ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"REDISEÑO DE LA RED PERIMETRAL QUE INCORPORA RECOMENDACIONES DE SEGURIDAD PARA UNA ENTIDAD FINANCIERA (PYME)"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

JOSE LUIS RAMIREZ MEJIA

GUAYAQUIL- ECUADOR

AÑO 2016

AGRADECIMIENTO

Agradezco a Dios por su grata voluntad de permitirme avanzar en cada meta propuesta y así poder alcanzar los objetivos planteados, a mi familia y amigos por su constante compañía y apoyo en las diferentes etapas de la vida.

José Luis Ramírez Mejía.

DEDICATORIA

A mis padres por su excepcional amor.

TRIBUNAL DE SUSTENTACIÓN

ING. LENIN FREIRE

DIRECTOR MSIA

ING. LENIN FREIRE

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

MGS. JUAN CARLOS GARCÍA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El presente trabajo tiene como finalidad mostrar un diseño de red perimetral con seguridad básica y su debilidad al tener un punto de fallo único donde se concentra toda la protección y acceso de tráfico de red a una institución financiera (PYME).

Luego de evidenciar lo expuesto, se realiza un re-diseño de la red perimetral incorporando recomendaciones de seguridad y aumentando el nivel de protección dividiendo en diferentes zonas el acceso a los equipos.

Es por esto, que se incorpora en el nuevo diseño dispositivos como Mitigadores de Ataques, Firewall UTM, Balanceador de Carga, Anti spam, Firewall de aplicaciones web (WAF) que incrementarán el resguardo de la información y equipos de la organización.

Dentro de esta solución se consideran recomendaciones que rigen actualmente dentro del ámbito de las instituciones financieras, como lo es la regulación de resolución JB-2012-2148.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

DMZ	Demilitarized zone (Zona desmilitarizada)
FIREWALL	Dispositivo Cortafuego de Hardware o Software para bloqueo o autorización de accesos
FTP	File Transfer Protocol
HA	High Availability (Alta disponibilidad)
IP	Internet Protocol (Protocolo de Internet)
IPS	Intrusion Prevention System (Sistema de prevención de intrusos)
ISP	Internet Service Provider (Proveedor de servicios de Internet)
JB	Junta Bancaria del Ecuador
LAN	Local Area Network (Red de Área Local)
Mbps	Megabits per second (Megabits por segundo)
SBS	Súper Intendencia de Bancos del Ecuador
SFTP	Secure File Transfer Protocol (Protocolo seguro de transferencia de archivos)
SPAM	Termino referente a correo o mensaje basura (correo no deseado)
UTM	Unified Threat Management (Gestión Unificada de Amenazas)
WAF	Web Application Firewall (Firewall de aplicaciones web)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Debido al constante avance tecnológico y a la creciente demanda de servicios sobre el Internet, las instituciones financieras brindan una gama amplia de servicios a sus clientes, facilitando de esta manera las actividades que necesiten realizar en la organización a la cual confían sus valores monetarios, sin necesidad de asistir de manera personal a las instalaciones de la organización.

Sin embargo, muchas empresas que se desenvuelven en este sector olvidan lo importante y necesario que es contar con seguridad de la información dentro de su infraestructura tecnológica, para eliminar las grietas de acceso no autorizadas que permiten la fuga de información que es utilizada para los fraudes informáticos.

Considerando la gran importancia y la criticidad de la información que manejan las instituciones financieras es imprescindible que incorporen dentro

de su esquema de red perimetral recomendaciones de seguridad para mitigar las amenazas a la cual se encuentran expuesta en el Internet.

Acorde a lo mencionado, en este documento se realiza un nuevo diseño de red perimetral segura basada en capas de protección para una institución financiera pyme. Este trabajo no detalla la implementación de equipos sobre la organización, pero si especifica cómo deben ser incorporados dentro del esquema de red perimetral y los beneficios que brinda tenerlos en la organización, cumpliendo con las regulaciones locales del país que rigen a las empresas del sector financiero como es la resolución JB-2012-2148.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

Las entidades financieras debido a las exigencias del mercado y para brindar mayor flexibilidad a sus clientes, colocan a su disposición una serie de productos en línea para facilitar las transacciones que necesitan realizar diariamente sin necesidad de estar físicamente en la organización.

Para poder cumplir lo expuesto, se colocan varios servicios en Internet sin los controles y permisos de acceso necesarios que garanticen la integridad, disponibilidad, confidencialidad y no repudio de sus sistemas. Esto se debe, que aún en la cultura organizacional de las empresas se

toma muy ligeramente los temas relacionados con la seguridad de la información, lo que resulta en pensar que es suficiente colocar un único equipo firewall multipropósito que proteja sus redes contra los diferentes ataques de los crackers.

Para una entidad financiera pyme este tipo de solución única genera un punto de fallo con poca capacidad de procesamiento de hardware (procesador, memoria y disco) que soporta todo el tráfico de entrada y salida de la red, concentrando el esfuerzo de seguridad en un diseño de red perimetral pobre dependiente de un solo dispositivo, constando que los diferentes servicios en línea que tienen las instituciones financieras están expuestos a una gran cantidad de amenazas que afecta el correcto funcionamiento de sus productos en Internet.

1.2 SOLUCIÓN PROPUESTA

Con base a lo mencionado, es importante que las Entidades Financieras (Pymes) posean las medidas de seguridad necesarias para proteger y garantizar la integridad, disponibilidad, confidencialidad y no repudio de la información, sistemas y servicios que ofrecen considerando un diseño de seguridad en la red perimetral en capas.

A lo expuesto y con el objetivo de cumplir con lo necesario a nivel de seguridad de la información, se propone Re-Diseñar la red perimetral incorporando recomendaciones de Seguridad para una Entidad

Financiera (Pyme), con la finalidad de que los servicios ofrecidos por la institución financiera sean confiables hacia los clientes/usuarios, atenuando la posibilidad de fraudes o fuga de información de la organización.

Es por esto, que es necesario la incorporación de varios equipos especializados que cumplan la función de protección y mitigación de los diferentes ataques a los sistemas, dividiendo el diseño de la red en diferentes zonas de resguardo, obteniendo como beneficios:

- Eliminación de único punto de fallo en la red perimetral.
- Descongestión del ancho de banda de Internet.
- Descentralización del proceso de seguridad informática.
- Arquitectura y diseño de la red perimetral distribuida.
- Cumplimiento mínimo a nivel de recomendaciones de seguridad de la información sobre los entes de regulación del país como es la Súper-Intendencia de Bancos del Ecuador.

CAPÍTULO 2

DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS DE SITUACIÓN ACTUAL

Actualmente la organización tiene un total de 1100 usuarios los cuales se encuentran distribuidos entre matriz y sus diferentes sucursales. La Matriz posee 278 usuarios, la Sucursal Mayor 142 usuarios y el resto de agencias que son un total de 56 manejan un promedio de 12 usuarios por ubicación.

El diseño de la red perimetral implementada en la institución financiera actual es básico y cuenta con un dispositivo firewall multipropósito Sonicwall 2400 que realiza las siguientes funciones:

- Filtrado de paquetes de acceso a la red
- Sistema de protección contra SPAM

- Proxy de Navegación hacia el Internet
- Control de prevención de intrusos (IPS)
- Publicación de servicios en Internet

Los servicios publicados, se manejan a través de una dirección IP Pública proporcionada por el proveedor de servicios de Internet (ISP), los mismos que se encuentra usando el Internet corporativo de la organización con un ancho de banda de 2 Mbps provocando que los sistemas tengan un pobre desempeño hacia los clientes (un promedio de 12000 clientes de los cuales participan de manera activa 4300) ya que compiten con los usuarios de la institución por el consumo de ancho de banda.

Los servicios que maneja la empresa financiera son:

- Portal web informativo y transaccional (para usuarios)
- Sitio web de facturación electrónica
- Servicio banca móvil
- Portal web transaccional corporativo (para empresas)
- Servicio de transferencia de archivos (FTP)

Con base a las características limitadas del equipo firewall instalado en la red, la navegación a Internet es lenta por el excesivo consumo del ancho de banda y el poco control por la falta de registros de navegación de los usuarios para poder realizar un ajuste de los permisos establecidos. Además, se presentan de manera constante caídas del servicio de Internet, correo electrónico, servicios publicados, por problemas de falta de recursos en el equipo firewall por el gran tráfico de red que debe soportar y los ataques que debe mitigar.

Existen casos de interrupción de los servicios de hasta 6 horas por problemas de ataque de denegación de servicio distribuido o saturación por correo basura.

La organización no cuenta con un sistema de protección de Alta Disponibilidad (HA) y no posee dispositivos adicionales especializados que descongestionen la carga de trabajo que posee el equipo firewall instalado, exponiéndolo como único punto de fallo en la red perimetral. A continuación, se presenta el diseño de la red externa de la institución:

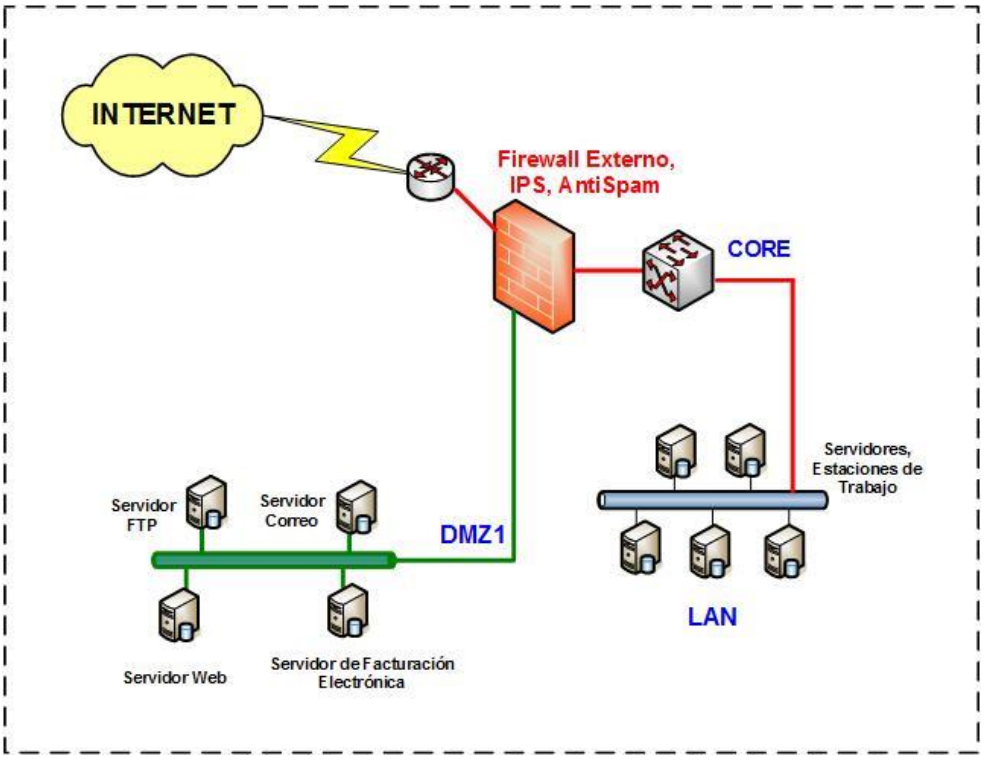


Figura 2.1 Diseño actual de la red

2.2 RE-DISEÑO LÓGICO DE LA RED PERIMETRAL ACTUAL

Debido a las debilidades mencionadas, se propone realizar un re-diseño de la red perimetral de la institución financiera que incorpore recomendaciones de seguridad y para ello es necesario tomar como marco referencial las regulaciones existentes para las empresas de este sector, que son dictaminadas por la Junta Bancaria y Auditadas en su cumplimiento por la Súper Intendencia de Bancos (SBS) del Ecuador.

Las resoluciones consideradas son:

- Resolución JB-2012-2148, Literal 4.3.8.3 [1]

- Resolución JB-2012-2148, Literal 4.3.11.5 [1]
- Resolución JB-2012-2148, Literal 4.3.11.8 [1]
- Resolución JB-2014-3066, Artículo 22 Literal 22.7 [2]

Las resoluciones señaladas con su respectivo literal indican, que debe incorporarse en la red dispositivos que contribuyan con el control, aseguren la integridad, disponibilidad, confidencialidad de la información de la organización mitigando la posibilidad de captura de los datos por terceros no autorizados. Para cumplir con lo señalado en los literales mencionados, se considera la inclusión de los siguientes equipos en el nuevo diseño de red perimetral:

1. Mitigador de ataques con módulo IPS
2. Implementación de firewall externo
3. Implementación de firewall interno
4. Balanceador de tráfico de red
5. Firewall de aplicaciones web

Luego de tener como referencia la regulación local se recomienda la incorporación de los siguientes dispositivos para descongestionar la

carga de trabajo y distribuirla en los diferentes equipos especializados creando capas de seguridad y acceso hacia nuestra red:

6. Implementación proxy server

7. Sistema anti spam y de cifrado de correo electrónico

Luego de la identificación de equipos necesarios según las regulaciones, se procede a esquematizar el nuevo diseño de la red perimetral que tendrá las siguientes zonas establecidas [3]:

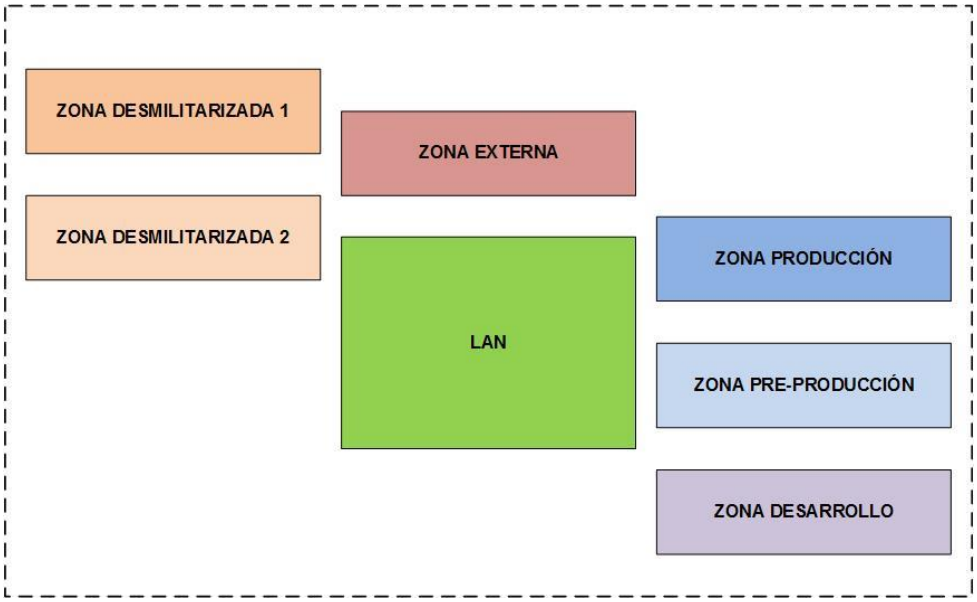


Figura 2.2 Definición de zonas protegidas de la red

Cada zona establecida corresponde a la siguiente definición:

Zona Externa.- referencia al mundo del Internet, los accesos externos, páginas web y servicios publicados de terceros, normalmente es de donde provienen los clientes de la entidad.

Zona Desmilitarizada 1.- contiene todos los equipos/servidores que estarán expuestos de manera directa al Internet ofreciendo los servicios de la institución financiera.

Zona Desmilitarizada 2.- en marca a los equipos que forman parte de los servicios publicados de la institución, sin embargo no necesitan estar expuestos al Internet pero manejan parte importante del proceso transaccional de la entidad financiera.

Zona Producción.- es donde se colocan todos los servidores internos que manejan importante información de la organización protegiéndolos de estar expuestos a los usuarios de la empresa.

Zona Pre-Producción.- contiene un grupo de equipos iguales a producción (no son los mismo equipos funcionales) necesarios para las pruebas y comprobaciones finales antes de pasar las aplicaciones a la zona de producción, la finalidad es que los programas nuevos cuenten con la estabilidad y seguridad necesaria para operar.

Zona Desarrollo.- ambiente de creación de aplicaciones donde se encuentran los equipos que trabajan los programadores de la entidad financiera, normalmente el equipo de trabajo solo tiene acceso a este ambiente y se encuentra filtrado a los equipos de producción y pre-producción.

Zona LAN.- lugar donde se establecen los usuarios de la red de la organización, podríamos indicar que colocamos los equipos escritorios de trabajos, portátiles, dispositivos móviles de los ejecutivos, etc.

Finalmente, se realiza el re-diseño de la red incorporando las recomendaciones de seguridad locales (vigentes en Ecuador) e internacionales [5] (tomadas de Cisco Systems) para la institución financiera (pyme):

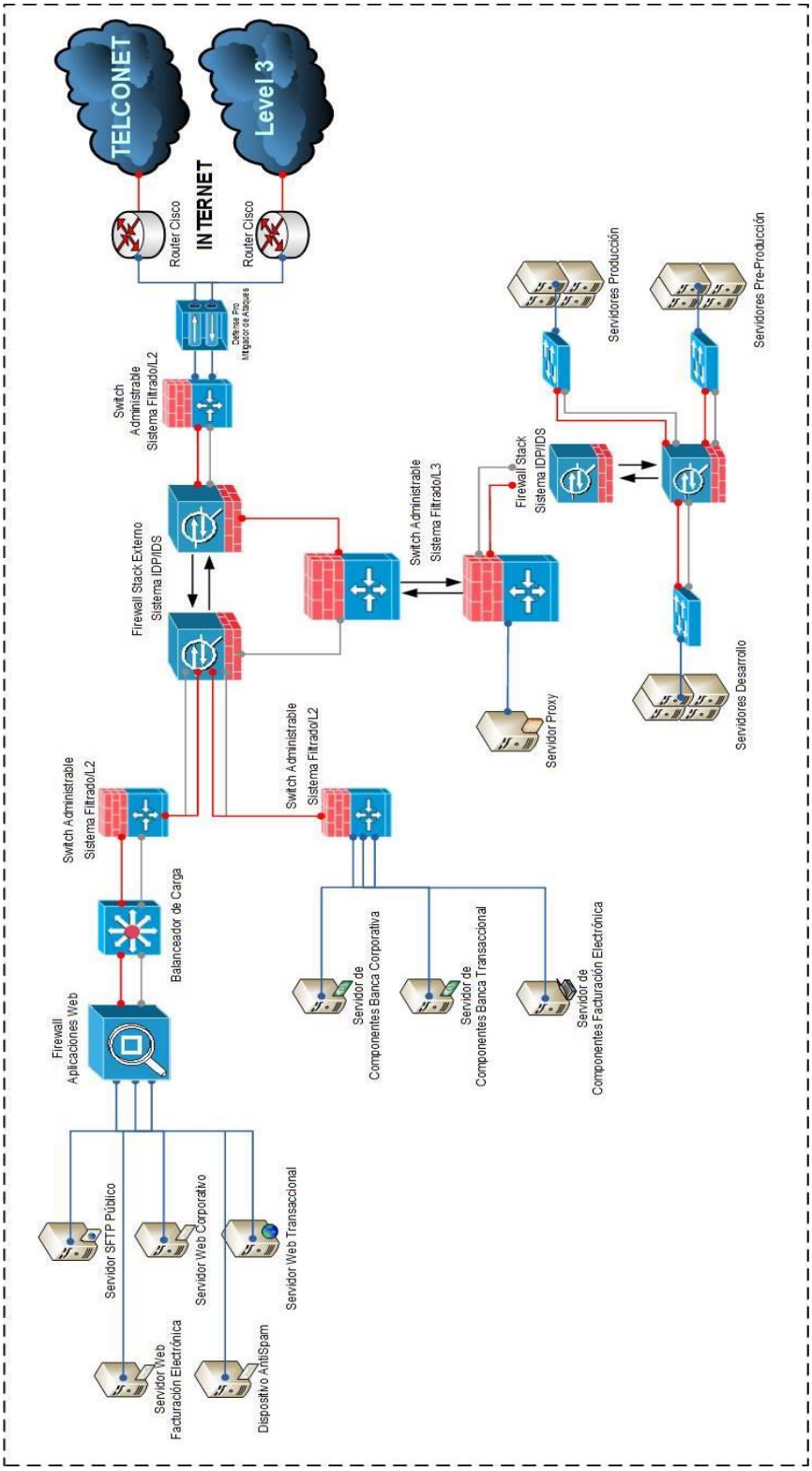


Figura 2.3 Nuevo Diseño de Red Perimetral

2.3 DISEÑO FÍSICO DE LA NUEVA RED PERIMETRAL

El nuevo diseño lógico de la red perimetral para la institución financiera, nos da la muestra para proceder con la instalación física de los equipos, obteniendo un modelo final de implementación como el siguiente:

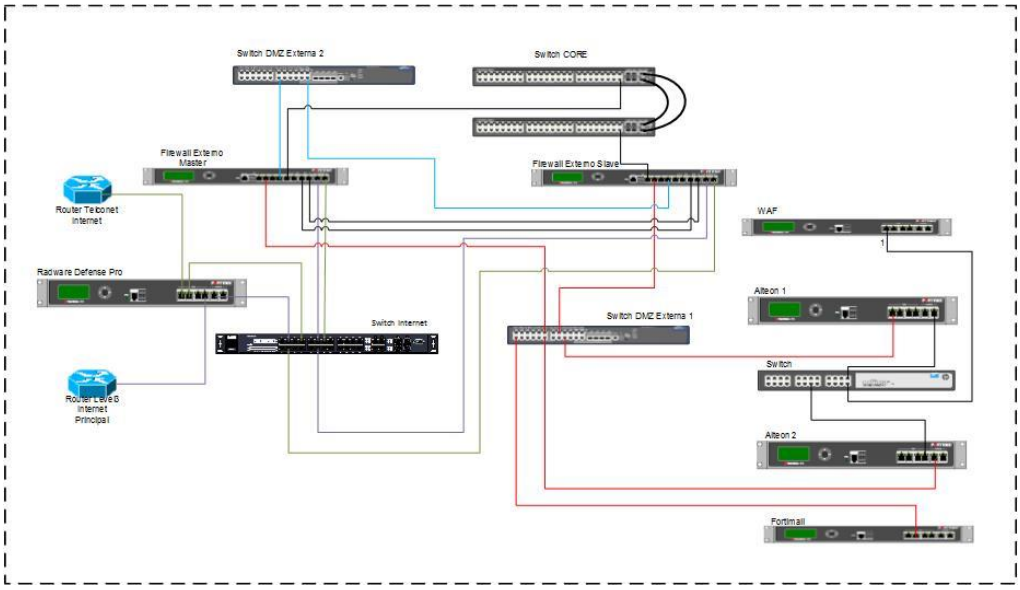


Figura 2.4 Diseño físico de la nueva red perimetral

Es importante mencionar que la figura 2.4 hace referencia a la implementación de equipos en la red perimetral de la red organizacional, al cual está enfocado este documento.

2.4 DETALLE DE LOS EQUIPOS INCORPORADOS EN LA NUEVA RED PERIMETRAL

La institución financiera en busca de mejorar su infraestructura tecnológica y seguridades, realizó una serie de inversiones e implementaciones de equipos con base al nuevo diseño de red perimetral desarrollado. A continuación detallamos sus funciones y características:

1. Mitigador de Ataques/IPS: se adquirió e instaló un equipo marca RADWARE Defense Pro en la parte perimetral de la red del Banco; este equipo es un appliance especializado en contener los ataques realizados por una persona con objetivos maliciosos hacia nuestra red y mitigarlos. Protege a la infraestructura contra la explotación de vulnerabilidades, propagación de malware, denegación de servicio por ataques individualizados o distribuidos y previene la saturación del canal de Internet [6].

   Al mismo tiempo este equipo brinda la protección IPS (Sistema de Prevención de Intrusos) de los ataques más conocidos según la base de datos del fabricante RADWARE

2. Reemplazo y Fortalecimiento de Políticas Firewall.- A fin de mejorar y fortalecer los accesos y salidas de nuestra red a los diferentes segmentos (Internet, DMZs, Comercios Externos), se realizó la incorporación de un nuevo firewall Fortigate 300C en reemplazo del equipo Sonicwall 2400, luego de ellos se revisó las políticas firewall para ajustar los permisos de la red, reduciendo los más permisivos y eliminando aquellos accesos que no son necesarios o ya no eran utilizados.

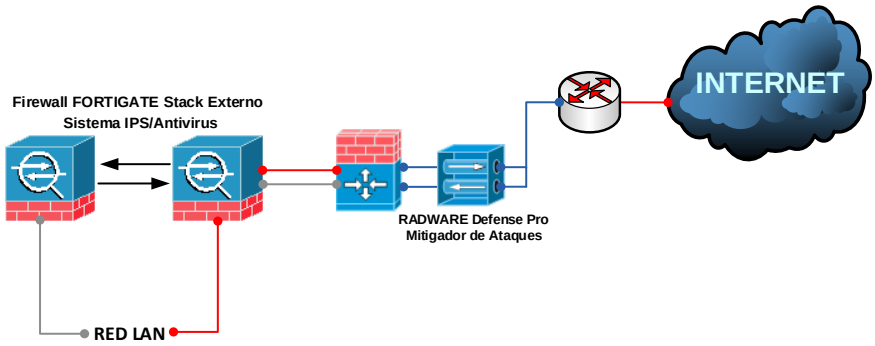


Figura 2.5 Interacción Firewall y Mitigador de Ataques

3. Balanceador de Carga.- Dispositivo Appliance que permite realizar una distribución de tráfico para evitar congestiones de los servicios, este equipo al balancear la carga de trabajo en diferentes servidores apoya a la mitigación de los ataques de denegación de servicio, para esta implementación la organización eligió el equipo RADWARE ALTEON 5224.

4. Firewall de aplicaciones web (WAF).- Equipo Appliance especializado a proteger los sitios web de los ataques del Internet conocidos como el SQLi, Blind SQL, XSS, LFI, RFI, etc. La institución financiera eligió la implementación del equipo RADWARE APPWAL 508.

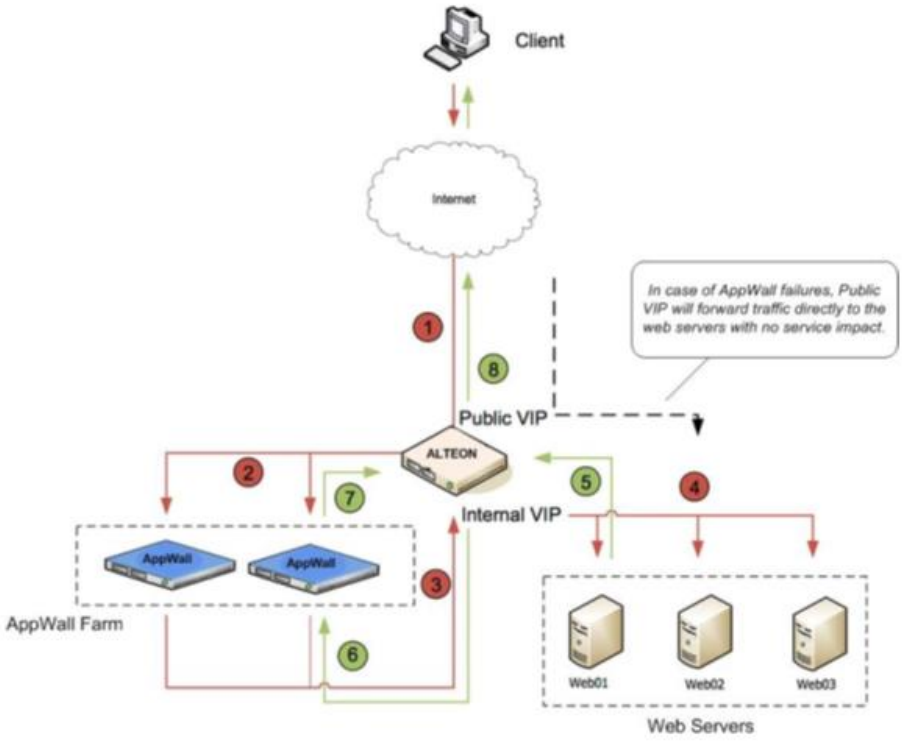


Figura 2.6 Diagrama funcional del Balanceador y el WAF

5. Sistema anti spam y de cifrado de correo electrónico.- Hardware con la capacidad de proteger de manera inteligente a la organización de las nuevas metodologías de ataque de correo

basura [4], permitiendo de manera adicional cifrar cada mensaje de correo electrónico que contiene información crítica del usuario/cliente. El dispositivo implementado es un Fortimail 400C.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 MITIGACIÓN DE ATAQUES

Dentro de la mitigación de ataques podemos observar que los equipos implementados están realizando la función especializada por la cual fueron adquiridos, como muestra de lo expuesto demostramos las siguientes capturas de pantalla:

Mitigador de Ataques – Radware Defense Pro:

Como podemos observar en la pantalla de la consola detecta un origen sospechoso que proviene del viejo continente y luego de ello realiza la notificación vía correo electrónico al grupo de respuesta de incidentes.

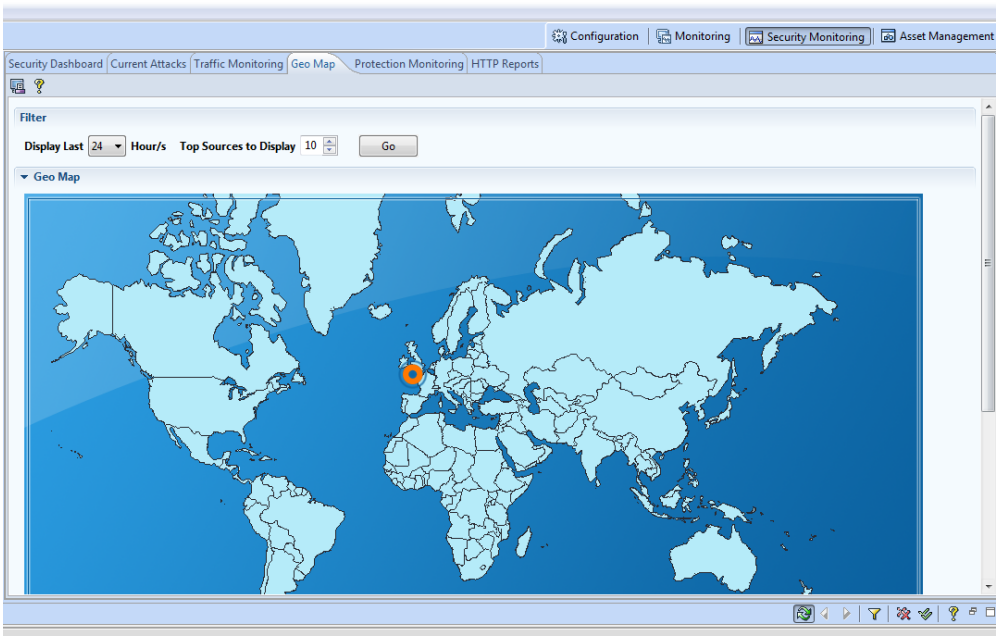


Figura 3.1 Detección de amenaza del mitigador de ataques

Figura 3.2 Mensaje del mitigador de ataques y su acción ejecutada

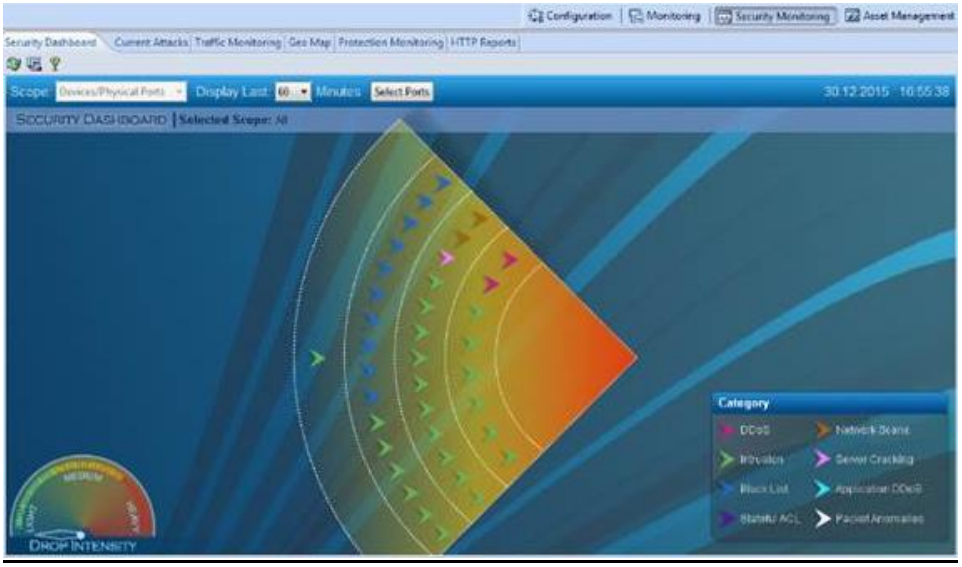


Figura 3.3 Dashboard de Progreso de ataques identificados

Esta pantalla es observada de forma permanente por el operador de seguridades y revisa los intentos de ataque, la herramienta con base a las reglas establecidas bloquea automáticamente los diferentes intentos de intrusión, sin embargo cuando vemos que el ataque es persistente y que se trata de un proceso automático, se procede a poner en lista negra la dirección IP del atacante para restringir de manera total cualquier intensión maliciosa.

Cortafuegos de Red - Firewall FORTIGATE:

En la pantalla de logs del firewall podemos observar las restricciones que se están realizando gracias al endurecimiento de las políticas y a las características de protección que presta el equipo.

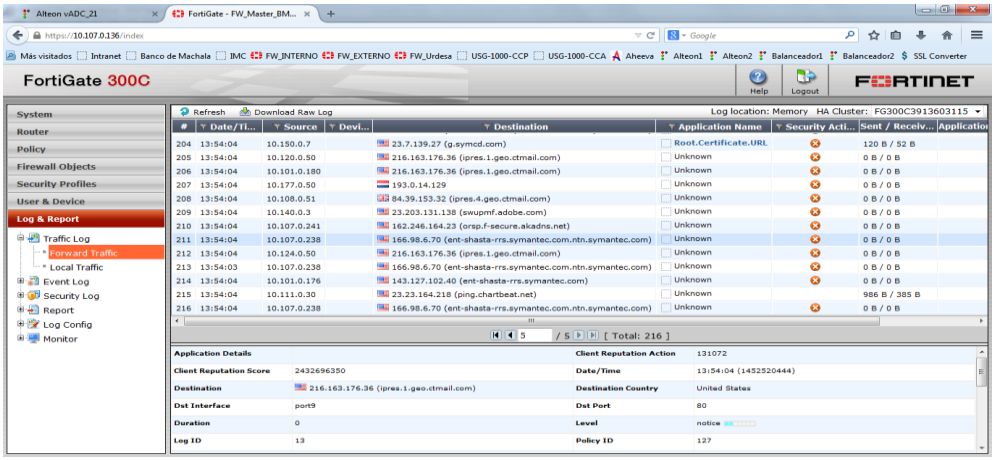


Figura 3.4 Registro de bloqueos del Firewall FORTIGATE 300C

Balanceador de Carga – Radware Alteon:

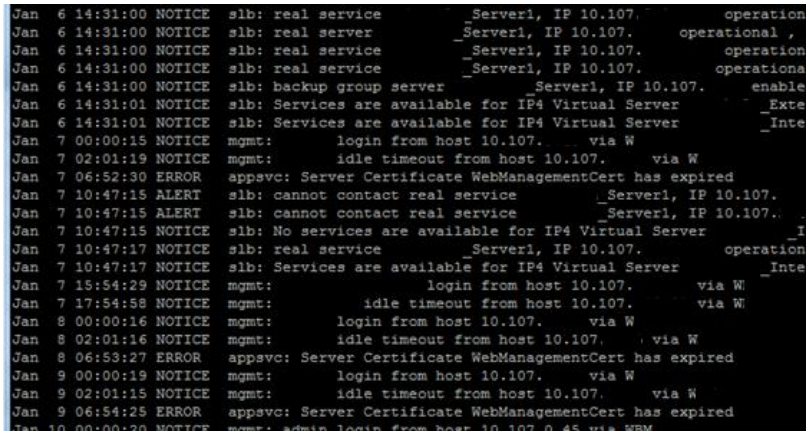


Figura 3.5 Distribución de tráfico de red del Balanceador

3.2 ESTADÍSTICA DE CONTROL

Luego de verificar que las herramientas implementadas están realizando el trabajo de prevención, bloqueo o denegación de acceso,

precautelando la disponibilidad, integridad y confidencialidad de la información, se muestra la estadística de los resultados obtenidos:

Tabla 1 Bloqueos de ataques del mitigador Radware

Categorías	Cuenta de Categoría
BlackList	203
Packet Anomalies	32
TCP Scan	2
DDoS	2
Intrusions	62
Server Cracking	58
HTTP Flood	34
UDP Scan	3
Total general	**396**

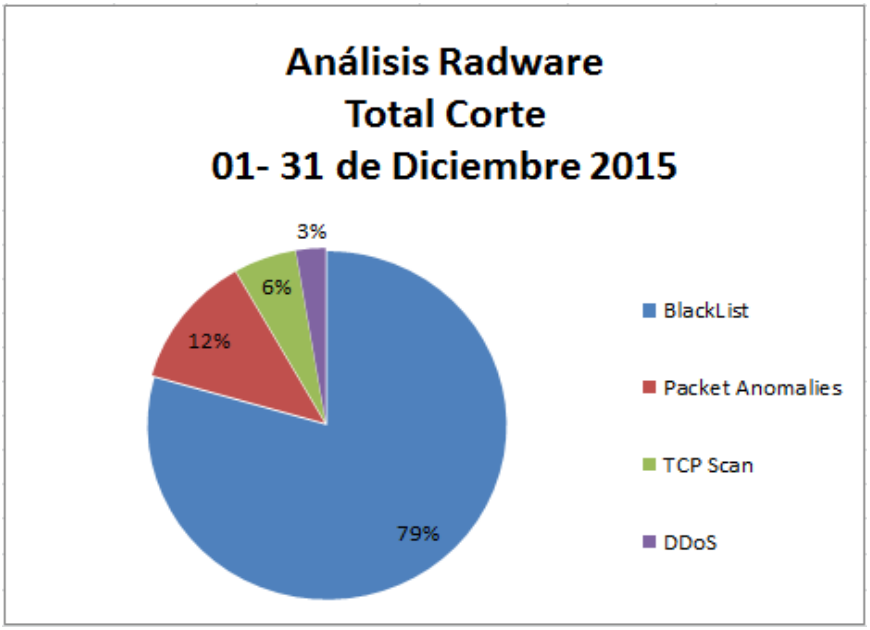
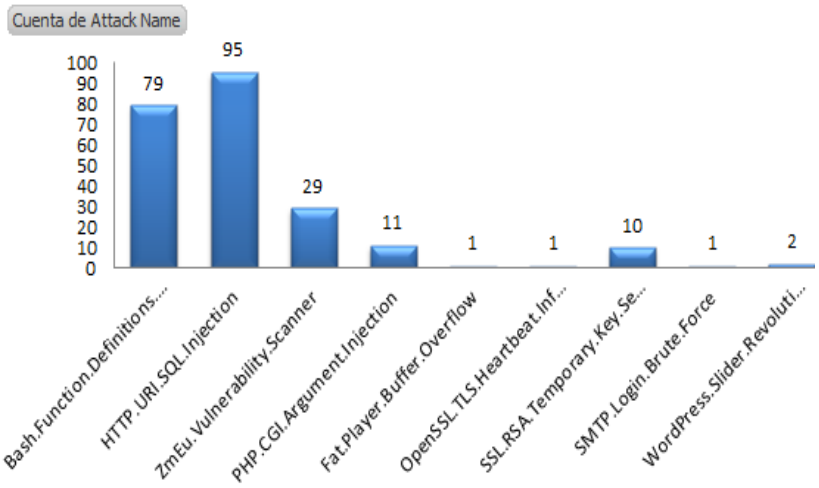


Tabla 2 Detección y bloqueo de ataques firewall perimetral

Etiquetas de fila	Cuenta de Attack Name
Bash.Function.Definitions.Remote.Code.Execution	79
HTTP.URI.SQL.Injection	95
ZmEu.Vulnerability.Scanner	29
PHP.CGI.Argument.Injection	11
Fat.Player.Buffer.Overflow	1
OpenSSL.TLS.Heartbeat.Information.Disclosure	1
SSL.RSA.Temporary.Key.Security.Bypass	10
SMTP.Login.Brute.Force	1
WordPress.Slider.Revolution.File.Inclusion	2
Total general	**229**



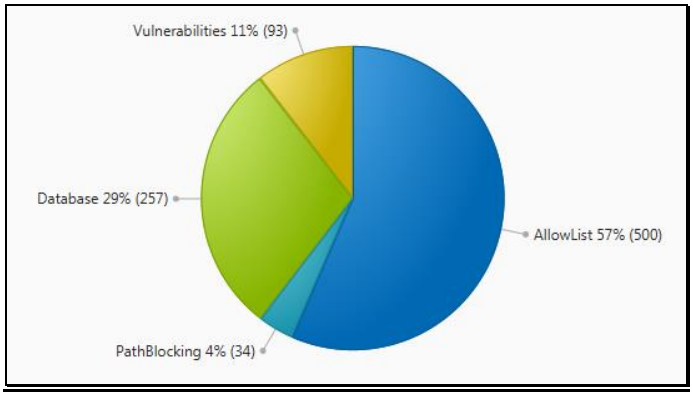


Figura 3.6 Detección y bloqueo de ataques del (WAF)

3.3 BALANCE DE RESULTADOS

Podemos notar una mejora radical del comportamiento en la red, con el cambio del diseño e implementación de los nuevos equipos se observa estabilidad de las aplicaciones, el tiempo de respuesta ha mejorado dentro de la infraestructura, existe un mejor uso del ancho de banda de Internet y la disponibilidad de los servicios es permanente. Los resultados actuales muestran una gran diferencia en la detección y prevención de ataques en comparación a los anteriores meses previa a la implementación. A pesar de no tener registros ni dispositivos que evidenciaran los ataques iniciales previa a la implementación, en el transcurso del tiempo los registros muestran que tiene una tendencia a la baja, en parte gracias al control y a la tarea de tomar las acciones preventivas necesarias para evitar futuros ataques, como lo muestra a continuación el cuadro comparativo en cifras del mes anterior vs el mes de marzo:

Tabla 3 Cantidad de ataques detectados Radware

Octubre	Noviembre	Diciembre
656	710	**646**

Tabla 4 Cantidad de ataques detectados Firewall

Octubre	Noviembre	Diciembre
54	347	**229**

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El re-diseño de la red perimetral que incorpora recomendaciones de seguridad para la institución financiera pyme, ha brindado beneficios importantes para la institución a nivel de seguridades, asegurando la disponibilidad y confidencialidad de sus sistemas.

2. Las soluciones implementadas muestran estabilidad y eficiencia a través de los controles aplicados al tráfico de la red generado por los usuarios internos/externos de la organización, dando espacio a la flexibilidad de personalizar cada política en caso de que sea necesario.

RECOMENDACIONES

1. La organización debe acompañar la solución implementada con una buena política de seguridad para complementar y fortalecer la seguridad de la información dentro de la institución financiera.

2. Se debe establecer un plan de mantenimiento y seguimiento de los equipos, con la finalidad de precautelar el correcto funcionamiento del hardware y en caso de fallo recuperarlo desde los respaldos.

3. Se debe incorporar una política de control de cambios para el nuevo diseño de la red perimetral y de esta forma garantizar la continuidad del servicio que brindan los sistemas implementados.

4. Se recomienda capacitar al personal técnico a cargo de los diferentes equipos, con la finalidad de brindar una correcta administración y se continúe con las actividades post-implementación de aseguramiento.

5. Migrar el servicio inseguro de transferencia de archivos (FTP) al servicio seguro de transferencia de archivos (SFTP) para garantizar el cifrado de la información que se transfiere entre un origen y destino, evitando de esta manera la intercepción de los datos.

BIBLIOGRAFÍA

[1] Junta Bancaria del Ecuador - SBS, Resolución JB-2012-2148, http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=760&vp_tip=2, Publicada el 26 de Abril del 2012

[2] Junta Bancaria del Ecuador - SBS, Resolución JB-2014-3066, http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=760&vp_tip=2, Publicada el 2 de Septiembre del 2014

[3] IBM Red Book, Understanding IT Perimeter Security, http://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf, Fecha de consulta Enero del 2016

[4] Cisco Systems, Informe anual de seguridades de Cisco 2015, http://www.cisco.com/web/ES/offers/lp/2015-annual-security-report/index.html, Fecha de consulta Enero del 2016

[5] Cisco Systems, Designing Perimeter Security, http://docstore.mik.ua/cisco/pdf/Cisco.Designing.Perimeter.Security.pdf, Fecha de consulta Enero del 2016

[6] RADWARE, Defense Pro, http://www.radware.com/Products/DefensePro/,

Fecha de consulta Enero del 2016