ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

MAESTRÍA EN SISTEMA DE INFORMACIÓN GERENCIAL

"IMPLEMENTACIÓN DE ALTA DISPONIBILIDAD EN SERVICIOS DE INTERNET, TRANSMISIÓN DE DATOS Y SEGURIDAD PERIMETRAL DE RED PARA UNA FRANQUICIA DE RESTAURANTES".

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

SARA MÓNICA MEDINA DÁVILA

GUAYAQUIL - ECUADOR

AÑO: 2016

AGRADECIMIENTO

Agradezco a Dios por ser mi fuente de fortaleza y pilar fundamental en mi vida para luchar día a día y lograr mis metas.

A mi padre quien ha motivado mi formación académica, sin dudar de mi capacidad, además de ser ejemplo permanente de superación personal y profesional.

A mi esposo quien representa gran esfuerzo y tesón en momentos de decline y cansancio.

A mis hijos por ser mi permanente inspiración para superarme cada día.

DEDICATORIA

A mi padre por estar a mi lado aconsejándome siempre. A mi esposo por hacer de mi una mejor persona a través de su amor y confianza. A mi madre por ser el ángel que desde el cielo guía cada uno de mis pasos.

TRIBUNAL DE SUSTENTACIÓN

Mgs. Lenin Freire Cobo

DIRECTOR DE LA MSIG

Mgs. Juan Carlos García P.

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El propósito de este trabajo es el de aportar conocimiento para la implementación de alta disponibilidad en los servicios de internet, transmisión de datos y seguridad perimetral, para asegurar la disponibilidad, integridad y seguridad de aplicaciones en línea incorporando tecnologías y protocolos dinámicos a la infraestructura de hardware mediante los protocolos disponibles para que el servicio sea capaz de recuperarse luego de una interrupción y continuar operando, además de realizar una implementación en una franquicia de restaurantes de comida rápida.

Durante el desarrollo de este documento, se describe cada uno de los elementos de físicos y lógicos, así como las consideraciones técnicas necesarias para tener la capacidad de recuperación automática de los servicios, que nos permite tener las aplicaciones críticas del negocio funcionando un 99.9%, lo que generalmente es un desafío entre costos y tiempos de inactividad de las aplicaciones, evitando molestias a los usuarios para que no perciban la falla del sistema ante una caída de enlace.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BGP:	Boder Gateway Protocol Protocolo dinamico.
EBGP:	External BGP. Protocolo dinamico de comunicación externa.
GARTNER:	Empresa consultora y de investigación de tecnologías de la Información.
HA:	High Availability (Alta Disponibilidad).
LAN:	Local Area Network. Refiere enlace de red interna.
UTM:	Unified Threat Management.
VRRP:	Protocolo de Redundancia Router Virtual.
WAN:	Wide Area Network. Refiere a los enlaces urbanos e interurbanos.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las aplicaciones que funcionan sobre los servicios de Internet y Transmisión de Datos, así como las transacciones de cobros en línea con tarjetas de crédito son cada vez más críticos, por lo tanto, se requiere un altísimo nivel de disponibilidad. Como consecuencia de esto la franquicia requiere implementar tecnologías que garanticen la continuidad y disponibilidad de los servicios e integridad de la información, aumentando el nivel de redundancia y tolerancia a fallos de los enlaces.

El objetivo de este documento es implementar una arquitectura de alta disponibilidad sobre los servicios de internet, transmisión de datos y balanceo de tráfico que evite las interrupciones de servicio. Realizaremos un breve análisis de los protocolos disponibles a nivel de red, y las consideraciones técnicas que se debe tener en cuenta para una correcta implementación y disponer de un alto desempeño en la recuperación automática de los servicios.

Finalmente tendremos claro la importancia de implementar de alta disponibilidad.

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del Problema

La Franquicia de restaurantes de comida rápida tiene presencia a nivel nacional y cuenta con aplicaciones que se deben ejecutar en línea ya sea con servicio de red de datos o conectividad a Internet, tales como acceso al sistema principal, correo electrónico, abastecimiento de insumos, intercambio de pedidos para despachos a domicilio, cobros con tarjeta de crédito.

Considerando que en la actualidad las aplicaciones en línea facilitan la comunicación y control de las operaciones del negocio, al presentarse un fallo en los servicios de internet o transmisión de datos afecta significativamente bajando drásticamente la productividad, perjudicando la operación, control y desenvolvimiento de las actividades, por ello es de vital importancia tener redundancia de enlaces que nos ayuden a mantener alta disponibilidad de las aplicaciones.

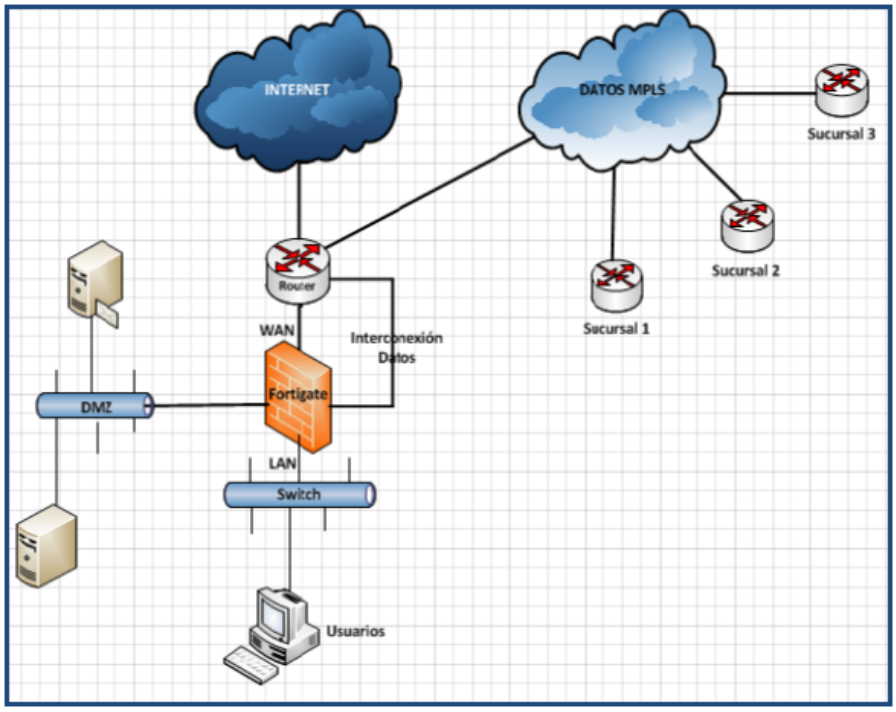

Figura 1.1: Situacion Anterior

En la Figura 1.1 podemos observar que los servicios de Internet, transmisión de datos y seguridad perimetral de red tienen un único enlace disponible y de manera centralizada las sucursales tienen salida al Internet a través del punto concentrador.

1.2 Solución Propuesta

La solución propuesta es la implementación de alta disponibilidad para los servicios de internet, transmisión de datos y seguridad perimetral de red introduciendo redundancias de enlaces, rutas físicas distintas, manteniendo el servicio disponible para la normal ejecución de tareas del negocio sin interrupciones.

Para ello examinaremos las consideraciones necesarias para la implementación:

- Instalación de Internet y transmisión de datos con dos proveedores diferentes, y cuya salida internacional sean distintas entre sí.

- De acuerdo a la infraestructura seleccionada, realizar la selección e implementación de protocolos de redundancia más apropiada para la conmutación.

- Selección de UTM con característica de alta disponibilidad y describir el proceso de implementación.

- Realizar la prueba de funcionalidad de conmutación por error en función de los parámetros implementados.

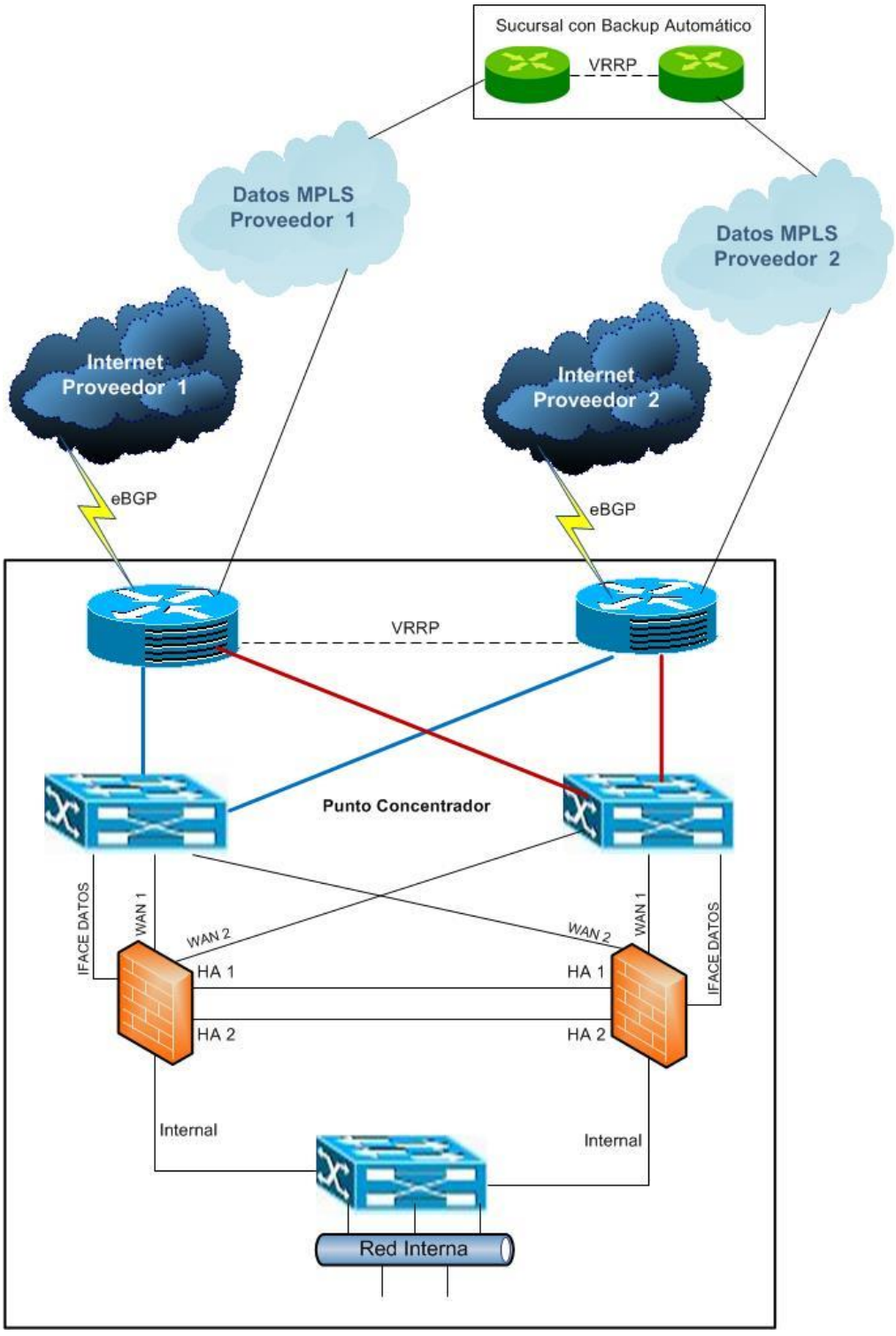

Figura 1.2: Situación Actual

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

Objetivos de la solución

En esta sección citamos los objetivos que se espera obtener con esta implementación.

- Implementar alta disponibilidad sobre los servicios de Internet, transmisión de datos y UTM (Firewall) para brindar mayor disponibilidad para las aplicaciones en línea y seguridad de la información.

- Evitar pérdidas económicas en la facturación de servicios en línea como pagos con tarjetas de crédito, abastecimiento de insumos y cierre de caja a tiempo.

- Evitar la fuga de los ingresos económicos, con la disponibilidad del enlace se tiene mayores registros por medio de los aplicativos, lo que

permitirá realizar un control de una manera óptima de los procesos.

- Reducir al máximo el tiempo de inactividad de los enlaces, la solución permite al usuario la continuidad de sus operaciones.

Selección de Proveedores de Internet, Transmisión de Datos y UTM

Es necesario de contar con dos proveedores de servicio que nos permita interconectar nuestras sucursales geográficamente distantes y contar con rutas físicas completamente independientes para la implementación de enlaces de respaldo, y de esta forma pueda brindarnos un nivel de servicio del 99.9% ya sea en forma independiente o con la contratación de ambos proveedores.

Para el servicio de Internet es necesario que la salida internacional de los proveedores sea distinta.

Selección de UTM

En esta sección se describe los principales fabricantes de UTM disponibles en el mercado de acuerdo al análisis de Gartner de Agosto 2015.

Luego de la revisión respectiva de esta información, se procede a analizar cuidadosamente el UTM sobre el cual se desea implementar la solución de protección y alta disponibilidad.

Finalmente se realiza un cuadro comparativo de las funcionalidades que nos ayudara a seleccionar el dispositivo adecuado.

.

2.1.1 Proveedores de UTM más importantes.

De acuerdo al análisis de Gartner de Agosto 2015, se destacan en el mercado entre los UTM las siguientes soluciones:

- Fortinet.
- Check Point Software Technologies.
- Sophos.

Figura 2.1: Análisis Gartner Agosto 2015.

2.1.2 FORTINET

Fortinet ha sido reconocido como líder en la industria de gestión

unificada de amenazas (UTM) de acuerdo con Gartner, Este dispositivo líder en el mercado de seguridad de redes con conmutación integrada se convierte en una solución integral de fácil manejo y costo total más bajo.

Los equipos Fortigate están en la capacidad de proveer redundancia ante fallos, debido a que están dotados para trabajar en cluster de alta disponibilidad (HA). [3]

Pueden trabajar en dos modos de operación, en modo activo/activo haciendo balanceo de carga del tráfico entre las diferentes unidades que componen el cluster o en modo activo/pasivo en la cual la unidad principal procesa el tráfico de la red y es monitoreado para poder sustituirlo en caso de caída.

Ambos equipos indistintamente del modo de operación, deben ser del mismo modelo y la misma versión del Firmware.

Características del protocolo de comunicación de alta disponibilidad:

- Las unidades del cluster se comunican a través del protocolo propietario de fortigate HA heartbeat.
- Permite sincronizar la configuración entre los equipos, de tal forma que se encuentre actualizada en función de los cambios que ocurran

en el dispositivo principal. Además de informarse entre ellos el estado de cada equipo y sus enlaces.

- Las interfaces para el intercambio de información entre cada uno de los equipos serán definidos por el administrador del equipo, y es recomendable que estas interfaces se configuren en forma redundante, es decir que se defina varios interfaces HA para realizar la función de alta disponibilidad, de tal forma que si uno fallara la información sea transmitida de forma automática por el otro enlace designado para esta función.

- En la figura 2.2, una unidad de seguridad FortiGate será instalado y conectado a otra unidad de FortiGate que ha sido previamente instalado para proporcionar redundancia si la unidad FortiGate principal falla. Esta configuración, denominada de alta disponibilidad (HA), nos ayuda a mejorar la fiabilidad de la red.

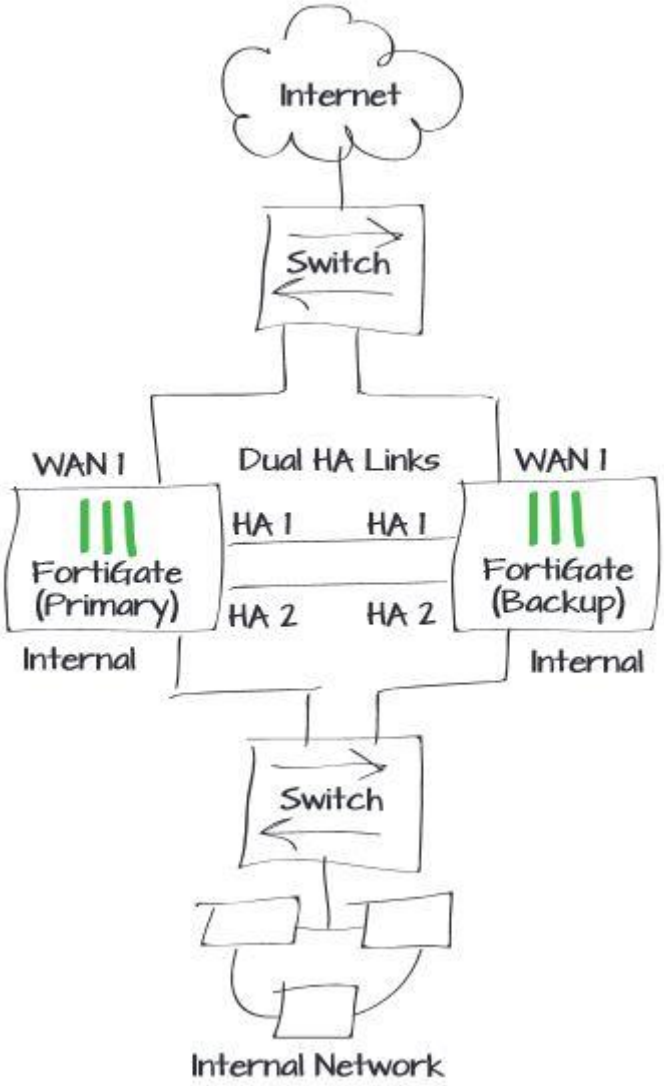

Figura 2.2: Alta disponibilidad con dos Fortigates.

Cluster Member	Hostname	Serial No.	Role
FORTINET FortiGate 100D WAN1 DMZ HA1 1 3 5 7 9 11 13 15 WAN2 MGMT HA2 2 4 6 8 10 12 14 16	Primary_FGT	FG100D3G12801361	MASTER
FORTINET FortiGate 100D WAN1 DMZ HA1 1 3 5 7 9 11 13 15 WAN2 MGMT HA2 2 4 6 8 10 12 14 16	Backup_FGT	FG100D3G12802485	SLAVE

Figura 2.3: Fortinet Modo Activo/Pasivo (HA)

2.1.3 Check Point Software Technologies

Ofrece Next Generaton Firewall un sistema de seguridad con rendimiento escalable para centros de datos con una plataforma de hardware multiblade el cual es capaz de brindar alto desempeño. Su objetivo es brindar el mejor equilibrio posible entre seguridad, costos y rendimiento. [6]

Las características más importantes son las siguientes:

- Proporciona continuidad del negocio mediante su característica de fuente de alimentación redundante.

- Permite una sincronización eficiente de la información del sistema y seguridad entre los componentes que garantizan su alto rendimiento.

- Dos appliances funcionan en modo de alta disponibilidad para eliminar los tiempos de inactividad.

- Soporta los protocolos IPv4, IPv6, ruteo dinamico.

  .

- Ademas de ofrecer alta disponibilidad, balanceo de carga, enrutamiento dinámico, esta solución unificada evita las amenazas avanzadas, como malware y botnets.

2.1.4 Sophos UTM

Esta marca ha sido diseñado un dispositivo de alta calidad para proteger las redes empresariales, cuenta con un CPU de multiples nucleos que a su vez proporciona niveles de rendimiento y flexibilidad imcomparable, aptos para ser implementados en centros de datos y salas de servidores. [5]

Sophos UTM protegen a los usuarios y servidores, controlando los accesos web y las aplicaciones, también protege los datos transferidos entre oficinas, trabajadores móviles o a través del correo electrónico, de esta manera ayuda reducir el riesgo y vulnerabilidades y que la información se pueda compartir de forma segura en cumplimiento de las normas corporativas. [5]

Las características más importantes son las siguientes:

- Máximo rendimiento con tecnología de cuatro nucleos Intel, que ofrecen velocidades de rendimiento en Gigas.

- Clústeres en modo activo/activo sin necesidad de balanceadores de carga externos, que ofrece redundancia de unidad integrada.

- Porporciona una unidad de disco duro integrada para almacenar

registros de los accesos y poder crear informes completos.

Protocolos de redundancia.

Detallaremos los protocolos dinámicos a utilizar en nuestra implementación en los distintos niveles de interfaz de conexión, WAN (comunicación externa), LAN (comunicación de la red interna) para los servicios de conectividad a internet y transmisión de datos:

- A nivel de conexión externa WAN utilizaremos el protocolo dinámico BGP para conectar nuestra red local con la red externa para acceder a Internet. Al conectarse a una organización externa se crean sesiones de peering BGP (EBGP) externas. Aunque BGP es un protocolo de gateway exterior (EGP). [4]

- A nivel de conexión interna, redundancia de equipo router de borde utilizaremos el protocolo estándar VRRP, en el cual todas los router involucrados tienen una única configuración de gateway, para lo cual los routers de borde comparten una dirección IP virtual, el cual será el default Gateway de la red interna. Los routers intercambian mensajes propios del protocolo para así coordinar cual es el router activo en cada intervalo de tiempo y en caso de falla el protocolo define que dispositivo tomara el status activo mientras se restablece el router principal. [4]

Parámetros para la adecuada selección del UTM.

Se realiza la comparación cualitativa de las características requeridas:

Tabla1: Cuadro comparativo de los UTMs.

	UTM		
Requerimiento	**Fortinet**	**Check Point**	**Sophos**
Soporte de alta disponibilidad activa / activa	SI	SI	SI
Soporte de alta disponibilidad activa / pasiva.	SI	SI	SI
Optimización de tráfico	SI	SI	SI
Aceleración WAN.	SI	SI	SI
Escaneo de Vulnerabilidades.	SI	SI	SI
Debe ofrecer soporte local certificado.	SI	SI	SI
Logging y generación de reporteria.	SI	SI	SI
Filtrado de contenido web.	SI	SI	SI
Proteccion de Servidores (datos críticos).	SI	SI	SI
Menor costo de licenciamiento.	SI	NO	NO
Menor costo de mantenimiento.	SI	NO	NO
Menor costo de capacitación.	SI	NO	NO
Interfaz amigable.	SI	SI	SI

Como podemos apreciar, la mayoría de fabricantes de UTMs han considerado todas las funcionalidades requeridas para protección y alta disponibilidad a nivel de seguridad perimetral.

Para nuestro caso, de acuerdo al análisis de las proformas obtenidas de representantes locales de los fabricantes, se optará por seleccionar el l
Fortinet, por ser el que tiene el menor precio de licenciamiento, mantenimiento y capacitación.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 Implementación de alta disponibilidad

En este capítulo detallamos los requisitos, consideraciones y pasos para la implementación de alta disponibilidad.

3.1.1 Requisitos básicos y sugerencias para la implementación del UTM de alta disponibilidad.

A continuación se detallan los requisitos clave:

- Los dos Equipos Fortigate deben ser del mismo modelo.
- La versión del Firmware debe ser la misma.
- El modo de operación debe ser el mismo (NAT o Transparente)

A continuación se detallan las sugerencias:

- Hostname diferentes para cada unidad, acorde a la función que tendrá cada equipo.

- Habilitar la Interface load balance.
- Utilizar enlace heartbeat dedicado conectándolos con cable cruzado, al menos dos interfaces para heartbeat. [2]
- Al usar sesión pickup, habilitar la opción de delay para mejorar el rendimiento. [2]
- Tener varios puertos en modo trunk en cada firewall conectados a distintos switches. [2]
- Definir el Fortigate primario con mayor prioridad.
- Configurar el grupo de alta disponibilidad.

3.2 Implementación de la Redundancia de Internet

Describiremos los requisitos, consideraciones y pasos para la implementación de alta disponibilidad.

A continuación se detallan los requisitos clave:

- Las IPs Públicas del cliente deben ser parte de una clase C de propiedad del cliente.
- El bloque de IPs públicas debe ser anunciado por los dos proveedores de servicio de internet.
- Ambos proveedores deben permitir los filtros DNS para las IPs Públicas del cliente.
- Definir el proveedor principal y el proveedor backup.

- El proveedor principal tendrá el mayor weight. [4]
- El sistema autónomo deber ser público y el mismo configurado en los router de borde de ambos proveedores. [4]
- Habilitar el intercambio de información con el peer vecino BGP. [4]

3.3. Implementación de la Redundancia de Transmisión de Datos

En este capítulo detallamos los requisitos, consideraciones y pasos para la implementación de alta disponibilidad en la transmisión de datos.

A continuación se detallan los requisitos clave:

- Definir el router principal y el router de respaldo.
- Definir el grupo vrrp en el que se trabajaran.
- Definir la prioridad.
- Definir la IPs Físicas e IP Virtual.
- El proveedor principal debe configurar el objeto que va a sensar para determinar la caída del enlace, y así pueda entrar a funcionar el router backup.
- El proveedor principal tendrá el mayor weight.

3.4 Tiempos de conmutación

En esta sección detallaremos el tiempo que le toma a cada protocolo conmutar y estar nuevamente disponible.

En VRRP el tiempo de inactividad del protocolo es de 3 segundos.

En BGP el tiempo de no disponibilidad es mayor ya que este va en función del tiempo que se tardan los router para compartir información, por defecto es de 2 minutos con 32 segundos. Este tiempo es modificable, sin embargo lo recomendable es trabajar con el default.

El HA de Fortigate el tiempos de inactividad es de 5 segundos.

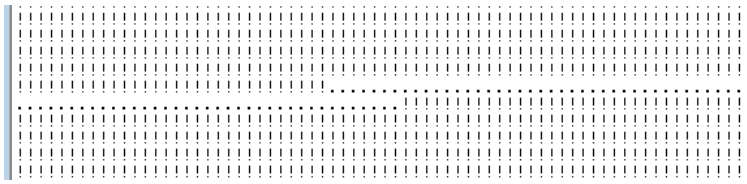

Figura 3.1: Tiempo de Inactividad BGP.

```
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 192.168.1.99: Destination net unreachable.
Reply from 192.168.1.99: Destination net unreachable.
Reply from 192.168.1.99: Destination net unreachable.
Reply from 192.168.1.99: Destination net unreachable.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=104ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
```

Figura 3.2: Tiempo de Inactividad del Protocolo HA.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

1. Este trabajo permite exponer de manera precisa las principales soluciones de alta disponibilidad que pueden ser implementadas a nivel de servicios de internet, transmisión de datos, seguridades perimetral de red disponible a nivel de mercado y en función de los protocolos dinámicos existentes, además de las consideraciones y requisitos técnicos que se debe tener en cuenta.

2. Este trabajo mostró de forma general, la metodología necesaria para la implementación en cada uno de los servicios analizados, la misma que tiene como finalidad principal ofrecer alta disponibilidad.
3. Finalmente se describen los parámetros que se deben cumplir para la implementación en cada uno de los servicios analizados, las mismas que involucran al proveedor y al personal de infraestructura de la empresa.

RECOMENDACIONES:

1. Se debe realizar las pruebas conmutación de enlaces.

2. Los enlaces y equipos deben ser monitoreados para garantizar que se encuentren activos, y en caso de falla tomar acciones correctivas de algún elemento de la red.

BIBLIOGRAFÍA

[1] Gartner, “Magic Quadrant for Unified Threat Management”, https://www.gartner.com/doc/3119922/magic-quadrant-unified-threat-management, [En línea][Fecha visita: 16 de febrero de 2016]

[2] Fortinet, “FortiOS Handbook – High Availability”, http://docs.fortinet.com/uploaded/files/2765/fortigate-ha-54.pdf, [En línea][Fecha visita: 15 de febrero de 2016]

[3] Fortinet, “Configuring active-pasive HA cluster that includes redundant interfaces - CLI”, http://docs-legacy.fortinet.com/fos50hlp/50/index.html#page/FortiOS%25205.0%2520Help/clustering.082.34.html, [En línea][Fecha visita: 12 de febrero de 2016]

[4] Cisco, “Configuración de una Red Básica BGP”, http://www.cisco.com/cisco/web/support/LA/111/1116/1116297_irg-basic-net.pdf, [En línea][Fecha visita: 12 de Febrero de 2016]

[5] Sophos, “Sophos UTM 425 ”, https://www.sophos.com/es-es/medialibrary/PDFs/factsheets/sophosutm425dsna.pdf, [En línea][Fecha visita: 12 de Febrero de 2016]

[6] Enteratech, “Check Point devela su gateway más rápido ”, https://enteratech.wordpress.com/2011/08/25/check-point-devela-su-gateway-mas-rapido/, [En línea][Fecha visita: 12 de Febrero de 2016]

[7] Fortigate, “Adding a backup Fortigate unit to improve reliability”, http://docs.fortinet.com/uploaded/files/1647/adding-a-backup-Fortigate-unit-

to-improve-reliability.pdf, [En linea][Fecha visita: 23 de Febrero de 2016]