ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“IMPLEMENTACIÓN DE UN CLUSTER DE FIREWALL - CHECKPOINT PARA REEMPLAZAR EL FIREWALL – ROUTER DE UNA ADMINISTRADORA DE FONDOS COMPLEMENTARIOS PROVISIONAL CERRADO.”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

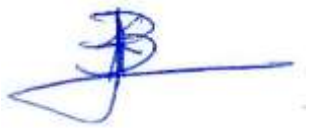
AUTOR

KATHIA ISABEL TELLO BAQUERO

GUAYAQUIL, JUNIO 2020

AGRADECIMIENTO

A Dios por permitirme haber concluido con una etapa más de mi formación académica, a mi esposo por haber sido mi apoyo en este proceso, a mi hija por el tiempo que dejé de estar con ella para lograr este objetivo y a mi sobrino por cooperar en el cuidado de la niña.



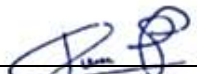
DEDICATORIA

Quiero dedicar este trabajo a mi hermana por enseñarme con su ejemplo a ser perseverante, por permitirme verme a través de sus ojos como una mujer profesional, madre y esposa.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenín Freire Cobo

CORDINADOR MSIG



MSIG. Juan Carlos García

PROFESOR DELEGADO POR EL

SUBDECANO DE LA FIEC

RESUMEN

Esta implementación tiene como objetivo principal brindarle a la Administradora de Fondos Complementarios Cerrados un Firewall - Router de alta disponibilidad, puesto que si alguno de sus nodos deja de funcionar el otro toma el control y gestiona todas las peticiones de transaccionalidad, provengan del ERP, Call Center, Correo institucional, Página Web y demás servicios publicados, sin detener sus actividades, para los usuarios sería imperceptible existe una falla.

Al utilizar un appliance para la administración de las reglas de acceso, otro appliance para la reportería, se deja el procesamiento en los dos nodos del cluster del Firewall, que al trabajarán con balanceo de carga, es decir ambos equipos procesarán las peticiones de los diferentes servicios que ofrece TI, incrementando la velocidad de respuesta.

Además, de optimizar el tiempo de respuesta de la navegación de las estaciones de trabajo, gracias a la implementación de un Proxy Linux, que además de proporcionar el Cache de las páginas frecuentes, gestionará las peticiones de descargas, validando las extensiones permitidas, los puertos de acceso, descargando así al Firewall de esta actividad.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

DMZ Zona desmilitarizada, segmento de red que publica sus servicios y es protegido por el Firewall.

ERP Enterprise Resourse Planning - Planificación de Recursos Empresariales.

GPO Directiva de Grupo, se utilizan para implementar configuraciones específicas en los equipos.

IP Internet Protocol – Protocolo de Internet.

MSIG Magíster en Sistemas de Información Gerencial.

QoS Quality of service - calidad de servicio.

TI Tecnologías de Información.

VPN Virtual Private Network – Red Privada Virtual, se utiliza para crear una extensión segura de una red local.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El presente documento describe la problemática de una Administradora de Fondos Complementarios, la solución que se implementó para solventarlo y la evaluación de los resultados obtenidos. A continuación se resume los apartados del documento. En el capítulo 1 – Generalidades, se describe el problema y se propone una solución que permite solventarlo. En el capítulo 2 – Metodología para el Desarrollo de la solución, se narrá desde el levantamiento de la información , el dimensionamiento tanto del hardware como el software requerido, así como el plan de acción, finalizando con la implementación de la solución la cual tiene dos etapas, la implementación del Proxy y la implementación del Cluster del Firewall. En el capítulo 3 – Evaluación de Resultados, donde se evalúa el monitoreo del funcionamiento del Cluster, se genera un informe comparativa y se listan los beneficios de la solución. Finalizamos el documento con las conclusiones y recomendaciones

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

La Administradora de Fondos Complementarios Provisional Cerrado contaba con 50 empleados cuando realizó la implementación de Firewall – Router del fabricante Checkpoint, el cual fue instalado en un Servidor HP ML 110 al cual se le adicionó dos tarjetas duales para tener 5 segmentos de red: Servidores, DMZ, Producción, Call Center, Internet. En este equipo se tenía instalado el Software del Fabricante Checkpoint, la consola de Administración (Smart- Dashboard) y la reportería (Smart- Report),

además, de las funciones de Firewall este equipo hacía las veces de un switch Core y de Proxy.

Cuando una estación de trabajo realizaba una transacción en el ERP la petición pasaba por el Firewall, pues éste validaba si la IP tenía permiso para acceder inclusive existen reglas con horarios establecidos. De igual forma ocurre con el Sistema del Call Center, todas las peticiones pasan por el Firewall antes de ir al Servidor de Base de Datos.

Toda la navegación pasa por el Firewall, valida en que grupo se encuentra, a que puertos tiene permiso y en que horarios. Protege la DMZ, es decir los Servidores que se tienen publicados, como página Web, Servidor de Correo, y Web Services reciben sus peticiones una vez que el Firewall las valide y se las transfiera.

Al incrementar a 150 el número de empleados el Firewall empezó a colapsar, se saturaba por la cantidad de peticiones que tenía que procesar, al haberse convertido en un punto crítico, cada vez que este equipo estaba inhibido ningún empleado que utilice computador puede trabajar, no se puede utilizar el ERP, ni el Call Center, ni correo institucional, ni navegar, además los servicios que se tenían publicados eran inaccesibles.

1.2 SOLUCIÓN PROPUESTA

La solución que se propone para resolver el problema detallado en la sección anterior es la Implementación de un Cluster de Firewall – Checkpoint que permita procesar ágilmente sin caídas de servicio, la transaccionalidad de la Administradora de Fondos Complementarios Provisional Cerrado, tanto del ERP, el Call Center, la DMZ y la protección contra intrusos.

Este cluster constará de un appliance checkpoint, dos nodos para el balanceo de carga y un appliance Smart 1 - Reports. El appliance tiene embebido el Sistema Operativo propietario del Checkpoint, que tiene el Smart-Dashboard, que es la herramienta donde se crean y configuran las redes, los grupos y cada uno de los objetos que requieren acceder a los recursos informáticos que provee TI, además de las reglas de acceso y/o restricciones las cuales constan con sus puertos de acceso y respectivos horarios.

Los dos nodos del Cluster del Firewall estarán en dos servidores HP DL360 G7 de características idénticas, a ambos equipos se les adicionó una tarjeta de fibra para que la velocidad de transferencia de datos sea la óptima, cuando uno de los nodos falle el otro de forma automática asume

todo el procesamiento, sin que se vean afectados los servicios informáticos.

Adicionalmente se implementará un proxy Linux para incrementar la velocidad de la navegación de los usuarios, gracias al caché que tiene el proxy, descongestionando además las peticiones de Navegación del Firewall – Checkpoint, puesto que todas las reglas de navegación referentes a horarios, descargas y puertos de navegación serían gestionadas en este equipo. En el Firewall – Checkpoint se tendría una única regla que le daría permiso de navegación, descarga y acceso a puertos de navegación específicos.

CAPÍTULO 2

METODOLOGÍA PARA EL DESARROLLO DE LA SOLUCIÓN

2.1 LEVANTAMIENTO DE LA INFORMACIÓN

El Oficial de Seguridades Lógicas es el encargado de Administrar el Firewall Checkpoint, es quien crea las reglas de acceso y denegación a los diferentes segmentos de red que posee la Administradora de Fondos Complementarios Provisional Cerrado, cada vez que ingresa un nuevo

equipo debe ser creado en Smart – Dasboard y colocado en la regla de acceso pertinente, como navegación, acceso al ERP o Call Center de ser el caso, cuando el equipo ya no debe tener los accesos se lo retira de los grupos y se lo elimina.

Si se requiere tener acceso a un puerto específico se lo debe colocar de forma explícita mediante una regla, la cual está formada por el objeto origen el objeto destino, el puerto y el horario. Todo cambio lógico que se realiza en el Smart – Dasboard se debe compilar y aplicar, para que se queden de forma permanente, esto es totalmente transparente para los usuarios, se lo realiza en caliente *. No así los cambios físicos como incremento de memoria, adicionar tarjetas de red, o mantenimientos físicos programados, requieren de una ventana de trabajo puesto que al estar apagado el Firewall – Checkpoint nadie puede trabajar.

Los respaldos de la configuración del Firewall Checkpoint se generan de forma automática todos los domingos a las 05h00 y se quedan dentro del mismo equipo, todos los lunes, de forma manual se genera un respaldo de las reglas de administración, ambos respaldos se extraen vía ftp al equipo del Oficial de Seguridad de la Información, se lo graba en un CD y se la copia en el equipo de contingencia y se la aplica para que se encuentre

actualizado, luego se entrega el CD del respaldo generado para que el operador lo almacene en el casillero del banco.

Existe un manual de configuración del Firewall Checkpoint, el cual tiene detallado los segmentos de red, la versión del Firewall instalada y los pasos a seguir para realizar una instalación desde cero, Las reglas de administración también se encuentran documentadas y están en custodia del Oficial de Seguridades, dado que las actualiza a medida que se dan los cambios.

El Oficial de Seguridades Lógicas monitorea los eventos de accesos denegados que hubieran ocurrido, esto con la finalidad de detectar posibles ataques recurrentes y realiza afinamientos trimestrales al Firewall.

2.2 DIMENSIONAMIENTO DEL HARWARE Y SOFTWARE REQUERIDOS

2.2.1 DIMENSIONAMIENTO DE SOFTWARE REQUERIDO

La Administrador de Fondos Complementarios Provisional Cerrado tiene una licencia Checkpoint Security Platform pero para la implementación de un cluster de Firewall Checkpoint se requiere un licenciamiento diferente, al tener una licencia vigente se le solicitará al proveedor una actualización para solo adquirir las restantes y así poder obtener las

licencias para la implementación, mismas que se detalla en la Tabla 1 - Licenciamiento Cluster de Firewall – Checkpoint.

Tabla 1 - Licencias del Firewall

Cantidad	Descripción
1	Upgrade License Checkpoint Security Platform a Blade Checkpoint Security Platform
1	License Blade Checkpoint Security Platform

Fuente: Elaborado por el autor

Tanto el appliance Smart-Dashboard como el appliance Smart 1 - Reports tienen embebido el Sistema Operativo propietario del Checkpoint, a los dos nodos del Firewall se les deberá instalar el Sistema Operativo del fabricante “checkpoint security platform”. El Proxy que se implementará será un Centos 6, distribución de Linux Red Hat Enterprise, cuya licencia no tiene costo, pero el soporte anual si.

2.2.2 DIMENSIONAMIENTO DEL HARWARE

Para la implementación del Clúster de Firewall – Checkpoint se requiere:

- Un appliance Smart 1 - Reports
- Un appliance Smart-Dashboard
- Dos servidores HP DL360 G7

Para implementar el Proxy se requerirá un servidor HP DL140 G4. El detalle de las características del Hardware requerido se encuentra en la tabla 2.

Tabla 2 - Características del Hardware requerido

Tipo	Modelo	Procesador	Core	RAM	Disco Duro
Firewall Nodo 1	HP Proliant DL360 G7	Xeon E5640 2.66GHZ	4	6GB	146 GB
Firewall Nodo 2	HP Proliant DL360 G7	Xeon E5640 2.66GHZ	4	6GB	146 GB
Smart-Dashboard	Appliance CheckPoint	----------	2	4GB	130 GB
Smart 1 – Reports	Appliance CheckPoint	----------	2	4GB	130 GB
Proxy	HP DL140 G3	1 Xeon 1.60 Ghz	1	8GB	132 GB

Fuente: Elaborado por el autor

2.3 GENERACIÓN DEL PLAN DE ACCIÓN

Para poder ejecutar el proyecto de Implementación de Clúster de Firewall se requieren un total de 58 días, como se muestra en la figura 2.1 – Cronograma, tiempo en el cuál se ejecutarán las dos fases, la Implementación como tal del Clúster, y la fase de implementación del Proxy que requiere 22 días, los cuales están incluido en el tiempo total del proyecto.

Nombre de tarea	Duración	Comienzo	Fin
Fase - Implementación de Cluster de Firewall	58 días	jue 01/03/18	vie 18/05/18
Fase - Implementación de Proxy	22 días	jue 01/03/18	vie 30/03/18

Nombre de tarea	Duración	Comienzo	Fin
Implementación de Cluster de Firewall	58 días	jue 01/03/18	vie 18/05/18
Adquisición de Hardware y Software	30 días	jue 01/03/18	mié 11/04/18
Configuración	13 días	jue 12/04/18	lun 30/04/18
Pruebas	9 días	mar 01/05/18	vie 11/05/18
Implementación	1 día	sáb 12/05/18	sáb 12/05/18
Monitoreo y estabilización	5 días	lun 14/05/18	vie 18/05/18
Implementación de Proxy	22 días	jue 01/03/18	vie 30/03/18
Preparación y configuración del Proxy	9 días	jue 01/03/18	mar 13/03/18
Pruebas	6 días	mié 14/03/18	mié 21/03/18
Implementación	4 días	jue 22/03/18	mar 27/03/18
Monitoreo y estabilización	3 días	mié 28/03/18	vie 30/03/18

Figura 2.1 – Cronograma de Implementación de Clúster de Firewall
Fuente: Elaborado por el autor

En virtud que el proyecto de implementación del Clúster de Firewall requiere de equipos que se deben importar, se iniciaría con la fase de implementación del Proxy, puesto que el equipo se lo tiene disponible de forma inmediata, adicionalmente con esto podemos alivianar la cargar del Firewall en cuanto a peticiones de navegación se refiere.

Esta implementación no tendría costos adicionales pues el trabajo sería realizado por personal interno del Departamento de Sistemas tomando un tiempo de 22 días laborables, tal como lo muestra la figura 2.2 – Cronograma Implementación de Proxy, se tendrían 9 días para la etapa de configuración, 6 días para la etapa de pruebas, 4 días para la implementación y 3 días de Monitoreo y estabilización.

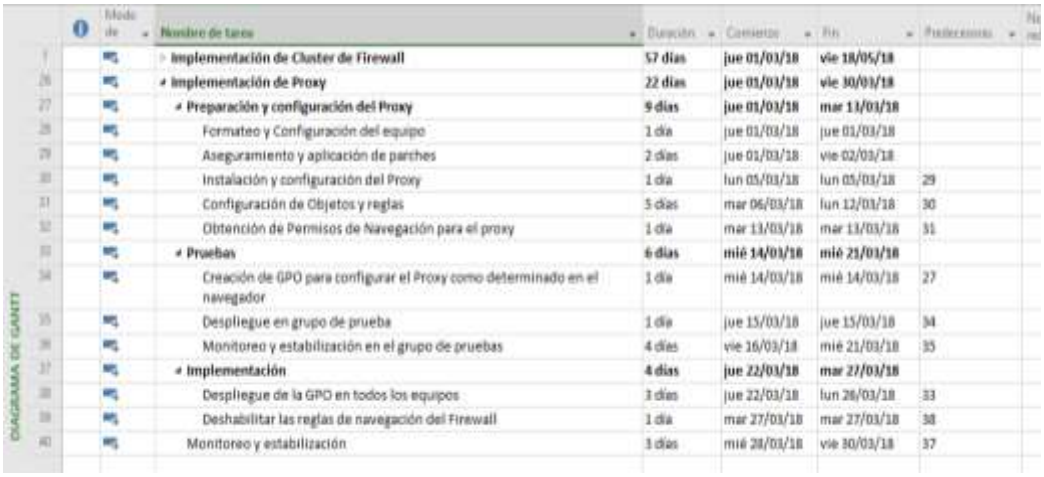


DIAGRAMA DE GANTT

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**Implementación de Cluster de Firewall**	**57 días**	**jue 01/03/18**	**vie 18/05/18**	
26		**Implementación de Proxy**	**22 días**	**jue 01/03/18**	**vie 30/03/18**	
27		**Preparación y configuración del Proxy**	**9 días**	**jue 01/03/18**	**mar 13/03/18**	
28		Formateo y Configuración del equipo	1 día	jue 01/03/18	jue 01/03/18	
29		Aseguramiento y aplicación de parches	2 días	jue 01/03/18	vie 02/03/18	
30		Instalación y configuración del Proxy	1 día	lun 05/03/18	lun 05/03/18	29
31		Configuración de Objetos y reglas	5 días	mar 06/03/18	lun 12/03/18	30
32		Obtención de Permisos de Navegación para el proxy	1 día	mar 13/03/18	mar 13/03/18	31
33		**Pruebas**	**6 días**	**mié 14/03/18**	**mié 21/03/18**	
34		Creación de GPO para configurar el Proxy como determinado en el navegador	1 día	mié 14/03/18	mié 14/03/18	27
35		Despliegue en grupo de prueba	1 día	jue 15/03/18	jue 15/03/18	34
36		Monitoreo y estabilización en el grupo de pruebas	4 días	vie 16/03/18	mié 21/03/18	35
37		**Implementación**	**4 días**	**jue 22/03/18**	**mar 27/03/18**	
38		Despliegue de la GPO en todos los equipos	3 días	jue 22/03/18	lun 26/03/18	33
39		Deshabilitar las reglas de navegación del Firewall	1 día	mar 27/03/18	mar 27/03/18	38
40		Monitoreo y estabilización	3 días	mié 28/03/18	vie 30/03/18	37

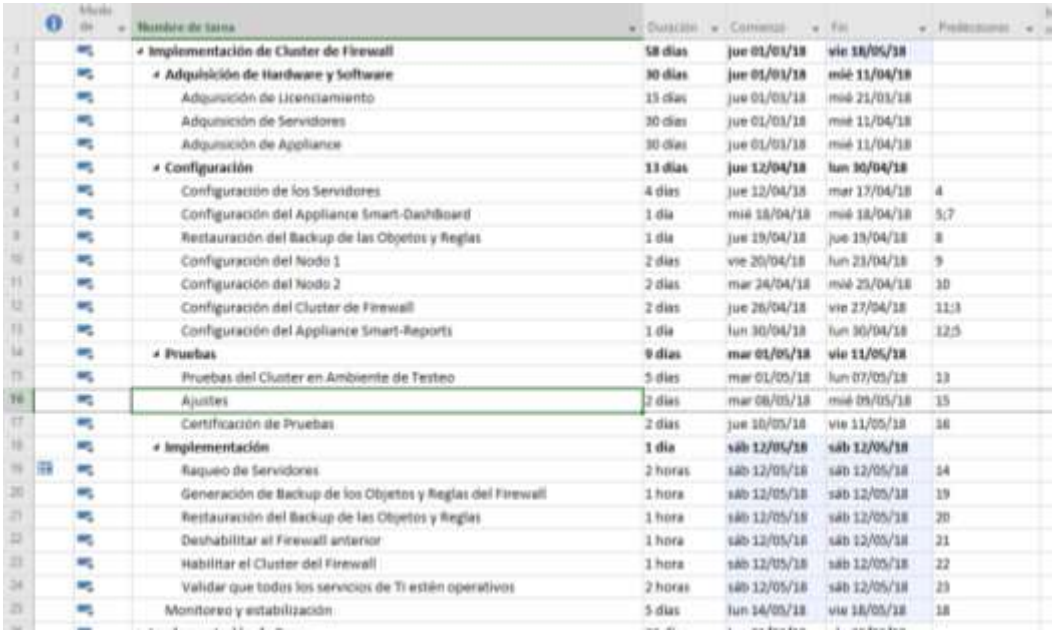
Figura 2.2 - Cronograma Implementación del Proxy
Fuente: Elaborado por el autor

Las reglas de navegación no se eliminan del Firewall, se las deshabilita con la finalidad de tener un plan B de navegación, en caso de que el Proxy no funcione se despliega la GPO para quitar el proxy por defecto y se habilita la política en el Firewall para que los equipos puedan navegar.

En paralelo se ejecuta la etapa de Adquisición de Hardware y Software de la fase de implementación de Clúster de Firewall, tal como lo muestra la figura 2.3 – Cronograma Implementación Clúster de Firewall, puesto que la importación de servidores y appliance tardan 30 días. Una vez recibidos se inicia la etapa de configuración en un lapso de 13 días, seguido de la etapa de Pruebas que se desarrollaran en 8 días, la implementación se efectúa en un solo día, en esta ventana de trabajo los servicios de TI no se encontraran disponibles; la estabilización se la realizará durante 5 días.

La ventana de trabajo para la implementación del Clúster del Firewall está asignada para un sábado para no afectar la operatividad diaria, adicionalmente en caso de haber complicaciones se tendría la noche del sábado y el domingo para solventarlos.

También se tiene contemplado el peor escenario, que la implementación falle, en cuyo caso se reversarían los cambios colocando nuevamente el Firewall anterior para garantizar que el lunes la operatividad no se vea afectada, y se tendría que volver a la etapa de pruebas, y posteriormente reprogramar una ventana de trabajo para la implementación.



	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**Implementación de Cluster de Firewall**	**58 días**	**jue 01/03/18**	**vie 18/05/18**	
2		**Adquisición de Hardware y Software**	**30 días**	**jue 01/03/18**	**mié 11/04/18**	
3		Adquisición de Licenciamiento	15 días	jue 01/03/18	mié 21/03/18	
4		Adquisición de Servidores	30 días	jue 01/03/18	mié 11/04/18	
5		Adquisición de Appliance	30 días	jue 01/03/18	mié 11/04/18	
6		**Configuración**	**13 días**	**jue 12/04/18**	**lun 30/04/18**	
7		Configuración de los Servidores	4 días	jue 12/04/18	mar 17/04/18	4
8		Configuración del Appliance Smart-Dashboard	1 día	mié 18/04/18	mié 18/04/18	5;7
9		Restauración del Backup de las Objetos y Reglas	1 día	jue 19/04/18	jue 19/04/18	8
10		Configuración del Nodo 1	2 días	vie 20/04/18	lun 23/04/18	9
11		Configuración del Nodo 2	2 días	mar 24/04/18	mié 25/04/18	10
12		Configuración del Cluster de Firewall	2 días	jue 26/04/18	vie 27/04/18	11;3
13		Configuración del Appliance Smart-Reports	1 día	lun 30/04/18	lun 30/04/18	12;5
14		**Pruebas**	**9 días**	**mar 01/05/18**	**vie 11/05/18**	
15		Pruebas del Cluster en Ambiente de Testeo	5 días	mar 01/05/18	lun 07/05/18	13
16		Ajustes	2 días	mar 08/05/18	mié 09/05/18	15
17		Certificación de Pruebas	2 días	jue 10/05/18	vie 11/05/18	16
18		**Implementación**	**1 día**	**sáb 12/05/18**	**sáb 12/05/18**	
19		Raqueo de Servidores	2 horas	sáb 12/05/18	sáb 12/05/18	14
20		Generación de Backup de los Objetos y Reglas del Firewall	1 hora	sáb 12/05/18	sáb 12/05/18	19
21		Restauración del Backup de las Objetos y Reglas	1 hora	sáb 12/05/18	sáb 12/05/18	20
22		Deshabilitar el Firewall anterior	1 hora	sáb 12/05/18	sáb 12/05/18	21
23		Habilitar el Cluster del Firewall	1 hora	sáb 12/05/18	sáb 12/05/18	22
24		Validar que todos los servicios de TI estén operativos	2 horas	sáb 12/05/18	sáb 12/05/18	23
25		Monitoreo y estabilización	5 días	lun 14/05/18	vie 18/05/18	18

Figura 2.3 - Cronograma Implementación Clúster de Firewall

Fuente: Elaborado por el autor

2.4. IMPLEMENTACIÓN DE LA SOLUCIÓN

2.4.1 IMPLEMETACIÓN DEL PROXY

Una vez descargado los archivos ISO del de Centos Linux, de la página Linux www.centos.org y generado el CD de instalación se realiza la instalación del Sistema Operativo, en el Servidor asignado para este efecto. Acto seguido se realiza el aseguramiento del Servidor y la aplicación de parches, para lo cual debe tener acceso a Internet. Acorde al cronograma, se realiza la Instalación del Proxy, posteriormente se inicia la configuración modificando el archivo squid.conf, así pasará de una configuración básica a la configuración que requiere la institución, habiendo creado las ACL necesarias para los permisos de navegación y descarga, con los horarios establecidos.

Con la finalidad de agilitar el despliegue de la configuración de navegación mediante el proxy como predeterminado se creó la GPO “Navegación Proxy”, en la fase de prueba será desplegada solo al grupo de prueba establecido, posteriormente se realizaría el despliegue en todos los equipos que se encuentren en el dominio.

Para tener variedad en el grupo de pruebas se eligió estaciones de trabajo, portátiles y servidores de diferentes áreas con diversos tipos de

permisos, como detalla la tabla #3, actividad que fue debidamente autorizado por las Jefaturas respectivas y en horarios específicos.

Tabla 3 - Equipos asignados para las pruebas

Tipo	Departamento	Observación
Estación de trabajo	Sistemas	Desarrollador
Estación de trabajo	Operaciones	Asistente de Cuentas
Estación de trabajo	Contabilidad	Asistente Contable
Portátil	Sistemas	Jefe de Sistemas
Portátil	Servicio al Cliente	Supervisor
Servidor	Sistemas	Servidor de Desarrollo

Fuente: Elaborado por el autor

En el tiempo de pruebas se realizaron ajustes en las ACL, especialmente en los que requerían puertos específicos como la asistente contable para acceder al SRI y subir los anexos que dicha entidad requiere, además de la descarga de los estados de cuentas de los diferentes bancos con los que la institución mantiene cuentas; en el asistente de cuentas se realizó el seguimiento de la descarga de los archivos de las aseguradoras.

En el Servidor de Desarrollo se validó la restricción de navegación, en la portátil asignada a la Jefatura de Sistemas se validó navegación y descarga sin restricción de horarios, y en la portátil asignada al supervisor de servicio al Cliente la navegación en horarios permitidos y las restricciones a paginas no definidas como básicas.

En la Etapa de Implementación se realizó el despliegue de la GPO “Navegación Proxy” en todos los equipos, durante 3 días, se trabajó con el área de soporte para que validaran que los navegadores tuvieran configurados por defecto el Proxy, producto de esta actividad se obtuvo un listado de equipos que no se realizó el despliegue, porque los colaboradores no se encontraban laborando, por los motivos que se detallan en la tabla #4, a estos casos se les realizará el seguimiento a su retorno a la institución.

Tabla 4 - Equipos pendientes de aplicar GPO

Tipo	Departamento	Cargo	Observación
Estación de trabajo	Sistemas	Analista	Permiso Paterno
Estación de trabajo	Operaciones	Supervisor	Vacaciones
Estación de trabajo	Contabilidad	Auxiliar	Permiso Materno
Estación de trabajo	Recursos Humanos	Auxiliar	Permiso Médico
Portátil	Crédito	Jefe	Reunión fuera de la Institución
Portátil	Operaciones	Jefe	Reunión fuera de la Institución
Portátil	Contabilidad	Jefe	Reunión fuera de la Institución

Fuente: Elaborado por el autor

Finalmente se deshabilitó las reglas de navegación del Firewall, de las estaciones de trabajo, portátil y servidores, dejando activa solo la regla del Proxy, se realizó el monitoreo y estabilización durante tres días, tiempo en el cuál saltaron ciertas novedades que fueron solventadas de

forma inmediata y no generaron mayor impacto en la operatividad de la institución.

Los servicios de navegación quedaron operativos quitando al Firewall la carga de atender las peticiones de navegación, descarga y subidas de archivos, que ahora son atendidos por el Proxy implementado.

2.4.2 IMPLEMENTACIÓN DEL CLÚSTER DEL FIREWALL

En este apartado se detallará la configuración de los servidores, la configuración del Appliance Smart-DashBoard, la restauración del backup de las objetos y Reglas, la configuración del Clúster de Firewall, y finalmente la configuración del Appliance Smart-Reports.

Con la finalidad de recordar que es una RAID me permito citar a Rosero y su definición de esta, con apoyo de la figura 2.4.

RAID es una tecnología de almacenamiento que permite combinar dos o más discos, de forma que sean vistos como una unidad lógica en la que se almacenan los datos de forma redundante, donde las operaciones I/O se colocan en un nivel equilibrado, mejorando el rendimiento del sistema. Incrementando el tiempo medio entre errores (MTBF) y por ende se incrementa la tolerancia a fallos de discos. (Rosero, 2012, p.27).

Figura 2.4 - Diagrama RAID
Fuente: Elaborado por el autor

Existen varios niveles de RAID, con diferentes características y funcionalidades, de los cuales el ideal para la configuración de los discos duros de los servidores que realizarán las funciones de nodos del Cluster de Firewall es el RAID 1 (Disk mirroring), puesto que replican la información de un disco a otro, toda información que se almacene en un disco de forma automática e inmediata se escribe en el disco espejo, de allí su nombre mirroring. En la figura 2.5 se ilustra la funcionalidad del RAID 1 (Mirroring).

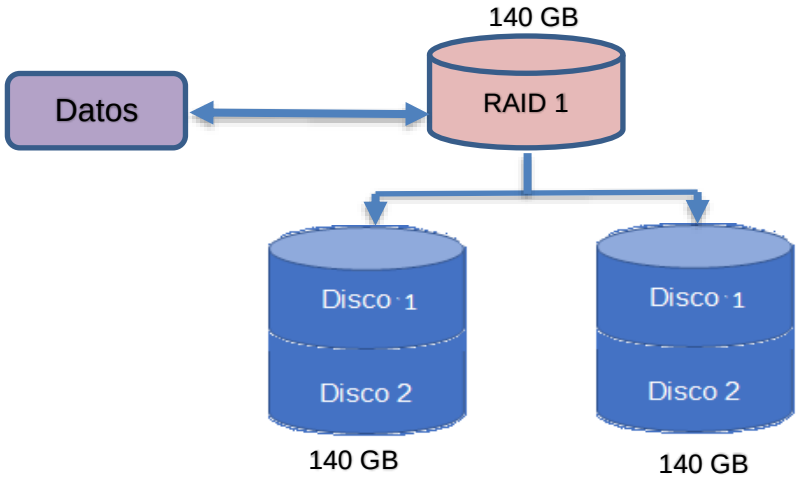


Figura 2.5 - RAID 1 (Mirroring
Fuente: Elaborado por el autor

Pese a que el RAID 1 sacrifique espacio de almacenamiento dejando dos discos físicos, en una sola unidad lógica de almacenamiento, para nuestro proyecto la prioridad es la alta disponibilidad que nos ofrece este tipo de RAID, si se avería un disco duro físico será trasparente para el servidor, puesto que emitirá una alerta, pero seguirá funcionando sin impactar los servicios, puesto que los datos almacenados están replicados en el disco que se encuentra en buen estado. En los dos servidores HP Proliant DL360 G7 se utiliza el mismo tipo de arreglos de discos, RAID 1.

Dado que los Appliances son equipos que ya traen embebidos el sistema operativo del fabricante, los drivers y arreglos de discos duros ya vienen pre-establecidos, no es necesario una configuración física, solo se realiza la configuración lógica, siendo un paso indispensable asesinarle una dirección IP a cada uno de las appliance, tanto al Smart-Dashboard como al Smart 1 – Reports. A continuación, detallo la configuración efectuada en cada uno de ellos.

a) Configuración del Checkpoint SmartConsole – Dashboard

SmartConsole – Dashboard, conocida también como consola de administración del Checkpoint es la herramienta que permite crear las reglas de permisos y denegación de cada uno de los segmentos de red

que tiene la institución. Tal como se muestra en la figura 2.6 – SmartConsole – Dasboard, las reglas están conformadas por No, Name, Source, Destination, PVN, Services & Applications, Action y Track.

Figura 2.6: SmartConsole – Dashboard
Fuente: Elaborado por el autor

Con finalidad de comprender mejor cada componente de las reglas listo una breve descripción de ellos:

- **No**.: número secuencial que es asignado de forma automática por la herramienta.
- **Name:** El nombre es opcional, se utiliza como una descripción corta de la utilidad de la regla.
- **Source:** Se coloca el objeto desde donde se establecerá la comunicación, pudiendo ser este un equipo, un grupo o un segmento de red.

- **Destination:** Se coloca el objeto destino, es decir aquel que recibirá las peticiones o que brindará el servicio, pudiendo ser este un servidor, un equipo, un grupo o un segmento de red, generalmente se trata de servidores que proveen servicios sean internos o publicados en la Web
- **PVN:** es utilizado solo cuando la conexión se realizará mediante PVN, caso contrario debe omitirse.
- **Services & Applications:** se selecciona el servicio o aplicación que será utilizada, por ejemplo, **IIS** (Internet Information Server), al colocar el servicio o aplicación se encuentra encapsulado los puertos por los que puede comunicarse, en versiones anteriores se tenía que listar los puertos y si existía una omisión la petición era denegada.
- **Action:** se debe seleccionar el tipo acciòn que se realizarà en la regla que se está creando, se utiliza **Accept** cuando se trata de una regla de acceso permitido**, Drop** cuando se trata de una regla de denegación, **Ask, Inform (UserCheck message), and Reject.**
- **Track**: se define si las peticiones que se realicen por la regla sean o no registrada en los logs, por buenas prácticas se recomienda que toda regla se registre en log, para hacer seguimientos y correlaciones a futuro.
- **Install On:** Generalmente se coloca el objeto tipo firewall donde se aplican las políticas

- **Time:** se coloca el horario que tiene permitido o denegado el acceso, dependiendo del tipo de regla que se esté creando, puede especificarse rango de horas, de días. Si se omite un horario no se limita el tiempo, siendo implícito 24 horas 7 días a la semana.
- **Comment:** se utiliza para colocar descripciones que permitan a futuro saber la finalidad de la regla, no es obligatorio, pero si recomendable, por temas de administración.

Si bien es cierto que no es obligatorio colocar un Origen (Source), Destino (Destination), o Servicio (Services & Application), también es cierto que las buenas prácticas de seguridad nos recomiendan hacerlo, caso contrario serían reglas abiertas que quitarían el propósito de un Firewall. Siendo la excepción la regla de “CLean up”, donde se coloca “ANY” en el Origen (Source), en el Destino (Destination), y en el Servicio (Services & Application), pero siempre colocando “DENY” en Acción (Action), esta regla indica que ningún origen puede acceder a ningún destino por ninguna, así detiene accesos indebidos a segmentos

Las reglas básicas de un Firewall Checkpoint recomendadas por el fabricante se encuentran detalladas en la tabla 5, pero en virtud que la institución ya cuenta con reglas creadas lo que realizamos es una revisión de ellas.

Tabla 5 - Reglas Básicas de Firewall Checkpoint

No	Name	Source	Destination	Service	Action	Track	Install On
1	Stealth	NOT internal	GW-group	Any	Drop	Alert	Policy Targets
2	Critical subnet	Internal	Finance HR R&D	Any	Accept	Log	CorpGW
3	Tech support	TechSupport	Remote 1-web	HTTP	Accept	Alert	Remote1GW
4	DNS server	Any	DNS	Domain UDP	Accept	None	Policy Targets
5	Mail and Web servers	Any	DMZ	HTTP HTTPS SMTP	Accept	Log	Policy Targets
6	SMTP	Mail	NOT Internal net group	SMTP	Accept	Log	Policy Targets
7	DMZ & Internet	IntGroup	Any	Any	Accept	Log	Policy Targets
8	Clean up rule	Any	Any	Any	Drop	Log	Policy Targets

Fuente: Administration Guide – Check Point Security Management [2]

b) Configuración del Checkpoint Reports.

El Checkpoint Reports me permite dejar configurados los tipos de reportes que como Administrador de la seguridad lógica se utilizaría de forma frecuente, cabe indicar que todas las reglas que se configuran en

la consola de administración con track quedan registradas en los logs que el firewall almacena.

Cada vez que se necesite monitorear un tráfico específico se lo puede realizar de forma inmediata, también se permite revisar sucesos ocurridos en días, o semanas anteriores; permite realizar búsquedas por objetos específicos, desplegando todas las actividades realizadas que hubieran pasado a través del firewall, por ejemplo, si una estación de trabajo reporta que tiene problemas para acceder al Aplicativo Core se puede consultar todas las actividades de dicho equipo y ver si sus accesos están siendo permitidos o denegados, o si está tratando de acceder por algún puerto que no estuviera permitido. (Figura 2.7 - Reports)

También permite hacer correlación de eventos que son de suma importancia para detectar ataques de forma oportuna, existen virus o malware que pudieran encontrarse en las estaciones de trabajo por falta de actualización de antivirus o falta de parches del sistema operativo, lo que podría resultar en un ataque por denegación de servicios, es decir generar peticiones infinitas hasta hacer que un determinado servidor colapse.

El Firewall Checkpoint bloquea la estación de trabajo para evitar que el servidor colapse y deja en el log del Firewall el motivo del bloqueo, con lo cual el equipo de soporte a usuario puede realizar las remediaciones pertinentes en la estación de trabajo sin que existan afectaciones generales por la caída de un servicio.

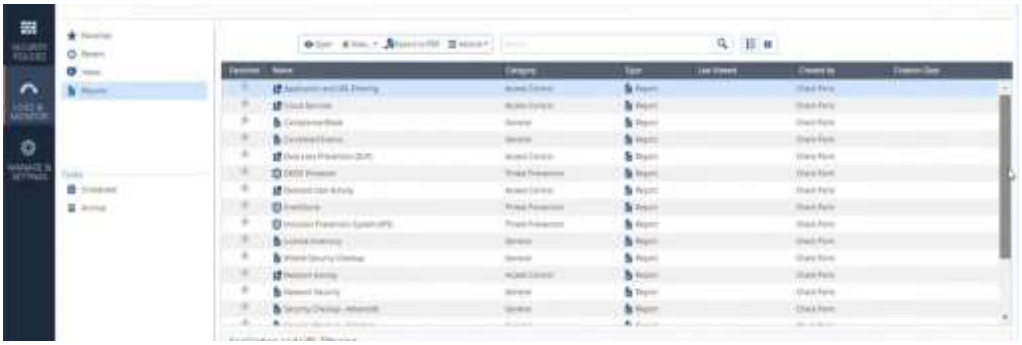


Figura 2.7 - Reports
Fuente: Elaborado por el autor

Siguiendo las buenas prácticas se debe dejar acceso al Checkpoint Reports solo a los equipos que administren el mismo y por los puertos establecidos.

c) RESTAURACIÒN DE CONFIGURACIÒN, LOGS, OBJETOS Y REGLAS DEL FIREWALL.

Se restauró la configuración del Firewall – Checkpoint incluyendo los logs, obtenido del respaldo que se genera los domingos en el Firewall de producción, tal como lo muestra la figura 2.8, el lunes se generó un respaldo de las reglas y objetos del Firewall de producción,

adicionalmente se imprimió las reglas para compararlas una a una contra el respaldo restaurado.

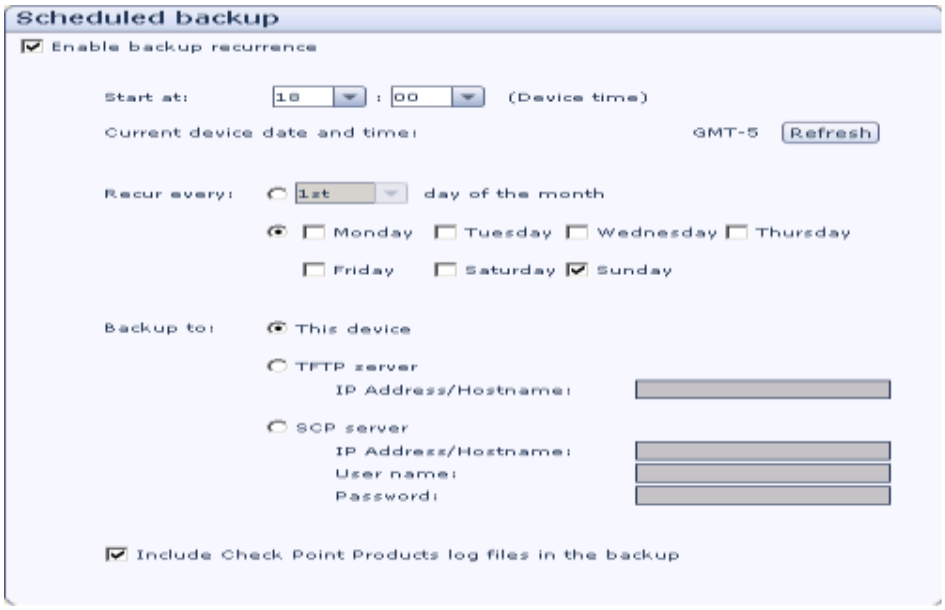


Figura 2.8 - Respaldo Calendarizado
Fuente: Elaborado por el autor

Para restaurar los objetos y reglas del Firewall que se ingresó en modo expert con la contraseña respectiva, acto seguido nos ubicamos en la ruta destinada para el efecto colocando el comando $FWDIR/bin/upgrade_tools, seguido de la ejecución del comando o ./upgrade_import backupfw_añomesdia.tgz, donde backupfw_añomesdia.tgz es el nombre del respaldo a restarurar; finalizamos con la ejecución del comando cpstart, el cual permite iniciar los servicios del firewall que son detenidos de forma automática mientras se realiza la restauración de las reglas y objetos.

Se validó las direcciones IP de cada uno de los Servidores de la institución, los segmentos de red existente, las direcciones Públicas de los servidores que se tienen publicados, las VPN configuradas y las estaciones de trabajo consideradas como críticos.

Adicionalmente, se dispuso al Administrador de seguridades lógicas que todas las solicitudes de nuevos accesos, restricciones o cambios de cualquier índole que se realizaran en el Firewall de producción sean registradas en la bitácora, para poder incorporarlos en el ambiente de pruebas.

d) CONFIGURACIÒN DEL CLÚSTER DE FIREWALL

Para realizar la configuración del Clúster del Firewall de Checkpoint debemos establecer la topología de red del Clúster, previo a haber registrado la licencia, caso contrario no se habilitan las opciones de Clúster. Basados en la tabla 6, asignamos las direcciones IP a cada uno de los nodos de forma física y de forma lógica al Clúster, con la finalidad de facilitar la identificación tanto del clúster como de la de los nodos que lo conforman, les asignamos direcciones IP secuenciales por cada uno de los segmentos que administrará el Firewall.

Tabla 6 - Topología del Firewall

Nombre	Clúster	Nodo 1	Nodo 2	Tipo
Eth0	xxx.xxx.xxx.1	xxx.xxx.xxx.2	xxx.xxx.xxx.3	Clúster
Eth1	yyy.yyy.yyy.1	yyy.yyy.yyy.2	yyy.yyy.yyy.3	Clúster
Eth2	zzz.zzz.zzz.1	zzz.zzz.zzz.2	zzz.zzz.zzz.3	Clúster
Eth3	aaa.aaa.aaa.1	aaa.aaa.aaa.2	aaa.aaa.aaa.3	Clúster
Eth4	bbb.bbb.bbb.1	bbb.bbb.bbb.2	bbb.bbb.bbb.3	Clúster
Eth5	ccc.ccc.ccc.1	ccc.ccc.ccc.2	ccc.ccc.ccc.3	Clúster

Fuente: Elaborado por el autor

En cada una de las tarjetas físicas asignamos un segmento de red a la que el Clúster de Firewall controlará el tráfico, permitiendo que todos estén protegidos y los accesos y o denegaciones sean monitoreados y queden registrados.

Una consideración de gran importancia es seleccionar la opción “All IP Addresses behind Cluster Members ares bases on Topology information”, como se muestra en la figura 2.9, puesto que todos los nodos de un Clúster deben tener la misma topología.

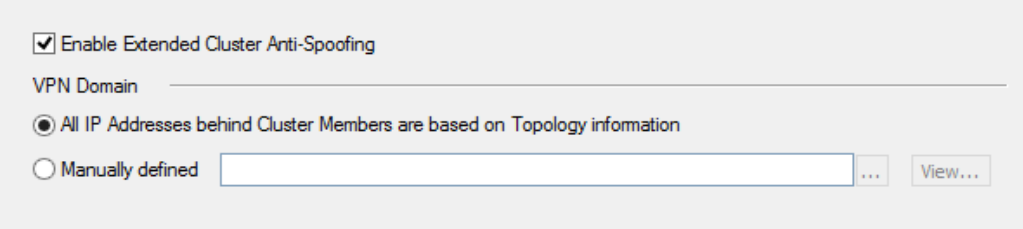


Figura 2.9 - Aplicación de Topología
Fuente: Elaborado por el autor

Para consultar la configuración de las tarjetas de red de un nodo ingresamos remotamente desde el equipo del administrador del Firewall a través del puerto previamente establecido, y se coloca el usuarios y contraseña respectiva, una vez en la consola remota escribirnos el comando “show configuration” acto seguido se muestra una ventana similar a la figura 2.10, es importante revisar que se encuentre activa (state on), que tenga la IP y mascara correcta. Debemos realizar esta consulta por cada uno de los nodos del Clúster. También se puede realizar la consulta en el ambiente gráfico como se muestra en la figura 2.11.

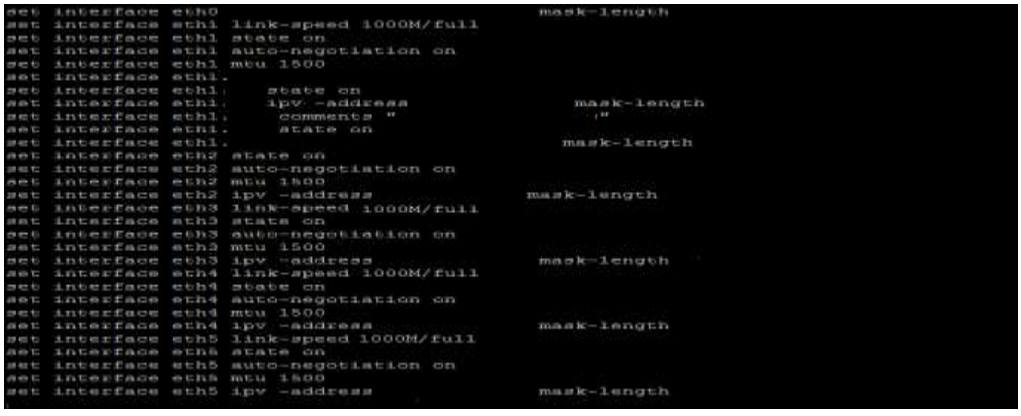


Figura 2.10 - Estado de las Tarjetas de Red – modo comando
Fuente: Elaborado por el autor

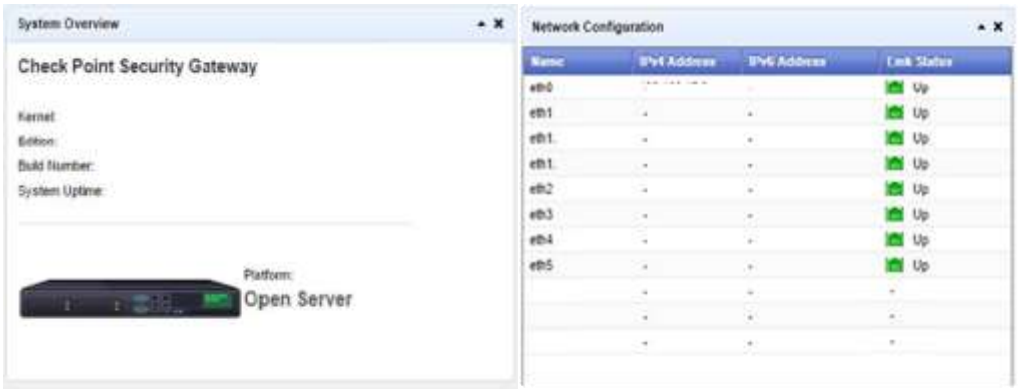


Figura 2.11 - Estado de las Tarjetas de Red – modo Gráfico
Fuente: Elaborado por el autor

Se creó el clúster de firewall de modo gráfico eligiendo la opción Clúster del menu Gateways & Servers, con la ayuda del Wizard creamos cada uno los nodos que formarán el Cluster, y finalmente agregamos los nodos al Gateway existente.

Una vez creados los nodos debe configurarse el tipo de Balanceo de carga que tendrán los nodos, hemos seleccionado el modo Unicast, que establece un nodo pivote encargado de evaluar su carga y si está libre lo procesa caso contrario lo envía al otro nodo que éste sea quien lo procese, la distribución de carga será 30% para el nodo pivot y 70% para el otro nodo, tal como lo evidencia la figura 2.12.

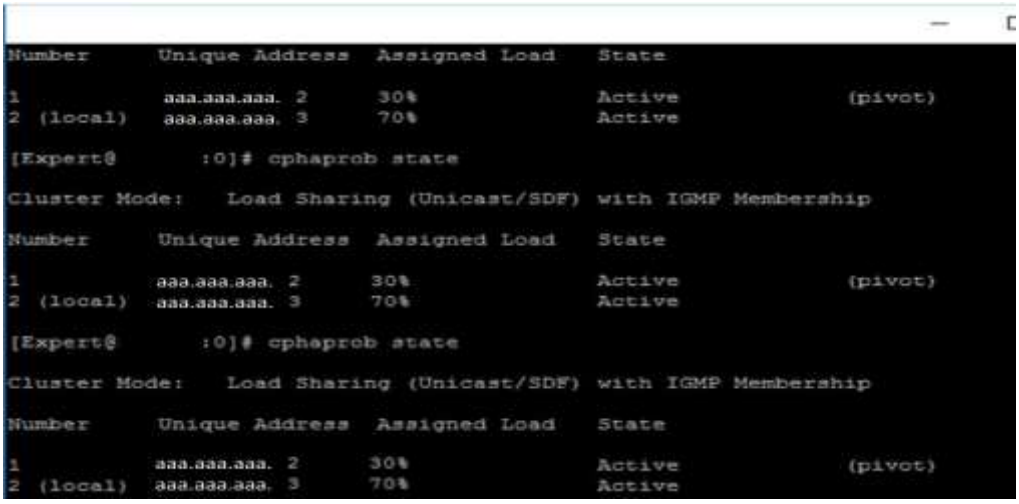


Figura 2.12 - Distribución de Carga
Fuente: Elaborado por el autor

El nodo que tiene 70% es el que realiza la mayor cantidad de transacciones, puesto que cada petición que recibe la procesa de forma inmediata, pese a esto no significa que el nodo pivot que tiene asignado el 30% realice menos cantidad de procesamiento, puesto que él recibe todos los paquetes y decide si procesarlo él directamente o asignárselo al otro nodo.

En caso de que el nodo pivot sufra alguna avería de forma automática el otro nodo toma su rol y para los usuarios es totalmente transparente que existe un problema, puesto que los todos los servicios siguen habilitados. Esto se logra gracias a que el nodo secundario siempre está censando al pivot y al momento que no recibe respuesta asume el control del Clúster sin necesidad de interacción humana.

e) PRUEBAS

En este periodo se revisaron que los equipos designados para las pruebas realicen las interacciones pertinentes, con los equipos del ambiente de QoS, se probó el acceso y funcionamiento al Aplicativo CORE.

Se monitoreó el funcionamiento del Clúster del Firewall desde la estación del Administrador de seguridad lógica, validando que ambos nodos se encuentren operativos, mientras que con el Appliance de reportaría se evidenciaba el tráfico que atendía y/o denegaba las peticiones del aplicativo CORE desde las estaciones de trabajo asignadas para el efecto hasta el servidor de pruebas del aplicativo CORE y desde él hacia el Servidor de Base de Datos de Pruebas, pudiendo concluir que no existen inconvenientes y que es transparente para el aplicativo la existencia del clúster, puesto que lo percibe como un solo Firewall, tal como lo hacía con el Firewall de producción.

Se envió a generar procesos de fin de mes que demandan tiempo y procesamiento prolongado, 12 horas aproximadamente, tiempo en el cual desconectábamos el nodo secundario del Clúster y la operatividad no se vio comprometida, el proceso seguía ejecutándose, se conectó

nuevamente el nodo secundario y fue detectado por el nodo pivot de forma inmediata, sin interrumpir el procesamiento.

También se desconectó el nodo pivot y el nodo secundario asumió el control de forma inmediata sin detener la ejecución del proceso de fin de mes que estaba en curso. Se detectaban los cambios era la estación de trabajo del Administrador de seguridad lógica puesto que se desconectaban los accesos hacia los nodos cuando se le desconectaban los cables de red, así como en la consola de administración SmartConsole – Dashboard, se veía el estado de los nodos y las interfaces de sus tarjetas que se alternaban entre up (activa) y down (inactiva) dependiendo de las acciones que se estaban realizando.

Los servicios que no se pudieron probar fueron los que requieren de publicación, es decir el sitio web institucional, el correo electrónico, y el IIS, mismos que serán monitoreados en la etapa de implementación.

f) IMPLEMENTACIÓN

El lunes se mantuvo una reunión con los jefes departamentales para recordarles los compromisos con este proyecto que estaba en su etapa final, para el sábado de la implementación del Clúster de Firewall deberán asistir a las 14h00 el personal clave para validar la operatividad del aplicativo CORE, Call Center, servicios con los bancos, y servicios

publicados implementación del Firewall, detallados en la tabla 7 – Distribución de Validación de Servicios.

Tabla 7 - Distribución de Validación de Servicios

Tipo	Departamento	Cargo	Servicio
Estación de trabajo	Sistemas	Operador	ERP – Procesos Batch Generación de Respaldos
Estación de trabajo	Operaciones	Supervisor de Cuentas	Canal Banco Central ERP – Modulo de Cuentas ERP – Modulo de Crédito
Estación de trabajo	Contabilidad	Supervisor Contable	Entes reguladores Entidades Bancarias Entidades Gubernamentales
Estación de trabajo	Servicio al Cliente	Asistente	ERP – Modulo de Cuentas ERP – Modulo de Crédito
Estación de trabajo	Call Center	Supervisor	Ejecución Campañas salientes Ejecución Campañas entrantes
Estación de trabajo	Call Center	Agente	Generación de Reportes Creación de campañas
Portátil	Tesorería	Analista	Canal Bolsa de Valores

			Canal Banco Central ERP – Módulo tesorerìa
Portátil	Servicio al Cliente	Supervisor	Correo saliente y entrante, fuera y dentro del dominio. ERP – Generación de Consultas
Servidor	Sistemas	Supervisor de Desarrollo	Ambiente de pruebas Accesos a Servicios de Terceros
Estación de Trabajo	Sistemas	Administrador de Servidores	Revisión de accesos Revisión de Servicios de TI
Estación de Trabajo	Sistemas	Administrador de Redes	Canales Segmentos de redes

Fuente: Elaborado por el autor

El viernes al medio día se les remitió el correo a los usuarios recordándoles que el sábado no estarían habilitado los servicios de TI. Además de la creación de la regla de acceso para el sábado a los equipos de los usuarios que validarían los servicios el sábado tengan el acceso requerido. Regla que será deshabilitada al terminar las validaciones.

La implementación inició a las 07h00 AM con el raqueo de los dos Servidores, que hacen las veces de nodos del Firewall, y de los dos

Appliances (el Smart-Dashboard y el Smart 1 – Reports), a la par se generaron los respaldos de los logs y posteriormente el respaldo de los Objetos y Reglas del Firewall, en modo comando, ingresando al directorio asignado para el efecto ejecutando la sentencias:

- cd $FWDIR/bin/upgrade_tools
- ./ upgrade_export backupfw_añomesdia.tgz

Donde añomesdia son la referencia del respaldo que se genera. Una vez generado el respaldo lo enviamos al equipo del Administrador de seguridades lógicas para grabarlo en un CD, el cual utilizaremos para restaurar las reglas en el clúster y posteriormente será entregado al operador para el registro y almacenamiento correspondiente. A las 09h00 se apago el Firewall quedando por ende inactivos los servicios de TI, mismos que estarían habilitados cuando el Clúster de Firewall se encuentre habilitado en el ambiente de producción.

Para la restauración de las reglas y objetos entramos como usuario Administrador y colocamos la contraseña respectiva, luego cambiamos a modo expert y colocar la contraseña respectiva, habilitamos la unidad de CD ejecutando la instrucción mount /mnt/cdroom, copiamos el respaldo desde el CD hacia el Firewall ejecutando la instrucción cp /mnt/cdroom archivo $FWDIR/bin/upgrade_tools, restauramos el respaldo mediante el

comando ./upgrade_import backupfw_añomesdia.tgz, desmontamos la unidad de CD ejecutando la instrucción umount /mnt/cdroom, colocamos los cables de red de los diferentes segmentos en cada uno de los nodos del Firewall y finalmente iniciamos los servicios mediante el comando cpstart.

Validamos el estado de los nodos los cuales deben mantenerse como se muestra en la figura 12 – Distribución de carga, de igual manera revisamos el estado de las tarjetas de cada uno de los nodos, mismas que se encontraban habilitados igual que en la figura 11.

Se realizó la validación externa de la licencia del Clúster de Firewall dado que ya tiene salida con la IP pública asignada, la cual resultó exitosa.

La validación de los Servicios de TI inició con el personal de Sistemas, asignados para este efecto.

- El Administrador de Servidores puedo acceder a los Servidores, Controlador de Dominio, Web, Correo, Call Center, ERP y Proxy, sin inconvenientes.
- El Administrador de Redes pudo acceder a los canales, y a los diferentes segmentos de red que mantiene la institución.
- El operador ingresó al aplicativo ERP e inició la ejecución de procesos en lotes que ejecuta los sábados, realizó la copia de los respaldos

generados automáticamente de forma periódica y automática de la Base de Datos y de las configuraciones de los servidores. Actividad que duro 3 horas y no se interrumpió en ningún momento.

- El Supervisor de desarrollo revisó los servidores del ambiente de pruebas y Accesos a Servicios de Terceros, mismos que resultaron exitosos. Además de realizar envío de correo internos y a dominios externos, tanto entrantes como salientes.
- El Call Center fue validado por la Supervisora del Call Center y un agente asignados para este efecto, las llamadas se pudieron ejecutar sin novedades, así como el acceso a los reportes, grabaciones de llamadas salientes y/o entrantes.
- El Aplicativo ERP en sus diferentes módulos fueron validados por los usuarios detallados en la tabla 7 - Distribución de validación de servicios.
- Los accesos a los entes reguladores, entidades Bancarias y entidades Gubernamentales, fueron validados por el Supervisor Contable, no existieron novedades.
- Tesorería y Operaciones validaron el acceso al Canal del Banco de Central, y a la Bolsa de Valores, sin inconvenientes.

El personal de Soporte a usuario realizaba acompañamiento en cada una de las áreas donde estaban efectuando las transacciones operativas,

pruebas de accesos a sitios web restringidos o a segmentos no asignados, a la par el Administrador de seguridades lógicas monitoreaba el tráfico desde el Smart 1 – Reports, revisando los accesos permitidos y las denegaciones efectuadas.

Se detuvo los servicios del Nodo secundario del Clúster del Firewall y para los usuarios era transparente, nunca se les detuvo sus conexiones ni les apareció errores de ninguna índole. Se los habilitó nuevamente y los procesos continuaban. Se detuvo los servicios del nodo pívot y el nodo secundario tomo el control sin afectar las transacciones en curso, ni las nuevas peticiones. Por lo antes expuesto se da como exitosa la implementación del Clúster del Firewall.

2.5 ESTABILIZACIÓN DE LA SOLUCIÓN

El operador y los administradores de servidores y redes respectivamente monitorearon los servicios durante el domingo, mismos que no presentaron problemas y ni novedades.

Durante la semana de estabilización el personal Infraestructura Tecnológica y el personal de soporte a usuario llegaron una hora antes de la hora entrada habitual, con la finalidad de solventar novedades que pudieran presentarse. En este lapso se registraron 5 equipos que no podían acceder al aplicativo ERP, esto debido que sus direcciones IP cambiaron,

se procedió a actualizar las IP dichos objetos en la consola de administración SmartConsole – Dashboard se compilaron y aplicaron las reglas, y tuvieron los accesos nuevamente, los cuales se detallan en la tabla 8.

Tabla 8 – Equipos con novedades

Tipo	Departamento	Cargo
Estación de trabajo	Atención al Cliente	Supervisor
Estación de trabajo	Operaciones	Ayudante
Estación de trabajo	Crédito	Supervisor
Estación de trabajo	Call Center	Agente
Portátil	Tesorería	Jefe

Fuente: Elaborado por el autor

De los equipos listados en la tabla 8, solo uno era crítico, el asignado a la Jefatura de Tesorería, pero fue resuelto rápidamente.

En cuanto a la estabilización de la implementación del Proxy fue realizada previamente, puesto que era la primera etapa a ejecutarse. Durante la estabilización se aplicó la política de navegación mediante el proxy a los equipos que estaban pendientes, detallados en la Tabla 4, puesto que al no tener permisos de navegación a través del Firewall y al no tender configurado el proxy no podían navegar, ni consumir ningún servicio que requiera de internet, como el correo institucional.

2.6 DOCUMENTACIÓN

Dada la criticidad del servicio que proporciona el Firewall, la documentación es de suma importancia, razón por la cual se crearon y/o actualizaron los documentos que listo a continuación:

- Creación del Manual de Configuración del Proxy, documento que contiene la versión del sistema Operativo y los parches instalados en el Proxy, el contenido del archivo squid.conf donde se encuentra la lista de control de acceso.
- Actualización del Manual de Configuración del Smart-Dashboard, puesto que ahora es un applicance, este documento contiene la configuración, la dirección IP asignada, el listado de los equipos que pueden acceder a administrarlo.
- Actualización del Manual de Configuración del Smart1-Reports, puesto que ahora es un applicance, este documento contiene la configuración, la dirección IP asignada, el listado de los equipos que tienen acceso a los reportes de monitoreo y logs del Firewall.
- Creación del Manual de Configuración del Clúster de Firewall – Checkpoint, contiene un detalle de la configuración de cada uno de los nodos, y un paso a paso de cómo crear el clúster.

- Actualización del Manual de Administración del Firewall, donde se incluyó como monitorear los nodos del Clúster, como detener un nodo, como iniciarlo; además se actualizó el detalle de las reglas y objetos.
- Actualización del Manual de Respaldos, se incluyó el respaldo de la configuración del Proxy y sus logs, se modificó la sección del respaldo de la configuración del Firewall y sus logs.
- Se generaron dos informes, uno de implementación del Proxy y otro de la implementación del Clúster de Firewall.

Con la documentación antes detallada el Personal de TI tendrá a donde recurrir cuando se requiera hacer cambios por afinamientos o actualización de versiones. Así como cuando se requiera realizar mantenimientos físicos a los servidores y se necesite validar que quedan operativos los servicios que en ellos están implementados.

CAPÍTULO 3

EVALUACIÓN DE RESULTADOS

3.1 MONITOREO DEL FUNCIONAMIENTO DEL FIREWALL.

Desde el inicio del proyecto se monitoreaba el funcionamiento del equipo del Firewall, mismo que tenía un procesamiento elevado y en varias ocasiones colapsó dejando sin servicio de TI a la institución, puesto que alojaba en un solo equipo al Firewall, la consola de Administración y la de reportes; además gestionaba todo el tráfico de navegación. Este

monitoreo se mantuvo inclusive luego de la implementación del Clúster de Firewall, el análisis de ello se lo realiza en el apartado 3.2 de este documento.

Diariamente se revisada el estado de los nodos del Clúster del Firewall, los cuales permanecieron disponibles, no hubo caídas de ningún tipo; puesto que sus interfaces de red permanecieron habilitadas durante todo el periodo, no hubo perdidas de conexión entre los nodos ni entre los diferentes segmentos de red Gateway-Firewall.

Desde el Smart 1 – Reports, se monitoreaba el nivel de tráfico que atendían los nodos, se revisaban los paquetes denegados (drop), con la finalidad de validar si se trataba de un equipo tratando de acceder a un servicio no autorizado o el tráfico denegado era por que algún equipo cambió de IP.

Semanalmente se revisaba que se hubiere realizado el respaldo de la configuración del Firewall, desde antes de la implementación del Clúster del Firewall estaba programada la generación de forma automática, y se ha seguido ejecutando sin novedades. Cabe indicar que este respaldo incluye también los logs del Firewall.

Para que se complemente el respaldo de la configuración del Firewall, se accede semanalmente a la Consola de Administración Smart-Dashboard,

para generar el respaldo de las reglas y objetos, este lo realiza de forma manual el Administrador de la Seguridad Lógica; validando además la conectividad y disponibilidad del Smart-Dashboard.

3.2 GENERACIÓN DE INFORME COMPARATIVO

Desde el arranque del proyecto y posterior a la finalización de este, se almacenaron los datos referentes procesamiento, tráfico de red, latencia y consumo de disco, tanto del firewall anterior como del Clúster del Firewall, teniendo un total de 17 semanas de monitoreo, con la finalidad de poder realizar el informe comparativo.

La gráfica 3.1 - Consumo de CPU, muestra sobre el 80% el consumo desde la semana 1 hasta la semana 6, periodo en cual el Firewall era Gateway y Proxy a la vez; se nota una disminución del porcentaje de consumo desde la semana 7, es decir luego de la implementación del Proxy, llegando a un máximo de 60% de consumo; a partir de la semana 12 el consumo no supera el 30% gracias a que en ese lapso se tienen dos nodos que funcionan como uno solo equipo, es decir luego de la implementación del Clúster del Firewall.

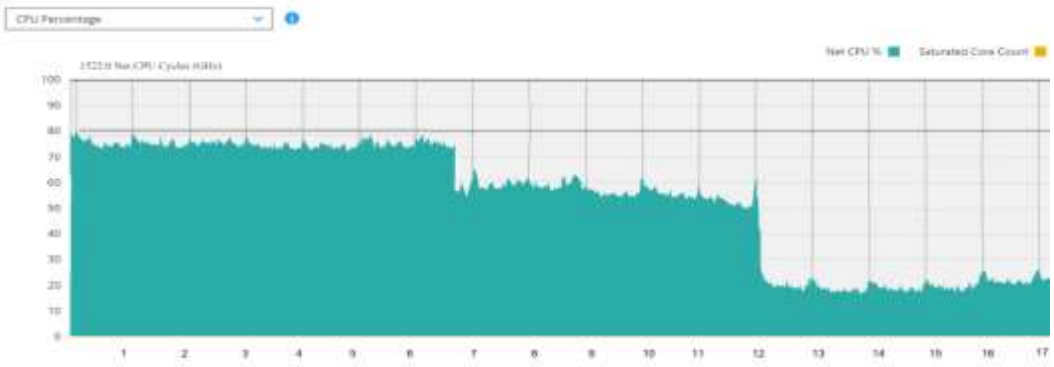


Figura 3.1 - Consumo de CPU
Fuente: Elaborado por el autor

La gráfica 3.2 – Tráfico de red, muestra una disminución desde la semana 7, luego de la implementación del Proxy, puesto que las peticiones de navegación ahora son procesadas por él y no por el Firewall, el comportamiento se mantiene inclusive luego de la semana 12, puesto que la implementación del Clúster del Firewall no disminuye la cantidad de peticiones ni de transaccionalidades que pasan a través del Clúster.

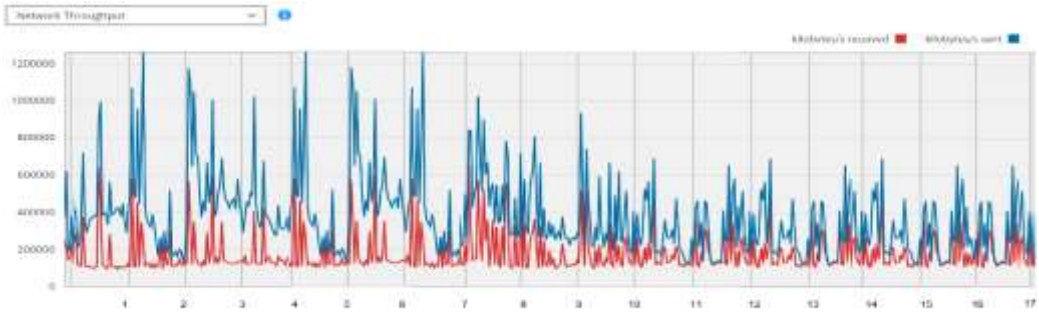


Figura 3.2 - Tráfico de Red
Fuente: Elaborado por el autor

En la figura 3.3 – Consumo de Disco Duro, se muestra una disminución desde de la implementación del Proxy, puesto que las peticiones de navegación y el registro del mismo quedan almacenados en el Proxy y no en el Firewall, con la implementación del Clúster del Firewall disminuye

aún más, puesto que ahora se registran en el appliance Smart 1 – Reports, al estar diseñado específicamente para ello tiene una velocidad mayor que el equipo anterior.

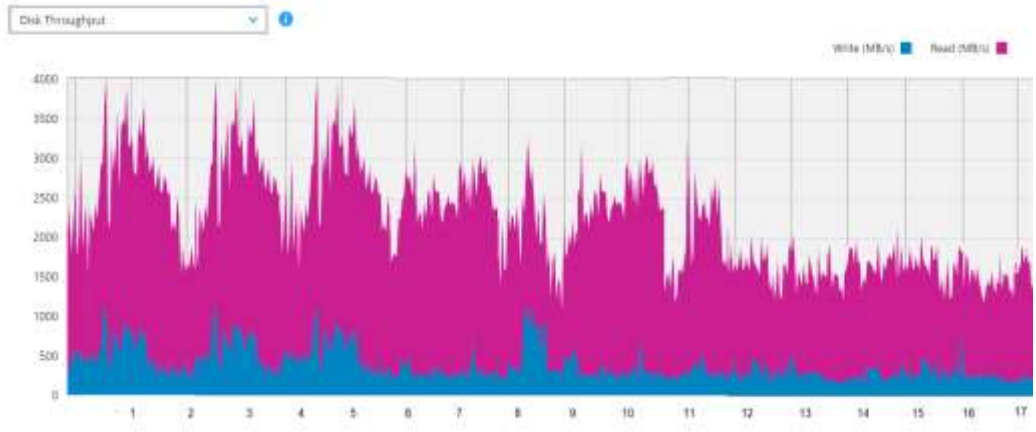


Figura 3.3 – Consumo de Disco Duro
Fuente: Elaborado por el autor

La gráfica 3.4 - Latencia, permite evidenciar latencias de hasta 5 ciclos, desde la semana 1 hasta la semana 6, periodo en cual el Firewall era Gateway y Proxy a la vez; se nota una disminución desde la semana 7, es decir luego de la implementación del Proxy; con la implementación del Clúster del Firewall a partir de la semana 12 la latencia no supera los 1,5 ciclos, teniendo dos nodos para atender los requerimientos el tiempo de espera es muy bajo e imperceptible para los usuarios.

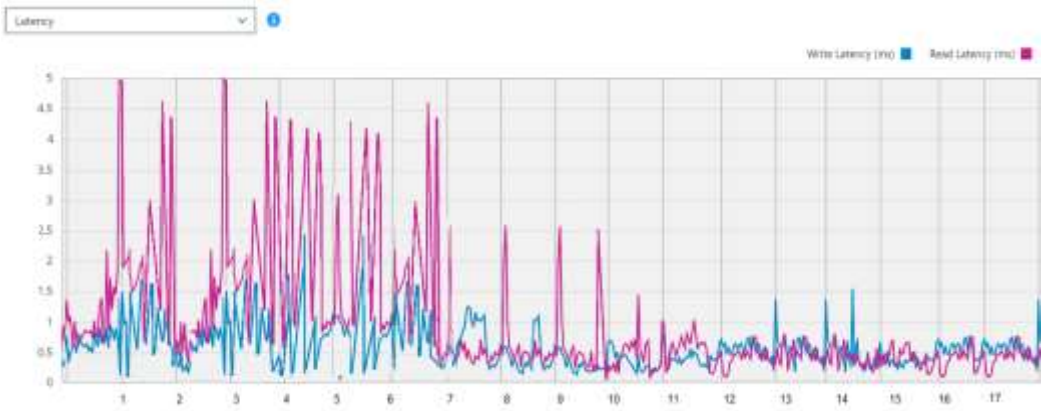


Figura 3.4 - Latencia

Fuente: Elaborado por el autor

Los registros antes analizados se realizan automáticamente, no así los registros de los inconvenientes que reportaban los usuarios, estos los hacía de forma manual el personal de soporte a usuario. En base a esta información se elaboró la tabla 9 - Seguimiento de errores por desconexión Reportados, la cual consta del número de errores y el promedio reportados de lunes a viernes, el fin de semana, así como el total, adicionalmente tiene una sección para identificar cuantos errores corresponde al fin de mes, cabe indicar que estos no suman al total de errores por encontrarse inmersos en los rexportados de lunes a viernes o fin de semana.

Analizando la tabla 9, podemos evidenciar como la ejecución de la primera etapa de la solución redujo de 1369 a 949 el número de errores reportados por desconexiones y/o saturación del Firewall, disminuyó en un 31% el número de errores, puesto que el Proxy gestionaba las peticiones por

navegación liberando al Firewall de ese procesamiento. Con la implementación del Clúster de Firewall se registraron solo 5 errores durante el monitoreo de la solución implementada, teniendo una reducción del 69% de los errores reportados por desconexiones.

Tabla 9 - Seguimiento de errores por desconexión Reportados

	Total de Errores Reportados		Reportados de lunes a viernes		Reportados en fin de semana		Reportados en fin de mes	
Etapas	**Número de Errores**	**Promedio**	**Número de Errores**	**Promedio**	**Número de Errores**	**Promedio**	**Número de Errores**	**Promedio**
Antes de la Implementación del Proxy	1369	37.0	1247	49.9	27	2.7	277	55.4
Después de la Implementación del Proxy	949	21.1	937	28.4	9	12.0	380	34.5
Después de la Implementación del Clúster de Firewall	5	0.2	5	0.2	0	0.0	0	0.0

Fuente: Elaborado por el autor

3.3 BENEFICIO DE LA SOLUCIÓN

- La implementación de la solución, liberó de carga operativa al personal de TI que estaba dedicado al 100% a atender los incidentes presentados por la saturación del Firewall, permitiéndoles dedicarse a proyectos que generen valor a la institución y resarcir la imagen que se había deteriorado por los incesantes problemas que tenían los usuarios por desconexiones.

- A más de eliminar los problemas de conexión por la saturación de equipo que hacía las veces de firewall, con la implementación del Clúster de Firewall la institución incrementó su nivel de tolerancia a fallos puesto que si un nodo tuviera un inconveniente el otro nodo asume toda la carga, gestionando las peticiones que estén en curso y las futuras, siendo imperceptible para el usuario el problema ocurrido.

CONCLUSIONES Y RECOMENDACIONES

Las conclusiones y recomendaciones son producto de la implementación de la solución y en aras de que la solución se mantega estable.

CONCLUSIONES

1. Con la Implementación del Proxy mejoró en un 69% el tiempo de respuesta en cuanto a las peticiones de navegación, puesto que eran atendidas por el Proxy y si él las tenía en memoria no hacía la petición al Firewall si no que la enviaba al equipo del usuario, descongestionando además ese procesamiento del Firewall puesto que

las reglas de navegación eran controladas por el Proxy, puestos de navegación, sitios permitidos y/o restringidos.

2. La implementación del Clúster de Firewall fue exitosa, el tiempo de respuesta del Aplicativo ERP tuvo un cambio evidente, los usuarios ejecutaban sus transacciones cotidianas ágilmente, los procesos operativos de la institución ya no se vieron retrasados por los errores de conexión.
3. Los procesos en lote que se ejecutaba en las noches el operador se hacían en tiempos menores al promedio, la extracción de los respaldos de los servidores hacia la unidad de respaldo se podía ejecutar durante el día puesto que la conexión ya no se interrumpía.

RECOMENDACIONES

1. Realizar monitoreo semestrales a los servidores, que permitan evaluar el nivel de procesamiento, tráfico de red, acceso a disco y latencia, con la finalidad de planificar la renovación del equipamiento de forma oportuna.
2. Mantener el registro de incidentes para que sean evaluados mensualmente por el administrado de seguridades lógicas, afín de detectar de forma oportuna posibles anomalías en los servicios de TI.
3. Mantener el licenciamiento del Firewall, con la finalidad de que se pueda acceder a las nuevas versiones que libere el fabricante.

4. Contratar el soporte con el fabricante 24x7 por el lapso de un año, con esto cualquier inconveniente que se presente el fabricante enviará alguno de sus partners certificados para que resuelvan el incidente sin restricción de horario, es decir, las 24 horas del día, los 7 días de la semana.
5. Incluir a los nodos del Firewall en el contrato que tiene la institución de mantenimiento preventivo con reposición de piezas y partes, un mes antes de la culminación de la garantía del fabricante.

BIBLIOGRAFÍA

[1] Rosero, V. V. (10 de Julio de 2012). *Estudio de tecnologías informáticas para asegurar la continuidad de servicios de sistemas computacionales mediante virtualización.* Obtenido de Universidad Técnica del Norte: http://repositorio.utn.edu.ec/handle/123456789/1905

[2] Checkpoint, Guia de Administraciòn, https://dl3.checkpoint.com/paid/9d/9d29af5a51f26454dfcec40ad950af6a/CP_R80_SecurityManagement_AdminGuide.pdf?HashKey=1596323254_1d1a3438678b2f268e6eb87ae43b8381&xtn=.pdf, fecha de consulta junio de 2020

[3] SofwareLab Blog, Definición de Firewall https://softwarelab.org/es/que-es-un-firewall/, fecha de la consulta junio de 2020

[4] CISET Centro de Innovación y Soluciones Empresariales y Tecnológicas, Firewall o cortafuegos https://www.ciset.es/glosario/444-firewall, fecha de la consulta junio de 2020

[5] Welivesecurity, Definición Proxy Web, https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/, fecha de la consulta junio de 2020

[6] OSTEC Blog, Definición Proxy Web, https://ostec.blog/es/seguridad-perimetral/proxy-web-tipos-y-terminologias, fecha de la consulta junio de 2020

[7] Check Point, Software Technologies LTD, https://www.checkpoint.com/about-us/company-overview/, fecha de la consulta junio de 2020

[8] UNAM Universidad Nacional Autónoma de México, Revista, Definición de Cluster, http://www.revista.unam.mx/vol.4/num2/art3/cluster.htm, fecha de la consulta junio de 2020

[9] Infranetworking, Blog, Definición Cluster, https://blog.infranetworking.com/servidor-en-cluster/, fecha de consulta junio de 2020

[10] Cabridge University, Dictionary, Definition appliance, https://dictionary.cambridge.org/es/diccionario/ingles/appliance, fecha de consulta junio de 2020

[11] Revista Gerencia, Definición de appliance, http://www.emb.cl/gerencia/articulo.mvc?xid=4448&tip=14&xit=appliances-de-seguridad-proteccion-en-todos-los-segmentos, fecha de consulta junio de 2020

[12] PC Magazine, Definición de latencia, https://www.pcmag.com/encyclopedia/term/latency, fecha de consulta junio de 2020

GLOSARIO

Firewall llamado también corta fuegos, es un software que permite controlar los accesos a la red, brindando seguridad a la misma. [3], [4]

Proxy Web Software que permite administrar las peticiones de navegación, reduciendo el tiempo de respuesta gracias a su caché. [5], [6]

Check Point marca de un fabricante de productos de Seguridad Lógica. [7]

Clúster conjunto de servidores que se muestran lógicamente como un solo servidor, cada uno de los equipos que forman parte del clúster son llamados nodos. [8], [9]

Appliance Componente hardware cerrado. [10], [11]

Latencia Suma de los tiempos de espera. [12]