naturaleza de su función, no requiere funcionalidades de protección de perímetro)	Throughput mínimo: 700 Mbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, identificación de usuarios y redes (Next Generation Firewall)
		Mínimo 1700 conexiones nuevas por segundo	
		Mínimo 210 mil sesiones concurrentes	
Clúster de Publicación			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección de las aplicaciones que se publican hacia Internet (requiere la funcionalidades de firewall, NAT y acceso VPN	Throughput mínimo: 216 Mbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, identificación de usuarios y redes, VPN, antivirus, antibot (Next Generation Threat Prevention)
		Mínimo 500 conexiones nuevas por segundo	
		Mínimo 30 mil sesiones concurrentes	
		Mínimo 500 VPN site-to-site	
		Mínimo 2000 VPN client-to-site	
Clúster de Servicios Internos			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección a los usuarios internos frente a amenazas y control de acceso a Internet mediante sus módulos de control activos (para todos los usuarios que al día de hoy ingresan vía proxy)	Throughput mínimo: 1 Gbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, control de aplicaciones, filtrado URL, antivirus, antibot (Next Generation Firewall)
		Mínimo 136 mil conexiones nuevas por segundo	
		Mínimo 3,4 millones de sesiones concurrentes	
		Protección para al menos 30 mil usuarios	
		Mínimo 10 mil usuarios concurrentes	

Tabla 4.7 – Componentes de la nueva arquitectura de seguridad perimetral para el Data Center Principal

Fuente: El autor

Gestor de Administración, Registros y Reportes			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Permitirá la administración integral de la solución de seguridad perimetral y de los firewalls desplegados en las unidades médicas de tercer y las demás dependencias administrativas, brindando capacidad de correlación de eventos y reportería	Virtualizable	Reportería en tiempo real, correlación de eventos locales y globales, administración centralizada de políticas locales y globales
		Soportar todos los compontes de la solución de seguridad	
		Soportar al menos un crecimiento del 50%	
		Soportar al menos 10 zonas de administración	
		Al menos 10 TB de almacenamiento	
Gestor de Auditoría de Reglas			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Permitirá llevar un control y realizar tareas de auditoría de las reglas, permisos y cambios efectuados en la totalidad de los firewalls que forman parte de la nueva arquitectura	Virtualizable	Correlación de eventos, gestor de estadísticas, higiene de reglas
		Soportar todos los compontes de la solución de seguridad	
		Soportar al menos un crecimiento del 50%	
Switches de Conexión			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
2	Permitirán la interconexión de todos los componentes de la nueva arquitectura de seguridad perimetral a desplegarse en el DC de la DNTI en Quito	Throughput mínimo: 480 Mbps	Switching de ultra alta velocidad, funciones de capas 2, 3 y 4
		Al menos 13 interfaces 10 GE SFP+ cada uno	
		Al menos 10 interfaces 1000Base-T cada uno	

Tabla 4.8 – Componentes de la nueva arquitectura de seguridad perimetral para el Data Center Principal (continuación)

Fuente: El autor

Hospital "Carlos Andrade Marín"

Clúster de Protección HCAM			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección a los usuarios internos frente a amenazas y control de acceso a Internet mediante sus módulos de control activos	Throughput mínimo: 1,5 Gbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, identificación de usuarios y redes, antivirus, antibot, filtrado URL, control de aplicaciones e IPS
		Mínimo 21 mil conexiones nuevas por segundo	
		Mínimo 517 mil sesiones concurrentes	
		Protección para al menos 5 mil usuarios	
		Soporte para enrutamiento vía BGP automático	

Tabla 4.9 – Componentes de la nueva arquitectura de seguridad perimetral para el Hospital "Carlos Andrade Marín"

Fuente: El autor

Hospital "Teodoro Maldonado Carbo"

Clúster de Protección HTMC			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección a los usuarios internos frente a amenazas y control de acceso a Internet mediante sus módulos de control activos	Throughput mínimo: 1,5 Gbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, identificación de usuarios y redes, antivirus, antibot, filtrado URL, control de aplicaciones e IPS
		Mínimo 20 mil conexiones nuevas por segundo	
		Mínimo 500 mil sesiones concurrentes	
		Protección para al menos 6 mil usuarios	
		Soporte para enrutamiento vía BGP automático	

Tabla 4.10 – Componentes de la nueva arquitectura de seguridad perimetral para el Hospital "Teodoro Maldonado Carbo"

Fuente: El autor

Hospital "José Carrasco Arteaga"

Firewall de Protección HJCA			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección a los usuarios internos frente a amenazas y control de acceso a Internet mediante sus módulos de control activos	Throughput mínimo: 1 Gbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, identificación de usuarios y redes, antivirus, antibot, filtrado URL, control de aplicaciones e IPS
		Mínimo 10 mil conexiones nuevas por segundo	
		Mínimo 240 mil sesiones concurrentes	
		Protección para al menos 2 mil usuarios	
		Soporte para enrutamiento vía BGP automático	

Tabla 4.11 – Componentes de la nueva arquitectura de seguridad perimetral para el Hospital "José Carrasco Arteaga"

Fuente: El autor

Centro Médico "La Mariscal"

Firewall de Protección La Mariscal			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección a los usuarios internos frente a amenazas y control de acceso a Internet mediante sus módulos de control activos	Throughput mínimo: 750 Mbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, identificación de usuarios y redes, antivirus, antibot, filtrado URL, control de aplicaciones e IPS
		Mínimo 2 mil conexiones nuevas por segundo	
		Mínimo 25 mil sesiones concurrentes	
		Protección para al menos 300 usuarios	
		Soporte para enrutamiento vía BGP automático	

Tabla 4.12 – Componentes de la nueva arquitectura de seguridad perimetral para el Centro Médico "La Mariscal"

Fuente: El autor

Edificio de "Procesos Gobernantes (Zarzuela)"

Firewall de Protección Zarzuela			
Cantidad	**Descripción**	**Requisitos mínimos**	**Características**
1	Para protección a los usuarios internos frente a amenazas y control de acceso a Internet mediante sus módulos de control activos	Throughput mínimo: 500 Mbps (con un mínimo de 40% de trafico SSL y todas sus funcionalidades activas)	Firewall, identificación de usuarios y redes, antivirus, antibot, filtrado URL, control de aplicaciones e IPS
		Mínimo 2 mil conexiones nuevas por segundo	
		Mínimo 40 mil sesiones concurrentes	
		Protección para al menos 400 usuarios	
		Soporte para enrutamiento vía BGP automático	

Tabla 4.13 – Componentes de la nueva arquitectura de seguridad perimetral para el Edificio "Procesos Gobernantes (Zarzuela)"

Fuente: El autor

Cabe mencionar que la arquitectura no incluye información que por su naturaleza es confidencial, tales como el detalle del direccionamiento IP, VLAN desplegadas, segmentos de red detallados sensibles (por ejemplo, bases de datos, aplicativos…), configuraciones de otros equipos involucrados (IPS, switch de capa 3 para comunicación entre clústeres, optimizadores, balanceadores, routers)

La arquitectura propuesta está basada en la metodología Check Point SDP, misma que posibilitará el aprovechamiento de la actual segmentación de componentes, agrupación de servicios, naturaleza de servicios y aplicaciones, estructura de la red disponible, permitiendo un crecimiento protegido y funcional, centrado en la seguridad perimetral, ajustándose tanto a las necesidades y amenazas actuales y futuras que afronta la institución, lo que la convierte en una solución robusta, flexible y confiable.

Teniendo entonces en cuenta lo antes expuesto, a continuación se muestra un diagrama con la arquitectura propuesta para la institución.

DIAGRAMA DE LA ARQUITECTURA PROPUESTA

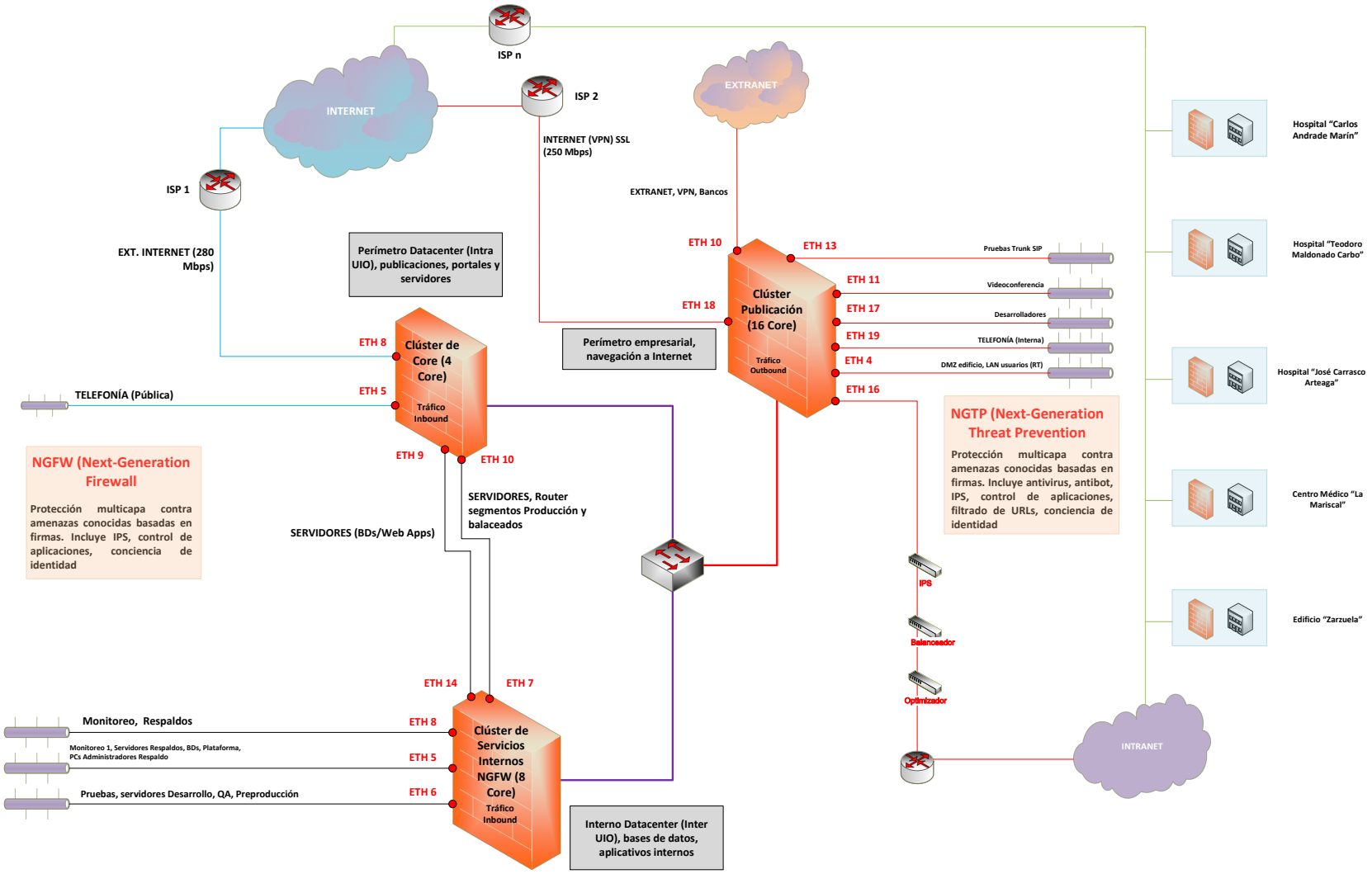


FIGURA 4.1 – DIAGRAMA DE LA NUEVA ARQUITECTURA DE SEGURIDAD PERIMETRAL PROPUESTA PARA LA INSTITUCIÓN

Fuente: El autor

COMPARATIVA FRENTE A LA SITUACIÓN ACTUAL

La arquitectura propuesta presenta una serie de ventajas frente a la actualmente disponible, desde la mejor separación de los segmentos de red y zonas que conforman el perímetro de la institución, hasta la inclusión de nuevas funcionalidades gracias a los nuevos equipos.

	Arquitectura actual	Arquitectura propuesta
Año	2010	2018
¿Aplicada?	Sí	No
Elementos	1 clúster de Internet	1 clúster de core
	1 clúster de Intranet	1 clúster de publicación
	1 gestor de administración	1 clúster de servicios internos
	1 gestor de auditoría	1 gestor de administración, registros y reportes
	1 gestor de eventos	1 gestor de auditoría de reglas
		1 clúster de protección para HCAM
		1 clúster de protección para HTMC
		1 clúster de protección para HJCA
		1 firewall de protección para CM "La Mariscal"
		1 firewall de protección para edificio "Zarzuela"
		2 switches de conexión
Características	Clúster Internet: Firewall	Clúster de core: Firewall
	Clúster Intranet: Firewall	Clúster de publicación: Firewall, antivirus, antibot, VPN
		Clúster de servicios internos: Firewall, control de aplicaciones, filtrado URL, antivirus, antibot
		Clúster HCAM: Firewall, control de aplicaciones, IPS, filtrado URL, antivirus, antibot
		Clúster HTMC: Firewall, control de aplicaciones, IPS, filtrado URL, antivirus, antibot
		Firewall HJCA: Firewall, control de aplicaciones, IPS, filtrado URL, antivirus, antibot
		Firewall CM "La Mariscal": Firewall, control de aplicaciones, IPS, filtrado URL, antivirus, antibot
		Firewall "Zarzuela": Firewall, control de aplicaciones, IPS, filtrado URL, antivirus, antibot
¿Escalable?	No	Sí
¿Mejorable?	No (ni aún con repotenciación)	Sí
¿Soporte del fabricante?	No	Sí

Tabla 4.14 – Comparativa entre la arquitectura actual y propuesta de seguridad perimetral

Fuente: El autor

La principal ventaja de la arquitectura propuesta es que proporcionará un control centralizado de reglas y permisos aplicados, tanto en los equipos que conforman los clústeres de core, publicación y servicios internos, como en los clústeres y equipos que serán desplegados en las unidades médicas de tercer nivel (hospitales “Carlos Andrade Marín”, “Teodoro Maldonado Carbo”, “José Carrasco Arteaga”, Centro Médico “La Mariscal”) o en dependencias administrativas (edificio “Zarzuela”), lo cual permitirá al personal técnico de la institución llevar un control granular de los permisos aplicados en cada sitio. De esta manera, cada cambio deberá pasar por dos filtros, siendo el primero el administrador local de la plataforma, y el segundo y más importante, el administrador del multidominio en la DNTI.

El componente de firewall de la arquitectura se ejecutará sobre la última versión del fabricante, contando así con las últimas actualizaciones y mejoras de la misma, y con el derecho de acceso a soporte técnico por parte de representantes locales y el mismo fabricante. Adicionalmente, las licencias de la herramienta actualmente disponible podrán ser reutilizadas (puesto que pertenecen al IESS a perpetuidad), debiéndose renovar el soporte, acceso a las actualizaciones del fabricante, y mantenimiento del software.

La herramienta de filtrado de contenido permitirá controlar el acceso a sitios web, tarea que actualmente se realiza mediante una serie de servidores proxy, los cuales muchas veces presentan problemas debido a la manipulación por parte de personal no idóneo.

El componente IPS a ser desplegado en los equipos destinados a las unidades médicas de tercer nivel y dependencias administrativas permitirá aligerar el trabajo de la solución de IPS actualmente disponible en la institución, por lo que la carga del equipo IPS asignado a la protección de la Intranet de la institución será menor, debido a que parte de la misma podrá ser analizada desde los clústeres y firewalls que lo implementan.

Los componentes de antivirus y antibot brindarán una capa adicional de seguridad a los equipos de usuario final dentro de la red, ya que todo el tráfico tanto entrante como saliente

será analizado en busca de posibles infecciones de virus o acciones de comando y control sobre equipos infectados.

Tanto el gestor de reportes como el de auditoría de reglas funcionarán en conjunto con toda la solución, permitiendo llevar a cabo tareas se seguimiento, control de cambios, obtención de reportes.

Una ventaja adicional es que el personal del área de Redes de la DNTI conoce las peculiaridades del hardware, software y herramientas del fabricante de la actual solución, motivo por el cual todos los conocimientos adquiridos durante los años de explotación de la actual arquitectura serán aplicables a la nueva, requiriéndose capacitación específica respecto a las nuevas funcionalidades de la herramienta, sistema operativo y demás elementos que la componen (como por ejemplo, la gestión multidominio, reportería unificada, conciencia de identidad de aplicaciones); lo cual permitirá la efectuar las tareas necesarias para la preparación de la migración hacia la nueva arquitectura, instalación de los nuevos equipos, migración de reglas, permisos, registros y demás, puesta en funcionamiento, depuración y troubleshooting y finalmente la explotación de la nueva arquitectura en un período de tiempo corto.

La arquitectura propuesta ha sido diseñada para ser escalable y adaptable a las nuevas necesidades, apuntando a un crecimiento apreciable de los requerimientos de cómputo, tecnológicos y servicios de la institución en un período no menor a 5 años, teniendo en cuenta el aumento del parque tecnológico, aplicación de nuevas tecnologías, acceso remoto a prestadores externos, consumo de servicios por parte de entidades externas, ingreso seguro a la red tipo BYOD (Bring Your Own Device), computación móvil, investigación docente en unidades médicas, construcción e inclusión de nuevos hospitales al entorno de la DNTI, desarrollo de nuevas aplicaciones y despliegue de nuevos servicios así como otras necesidades que aparecerán en un futuro próximo, debido al abanico de servicios y responsabilidades propias de la institución.

CAPÍTULO V – CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El presente trabajo empezó teniendo como meta la realización de un análisis del estado de una arquitectura de seguridad perimetral basada en firewalls de la que es sin temor a equivocaciones, la institución más grande, y tecnológicamente, una de las más avanzadas del Ecuador.

Se efectuó un desarrollo teórico secuencial pertinente a las redes de comunicaciones y tecnologías de la información, iniciando desde algo tan básico como los modelos de referencia OSI y TCP/IP, pasando por las distintas tecnologías de red y los equipos asociados, dispositivos de seguridad de red, metodologías de diseño de redes y arquitecturas de seguridad, para luego continuar con una breve pero concisa descripción de su arquitectura actual, los riesgos a los que se encuentra expuesta, sus necesidades y amenazas.

Una vez estudiadas, se puede concluir que las metodologías expuestas han sido desarrolladas por los líderes en su ramo de la industria, y que fueron creadas en base a sus respectivas experiencias en el desarrollo de nuevas tecnologías, oferta de productos y la explotación de servicios aplicables a las tecnologías de la información y comunicaciones, siendo este entorno particularmente cambiante y exigente.

Cisco Systems pregona y dirige sus esfuerzos al diseño lógico, práctico, razonado y robusto de redes, considerando a éstas como el elemento principal de un entorno de comunicaciones eficiente y seguro. Por ello ha desarrollado varias metodologías al respecto, descritas de forma breve pero efectiva: en el presente documento a SONA, PPDIOO, Top-Down, Bottom-Up y SAFE.

Se puede concluir que la arquitectura SDP de Check Point, es a la vez una metodología, que está centrada en la planeación y creación de sistemas de seguridad perimetral basado en capas, seguros y flexibles. SDP se preocupa de la protección de todo el horizonte de red y servicios, desde una estación de trabajo de un usuario, hasta las aplicaciones y servicios ofrecidos por la institución.

IBM brinda con ISF una arquitectura capaz de integrar los ejes del negocio con los de seguridad, gracias a un modelo de Gobierno de seguridad, gestión de riesgos y cumplimiento, formado por un conjunto de dominios de seguridad, capaces de describir el entorno de una institución. Una de las grandes ventajas de esta metodología es que está en capacidad de involucrar a todos quienes forman parte del entorno tecnológico institucional, desde administradores de bienes tecnológicos, pasando por desarrolladores y llegando hacia los usuarios finales; mientras que la otra es que permite tener una visión de seguridad en término de productos y proveedores neutrales, aplicable a los marcos regulatorios TOGAF, COBIT e ISO27002, así como al estándar PCI-DSS.

Una vez comparadas las arquitecturas y metodologías de los fabricantes, sus características, bondades y ventajas, se concluye que SDP deberá ser la arquitectura sobre la cual se planteará el nuevo modelo de seguridad perimetral.
Cabe mencionar que la arquitectura de seguridad perimetral actualmente disponible en la institución, se encuentra basada en SDP, siendo éste un punto a favor respecto al planteamiento de la nueva arquitectura, así como saber que el personal técnico que administra y opera los equipos de conforman la actual, requerirán un menor tiempo de adaptación y aprenderán pronto las bondades y características de los nuevos equipos.

Se concluye también que, pese a ser una alternativa aplicable y económicamente viable, la repotenciación de la arquitectura actual de seguridad perimetral no es la mejor opción, debido a las nuevas necesidades y amenazas de la institución, mismas que fueron expuestas en el capítulo correspondiente.

Según lo expuesto en el capítulo correspondiente, la arquitectura de seguridad perimetral actual es insuficiente ante las necesidades actuales de la institución, y debe ser reemplazada a la brevedad posible.

Todo sistema de seguridad es tan fuerte como su eslabón más débil.

La información de una organización como el IESS tiene un valor incalculable, y es por ello que se la debe proteger contra las distintas amenazas a las que se encuentra expuesta, examinando las vulnerabilidades y minimizando los riesgos.

RECOMENDACIONES

Establecer un lineamiento tecnológico a largo plazo, en el que la arquitectura de seguridad perimetral sea considerada como prioritaria, de tal modo que la misma siempre se encuentre actualizada, esté en capacidad de cumplir su función, y su mejora o reemplazo no dependa de terceros factores, tales como cambio de autoridades, planificación económica, entre otros.

Realizar auditorías periódicas de los distintos equipos de cómputo de la institución, lo que permitirá tener conocimiento del estado de los mismos y saber cuáles son las medidas a tomarse. Esto permitirá también proteger el perímetro de seguridad.

Realizar procesos de hardening en los distintos dispositivos de red responsabilidad de la institución en el ámbito de su competencia; tales como computadores personales y laptops, servidores de red y de aplicaciones específicas, switches, entre otros.
Esto puede referirse a, pero no está limitado a la aplicación y depuración de listas de control de acceso en switches, y servidores, ejecutar configuraciones específicas de seguridad en equipos, instalación de antivirus, etc.

Solicitar al proveedor del servicio de enlace de datos e Internet, la aplicación de listas de control de acceso en sus enrutadores, de tal manera que éste se convierta en una de las principales líneas de defensa del perímetro y barrera ante ataques y otros eventos similares.

Establecer y socializar la propuesta mediante el correspondiente proyecto, teniendo en cuenta a los distintos actores, sus labores y responsabilidades dentro de la institución, desde los directores hasta los usuarios finales, ya que de esta manera los involucrados tendrán conciencia respecto a los recursos informáticos de la institución.

Informar y capacitar a los distintos usuarios de la red de la institución acerca de las políticas de buen uso de los recursos informáticos.

Considerar que de acuerdo a la constante evolución tecnológica, oferta de nuevos servicios y facilidades de acceso a los recursos de cómputo, cada vez se hace más complejo el poder determinar dónde se encuentra el perímetro informático. Se recomienda establecer y mejorar las políticas de acceso a los mismos, de tal manera que la arquitectura de seguridad esté siempre en capacidad de controlarlos.

BIBLIOGRAFÍA

Alani, M. M. (2014). *Guide to OSI and TCP/IP Models.* London: Springer.

Buecker, A., Andreas, P., & Paisley, S. (2008). *Understanding IT Perimeter Security.* New York: IBM ITSO.

Buecker, A., Arumkumar, S., Blackshaw, B., & Borrett, M. (2013). *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security.* New York: IBM ITSO.

Buecker, A., Dobbs, M., Filip, W., Finley, C., & Jeremic, V. (2011). *Network Intrusion Prevention Design Guide - Using IBM Security Network IPS.* New York: IBM ITSO.

Check Point Software Technologies, L. (2014). *Software Defined Protection- Enterprise Security Blueprint.* San Carlos: Check Point Software Technologies, Ltd.

Convery, S. -T. (2001). *Cisco SAFE.* San José: Cisco Press.

Dulaney, E. -E. (2014). *CompTIA Security+ Study Guide.* Indianapolis: John Wiley & Sons, Inc.

Gheorghe, D. (2012). *Cisco CCDA Simplified - Study Guide.* London: Reality Press Ltd.

Matos da Silva Pires de Moraes, A. (2011). *Cisco Firewalls.* Indianapolis: Cisco Press.

Oppenheimer, P. (2011). *Top-Down Network Design.* Indianapolis: Cisco Press.

Tittel, E. (2012). *Unified Threat Management for Dummies.* New Jersey: John Wiley & Sons, Inc.