UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

BUENAS PRÁCTICAS EN LA ADMINISTRACIÓN DE SEGURIDAD PERIMETRAL DE UN FIREWALL EN UNA EMPRESA DEL SECTOR DE TELECOMUNICACIONES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADO POR:

Tito Alvaro Choque Carlos

LIMA – PERÚ

2014

DEDICATORIA

Este trabajo está dedicado a mi madre Marina Carlos y a mi padre Tito Choque quienes gracias a sus enseñanzas de día a día forjan en mí una gran persona.

Gracias a mis hermanos Lidia, Victor y Cesar que a través de sus consejos y estilos de vida peculiares ayudan a llevar mi vida de una manera feliz y original.

No puedo olvidarme de mis adorables sobrinas Diana, Fiorella y Cinthya con quienes la vida se hace más alegre.

También agradecer a mi amor Laura quien día a día endulza mi vida.

ÍNDICE

LISTA DE FIGURAS

RESUMEN

En la actualidad las empresas tienen la obligación de agilizar el tiempo de interacción sobre los procesos que manejan, muchos de estos procesos serán manuales, otros operativos y otra gran parte necesariamente tendrán que ser digitales, esto con la finalidad de mejorar los tiempos de respuesta a través de la automatización de los equipos digitales, computadoras, impresoras, teléfonos digitales, Smartphone, máquinas industriales, etc. así como también posicionar la empresa dentro de la internet para poder llegar a más clientes.

En este gran esfuerzo de mantener una parte de sus procesos de manera digital obligará a las empresas a comunicarse a través de la internet, motivo por el cual, algunas en su esfuerzo de agilizar sus procesos caerán en el peligroso círculo vicioso de obviar la seguridad para no generar demoras ni controles que les demanden análisis de tiempo así como detener proyectos por obviar la seguridad informática en los cuales se desea ingresar de manera más agresiva hacia la internet tan solo por la obligación de llegar a los clientes.

Actualmente las empresas libran una guerra sin cuartel por tratar de posicionar su marca en internet, para esto se lanzan de manera agresiva a digitalizarse sin un análisis minucioso de seguridad sobre sus proyectos en internet, una muestra de esto es la gran cantidad de vulnerabilidades encontradas desde el primer día de ubicar sus páginas webs, aplicaciones digitales, servicios en la web, servicios de correo, servicio de archivos etc. dentro de la internet.

El informe anual de seguridad de Cisco del 2013 muestra como las vulnerabilidades siguen manteniéndose pero ahora cambian los métodos,

muchos de estos ataques se desarrollan de manera más ordenada, en la mayoría de las casos los atacantes comparten su información con la finalidad de ser mejorada por otros atacantes lo cual genera un círculo de mejora sobre la herramienta de ataque.

Ante estas amenazas las empresas deben tener una buena protección de la red privada de su organización, actualmente el equipo de red que ayuda a la protección de ataques y control es el firewall, motivo por el cual las empresas están en la obligación de implementar equipos de seguridad dentro de su organización los cuales permitan proteger a la organización de los ataques externos.

También debemos resaltar que no solo basta con la implementación de instalar los equipos de seguridad, estos también deben estar configurados correctamente para poder tener un correcta protección, motivo por el cual nosotros recomendamos el uso de estándares y buenas prácticas para poder tener una mejor defensa perimetral de red, en la cual la empresa no pueda ser víctima de los atacantes.

DESCRIPTORES TEMÁTICOS

- Seguridad Perimetral
- Ataques de red
- Firewall
- UTM

INTRODUCCIÓN

Las empresas de telecomunicaciones que pueden alquilar servicios de seguridad como firewall, ips, router, antispam, balanceadores de carga. etc. tienen la difícil tarea de tratar de entender las configuraciones en los equipos de seguridad que alquilan a sus clientes, esto para mantener una configuración óptima de la red de la organización, con la finalidad de reducir el riesgo en el cual los servicios publicados de la organización puedan ser explotados.

Para esto vamos a recomendar una serie de buenas prácticas para poder minimizar el riesgo en el cual la red interna de una organización pueda ser vulnerada, para esto atacaremos dos puntos principales:

Optimizar el uso de ancho de banda hacia INTERNET.
Estructurar las políticas de firewall, lo cual permitirá al administrador de red realizar configuraciones de manera rápida y segura.

En este escenario es de vital importancia mitigar el riesgo ocasionado por una mala configuración en las reglas del firewall y la correcta aplicación de las firmas del módulo IPS, motivo por el cual es importante definir que es un firewall, debido a que el firewall es la primera línea de defensa de los atacantes que deseen ingresar a la red de la organización. También empezaremos a aplicar las firmas IPS proveniente del UTM, las firmas IPS nos permite realizar una protección íntegra bloqueando los posibles ataques que esta detecta, esto es fundamental cuando se publican servicios hacia internet.

En la actualidad la escala de ataques en la red ponen en peligro la continuidad de los negocios en internet, motivo por el cual los tipos de

ataques como la Denegación de Servicios, Spam, Phishing, etc. deben ser trabajados con equipos appliance dedicados, esto debido a la gran cantidad de recursos que consumen estos ataques, motivo por el cual el trabajo buscará lo siguiente:

- Recomendaciones en la configuración de las reglas, para un mejor control de los usuarios y una restricción óptima de las redes del firewall.
- Recomendaciones para poner las firmas ips, que puedan detener los ataques de los servicios publicados hacia internet.

Esto con la finalidad de no sobrecargar los servicios a través de la aplicación de todos los módulos que el UTM nos puede brindar.

En el capítulo 4 podremos encontrar las recomendaciones para las configuraciones de las reglas del firewall. Para luego proceder a buscar en el firewall los posibles errores de configuración que se pueda encontrar en el firewall, para esto como siempre se recomienda empezar a revisar cómo se encuentran declarados los parámetros, esto debido a que muchos de estos pueden estar declarados de manera general o por defecto y esto en muchos casos son los principales errores de configuración debido a que los parámetros se encuentran mal declarados o reglas del firewall registradas de forma ambigua.

CAPÍTULO I: PENSAMIENTO ESTRATÉGICO

1.1 DIAGNÓSTICO FUNCIONAL

ORGANIZACIÓN

En Tgestiona Perú deseamos ofrecerle a las empresas líderes como la suya la oportunidad de rentabilizar sus operaciones y optimizar su negocio a través de la tercerización de sus áreas administrativas. Así, su empresa se podrá concentrar en las actividades centrales de su negocio y delegar los temas de soporte a las operaciones en manos de especialistas.

CLIENTES

Entre los clientes principales tenemos a los siguientes:

MOVISTAR
ATENTO
DHL
ONPE
INTERBANK
MIBANCO
RIPLEY
RIMAC
TELEFÓNICA

EDELNOR
SEDAPAL
OSINERG

PROVEEDORES

Debido a que Tgestiona es una empresa que se encuentra ubicada en el sector de la tercerización en su gran mayoría de procesos tecnológicos, esta tiene que buscar los mejores proveedores internacionales para entregar un mejor servicio a sus clientes, entre los principales proveedores tenemos:

- Microsoft
- Cisco
- Oracle
- SAP
- Telefónica

PRODUCTOS

Tgesitona es una organización en la cual la mayoría de sus productos ayuda a los clientes a atender procesos dentro de su organización, dentro de sus principales productos tenemos:

- Servicios de Gestión Humana
- Servicios de Facilites Management
- Servicios de Recaudación y Cobranza
- Servicios de Tecnologías y Sistemas de Información
- Servicios de Consultoría y Soluciones de Negocios
- Servicios de Gestión Logística
- Servicios de Contabilidad, Tesorería y Tributos
- Servicios de Gestión de Seguridad Logística

1.2 DIAGNÓSTICO ESTRATÉGICO

MISIÓN

Somos una organización internacional especializada en brindar servicios de soluciones de negocio confiables, eficientes y oportunas, para permitir a nuestros clientes enfocarse en las actividades que les generen mayor valor. Lo hacemos con un equipo humano comprometido y capacitado, asegurando un crecimiento sostenido y rentable para nuestros accionistas y contribuyendo al desarrollo de nuestros empleados y de la sociedad.

VISIÓN

Ser la organización líder en la prestación de servicios de soluciones de negocio a nivel nacional e internacional, reconocido por contribuir al crecimiento sostenido y rentable de nuestros clientes y de nuestro negocio, y al desarrollo de nuestro equipo humano y de la sociedad.

VALORES

- Imparcialidad
- Credibilidad
- Respeto
- Innovación
- Confianza

1.3 ANÁLISIS INTERNO

FORTALEZAS

- Ser una empresa líder en volumen de actividad, acostumbrados a dar servicio a empresas con gran volumen de negocio.
- Permiten alcanzar la excelencia tecnológica. Minimizar los costes de las nuevas tecnologías y eliminar inversiones en sistemas y en actualización de versiones. Disfrutar de sistemas de soporte de última generación.
- Tener una amplia presencia internacional, especialmente en Latinoamérica donde contamos con sedes en Brasil, Argentina, Chile y Perú.
- Precios competitivos para todos los servicios ofertados.
- Poseer un amplio catálogo de servicios que nos permite cubrir la gran diversidad de necesidades de nuestros clientes.
- Ofrecer un servicio eficiente y de calidad basado en las mejores prácticas y la homogeneización de los procesos, sujetos a mejora continua y soportada por la tecnología más adecuada, según cada caso.
- Disponer de un amplio equipo de profesionales, con expertos asesores en cada materia.

DEBILIDADES

- Falta de publicidad en los medios.
- Se tiene productos con características que no se diferencian.
- Se observa descontento por los salarios bajos.

- Los contratos son establecidos por meses.

1.4 ANÁLISIS EXTERNO

OPORTUNIDADES

- El sector de TI en el Perú crece cada vez más.
- El mercado de seguridad está empezando a formarse.
- Se observa una fuerte tendencia a tercerizar los servicios de TI.
- Cuenta con el respaldo de telefónica.

AMENAZA

- Se observa que hay empresas posicionadas en el mercado.
- Se observa una competencia muy agresiva.
- Los contratos pueden terminar en cualquier momento.

CAPÍTULO II: MARCO TEÓRICO

2.1 INTERNET

Actualmente el internet es una herramienta fundamental para que todas las personas, organizaciones, empresas, estado, etc. puedan mantenerse comunicados a través de los equipos de red para poder satisfacer las diferentes necesidades a través de la comunicación.

La internet es un conjunto de redes interconectadas la cual permite la comunicación a través del protocolo TCP/IP, a través de la internet las personas pueden comunicarse de una manera rápida, actualmente el uso de las páginas webs, servicios de correos, mensajería instantánea, visualización de videos, etc. son parte del tráfico que fluye en internet.

Actualmente la INTERNET es de uso estatal, militar, empresarial y civil, pero originalmente INTERNET no nace como un proyecto para el uso general, este se remonta a la creación del proyecto ARPANET (1), el proyecto ARPANET fue creado en septiembre del 1969 por la organización ARPA, el proyecto ARPANET fue un encargo del Departamento de Defensa de los Estados Unidos, el proyecto ARPANET se crea por la necesidad de mantener la comunicación digital entre las organizaciones militares después de poder sufrir un potencial ataque de una bomba nuclear, recordemos que en esta época Estados Unidos se encontraba en la época de la GUERRA FRÍA contra su antiguo rival de la época quién era la URSS, en esta época el

temor principal era un posible conflicto bélico en la cual ambos bandos se lanzasen bombas nucleares lo cual para el caso de Estados Unidos podría dejar incomunicado a los grupos militares, esto motivó principalmente al desarrollo una red que mantuviese comunicado a las organizaciones militares a pesar de sufrir un ataque nuclear.

Como toda tecnología recién creada la ARPANET empezó a sufrir ataques informáticos, los militares preocupados por sufrir algún tipo de espionaje o a ataque informático a través de la ARPANET decidieron crear una red llamada MILNET, luego con el nombre de ARPANET-INTERNET se orientó a la investigación.

En 1984 la Fundación Nacional para la Ciencia crea su red informática denominada NSFNET para luego en 1988 decidirse a utilizar como backbone a ARPANET-INTERNET. En febrero de 1990 se decide desmontar ARPANET debido a la obsolescencia y dejar libre a INTERNET, para esto el Pentágono decide encargar la gestión de INTERNET a la Fundación Nacional para la Ciencia, luego con la desregularización de leyes sobre la INTERNET y el creciente uso de ordenadores motivo a que se privatice el uso de INTERNET a las empresas privadas, fue a partir de este momento que la INTERNET empieza a crecer y será la base para que los ordenadores puedan estar interconectados.

2.2 SEGURIDAD INFORMÁTICA

Actualmente con la masificación del uso de internet en las pc, servidores, celulares, etc. para el uso desde las actividades cotidianas, empresariales y gubernamentales la INTERNET empieza a ser un objetivo fundamental para los atacantes, pero esto no empezó ahora, esto viene desde la creación de la red ARPANET, para esto mostraremos los ataques informáticos más importantes en los inicios de la INTERNET:

- Desarrollo del juego CoreWars. 1960

  En realidad, CoreWar no fue un virus informático, sino más bien un juego. CoreWars afectaba la memoria de las computadoras y podía auto replicarse. Este juego fue desarrollado por un grupo de programadores de la compañía Bell Computer, y era una sencilla aplicación que competía con el resto de los programas que se ejecutaban en una computadora con el fin de obtener el control absoluto de la memoria del equipo.

- Creación de Creeper. 1971

  Creeper fue el primer virus que incluía las características típicas de un verdadero malware. Creado por Bob Thomasy, fue especialmente escrito para atacar al sistema operativo Tenex. Cuando Creeper llegaba a una computadora, por lo general por intermedio de los nodos de la ARPANET, el malware se auto ejecutaba y comenzaba a mostrar el siguiente mensaje: "I'm the creeper, catch me if you can!", que en español sería algo así como "¡Soy la enredadera, atrápame si puedes!".

- Elk Cloner 1982

  Es el primer virus conocido que tuvo una expansión real y no como un concepto de laboratorio. Rich Skrenta, un estudiante de instituto de 15 años, lo programó para los Apple II. Elk Cloner se propagaba infectando los disquetes del sistema operativo de los computadores Apple II. Cuando la computadora arrancaba desde un disquete infectado, también lo hacía el virus de forma automática. Se diseñó para ser molesto puesto que después de un número determinado de arranques del sistema, el virus mostraba un pequeño poema.

- El Primer Gusano: Gusano de Morris 1988

  El Gusano MORRIS fue el primer ejemplar de malware auto replicable que afectó a Internet. El 2 de noviembre de 1988, durante unas horas, aproximadamente el 10% (6000 equipos, incluidos los de la NASA) de todas las máquinas de Internet se vieron afectadas por este 'gusano'. El programa intentaba averiguar las contraseñas de otras computadoras, usando una rutina de búsqueda que permutaba los nombres de usuarios conocidos, una lista de las contraseñas más comunes y también búsqueda al azar. Llevó a su creador a ser la primera persona condenada por la justicia bajo un delito de fraude y de abuso informático. Ahora Morris es profesor del MIT.

- CIH 1998

  Daño estimado: 20 a 80 millones de dólares, sin contar el precio de la información destruida. CHI es reconocido como uno de los más peligrosos y destructivos virus jamás vistos. El virus infectó los archivos ejecutables de Windows 95,98 y ME y fue capaz de permanecer residente en memoria de los ordenadores infectados para así infectar otros ejecutables. Lo que lo hizo tan peligroso fue que en poco tiempo afectó muchos ordenadores, podía reescribir datos en el disco duro y dejarlo inoperativo.

- Klez, un virus que se "actualiza". 2001

  A través de un correo infecta, se replica y se reenvía a la lista de contactos de la víctima. Es capaz de anular una CPU, aunque dependiendo de la versión logra alojarse como un Troyano, e incluso aparecer como una herramienta del propio Antivirus. Instauró el "spoofing" como moda, lo que en palabras simples es un correo suplantando un remitente.

- Código Rojo y Código Rojo 2, vulnerabilidad absoluta. 2001
  Este gusano se hizo popular mediante un ataque de denegación de servicio (DDoS) a la Casa Blanca. A través de una vulnerabilidad del sistema operativo, el gusano se instalaba en los equipos que no tenían un parche de seguridad de Microsoft, dejando al usuario sin control de su equipo, quedando en completa vulnerabilidad ante la persona que mandó el virus. Su creador no es conocido, aunque se originó en China y ya ha costado más de US$ 2.750 millones en pérdidas.

- SQL Slammer/Zafiro, el más rápido de la historia. 2003
  Sólo 10 minutos tardó en dejar la red mucho más lenta. Su ataque fue increíblemente agresivo, pues aprovechó una falla en la base de datos del servidor SQL de Microsoft, saturando archivos en todo el mundo. Entre sus víctimas "ilustres" destacan el servicio ATM del Bank of América, el servicio de 911 de Seattle y la cancelación de vuelos de Continental Airlines. No tiene "autor" conocido. Generó más de US$ 1200 millones en pérdidas.

- MyDoom, el peor "gusano" de todos 2004
  Tal como los demás representantes de los "worms", crea una puerta trasera para acceder al S.O. En su versión más común, tiene dos etapas. Primero, genera un ataque DDoS, que causó notoriedad en 2004, y luego busca distribuirse a través de las cuentas de correo. Además, envía una petición a un motor de búsqueda externo, por lo que en su momento logró generar algunos problemas de velocidad en Google. Su impacto en la industria es de US$ 38.500 millones, y hasta ahora no tiene a un creador conocido. Fue considerado por Microsoft el Virus más destructivo de la historia, destruía el sector Zero del disco y para ese entonces, no se tenía arreglo.

- Commwarrior-A 2005

  Es el primer virus conocido de teléfono móvil capaz de replicarse a través de mensajes MMS. Originalmente dirigido a Symbian Serie 60 no dieron lugar a una epidemia. Sin embargo, su capacidad de propagarse a través de servicio de mensajería multimedia (MMS) preocupó a algunos expertos en el momento de su descubrimiento. Se cree que el virus se originó en Rusia debido a que contenía el texto que indica "HET OTMOP03KAM!" que se podría traducir como 'No a los muertos cerebrales'.

- Leap-A/Oompa-A, 2006

  Diseñado para atacar los sistemas Mac. Leap-A (también conocido como Oompa A) entró en escena usando el iChat para propagarse en equipos vulnerables. Tras infectar, buscaba en los contactos del servicio de mensajería y enviaba un mensaje a cada persona con un archivo corrupto en forma de una imagen JPEG. Aunque no generó tantos problemas ni costos económicos, demostró que Mac no está inmune al software malicioso.

- Sirefef, el rootkit que zombifica tu PC (Botnet) 2012

  Escurridizo y complejo, Sirefef, es conocido también como ZeroAccess. Es un virus cuyo propósito principal es convertir el PC infectado en un nodo de una enorme red de ordenadores (botnet). El propósito de la red infectada es ganar dinero haciendo clic en anuncios publicitarios o instalando falsos antivirus que solicitan dinero a cambio de limpiezas inmediatas y milagrosas. El usuario no se da cuenta de nada, pero el uso de la conexión es constante, y puede llegar a 32GB mensuales de más (equivalente a 45 películas). Y en el peor de los escenarios posibles, el PC zombi puede participar en acciones de ciberguerra.

- Una compañía con sede en Holanda lanza un ataque Dos. 2013
  Dicha compañía es yberbunker, una empresa holandesa de alojamiento web. Spamhaus, organización que trabaja en colaboración con proveedores de correo para luchar contra el correo no deseado, incluyó a Cyberbunker en la lista negra de organizaciones dedicadas al envío de correo electrónico no deseado. Como consecuencia (represalia) de lo anterior Cyberbunker ha llevado a cabo un ataque masivo de denegación de servicio que ha alcanzado los 300 GB de información por segundo contra los sistemas de la organización antispam, provocando no solo un colapso de Spamhaus sino una congestión en la red de carácter mundial.

2.3 FIREWALL

El firewall también denominado cortafuegos es un dispositivo que nos permite controlar el acceso de entrada y salida en una red, esto con la finalidad de mantener afuera a los atacantes, pero la idea de un firewall o no es algo nuevo, el ser humano desde las épocas medievales utilizaban los muros para poder proteger y controlar a la población, un gran ejemplo de esto es la gran muralla china la cual protegía al reino chino de las invasiones mongoles, quienes eran sus feroces enemigos, también debemos recordar a las ciudades medievales europeas las cuales se encontraban rodeadas de muros fortificados que les permitía protegerse de las invasiones de los enemigos.

En la actualidad el firewall permite a una organización poder defenderse de los potenciales ataques que se encuentran en la red, como se sabe actualmente la INTERNET es un lugar inseguro en el cual las organizaciones pueden ser víctimas de un robo de información y/o un ataque.

Para esto describiremos las generaciones de los firewall:

Primera generación

Esa primera generación tenía un filtrado de paquetes totalmente básico. El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí (por lo general utiliza una combinación del emisor del paquete y la dirección de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto).

Segunda generación

Esta segunda generación de cortafuegos tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por los cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

Tercera generación - cortafuegos de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI. En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete. El mejor ejemplo de cortafuegos de aplicación es ISA (Internet Security and Acceleration).

2.4 GESTIÓN UNIFICADA DE AMENAZAS

Los sistema firewall con Gestión Unificada de Amenazas (UTM) Protección desde dentro y desde fuera nacieron en 2007 y se presentaron como la mejor solución de seguridad para las pymes por tratarse de tecnologías integradas que cubren todas las necesidades básicas de protección. Cinco años de crecimiento vertiginoso han convertido al mercado **UTM** en unos de los más candentes del mundo de las telecomunicaciones.

Según un análisis titulado Cuadrante Mágico sobre herramientas de Gestión Unificada de Amenazas (UTM) realizado por Gartner, compañía especializada en consultoría TIC a nivel mundial, el mercado UTM se valoró en 2011 en nada menos que 1.280 millones de dólares. Y las previsiones apuntan a que en 2017 habrá crecido un 15% más. Un crecimiento espectacular en pocos años.

El secreto: integrar múltiples funciones de seguridad en un único dispositivo cubriendo las exigencias básicas de protección integral. Con una combinación de firewall, del protocolo de capa de conexión segura (Secure Sockets Layer – SSL) de VPN (Redes Privadas Virtuales) y del sistema de prevención de intrusiones IPS (Intrusion Prevention System), se proclamó como la mejor solución para las pymes .Y estaba en lo cierto porque responde a necesidades que algunas empresas no se había llegado a plantear, gracias a un amplio abanico de modelos, que soportan múltiples capacidades de gestión y de informes y están diseñados para un fácil manejo.

Las funciones básicas de seguridad de un sistema UTM son:

- Prevención y detección de intrusos en la red centrada en el bloqueo de ataques contra PC y servidores (IDS/IPS).
- Detección y bloqueo de antivirus y antimalware
- Filtrado antispam
- Filtrado del contenido web y URL
- Funciones habituales de firewall (cortafuegos)
- Acceso remoto y site-to-site (de sitio a sitio) con soporte en VPN y SSL (basado en navegador).

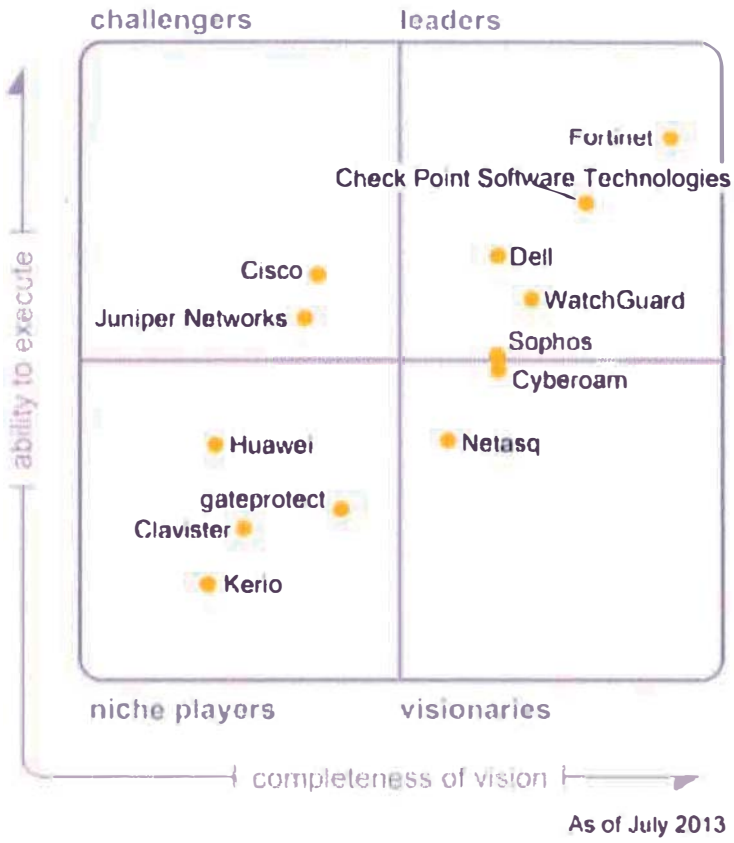
Sin embargo, la alta escalabilidad y capacidad integradora de esta tecnología y el rápido desarrollo de funciones complementarias han conseguido que la Gestión Unificada de Amenazas supere las fronteras del mercado pyme y dé el salto al de las grandes empresas, que comienzan a sustituir sus sistemas de seguridad de red por soluciones UTM que pueden implementar con las funciones que más les convengan. Esta tendencia denominada XTM (eXtensible Threat Management) se configura como la nueva generación de sistemas de Gestión Unificada de Amenazas.

Las soluciones UTM-XTM cuentan, además de las funciones básicas de un sistema UTM, con una variedad creciente de características, entre las que destacan:

- Seguridad en la mensajería.
- Cortafuegos (firewall) de aplicaciones web
- Seguridad y filtrado antispam del correo electrónico
- Prevención de pérdida de datos
- Gestión centralizada a través de interfaces gráficas
- Monitorización de la latencia y correlación de eventos
- Automatización de autenticación de usuarios de red

El desarrollo de estas nuevas funcionalidades permite a las plataformas XTM llevar los sistemas UTM mucho más allá incorporando funciones de red y de gestión, y opciones de seguridad avanzadas. De forma que las organizaciones puedan configurar la seguridad que mejor se acople a sus necesidades.

Según el cuadrante de Garnert ubicado en la figura 1 Fortinet se ubica como la empresa que tiene el mejor UTM en el mercado a nivel mundial, así como su agresiva política de innovación de sus productos a través de sus firmwares, motivo por el cual trae mucha expectativa al mercado de la seguridad de redes.



Source: Gartner July 2013)

Figura 1: Cuadrante de Empresas de Seguridad de Red

2.5 SISTEMA DE PREVENCIÓN DE INTRUSOS

Los sistemas de prevención de intrusiones, también conocidos como sistemas de prevención y detección de intrusiones, son dispositivos de seguridad de red que supervisan la red y/o actividades maliciosas de la red. Las principales funciones de los sistemas de prevención de intrusiones son identificar las actividades maliciosas, registrar la información sobre esta actividad, intentar bloquear/detenerlo y denunciarlo.

Los sistemas de prevención de intrusiones se consideran extensiones de los sistemas de detección de intrusos, ya que las actividades tanto tráfico en la red y/o sistema de actividad maliciosa. Las principales diferencias son, a diferencia de los sistemas de detección de intrusos, los sistemas de prevención de intrusiones se colocan en línea y son capaces de prevenir

activamente/bloquear intrusiones que se detectan. Más específicamente, IPS pueden tomar acciones como el envío de una alarma, dejando caer los paquetes maliciosos, restablecer la conexión y/o bloquear el tráfico desde la dirección IP infractora. Un IPS también puede corregir los errores de comprobación de redundancia cíclica, unfragment flujos de paquetes, evitar problemas de TCP secuenciación, y limpiar el transporte no deseados y opciones de capa de red.

Clasificaciones

Los sistemas de prevención de intrusiones se pueden clasificar en cuatro tipos diferentes:

- Sistema de prevención de intrusiones basado en red: controla toda la red para el tráfico sospechoso mediante el análisis de la actividad de protocolo.

- Los sistemas de prevención de intrusiones inalámbricas: monitorear una red inalámbrica para el tráfico sospechoso mediante el análisis de protocolos de redes inalámbricas.

- Análisis de comportamiento de red: analiza el tráfico de red para identificar las amenazas que generan los flujos de tráfico inusuales, tales como ataques de denegación de servicio, ciertas formas de malware y violaciones de política.

Organiza el sistema de prevención de intrusiones basado en un paquete de software que controla un único host para detectar actividades sospechosas mediante el análisis de los acontecimientos que ocurren dentro de ese host.

Métodos de detección:

La mayoría de los sistemas de prevención de intrusos utilizan uno de los tres métodos de detección: detección basa en firmas, anomalía basada en estadísticas de detección y de estado de detección de análisis de protocolo.

- Detección basada en firmas: este método de detección utiliza firmas, que son patrones de ataque que están pre configurados y predeterminado. Un sistema de prevención de intrusiones basado en la firma controla el tráfico de la red para los partidos a estas firmas. Una vez que se encuentra una coincidencia el sistema de prevención de intrusiones toma la acción apropiada. Las firmas se pueden explotar o basado en la vulnerabilidad basada. Aprovechar las firmas basadas en analizar los patrones que aparecen en las hazañas de ser protegidos en contra, mientras que las firmas basadas en vulnerabilidades analizar vulnerabilidades en un programa, su ejecución y las condiciones necesarias para explotar dicha vulnerabilidad.

- Anomalía basada en estadísticas de detección: este método de detección se basa en la línea base del rendimiento de las condiciones medias de tráfico de red. Después se crea una línea de base, el sistema intermitentemente muestras de tráfico de red, utilizando el análisis estadístico para comparar la muestra a la línea de base conjunto. Si la actividad está fuera de los parámetros de referencia, el sistema de prevención de intrusiones toma la acción apropiada. La intrusión en particular en este caso, supervisa los usuarios y los comportamientos de la red.

- De estado de detección de análisis de protocolo: este método identifica las desviaciones de los estados del protocolo mediante la comparación de eventos observados con "perfiles predeterminados de definiciones generalmente aceptadas de la actividad benigna."

2.6 GUÍAS DE CONFIGURACIÓN DE SEGURIDAD PERIMETRAL

Para poder realizar una buena configuración en el firewall se debe buscar una estándar el cual nos pueda recomendar las buenas prácticas asociadas a los permisos y configuración de un firewall, para esto citaremos el estándar de la **NIST (N**ational Institute International **T**echnology), estas recomendaciones realizadas por el **NIST** serán un apoyo para realizar una configuración que pueda mitigar los riesgos de sufrir un ataque externo o ataque interno, en esta guía de recomendación de configuración de firewall podremos visualizar recomendaciones por parte del **NIST**.

En esta guía nosotros podemos comprender el funcionamiento del firewall, esto nos ayudará a entender los componentes internos que pueden ser aprovechados para obtener una mayor seguridad aplicada a la red de una empresa, como Application-Proxy Gateways, Unified Threat **M**anagement (UTM), Web Application Firewalls.

Esta guía nos brinda una seria de recomendaciones al momento de generar las políticas del firewall basadas en **IP**, protocolos, aplicaciones, etc. En la actualidad los administradores de red y/o del firewall tienen la costumbre de generar políticas en el firewall basadas en ip, esto sumado al abandono y/o falta de revisión de las reglas genera ips libres con permisos en algunos casos totalmente libres.

Pero nuestra configuración sobre las políticas del firewall es una empresa la cual ya tiene instalado su respectivo firewall, pero ¿qué

sucedería si una organización desea implementar un firewall para la seguridad de su red?, para esto la guía nos permite identificar los pasos necesarios para una correcta implementación de un firewall, como el Planeamiento, Configuración, Test, Desplegar y Administrar. Con estas fases nosotros podemos realizar una correcta implementación del firewall, debido a que la implementación de un firewall en una red puede ocasionar la perdida de conectividad hacia las diferentes redes como DMZ, INTERNET, VPN, etc. de una organización.

CAPÍTULO III: PROCESO DE TOMA DE DECISIONES

3.1 IDENTIFICACIÓN DEL PROBLEMA

CONTEXTO

El cliente de Tgestiona es una empresa la cual su principal negocio está en la venta de sus productos industriales, motivo por el cual gran parte de sus servicios está orientado a la venta de sus productos y asesoría del uso, motivo por el cual los temas relacionados a la tecnologías de información son el soporte de la organización.

Como la gran mayoría de las organizaciones buscan la ayuda de la resolución de ciertos procesos en los cuales son parte de los procesos de soporte que ayudan a la organización al funcionamiento de las operaciones del día a día, para este caso el cliente busca que la seguridad perimetral de su red sea también vista por sus proveedores, y como toda empresa que desea operar de acuerdo a las exigencias de sus clientes y la alta competitividad de la competencia se observa que en muchos casos se obvia la correcta configuración de seguridad de perimetral.

Como la gran mayoría de empresas es comprensible la exigencia de las áreas de ventas por concretar las ventas con más clientes en el menor tiempo posible, los cuales en su

mayoría se mejoran y se acortan gracias a la tecnología de la información. Este esfuerzo de agilizar los tiempos de respuesta a través de la tecnología de información recae en las áreas de tecnología de información, quienes con el día a día se tratan de resolver estos problemas a veces dejando de lado la seguridad de la red, como también el desempeño de la red para poder conectarse a internet, además de la exposición a las vulnerabilidades a la cual está sometido a publicar servicios, como página web, correo, etc.

PROBLEMA PRINCIPAL

El cliente de Tgestiona tiene lentitud cuando los usuarios desean navegar hacia INTERNET.

El cliente de Tgesitona no tiene una estructura parametrizada en el firewall para poder realizar la configuración de reglas de manera rápida y segura.

PROBLEMÁTICA

Antes de empezar a revisar las políticas de seguridad del firewall debemos revisar cómo se encuentra la topología de red actual, motivo por el cual mostraremos la topología de red de la organización actualmente.

Topología de red

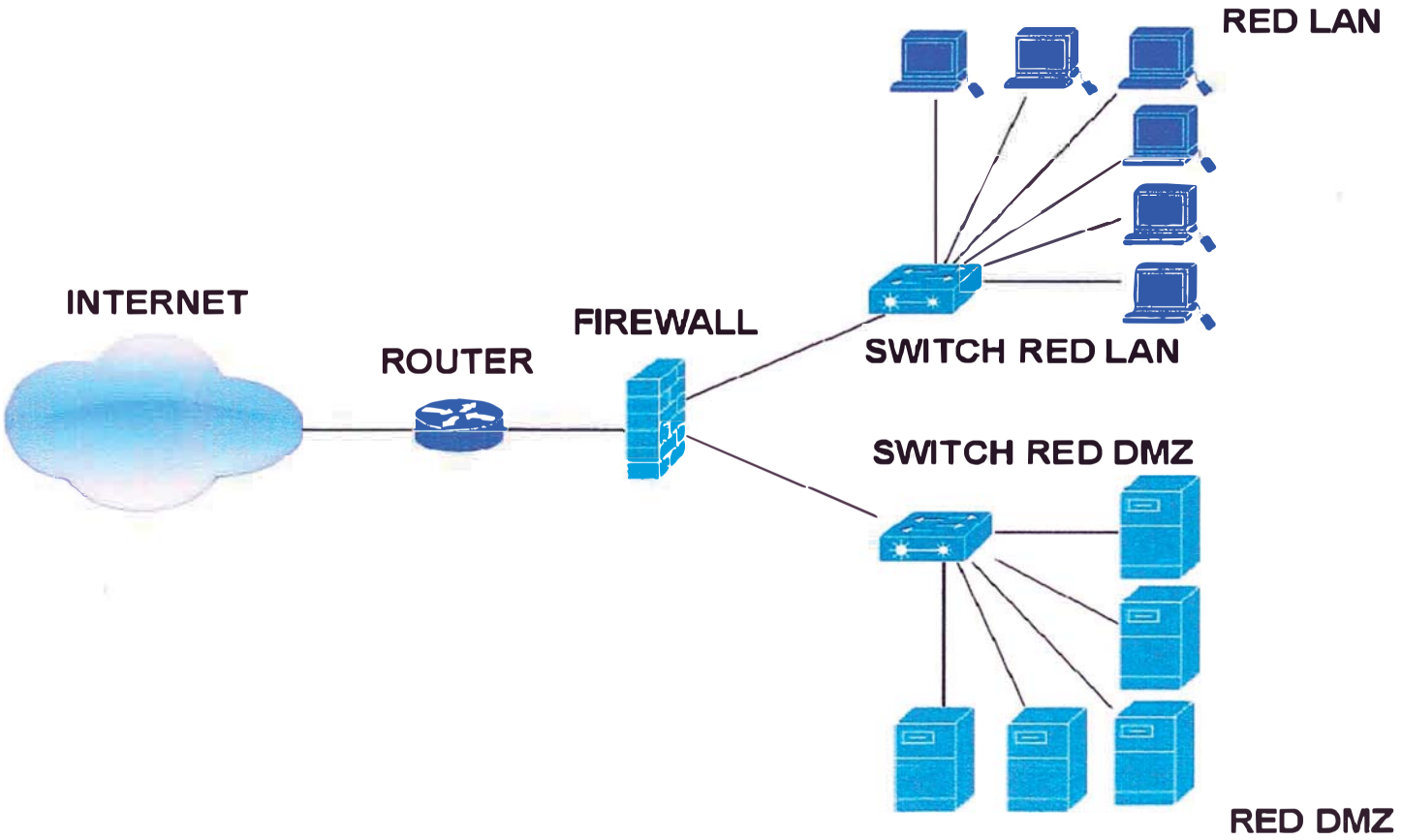


Figura 2: Topología de red del cliente

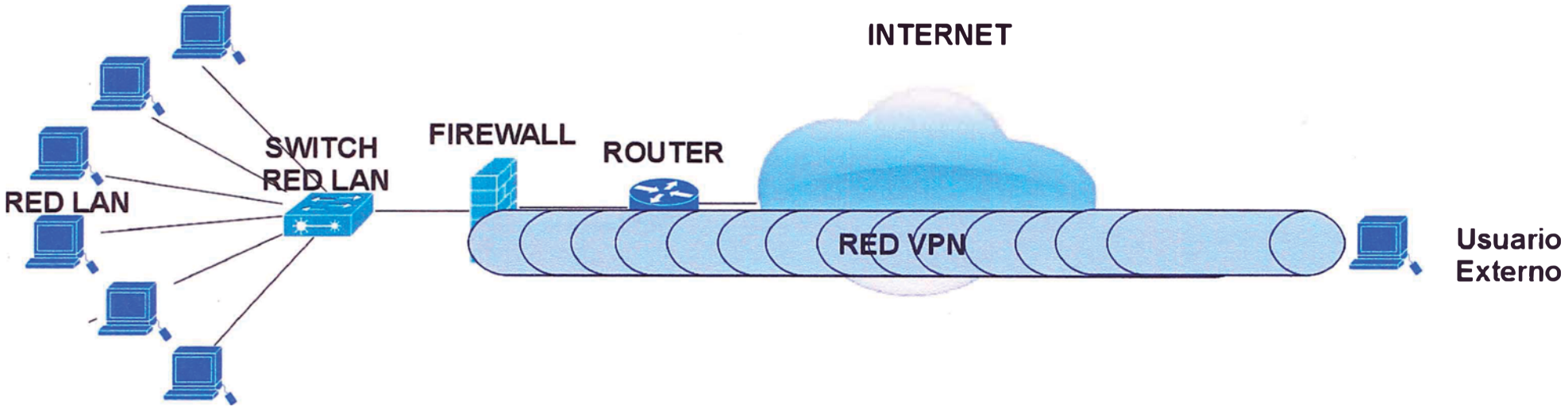


Figura 3: Topología de la Red VPN-LAN del Cliente

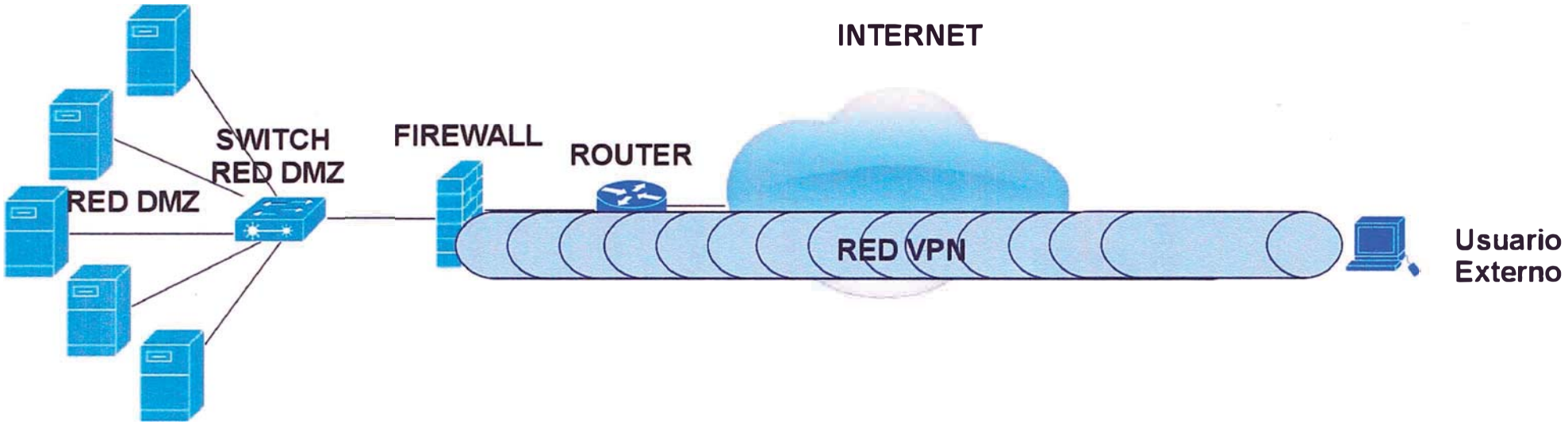


Figura 4: Topología de la Red VPN-DMZ del Cliente

Las observaciones encontradas desde la red LAN hacia INTERNET, esto se puede visualizar de la siguiente forma:

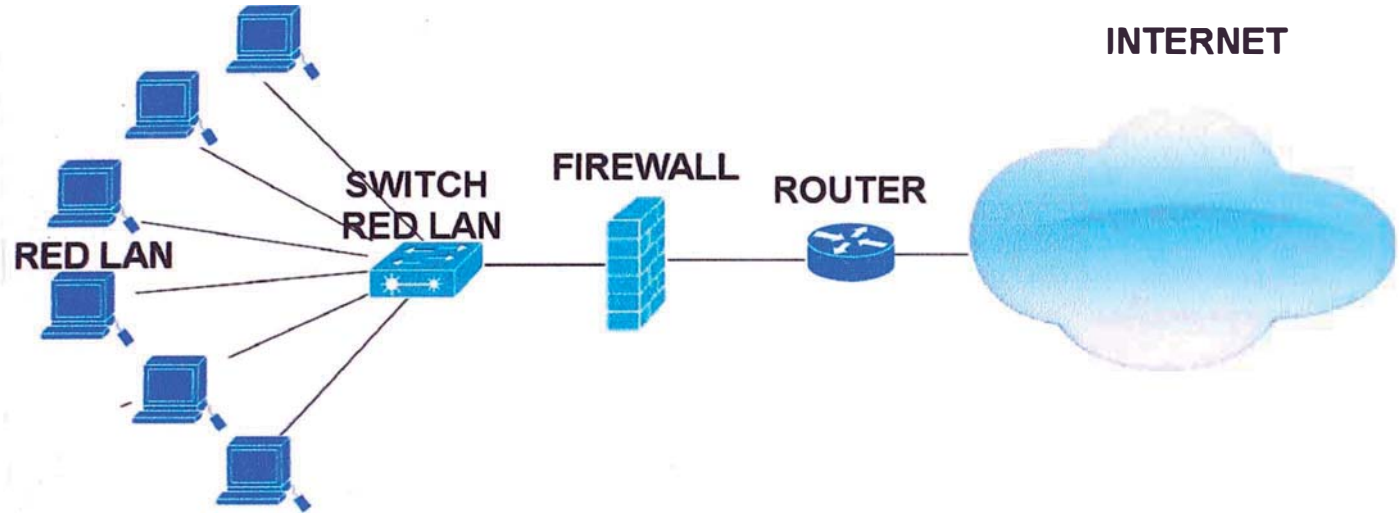


Figura 6: Topología de Red LAN-WAN

Aquí se encontraron las reglas asociadas al estado actual del firewall:

Se encontró una regla que permitía salir a toda la red LAN sin ningún tipo de restricción hacia internet, esta regla estaba ubicada en el primer lugar la cual permite pasar a toda la red LAN dejando de lado las reglas posteriores a la salida desde la red LAN hacia INTERNET.

Se encontró varias reglas las cuales salen a través de las IP's de la red LAN de manera dispersa, esto genera un ambiente de desorden en el cual no es posible saber que IP pertenece a algún integrante de la organización, esto con la finalidad de tener un mejor control.

Se encontró que no hay restricciones en los puertos de salida desde la red LAN hacia INTERNET, muchas ips salen hacia INTERNET sin una restricción de los puertos, esto es algo peligroso debido a que algunas máquinas podrían usar programas que utilizan la conexión a internet o estar infectadas deteriorando el ancho de banda.

Las observaciones encontradas en la red DMZ las podemos visualizar a través de la siguiente topología:

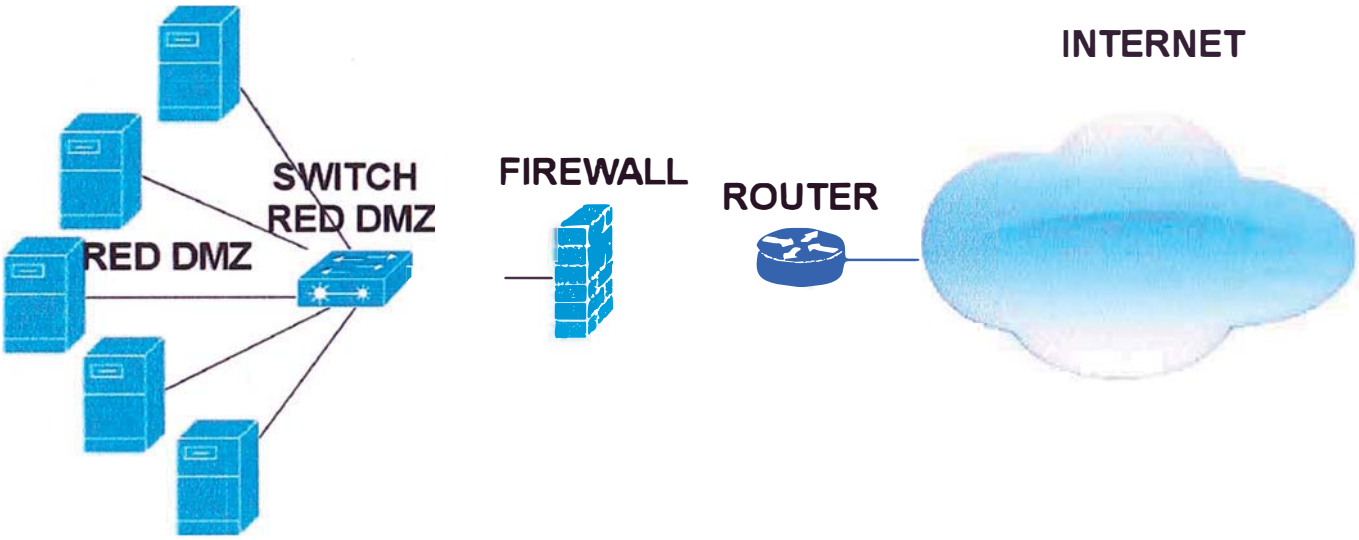


Figura 7: Topología de Red DMZ-WAN

Se encontró que sólo se permite salir hacia INTERNET a un servidor de la red DMZ, pero este no tiene restricción en los puertos de salida hacia INTERNET, esto es peligroso debido a que algunos servidores pueden estar infectados y pueden estar enviando información a través de otros puertos.

Las observaciones encontradas desde la red LAN hacia la red DMZ las podemos visualizar a través de la siguiente topología:

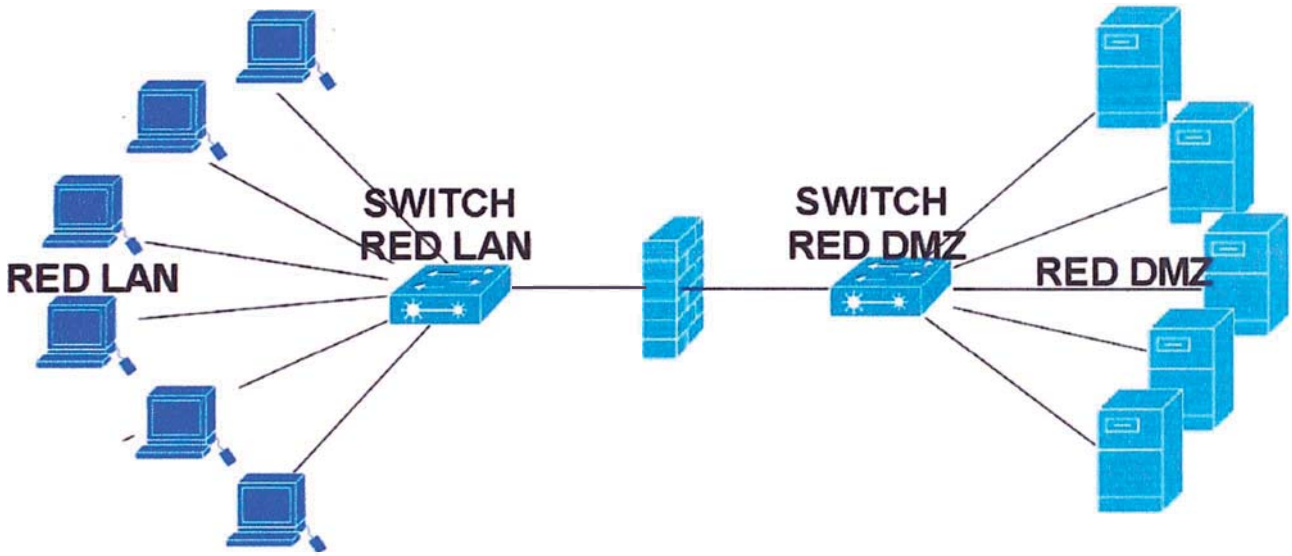


Figura 8: Topología de Red LAN-DMZ

Se encontró que la red LAN puede llegar hacia cualquier servidor de la red DMZ, esto debido a que no se encuentra alguna regla que pueda restringir los hosts como origen desde la red LAN, tampoco se encontró alguna regla que pueda restringir el destino a nivel de IP's, esto es peligroso debido a que muchos usuarios pueden acceder a todos los servidores de la red DMZ, como se comentó el informe de la empresa IDC "Insider Risk Management: A Framework Approach to Internal Security" un 19% de las empresas encuestadas afirma que los ataques a sus equipos informáticos y robo de información que sufrieron por parte de sus empleados fue de manera intencionada, mientras que un 26% afirma que los ataques que sufrieron resulta ser una combinación de manera intencionada y a la vez no intencionada.

Se encontró que la red LAN puede llegar a utilizar cualquier servicio de la red DMZ, esto debido a que no se encuentra alguna regla que pueda restringir el acceso a nivel de los puertos hacia los servidores de la red DMZ.

Se encontró que la red DMZ puede llegar hacia todos los hosts de la red LAN. Esto es peligroso debido a que los servidores se encuentran publicando servicios hacia INTERNET y estos pueden ser vulnerados en algún momento, motivo por el cual un atacante habiendo ganado acceso en algún servidor de la red DMZ puede luego llegar hacia la red LAN si encuentra alguna regla permitida.

Se encontró que la red DMZ puede llegar a los servicios de los hosts ubicados en la red LAN, esto es peligroso debido a que los servidores se encuentran publicando servicios hacia INTERNET y estos pueden ser vulnerados en algún momento, motivo por el cual un atacante habiendo ganado acceso en algún servidor de la red DMZ puede luego llegar a vulnerar los servicios de la red LAN si encuentra publicado internamente algún servicio mal configurado o vulnerable.

Se encontró que los usuarios que ingresan por la VPN tienen permisos para acceder a todos los hosts de la red LAN, esto es peligroso debido a que muchos de ellos podrían intentar acceder a máquinas o servicios a los cuales no le está permitido el acceso así como podría infectar los hosts de la red LAN en caso de que la máquina de la red VPN se encuentre infectada.

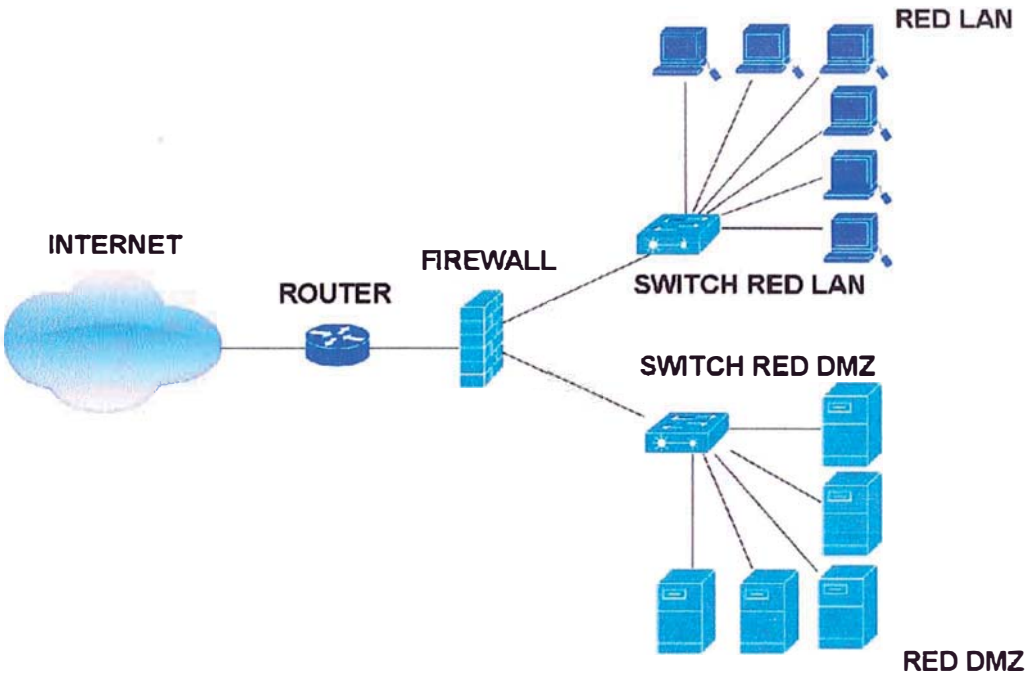


Figura 9: Topología de la publicación de servicios hacia INTERNET

Se encontró servicios publicados a INTERNET desde la red LAN como Servicio Web, SSH, Escritorio Remoto, Aplicaciones propias de la empresa, las cuales no tenían firmas IPS asociadas al servicio publicado hacia INTERNET, esto es peligroso debido a que muchos atacantes pueden explotar las vulnerabilidades de los servicios publicados que en muchos casos no son actualizadas con su respectivo "parche" de actualización, las firmas IPS nos ayudarán a reducir el riesgo de explotar una vulnerabilidad por parte de los atacantes.

Se encontró servicios publicados a INTERNET desde la red DMZ como MSQL, SMTP, POP3, IMAP, POP3S, IMAPS, Puerto administrador del servicio Mail, las cuales no tenían firmas IPS asociadas al servicio publicado hacia INTERNET, esto es peligroso debido a que muchos atacantes pueden explotar las

vulnerabilidades de los servicios publicados que en muchos casos no son actualizadas con su respectivo "parche" de actualización, las firmas IPS nos ayudarán a reducir el riesgo de explotar una vulnerabilidad por parte de los atacantes.

El principal problema se puede observar en una mala práctica la cuales común de permitir abrir todos los puertos para salir hacia internet, conectarse al dmz, conectarse vía vpn ssl, motivo por el cual se observa que muchas ips se encuentran con la solicitud de todo el puerto abierto, lo cual expone demasiado a que la pc pueda estar infectada y está utilizando algunos otros puertos para realizar ataques o robar información a través de otros puertos.

3.2 PLANTEAMIENTO DE ALTERNATIVAS DE SOLUCIÓN.

Para poder solucionar estos dos problemas el administrador tendrá las siguientes alternativas:

- Consultar a un experto.
- Solicitar un trabajo en grupo con Tgestiona.

	Asesor Externo	Trabajo en Grupo con Tgestiona*
Costo	$ 150 por hora	$ 25 por día
Tiempo	4 días (32 horas)	3 semanas a 5 semanas
Trámite	Contrato directo	Coordinar con el grupo, previa evaluación acuerdo con los encargados
Compromiso	Se termina luego de la recomendación	Se mantiene la evaluación por parte del equipo

* Actualmente Tgestiona alquila el firewall con la licencia de ips, motivo por el cual Tgestiona colabora con las solicitudes de configuración del cliente, pero no se hace responsable por las malas reglas que este realice en el firewall.

3.2.1 Alternativa 1: Contratar un Asesor Externo

Actualmente existe en el mercado pocas personas que se encuentren certificadas en el manejo de firewall Fortigate, esto se debe a que el Firewall Fortigate es un producto algo nuevo en el mercado peruano, motivo por el cual se encuentran pocos expertos que dominen la correcta configuración del firewall Fortigate, aquí detallaremos las ventajas y desventajas sobre esta alternativa:

Ventajas:

- El asesor externo tiene un fuerte conocimiento sobre la administración del firewall fortigate.
- El asesor externo tiene experiencia en el campo seguridad de red, esto será útil cuando el asesor combine la configuración correcta del firewall con el conocimiento de seguridad de red.
- El asesor experto emitirá una opinión imparcial con respecto al rendimiento del firewall, esto se debe a que en base a su experiencia informará si el firewall se encuentra desempeñando correctamente su tarea de proteger la red perimetral del cliente.

Desventajas:

- El precio del asesor externo se ubica en un promedio de 150$ por hora, para este trabajo se estima aproximadamente unas 32 horas lo cual costaría a la empresa una cantidad de **$ 4800**, este precio es elevado debido a que pocas personas cuentan con la certificación de la empresa Fortinet.

- El pago al asesor externo tiene que ser sustentado a la dirección, esto puede traer discrepancias o malos prejuicios debido a que se puede pensar que el área de TI no tiene el conocimiento necesario para administrar el equipo.
- El asesor externo puede tener conocimiento de la red interna de la organización así como los servicios que publica, motivo por el cual puede sufrir un ataque por parte del asesor externo cuando este finalice su contrato.

3.2.2 Alternativa 2: Coordinar Trabajo en Grupo con Tgestiona

Actualmente Tgestiona alquila el firewall a su cliente, motivo por el cual Tgestiona puede apoyar al cliente con la mejora de la configuración del equipo con la finalidad de mejorar su atención al cliente para mantener una buena imagen.

Ventajas:

- Tgestiona cuenta con su centro de operaciones de seguridad, los cuales tienen el conocimiento necesario para proceder a revisar las reglas con el cliente.
- Tgestiona cobraría menos cantidad de dinero, debido a que cuenta con el centro de operación de seguridad el cual ayuda
- El compromiso después de realizar las configuraciones se mantiene debido a que Tgestiona seguiría colaborando para implementar políticas seguras en base a lo realizado.

Desventaja:

- Se tiene que solicitar un permiso a Tgestiona para poder realizar la revisión y mejora de la red, no es común pero puede haber la

posibilidad de no realizar la revisión del firewall por el cliente debido a temas legales.

- El tiempo que toma Tgestiona es bastante, la mejora dura un aproximado de 4 semanas.
- Si Tgestiona encuentra algún mal rendimiento en el equipo esto no sería informado al cliente con la finalidad de no mostrar sus defectos del equipo.
- Tgestiona puede utilizar esta colaboración como un pretexto para ofrecer al cliente otros productos de seguridad que ayuden a defender su red de datos y no realice una óptima configuración en base a lo que ofrece el firewall.

3.3 SELECCIÓN DE UNA ALTERNATIVA DE SOLUCIÓN

3.3.1 IDENTIFICACIÓN DE LOS CRITERIOS DE SELECCIÓN:

Para proceder a elegir una alternativa nosotros debemos tener los criterios los cuales serán la base para poder elegir la mejor alternativa, para esto identifique las siguientes alternativas sobre la cual la empresa puede elegir:

1.- Costo de revisión.

Este criterio es importante debido a que el cliente de Tgestiona elegirá el pago menos costoso entre las dos opciones, esto con la finalidad de tener una aceptación y/o apoyo en su respectiva directiva.

2.- Conocimiento del manejo del Firewall.

Este criterio es fundamental debido a que la alternativa elegida deberá tener bastante conocimiento para proceder a realizar una configuración correcta.

3.- Tiempo de implementación de la mejora de reglas del firewall.

Este criterio nos ayudará a medir el tiempo en el que demora la implementación de las reglas del firewall con la finalidad de proyectar el plan de implementación de reglas para el tiempo elegido.

4.- Factibilidad para elegir entre el trabajo de un experto o el trabajo en grupo con Tgestiona.

Este criterio es importante debido a que el cliente tendrá que evaluar la factibilidad de elegir entre contratar un externo o solicitar a Tgestiona el servicio de revisión del firewall.

3.3.2 DETERMINACIÓN DE PESOS DE LOS CRITERIOS

Para elegir la mejor opción tendremos que poner un peso a cada uno de los criterios que se detalló anteriormente, estos criterios fueron evaluados por el área de sistemas de la organización de Tgestiona, debido a la experiencia que tiene en el mercado con la administración de equipos para la seguridad perimetral.

Criterio	Peso
Costo de revisión	30 %
Conocimiento del manejo del Firewall	40 %
Tiempo de implementación de la mejora de reglas del firewall	15%
Factibilidad para elegir entre el trabajo de un experto o el trabajo en grupo con Tgestiona	15%

MODO DE CALIFICACIÓN

Para la calificación elegiremos el rango del 1 al 5, el cual detallaremos los valores para cada uno de los valores:

Puntaje	Calificación
1	Pésimo
2	Regular
3	Bueno
4	Muy Bueno
5	Excelente

COMPARACIÓN DE ALTERNATIVAS

Criterio	Peso	Alternativa 1		Alternativa 2	
		Eva.	Pond.	Eva.	Pond.
Costo de revisión	30%	1	0.3	3	0.9
Conocimiento del manejo del Firewall	40%	4	1.6	5	2
Tiempo de implementación de la mejora de reglas del firewall	15%	4	0.6	2	0.3
Factibilidad para elegir entre el trabajo de un experto o el trabajo en grupo con Tgestiona	15%	2	0.3	4	0.6
Puntaje Total			2.8		3.8

Ahora procederemos a evaluar las 2 alternativas que se mostraron, para esto debemos tener en cuenta el peso de los criterios con el modo de la calificación.

De la evaluación se tomará como opción la segunda alternativa por ser la más viable para el cliente.

De las alternativas mostradas, la primera que consiste en contratar un experto para que revise demandará un cantidad

aproximada de $ 4800, lo cual puede ser resuelto aproximadamente en dos días, si bien el tiempo es corto el problema radica en solicitar el monto al directorio, tan solo con la finalidad de ajustar los requerimientos del firewall, lamentablemente como en todas las empresas el solicitar requerimientos puede terminar siendo un arma de doble filo debido a que el directorio puede pensar el equipo de TI no es el adecuado para resolver estos problemas.

De la segunda alternativa la cual no cuesta dinero, pero si demandará la coordinación con el área de seguridad Tgestiona, para luego poder revisar y empezar el análisis lo cual le puede demorar de 3 a 5 semanas.

3.3.3 PLANES DE ACCIÓN PARA DESARROLLAR LA SOLUCIÓN PLANTEADA.

Para desarrollar el plan se coordinará los siguientes puntos:

- Coordinación con los ejecutivos de ventas: Este paso será el proceso regular de permiso, el cual una vez aprobado se procederá a la revisión de la configuración en el firewall.
- Revisión de los parámetros declarados en el firewall: Esto permite revisar cómo están declarados los parámetros, con la finalidad de revisar si estos se declararon de manera correcta,
- Revisión de las reglas del firewall: Esto es fundamental para poder corregir las posibles malas configuraciones o las reglas que exponen a que los servidores puedan ser objetivo de un ataque.

Orden	Detalle	Días
1	Coordinación con el área de seguridad de Tgestiona.	2 a 3 días (2.5 días)
2	Conversación vía telefónica y/o personal para analizar la red actual que tiene el cliente.	1 a 2 días (1.5 días)
3	Revisión del correcto registro de los parámetros del firewall de acuerdo a la red.	2 a 3 días (2.5 días)
4	Revisión de las reglas del firewall.	1 a 2 días (1.5 días)
5	Se le envían al cliente cada una de las reglas encontradas en el firewall, para que valide si seguirán siendo vigentes.	2 a 3 días (2.5 días)
6	Revisión de las firmas de IPS	1 a 2 días (1.5 días)
7	Se le envían al cliente cada una de las firmas de IPS para aplicarla de acuerdo a los servicios publicados, esto se le envía para que valide si desea aplicarlo.	2 a 3 días (2.5 días)
8	Se realizará recomendaciones sobre algunas configuraciones adicionales para optimizar el equipo.	1 día
9	Se le envía al cliente las configuraciones para los últimos ajustes, aquí el cliente decidirá si son aprobadas.	1 a 2 días (1.5 días)
10	El cliente debe de realizar las pruebas de conectividad entre sus redes, así como probar las restricciones entre las redes LAN, INTERNET, DMZ	1 día

CAPÍTULO IV: ANÁLISIS COSTO BENEFICIO

4.1 SELECCIÓN DE CRITERIOS DE EVALUACIÓN

Como se describió en el capítulo anterior las alternativas están basadas en la problemática motivo por el cual las describiremos de la siguiente forma:

1.- Costo de revisión.

Este criterio es importante debido a que el cliente de Tgestiona elegirá el pago menos costoso entre las dos opciones, esto con la finalidad de tener una aceptación y/o apoyo en su respectiva directiva.

2.- Conocimiento del manejo del Firewall.

Este criterio es fundamental debido a que la alternativa elegida deberá tener bastante conocimiento para proceder a realizar una configuración correcta.

3.- Tiempo de implementación de la mejora de reglas del firewall

Este criterio nos ayudará a medir el tiempo en el que demora la implementación de las reglas del firewall con la finalidad de proyectar el plan de implementación de reglas para el tiempo elegido.

4.- Factibilidad para elegir entre el trabajo de un experto o el trabajo en grupo con Tgestiona.

Este criterio es importante debido a que el cliente tendrá que evaluar la factibilidad de elegir entre contratar un externo o solicitar a Tgestiona el servicio de revisión del firewall.

4.2 COSTOS DE LA IMPLEMENTACIÓN

De acuerdo a la segunda alternativa que se eligió aquí se mostrará el costo en el cual incurrirá el cliente para pagar a Tgestiona para la mejora

Costo

El costo que se tomará será el de $ 25 por día, pero aquí debemos tener en cuenta que el costo empezará a correr después de haberse aprobado el proyecto.

Orden	Detalle	Días	Costo
1	Coordinación con el área de seguridad de Tgestiona.	2 a 3 días (2.5 días)	$ 0
2	Conversación vía telefónica y/o personal para analizar la red actual que tiene el cliente.	1 a 2 días (1.5 días)	$ 37.5
3	Revisión del correcto registro de los parámetros del firewall de acuerdo a la red.	2 a 3 días (2.5 días)	$ 62.5
4	Revisión de las reglas del firewall.	1 a 2 días (1.5 días)	$ 37.5
5	Se le envían al cliente cada una de las reglas encontradas en el firewall, para que	2 a 3 días (2.5 días)	$ 62.5

	valide si seguirán siendo vigentes.		
6	Revisión de las firmas de IPS	1 a 2 días (1.5 días)	$ 37.5
7	Se le envían al cliente cada una de las firmas de IPS para aplicarla de acuerdo a los servicios publicados, esto se le envía para que valide si desea aplicarlo.	2 a 3 días (2.5 días)	$ 62.5
8	Se realizará recomendaciones sobre algunas configuraciones adicionales para optimizar el equipo.	1 día	$ 25
9	Se le envía al cliente las configuraciones para los últimos ajustes, aquí el cliente decidirá si son aprobadas.	1 a 2 días (1.5 días)	$ 37.5
10	El cliente debe de realizar las pruebas de conectividad entre sus redes, así como probar las restricciones entre las redes LAN, INTERNET, DMZ	1 día	$ 0
	Total	**14 a 28 días (18 días)**	$ 387.5

De lo observado se puede visualizar que el costo promedio con Tgestiona es un aproximado de $ 387.5, esto comparado contra los $ 4800 resulta ser económico, aunque como se comentó el tiempo en el cual se implementa es mayor comparado contra los 4 días que ofrecía el asesor externo.

4.3 REVISION DE BUENAS PRÁCTICAS

Ahora que hemos decidido revisar las reglas del firewall tenemos que buscar los criterios sobre el cual podremos tener un firewall configurado correctamente:

1 .- Se tendrá una política restrictiva: Muchos firewall ofrecen la opción de tener una regla permisiva la cual permite todas salir a internet a todos, solo se negaran aquellas que explícitamente se encuentren declaradas. Es por eso que siempre se debe configurar para que al inicio el firewall tenga la regla de denegación implícita, esto significa que el firewall permitirá el acceso a aquellas reglas que se encuentren declaradas y negará la salida a aquellas reglas que no se encuentren declaradas.

2 .- Se habilitan los puertos de navegación necesarios: Se observa en el firewall que muchas ips tienen salida hacia todos los puertos, esto en el equipo se traduce en un ANY, lo cual significa que el usuario pueda salir libre hacia internet usando todos los puertos de su pc, actualmente hay muchas aplicaciones que utilizan sus puertos los cuales son diferentes al HTTP, HTTPS, TCP_8080, DNS para esto se debe permitir sólo los puertos necesarios con la finalidad de que los usuarios no hagan un mal uso del consumo hacia internet.

3.- Se debe restringir el acceso de la red LAN permitiendo sólo las redes permitidas hacia Internet: Se observa que hay reglas como origen ALL, esto significa que cualquier dispositivo de la red puede salir y conectarse hacia el otro destino, para esto es fundamental declarar las redes, hosts, subnets que podrán salir hacia el otro destino, esto se hace con la finalidad de que los usuarios no puedan elegir cualquier ip y poder llegar hacia el otro destino.

4 .- Se debe bloquear el acceso desde la red DMZ hacia LAN: Se observa que la red DMZ puede llegar hacia la red LAN sin ningún tipo de restricción, esto puede ser un problema a futuro debido a que los servidores DMZ publican servicios hacia internet, cuando un servidor publica servicios hacia internet estos pueden ser vulnerados permitiendo que los atacantes lleguen a tener la administración del servicio publicado o en el peor de los casos de la administración del servidor, motivo por el cual los servidores ubicados en la DMZ no deben tener permisos para llegar hacia la red LAN, esto porque una vez que los atacantes tengan la administración del servidor estos pueden querer llegar hacia la LAN para poder vulnerar a los host ubicados en la red LAN.

5.- No se deben publicar servicios hacia INTERNET en la red LAN: Se debe revisar si se tienen publicación de servicios de la red LAN hacia INTERNET, esto con la finalidad de retirar las publicaciones hacia internet, debido a que los atacantes pueden explotar las vulnerabilidades de los servicios y puedan llegar al host de la red LAN y luego poder atacar al resto de hosts ubicado en la red LAN, poniendo en peligro la continuidad de las operaciones de la empresa.

6 .- Se debe restringir el acceso desde la red LAN hacia la DMZ: Se debe revisar los permisos desde la red LAN hacia la DMZ con la finalidad de proteger los servidores de un posible ataque interno, el estudio de la empresa IDC "Insider Risk Management: A Framework Approach to Internal Security" la cual informa que el 52% de las empresas sometidas al estudio de seguridad sufrieron un ataque informático de manera no intencionada por parte de los trabajadores, el 19% cree que los ataques informáticos fueron intencionados mientras que el 26% cree que los ataques informáticos fueron una combinación de ambos y el 3% no está seguro, motivo por el cual debemos tener cuidado al momento de permitir el acceso hacia los

servidores, además de tener cuidado con el manejo interno de los servidores.

7.- Se debe permitir la salida desde la red LAN hacia INTERNET por grupos: Se debe revisar cómo se encuentran asignadas la salida hacia INTERNET para la red LAN, es recomendable que sean por grupos con la finalidad de no generar reglas por IP que luego genere un desorden. Para esto es recomendable que salgan a través de grupos con la finalidad de aplicar la misma regla a todos los integrantes del mismo grupo, para esto es recomendable crear grupos d acuerdo a la organización como por ejemplo Finanzas, Secretaria, Ingenieros, Sistemas, Administración, Directiva, Operativo, etc. Esto ayudaría bastante a aplicar una regla al grupo y así poder controlarlo de manera global.

8.- Se debe restringir el acceso de los hosts desde la red VPN hacia la red LAN: Se debe revisar los permisos de los usuarios que acceden desde la red VPN hacia la LAN con la finalidad de no permitir el acceso total hacia toda la red LAN, esto es un peligro cuando un usuario desde la red VPN desea ingresar a otros dentro de la red LAN sin estar permitido.

9 .- Se debe restringir el acceso de los puertos desde la red VPN hacia la red LAN: Se debe revisar los permisos de los puertos, esto se debe a que cuando un usuario con una máquina infectada ingresa desde la red VPN hacia la red LAN pueda infectar a los hosts de la red LAN a través de los puertos no permitidos, para esto debemos sólo permitir los puertos necesarios, muchos trabajadores que ingresan a la red VPN y desean hacer un trabajo de manera remota en sus equipos o algunos servidores de la red LAN, para esto se debe restringir los puertos solamente para permitir a los trabajadores a

utilizar los servicios necesarios y no a todos los puertos los cuales pueden ser usados con una mala intención.

10.- Se debe restringir los horarios de salida hacia INTERNET: Se debe revisar si las reglas permiten salir hacia INTERNET con un control de horario, esto se debe a que muchos trabajadores pueden dejar prendidas sus máquinas con las malas prácticas de descargar archivos, programas, o realizar actualizaciones de manera indiscriminada

11 .- Se debe comentar las reglas que uno registra en el firewall: Se observa muchas reglas sin un registro de comentarios, algunas de estas aparentemente no tienen lógica, cuando el administrador del firewall registra las reglas, estas solo pueden ser entendidas por el administrador del firewall, en la actualidad se observa que la gran mayoría de los administradores de firewall no registran comentarios sobre las reglas implementadas, eso a futuro es un problema debido a que solo él podrá entenderlo y en caso de pasar el cargo a otra persona esta no podrá entenderlo, lo cual dificultará el trabajo y en el peor de los escenarios el nuevo administrador genere problemas cuando elimine reglas que no pueda entender.

12.- Se debe tener registro de log: Se debe revisar si todas las reglas permiten registrar los log con la finalidad de saber qué es lo que se encuentra realizando cada uno de los hosts dentro de la red.

4.4 RESULTADOS DE LA SOLUCIÓN PLANTEADA

De acuerdo a las recomendaciones descritas se decidió realizar cambios en las configuraciones debido a las posibles brechas de seguridad descritas anteriormente, aquí se detalla los resultados que se obtuvieron:

- Se eliminó la reglas que permitía salir desde la red LAN hacia INTERNET sin ningún tipo de restricción, aquí la empresa pudo encontrar IP's de usuarios que no deberían salir a INTERNET, pero estaban saliendo a través de esta regla.

- Se permite el agrupamiento de ips a través de grupos como INALÁMBRICO, USUARIOS, JEFATURA, INVITADOS.

- Se restringe los puertos de salida desde la red LAN hacia INTERNET para HTTP, HTTPS, DNS, TCP_8080, TCP_7777, FTP, RDP,

- Se eliminó la regla que permite a los servidores comunicarse desde la red DMZ hacia la red LAN, esto con la finalidad de evitar que algún servidor que posiblemente estuviese vulnerado o sea vulnerado en el futuro ya no pueda llegar a los hosts de la red LAN.

- Se restringe el acceso de hosts desde la red LAN hacia la DMZ, para esto también se permite el acceso a través de grupos para tener un mejor control.

- Se restringe el acceso a nivel de puertos como el HTTP, HTTPS, SMTP, POP3, MYSQL y otros orientados a la administración para el área de sistemas como SSH, RDP MYSQL IMAP, desde la red LAN hacia la DMZ, esto con la finalidad de evitar el acceso hacia servidores a personal no autorizado.

- Se creó reglas con horarios de salida para la red LAN, esto con la finalidad de salir hacia INTERNET desde las 7 am hasta las 10 pm de Lunes a Viernes, desde las 12 am hasta las 4 am para salir hacia los servicios de actualización de Windows para las máquinas que se

encuentren encendidas, desde las 7 am hasta las 6 pm para los días Sábados y Domingos

- Se restringió los destinos de acceso para la red LAN desde las VPN, esto con la finalidad de que los usuarios ingresen solo a los respectivos sitios de destino y no puedan acceder a otros.

- Se restringe el acceso de los puertos para la red LAN desde las VPN, esto con la finalidad de que los usuarios ingresen solo a los respectivos sitios de destino y no puedan acceder a otros.

4.4.1 CRITERIOS DE CONFIGURACIÓN

Ahora que hemos decidido revisar las reglas del firewall tenemos que buscar los criterios sobre el cual podemos tener un firewall configurado correctamente:

1 .- Se tendrá una política restrictiva: Ciertos firewall vienen por defecto con la regla de aceptación implícita, la cual permite conectarse diferentes zonas del firewall, solo se negaran aquellas que explícitamente se encuentren declaradas. Es por eso que siempre se debe configurar para que al inicio el firewall se tenga la regla de denegación implícita, esto significa que el firewall denegara todos los accesos entre sus zonas, solo se permitirá el acceso a aquellas reglas que se encuentren declaradas.

2 .- Se habilita los puertos de navegación necesario: Se observa en el firewall que muchas ips tienen salida hacia todos los puertos, esto en el equipo se traduce en un ANY, lo cual significa que el usuario pueda salir libre hacia internet usando todos los puertos de su pc, actualmente hay muchas aplicaciones que utilizan sus puertos los cuales son diferentes al HTTP, HTTPS, TCP_8080, DNS para esto se

debe permitir sólo los puertos necesarios con la finalidad de que los usuarios no hagan un mal uso del consumo hacia internet.

3.- Se debe restringir el acceso de la red LAN permitiendo sólo las redes permitidas hacia Internet: Se observa que hay reglas como origen ALL, esto significa que cualquier dispositivo de la red puede salir conectarse hacia el otro destino, para esto es fundamental declarar las redes, hosts, subnets que podrán salir hacia el otro destino, esto se hace con la finalidad de que los usuarios no puedan elegir cualquier ip y poder llegar hacia el otro destino.

4 .- Se debe bloquear el acceso desde la red DMZ hacia LAN: Se observa que la red DMZ puede llegar hacia la red LAN sin ningún tipo de restricción, esto puede ser un problema a futuro debido a que los servidores DMZ publican servicios hacia internet, cuando un servidor publica servicios hacia internet estos pueden ser vulnerados permitiendo que los atacantes lleguen a tener la administración del servicio publicado o en el peor de los casos de la administración del servidor, motivo por el cual los servidores ubicados en la DMZ no deben tener permisos para llegar hacia la red LAN, esto porque una vez que los atacantes tengan la administración del servidor estos pueden querer llegar hacia la LAN para poder vulnerar a los host ubicados en la red LAN.

5.- No se deben publicar servicios hacia INTERNET en la red LAN: Se debe revisar si se encuentran publicación de servicios la red LAN hacia INTERNET, esto con la finalidad de retirar las publicaciones hacia internet, debido a que los atacantes pueden explotar las vulnerabilidades de los servicios y puedan llegar al host de la red LAN y luego poder atacar al resto de hosts ubicado en la red LAN, poniendo en peligro la continuidad de las operaciones de la empresa.

6 .- Se debe restringir el acceso desde la red LAN hacia la DMZ: Se debe revisar los permisos desde la red LAN hacia la DMZ con la finalidad de proteger los servidores de un posible ataque interno, el estudio de la empresa IDC "Insider Risk Management: A Framework Approach to Internal Security" la cual informa que el 52% de las empresas sometidas al estudio de seguridad sufrieron un ataque informático de manera no intencionada por parte de los trabajadores, el 19% cree que los ataques informáticos fueron intencionados mientras que el 26% cree que los ataques informáticos fueron una combinación de ambos y el 3% no está seguro, motivo por el cual debemos tener cuidado al momento de permitir el acceso hacia los servidores, además de tener cuidado con el manejo interno de los servidores.

7.- Se debe permitir la salida desde la red LAN hacia INTERNET por grupos: Se debe revisar cómo se encuentran asignadas la salida hacia INTERNET para la red LAN, es recomendable que sean por grupos con la finalidad de no generar reglas por IP que luego genere un desorden. Para esto es recomendable que salgan a través de grupos con la finalidad de aplicar la misma regla a todos los integrantes del mismo grupo, para esto es recomendable crear grupos de acuerdo a la organización como por ejemplo Finanzas, Secretaria, Ingenieros, Sistemas, Administración, Directiva, Operativo, etc. Esto ayudaría bastante a aplicar una regla al grupo y así poder controlarlo de manera global.

8.- Se debe restringir el acceso de los hosts desde la red VPN hacia la red LAN: Se debe revisar los permisos de los usuarios que acceden desde la red VPN hacia la LAN con la finalidad de no permitir el acceso total hacia toda la red LAN, esto es un peligro cuando un usuario desde la red VPN desea ingresar a otros dentro de la red LAN sin estar permitido.

9 .- Se debe restringir el acceso de los puertos desde la red VPN hacia la red LAN: Se debe revisar los permisos de los puertos, esto se debe a que cuando un usuario con una máquina infectada ingresa desde la red VPN hacia la red LAN pueda infectar a los hosts de la red LAN a través de los puertos no permitidos, para esto debemos sólo permitir los puertos necesarios, muchos trabajadores que ingresan a la red VPN y desean hacer un trabajo de manera remota en sus equipos o algunos servidores de la red LAN, para esto se debe restringir los puertos solamente para permitir a los trabajadores a utilizar los servicios necesarios y no a todos los puertos los cuales pueden ser usados con una mala intención.

10.- Se deben restringir los horarios de salida hacia INTERNET: Se debe revisar si las reglas permiten salir hacia INTERNET con un control de horario, esto se debe a que muchos trabajadores pueden dejar prendidas sus máquinas con las malas prácticas de descargar archivos, programas, o realizar actualizaciones de manera indiscriminada

11 .- Se deben comentar las reglas que uno registra en el firewall: Se observa muchas reglas sin un registro de comentarios, algunas de estas aparentemente no tienen lógica, cuando el administrador del firewall registra las reglas, estas solo pueden ser entendidas por el administrador del firewall, en la actualidad se observa que la gran mayoría de los administradores de firewall no registran comentarios sobre las reglas implementadas, eso a futuro es un problema debido a que solo él podrá entenderlo y en caso de pasar el cargo a otra persona esta no podrá entenderlo, lo cual dificultará el trabajo y en el peor de los escenarios el nuevo administrador genere problemas cuando elimine reglas que no pueda entender.

12.- Se debe tener registro de log: Se debe revisar si todas las reglas permiten registrar los log con la finalidad de saber qué es lo que se encuentra realizando cada uno de los hosts dentro de la red

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1.- Se observó una reducción en el tiempo de espera de navegación hacia la INTERNET de 11 a 15 segundos a 2 a 6 segundos en los momentos de mayor uso de la navegación hacia INTERNET.

2.- Se tendrá un control sobre el acceso a nivel de servicios de los usuarios que navegan hacia INTERNET.

3.- Se tendrá un control sobre el acceso de los usuarios hacia los servicios y/o servidores en la DMZ.

4.- Para solucionar el problema de control sobre los usuarios se tuvo que crear grupos con la finalidad de agrupar las ips y/o rangos de acuerdo a las características del usuario en el trabajo.

5.- La restricción en el firewall permitió permitir que los usuarios utilicen servicios o puertos que no estén asociados a las actividades del trabajo del día a día, por ejemplo se encontró que algunos usuarios podían utilizar aplicaciones como torrents, lo cual generaba un deterioro en la conexión del ancho de banda desde la red LAN hacia INTERNET.

6.- La manera estructurada y parametrizada de los datos del firewall permitirá a los integrantes del área de TI y/o nuevos integrantes una compresión sobre el funcionamiento correcto de los permisos de la red.

RECOMENDACIONES

Debemos recordar que para mantener una seguridad optima en el firewall, tenemos que empezar por las reglas en el firewall, las cuales si se desean agregar y/o editar más adelante, estas deben ser analizadas y tratar de mantener la estructura de grupos y/o redes declaras, motivo por el cual aquí detallaré una serie de recomendaciones para mantener la seguridad más adelante.

Se recomienda al cliente migrar servicios publicados hacia INTERNET desde su red LAN hacia la DMZ, a pesar de recomendarle migrar los servicios publicados hacia INTERNET desde la red LAN hacia la red DMZ, este no aceptó por temas de trabajo, motivo por el cual se mantiene una potencial brecha de inseguridad debido a que se publica servicios desde la red LAN, para esto se le recomendó que migre los servicios hacia su red DMZ y así puedan llegar desde la red LAN hacia la red DMZ sin problemas y así poder aislar los servidores en la red DMZ.

Con la finalidad de mantener un orden sobre la administración de las ips registradas en el firewall se recomienda que cada vez que se desea agregar una ip, esta debe estar registrada con un nombre que pueda hacer referencia al servicio y/o persona que utilizara la ip, esto con la finalidad de no crear reglas para un ip y a la vez empiece a generar un desorden sobre las reglas creadas.

Si se desea publicar servicios, se recomienda llevarlo a un servidor y ubicarlo en la red DMZ, con la finalidad de que los usuarios en la red LAN no puedan acceder y al mismo tiempo se aplique restricciones para llegar a los servidores.

En caso de tener cuentas VPN se recomienda generar cuentas VPN para los usuarios internos y/o externos del cliente sean personales y unicas, no se debe generar cuentas genéricas y/o compartidas con la finalidad de tener un control único sobre las personas que acceden.

Se debe restringir el acceso hacia las páginas web de acuerdo a los grupos de navegación, esto ayudará a controlar las páginas de ocio que no deben ser permitidas para ciertos grupos de trabajadores a los cuales se les puede distraer o páginas de contenido eróticos o drogas para toda la organización con la finalidad de no hacer algún mal uso dentro de la organización.

Se debe asignar un control a la cantidad de ancho de banda de la salida de los usuarios de la red LAN hacia INTERNET, así como los servidores que deseen salir desde la red DMZ hacia INTERNET. Esto ayudar a controlar el ancho de banda de acuerdo a la necesidad o cargo de los trabajadores, recordemos que esto también permitirá disminuir el ancho de banda.

Se debe aplicar "Quality of Service" (QoS), a los grupos, o servidores que tengan los privilegios de salir con un buen ancho de hacia INTERNET con la finalidad de priorizar el tráfico hacia INTERNET hacia los grupos y/o servidores que desean navegar sin tener algún tipo de lentitud.

BIBLIOGRAFÍA

ISACA
2013 *Manual de preparación al examen CISM 2013*, USA

ISACA
2011 *Manual de preparación al examen CISA 2011*, USA

FORTINET
2012 *The Fortigate Cookbook*, Fortinet Publishing, 300 pp.

GUIZNARÁN RUÍZ, Carlos
2004 *Internet y la investigación científica: el uso de los medios y las nuevas tecnologías en la educación*. Bogotá, Cooperativa Editorial Magisterio, 341 pp.

GUTIÉRREZ GARAY, Sergio
2010 *Integración Social Digital: Social Media Internet*, DF México, Imagen Digital, 187 pp.

CHRISTIANSEN, Christian y Brian BURKE. Insider risk management: A framework approach to internal security, IDC, Noviembre 2009. Disponible en web:
http://www.imerja.com/files/file/White_Papers/RSA/IDC%20Report%20-%20Insider%20Risk%20Management.pdf

GLOSARIO

LAN : Proviene de las iniciales de "Local Area Network" la cual traducida al español sería la "Red de Área Local", esto se utiliza para describir la red interna de datos de una organización, esta red permite conectar a las ordenadores de la organización para poder conectarse a través de esta red o conectarse a otras redes de la organización.

DMZ: Proviene de las iniciales de "Demilitarized Zone" la cual traducida al español sería la red perimetral, esto se utiliza para describir la red que aloja los servidores de la organización, esta red permite que la organización pueda publicar servicios en la red de manera segura, esto se debe a que la DMZ no debe tener acceso hacia la red LAN, esto se hace con la finalidad de que si algún servidor ha sido vulnerado este no pueda tener acceso a la red LAN.

INTERNET: Es la red de red en la cual se concentran todo el contenido que se desea publicar como las páginas web, correos, telefonía ip, servidores de archivos, etc. Este conjunto de redes alberga el contenido al cual deseamos acceder para publicar información o buscar información en ella.

VPN : Proviene de las iniciales de "Virtual Private Network" la cual traducida al español sería "Red Privada Virtual", esta red permite conectar a un usuario de la organización ubicado físicamente en otro lugar que se encuentra lejos de la organización.

FIREWALL: Conocido también como "Cortafuegos", es un dispositivo de seguridad el cual se encuentra en la primera línea de defensa. El firewall permite a los administradores de red poder controlar el tráfico de red, tráfico de usuarios, publicar servicios, proteger de los ataques externos e internos.

FORTIGATE: Es el nombre de una marca de equipos firewall, estos equipos son producidos por la empresa FORTINET.

FORTINET: Es una empresa de Estados Unidos, la cual está orientada a vender productos relacionados a la seguridad de redes, la empresa FORTINET viene operando en el mercado de seguridad desde el año 2000. Actualmente

IPS: Conocido también como "Sistema de Protección de Intrusos", este equipo de seguridad nos permite luchar contra los atacantes externos e internos,

Topología de red: Es el diseño de cómo se encuentra estructurada la red, la conexión entre computadores, servidores, dispositivos de comunicación y seguridad.