ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN SISTEMA DE BALANCEO DE CARGAS EN LA RED PERIMETRAL DE UNA ENTIDAD FINANCIERA PARA AMBIENTES DE PRODUCCIÓN Y DE TESTING"

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

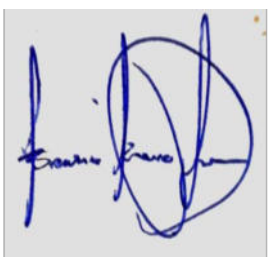
AUTOR

BRAULIO DANIEL RIVERO LUNA

GUAYAQUIL, FEBRERO 2021

AGRADECIMIENTO

Agradezco a mis Padres Luis (+) y Elsy por ser la guía de toda mi vida y por inculcarme los valores y la educación que han permitido que pueda desarrollarme en lo personal y profesional. A mi esposa Andrea e hijos Bruno y Paulo, por su apoyo incondicional y por ser la motivación principal de mi vida. A mis Suegros Ma. Elena y Carlos quienes fueron un gran apoyo durante el desarrollo de esta Maestría. A Dios, por todo lo anterior.



DEDICATORIA

Quiero dedicar este trabajo a mi familia, a mi esposa Andrea, a mis hijos Bruno y Paulo, a mis abuelos Carlos (+), Juanita (+), Marco (+), Alicia y Elena a mis Padres Luis (+) y Elsy, a mis hermanos Deidry y Sergio, a mis Suegros Ma. Elena y Carlos, a mis cuñados Carlos, Ricardo y Marcela y a mis sobrinos.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenín Freire Cobo

COORDINADOR DEL MSIG

MSIG. Juan Carlos García

PROFESOR DEL MSIG

RESUMEN

Este proyecto tiene como objetivo robustecer la infraestructura perimetral de una entidad financiera, implementando un sistema de balanceo que permita la distribución de conexiones desde internet hacia las cargas internas, y separando los ambientes de Producción y de Testing para facilitar las pruebas funcionales de los aplicativos que se encuentran en etapas de desarrollo.

A través de este documento describiremos las características de la plataforma, sus módulos, funcionalidadess de balanceo, monitoreo y de seguridad. Estas últimas, permiten agregar capas de protección a las aplicaciones que se publican a través de la plataforma con el fin de prevenir eventos de denegación de servicios o de explotación de vulnerabilidades que ejecutan los atacantes mediante técnicas tradicionales o través del uso de botnets.

La plataforma cuenta con un sistema de monitoreo integral que permitirá tener visiblidad de las instancias virtuales y sus diferentes módulos con el fin de que los administradores puedan tomar decisiones y planter mejoras sobre la solución desplegada.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Los sistemas de balanceo de cargas o “load balancing” son sistemas que básicamente realizan la distribución del tráfico de red o de aplicación que generan los clientes hacia las cargas que brindan un determinado servicio. Estos sistemas, al efectuar la distribución de cargas, contribuyen en la optimización de los recursos de los servidores y están en la capacidad de elevar el rendimiento de los aplicativos mediante técnicas de “catching” y aceleración. También, estos sistemas permiten crear espacios controlados para el mantenimiento de las aplicaciones, sin necesidad de interrumpir el servicio. Dependiendo de las implicaciones del cambio se podría operar normalmente sobre un servidor de la granja mientras otro servidor pudiera estar fuera de operación en revisión o mantenimiento.

La entidad financiera referenciada en este trabajo ya administra un sistema de balanceo de cargas. Sin embargo, dada la evolución de las tecnologías, de las amenazas informáticas y la necesidad de establecer ambientes de pre-producción perimetrales para las aplicaciones desarrolladas , inicia la tarea de efectuar la renovación tecnológica de su sistema de balanceo de cargas perimetral.

A continuación, revisaremos las generalidades del escenario a resolver en esta entidad financiera, los detalles del desarrollo e implementación de la solución y finalmente se evaluarán los resultados del proyecto desplegado.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

A la entidad financiera referida se le presentó la necesidad de desplegar para sus ambientes de Pre-Producción (testing) la publicación de servicios hacia internet de tal manera que pueda realizar las pruebas funcionales de sus aplicaciones sin afectar los ambientes de producción. Para esto, debe levantar un sistema que permita mantener los ambientes de producción bajo el esquema de balanceo actual y que además éste mismo sistema admita la separación o independencia de los ambientes de producción y preproducción. Adicionalmente, es necesario contar con un sistema de reportería y monitoreo que le brinde visibilidad del comportamiento del tráfico y las cargas que balancea.

La solución actual con la que cuenta la entidad sólo permite una instancia de balanceo que es la instancia de producción, mantiene un esquema de alta disponibilidad y de geo-redundancia que habría que soportar con la solución que se le proponga para alcanzar su objetivo. No cuenta con el sistema de reportería el cual habría que añadir a la propuesta.

1.2 SOLUCIÓN PROPUESTA

Las soluciones de balanceo no son nuevas, sin embargo, con el transcurrir de los años han evolucionado y agregado funcionalidades para establecer instancias independientes de balanceo bajo un mismo chasis o “appliance”. Esta funcionalidad es conocida como virtualización y es la característica básica que debe tener la solución propuesta. Adicionalmente, al ser componentes que se ubican frente a las aplicaciones, determinados fabricantes han agregado capas de protección ante amenazas informáticas que brindan un valor agregado a la seguridad de la entidad.

Para el despliegue de la solución, la entidad financiera estableció continuar con su fabricante actual F5, con la finalidad de que la transición hacia la nueva infraestructura sea lo más fluida posible y

manteniendo la continuidad de la marca líder en este tipo de soluciones.

Los siguientes alcances se definieron al proyecto para el despliegue de la solución:

- Instalación de equipos en las ubicaciones indicadas por la entidad financiera, en este caso en su Sitio Principal en la ciudad de Guayaquil y en su Sitio Alterno en la ciudad de Quito. Esto, con la finalidad de mantener la Geo-Redundancia de este servicio bajo esquemas de contingencia y/o pruebas de continuidad del negocio.

- Migración de las funcionalidades y configuraciones actuales de los equipos BIG-IP 4000s, de los módulos Local Traffic Manager, Global Traffic Manager y Access Policy Manager hacia la nueva infraestructura con la finalidad de mantener los servicios del ambiente de Producción.

- Configuración de instancias virtuales independientes para los ambientes de preproducción (testing) y producción, esto con la

finalidad de segregar los controles de cambios en dichos ambientes.

- Instalación de Licenciamiento F5 BEST Bundle con el addon de AWAF para mitigación de ataques de DDoS de L7 (Capa 7) en tráfico encriptado y análisis de comportamiento. Este alcance establece una capa de seguridad adicional a las aplicaciones en producción y en preproducción.

- Configuración de funcionalidades de control de acceso, para mantener la segregación de funciones en la administración del sistema entre las áreas respectivas.

- Integración con la consola de administración centralizada y de reportería, modelo F5 BIG-IQ para mantener visibilidad integral del sistema.

- Actualización del firmware a la última versión estable y recomendada por el fabricante con la finalidad de mitigar vulnerabilidades de las versiones anteriores.

Con este alcance definido la entidad financiera dio lugar al inicio del proyecto, con el cual espera mantener su esquema de alta disponibilidad y geo-redundancia con agregados de virtualización para la separación de ambientes y agregados de seguridad para la protección en capa 7 de las aplicaciones expuestas.

CAPÍTULO 2

DESARROLLO E IMPLEMENTACIÓN DE LA SOLUCIÓN

2.1. PREPARACIÓN DE LA INFRAESTRUCTURA

Para el despliegue de la solución propuesta se definió la continuidad de la marca F5, con la finalidad que la transición que implica una renovación de infraestructura sea lo menos compleja posible en cuanto a la migración de configuraciones del ambiente productivo y a la curva de aprendizaje del personal que administra la solución. Además, de acuerdo a los análisis de las consultoras tecnológicas del mercado, reconocen a F5 como líder en soluciones de distribución de carga para aplicaciones.

La solución propuesta contempla la utilización de 3 balanceadores de carga modelo i7800, 2 para el centro de datos en la ciudad de Guayaquil y 1 para el centro de datos en la ciudad de Quito. Los 3 equipos deben formar un cluster para mantener la alta disponibilidad en el centro de datos principal y la geo redundancia con el centro de datos alterno en la ciudad de Quito.

Las características principales de hardware de los balanceadores BIG-IP i7800 escogidos para el despliegue de la solución propuesta son las indicadas a continuación [1]:

- Procesamiento: 1 Procesador de 6 núcleos Intel Xeon (se traduce en una capacidad de 12 CPUs virtuales)
- Almacenamiento: de 1 a 2 discos de estado sólido con 480GB de capacidad.
- Memoria: Capacidad de 96GB de RAM.
- Fuentes de poder redundantes con funcionalidad de intercambio en caliente (Hot Swap) de 650W.
- Interfaces:
    - 8 interfaces con capacidad de alcanzar tasas de transferencia de 10Gbps. Se requieren transcievers SFP+ de cobre para la conexión física.

- 4 interfaces con capacidad de alcanzar tasas de transferencia de 40Gbps. Se requieren transcievers QSFP+ para la conexión física de fibra.
- 1 interfaz de 1Gbps asignado al puerto de administración (management port).
- 1 interfaz RJ45 para el puerto de consola (console port).
- 1 interfaz RJ45 para el puerto de conmutación por fallos (failover port).
- 1 interfaz USB 2.0 para la conexión de dispositivos de almacenamiento externo.

En lo que respecta al software para el despliegue de la solución el mismo es propietario de F5 y los módulos correspondientes se los habilitan en base a lo que el cliente haya adquirido.

El licenciamiento que se consideró para esta implementación se denomina BEST Bundle e incluye los siguientes módulos [2]:

- BIG-IP Local Traffic Manager (LTM): Módulo utilizado principalmente para el monitoreo y balanceo del tráfico que se dirige hacia las granjas de servidores publicados.
- BIG-IP DNS o Global Traffic Manager (GTM): Módulo utilizado principalmente para la resolución de nombres de dominio y para el balanceo del tráfico que va desde y hacia internet.

- BIG- IP Access Policy Manager (APM): Este módulo es utilizado para establecer políticas de conexión de acceso remoto tales como las VPNs “Client to Site” que se les configura a los funcionarios de la institución.
- BIG-IP Advanced Firewall Manager (AFM): Nuevo módulo que se incorporó como parte del empaquetado BEST para reforzar las protecciones a nivel de Seguridad Informática. Entre sus funcionalidades principales está la de establecer reglas de conexión en capa 3 (capa de red) y de inspeccionar tráfico cifrado SSL para prevenir a la organización de ataques informáticos embebidos sobre este protocolo.
- BIG-IP Application Security Manager (ASM): Es un módulo como su nombre lo indica orientado a administrar las capas de Seguridad a nivel de aplicaciones. Entre las funcionalidades más relevantes está la de protección a ataques de denegación de servicios a nivel de aplicaciones, Web Application Firewall (WAF), protección de APIs y protección contra Bots maliciosos.

2.1.1 REQUERIMIENTOS

En proyectos relacionados a la renovación de infraestructura es importante desde el inicio establecer los pre-requisitos para que

el proyecto en su fase de despliegue se ejecute sin mayores contratiempos.

Para la preparación de lo Infraestructura se definieron los siguientes requisitos:

- Requisitos del entorno físico:
    - Racks correctamente aterrizados
    - Espacio disponible de 1 unidad de rack para cada nodo.
    - Soporte de peso de 30 Libras para cada nodo
    - Temperatura ambiental entre 0°C a 40°C
    - Humedad relativa del 5 al 85% sin condensación.
    - Centro de Datos con capacidad para disipar el calor de 1024 BTU/Hora por cada equipo.
- Requisitos para la alimentación eléctrica
    - Capacidad de consumo de 300W por cada nodo.
    - Voltaje de corriente alterna entre 100 a 240 VAC
    - 2 tomas eléctricas correctamente instaladas de tipo NEMA L5-15P.
- Requisitos de cableado estructurado

- Para cada nodo se requieren 4 conexiones físicas con cableado UTP Categoría 6 para soportar tasas de transferencia mínima de 1Gbps.
- El rol de cada interfaz a configurar es el siguiente:
  - MGMT: Interface de Administración
  - SYN: Interface para sincronización de cambios
  - Internet: Interface para la interacción con redes externas en este caso, con redes públicas en Internet.
  - DMZ: Interface para la interacción con redes internas donde se encuentran las aplicaciones de la entidad.

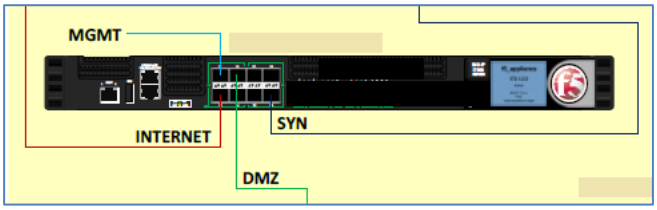


Figura 2.1. Roles de Interfaces en los nodos
Fuente: El Autor

- Requisitos para la configuración de los equipos
  - Nombre de host tanto de los componentes físicos como de los componentes virtuales.
  - Distribución de módulos requeridos para el aprovisionamiento de las instancias virtuales.

- Direccionamiento IP y Tags de VLANs para las interfaces MGMT, SYN, DMZ e INTERNET.
- Direccionamiento IP de los servidores NTP con los cuales los equipos sincronizaran la hora del sistema.
- Direccionamiento IP del servidor de autenticación desde donde se validarán las credenciales de los usuarios.
- Direccionamiento IP de los servidores que realizarán el monitoreo vía protocolo SNMP.

2.1.2 CONFIGURACIONES ADMINISTRATIVAS

Dentro de las configuraciones administrativas se aplicaron las siguientes acciones:

- Configuración de hostnames de cada nodo físico y de cada instancia virtual. En la siguiente tabla (Tabla 1) se indican ejemplos de los nombres de host que se requerieron para este proyecto:

Tabla 1.
Nombres de Host – Equipos Físicos e Instancias Virtuales

Nodo	Hostname	Descripción
Nodo 1 Físico	n1fisico.empresa.ec	Hostname ejemplo de equipo físico F5 i7800 Primario - Centro de Datos Principal
Nodo 2 Físico	n2fisico.empresa.ec	Hostname ejemplo de equipo físico F5 i7800 Secundario - Centro de Datos Principal

Nodo 3 Físico	n3fisico.empresa.ec	Hostname ejemplo de equipo físico F5 i7800 Alterno - Centro de Datos Alterno
Nodo 1 Virtual Producción	n1prod.empresa.ec	Hostname ejemplo de vcmp de producción Primario - Centro de Datos Principal
Nodo 2 Virtual Producción	n2prod.empresa.ec	Hostname ejemplo de vcmp de producción Secundario - Centro de Datos Principal
Nodo 3 Virtual Producción	n3prod.empresa.ec	Hostname ejemplo de vcmp de producción Alterno - Centro de Datos Alterno
Nodo 1 Virtual Preproducción	n1prep.empresa.ec	Hostname ejemplo de vcmp de preproducción Primario - Centro de Datos Principal
Nodo 2 Virtual Preproducción	n2prep.empresa.ec	Hostname ejemplo de vcmp de preproducción Secundario - Centro de Datos Principal

Dentro de la configuración del hostname se puede ya establecer la dirección IP de Administración que tendrá la interfaz destinada para este propósito.

- Actualización a la versión de sistema operativo más reciente y estable tanto en nodos físicos como en las instancias virtuales. La versión más estable y recomendada por fábrica para este proyecto fue la BIG-IP 14.1.0.2 Build 0.0.4 Point Release 2. Esta versión debe ser instalada en una ubicación de arranque para posteriormente aplicarla como ubicación de arranque predeterminada.
- Configuración de NTP a todos los nodos, tanto físicos como virtuales. Para esta configuración es necesario tener a la mano el nombre de host o IP de el o los servidores que concentran las peticiones de sincronización de hora en la red.

En este proyecto se establecieron 2 direcciones IP correspondientes a los servidores de hora de la red de la organización.

- Aplicación de certificados autofirmados para asegurar la comunicación web del portal de administración con los administradores, mediante el uso del protocolo seguro https. Las características a nivel de seguridad aplicadas sobre este certificado relacionadas con su llave pública fueron:
    - Tipo: RSA (Rivet Shamir Adleman), basado en el concepto de cifrado asimétrico (uso de llave pública y llave privada)
    - Tamaño en bits: 4096 bits.
- En lo que respecta a la Administración y usuarios lo recomendable es cambiar las claves de los usuarios por defecto que trae el sistema, tanto de las cajas físicas como de las instancias virtuales. Los usuarios configurados y modificados en el sistema fueron los siguientes:
    - “root”: Súper usuario para la administración mediante línea de comandos.
    - “admin”: Súper usuario para la administración mediante consola web

  - Usuarios externos: Estos usuarios son heredados del sistema “AAA” (Authentication, Authorization and Acounting) en donde a través del protocolo TACACS+ se asocian las credenciales de los diferentes administradores que acceden al sistema con las credenciales que mantienen estos usuarios en el dominio de la organización.

- Una de las configuraciones administrativas importantes que se aplicaron a estos componentes es la configuración de los sistemas de monitoreo SNMP (Simple Network Management Protocol) el cual permite tener visibilidad de la disponibilidad de los dispositivos y el comportamiento en lo que respecta al consumo de recursos. Para este caso se configuraron 3 sistemas administradores de red a los cuales se les remite los traps SNMP dentro de la organización.
- Dentro de las preferencias administrativas de seguridad del sistema se configuró el tiempo máximo de inactividad de las sesiones en 300 segundos, que las sesiones sean persistentes si se mantiene la IP de origen y también se configuró una anuncio de advertencia sobre el acceso no autorizado a los dispositivos.

2.1.3 APROVISIONAMIENTO

En la solución propuesta se planteó dividir la capacidad de los BIG-IP i7800 en dos instancias conocidas como vCMP (Virtual Clustered Multiprocessing). VCMP es una tecnología desarrollada por F5 que consolida las prestancias físicas de herramientas de propósito dedicado en instancias virtuales con capacidades predefinidas para una correcta operación de los módulos que se habilitan en ellas.

Las instancias que se definieron fueron 2 vCMP en los nodos del centro de datos en Guayaquil y 1 vCMP en el nodo del centro de datos en la ciudad de Quito. Los 2 vCMP de los nodos de Guayaquil corresponden a una instancia virtual para el ambiente de Producción y una instancia virtual para el ambiente de Preproducción. En cambio, la instancia virtual del nodo instalado en Quito corresponde a la instancia virtual de contingencia del ambiente de Producción.

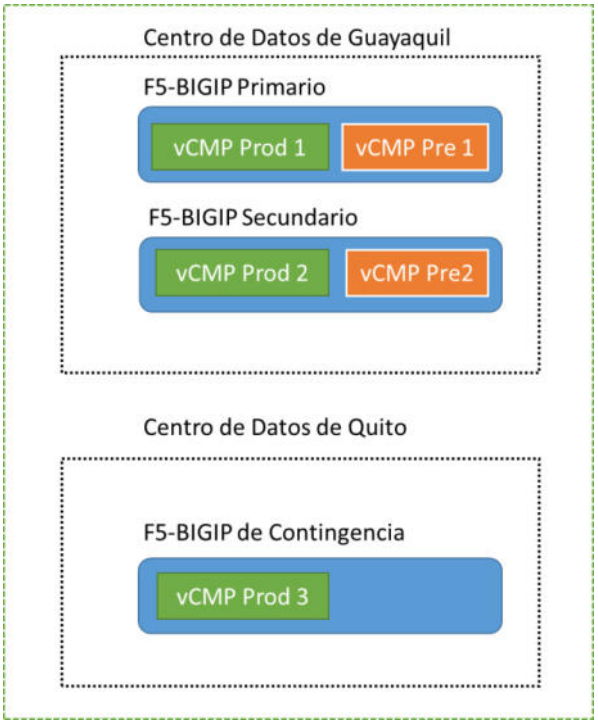


Figura 2.2 Distribución de vCMPs
Fuente: El Autor

En la Figura 2.2 se ilustra la distribución de los vCMPs en los respectivos nodos instalados en los centros de datos de cada ciudad. Cada vCMP cuenta con sus recursos asignados que los detallaremos a continuación:

Tabla 2.
Distribución de recursos Nodo 1 Guayaquil

Nodo 1 – Guayaquil	**vCPUs**	**Memoria RAM (GB)**	**Almacenamiento (GB)**
Capacidad Equipo Físico	12	96	480
vCMPs Producción	6	42,3	69
vCMPs Preproducción	2	14	69
Recursos Disponibles (Equipo Físico)	4	39,7	342

Tabla 3.
Distribución de recursos Nodo 2 Guayaquil

Nodo 2 – Guayaquil	vCPUs	Memoria RAM (GB)	Almacenamiento (GB)
Capacidad Equipo Físico	12	96	480
vCMPs Producción	6	42,3	69
vCMPs Preproducción	2	14	69
Recursos Disponibles (Equipo Físico)	4	39,7	342

Tabla 4.
Distribución de recursos Nodo 1 Quito

Nodo 1 – Quito	vCPUs	Memoria RAM (GB)	Almacenamiento (GB)
Capacidad Equipo Físico	12	96	480
vCMPs Producción	6	42,3	69
Recursos Disponibles (Equipo Físico)	6	53,7	411

En las tablas anteriores (Tabla 2, 3 y 4) se detallan los recursos de hardware asignados a cada instancia virtual configurada en los respectivos nodos. Así mismo se indican las capacidades de los nodos físicos y sus recursos disponibles luego de la asignación en las instancias virtuales. La asignación de vCPUs es fija, mientras que la asignación de memoria RAM y almacenamiento es variable y está sujeta al modo de operación de los módulos que se encuentren activos en cada instancia.

A continuación se detallan los módulos licenciados y activos en cada instancia y su modo de operación:

Tabla 5.
Modo de Operación de módulos licenciados

Módulos	vCMP de Producción (Nodos 1 y 2 de Guayaquil y Nodo 1 de Quito)	vCMP de Preproducción (Nodo 1 y 2 de Guayaquil)
Management (MGMT)	Small	Small
Local Traffic (LTM)	Nominal	Nominal
Application Security (ASM)	Nominal	Minimum
Global Traffic (DNS)	Nominal	Nominal
Access Policy (APM)	Nominal	None
Application Visibility and Reporting (AVR)	Minimum	Minimum
Advanced Firewall (AFM)	Nominal	Minimum

Los modos de operación de todos los módulos a excepción del Management (MGMT) son [3]:

- None / Disabled: Este estado especifica que el módulo se encuentra deshabilitado y no está ejecutándose en el sistema.
- Dedicated: Este estado indica que todos los recursos (CPU, Memoria y Disco) de la instancia en cuestión están asignados y dedicados a un solo módulo. En este estado todos los demás módulos pasan al estado “None/Disabled”
- Nominal: El módulo que se encuentre en este estado se mantiene activo con los recursos mínimos necesarios. Si hay más de un módulo activo bajo este estado, comparten los recursos disponibles de acuerdo a la demanda que presenten en un determinado período de tiempo.

- Minimum: En este estado, el módulo configurado sólo utiliza los mínimos recursos necesarios para su operación. No tiene opción a utilizar recursos disponbles del sistema.

Los modos de operación del módulo de Management (MGMT) son los siguientes:

- Small: No ocupa espacio en disco para su operación, sólo utiliza memoria RAM que es de 4GB.
- Medium: Se le asigna un espacio en disco de 200MB, más el espacio en memoria RAM que es de 4GB.
- Large: Se le asigna un espacio en disco de 500MB, más el espacio en memoria RAM que es de 4GB.

2.1.4 CONFIGURACIONES DE RED

Para la configuración de red de los nodos es importante tener en cuenta la ubicación de los equipos en la arquitectura de red de la organización. En este caso los nodos son ubicados en el perímetro, entre la red externa de internet y la red interna de la organización tal como se ilustra en la siguiente figura:

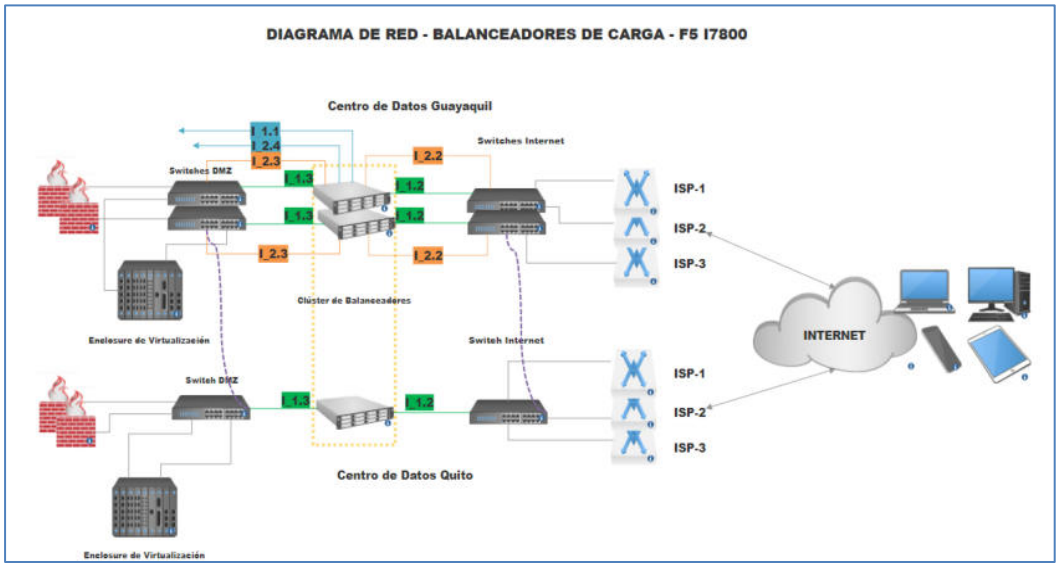


Figura 2.3 Diagrama de Red – Balanceadores de Carga – F5 i7800
Fuente: El Autor

Al estar en la frontera, entre internet y la red interna, el equipo tiene la visibilidad de todo el tráfico que ingresa y del que se dirige hacia el internet lo que lo convierte en un punto medular de acceso a los servicios digitales que ofrece la institución financiera a sus clientes. En esta ubicación es recomendable aplicar el modo de operación conocido como “full-proxy” el cual se caracteriza por separar el manejo y tratamiento de las sesiones de cara al cliente, de las sesiones que se establecen hacia los servidores aplicativos. La interacción de los clientes es directamente con el balanceador, y luego del balanceador hacia los servidores aplicativos se manejan sesiones independientes.

Las interfaces que asumieron los roles indicados anteriormente son las siguientes:

- I_1.1 (MGMT): Interfaz definida para manejar el tráfico relacionado con la administración de los equipos físicos y entes virtuales. En esta interfaz se definió una sola VLAN.
- I_1.2 (INTERNET): Interfaz definida para manejar el tráfico desde y hacia Internet a través de los enlaces que proveen los 3 ISPs que se ilustran en la Figura 2.3. En esta interfaz se definieron 5 VLANs, 1 por cada segmento de red que ofrecen los ISPs (1 ISP1, 2 ISP2 y 2 ISP3).
- I_1.3 (DMZ): Interfaz definida para interactuar con la red interna de la organización. En esta interfaz se definió una sola VLAN, utilizada para la interacción del balanceador con el Firewall Perimetral.
- I_2.2 (INTERNET_PRE): Interfaz definida para manejar el tráfico desde y hacia Internet que es utilizado para el ambiente de Preproducción. Se definió una sola VLAN para esta interfaz.
- I_2.3 (Preproducción): Interfaz para interactuar con la red interna de Preproducción. Se definió una sola VLAN sobre esta interfaz.

- I_2.4 (SYNC): Interfaz definida para la sincronización de los clústers para establecer el esquema de alta disponibilidad y geo-redundancia. En esta interfaz sólo se estableció una VLAN.

Tabla 6.
Subredes e interfaces configuradas

Nombre VLAN	ID VLAN	Descripción	Interfase
VLAN10 ISP 1	10	VLAN 10 de red externa ISP 1; Producción	1.2
VLAN20 ISP 2	20	VLAN 20 de red externa ISP 2; Producción	1.2
VLAN81 ISP 2	81	VLAN 81 de red externa ISP 2; Producción	1.2
VLAN40 ISP 3	40	VLAN 40 de red externa ISP 3; Producción	1.2
VLAN82 ISP 3	82	VLAN 82 de red externa ISP 3; Producción	1.2
VLAN4094 DMZ	4094	VLAN 4094 red interna de enganche DMZ; Producción	1.3
VLAN4092 MGMT	4092	VLAN 4092 red interna MGMT; Producción	1.1
VLAN4093 SYNC	4093	VLAN 4093 red interna SYNC; Producción	2.4
VLAN25 DMZ Preprod	25	VLAN 25 red interna de enganche DMZ; PreProducción	2.3
VLAN11 Internet Preproducción	11	VLAN 11 red externa ISP1 Preproducción; PreProducción	2.2

Con las VLANs definidas se establece el direccionamiento IP correspondiente de cada nodo y vCMP que interectúa con estas subredes. El direccionamiento IP requerido se lo obtuvo aplicando la siguiente tabla (Tabla 7):

Tabla 7.
Direccionamiento IP requerido

VLAN	Cantidad de IPs	Descripción
VLAN10 ISP 1	4	IP1 VLAN 10 de ISP1 - vCMP Producción Nodo 1 GYE
		IP2 VLAN 10 de ISP1 - vCMP Producción Nodo 2 GYE
		IP3 VLAN 10 de ISP1 - vCMP Producción Nodo 1 UIO
		IP4 VLAN 10 de ISP1 - FLOTANTE vCMP Producción
VLAN20 ISP 2	4	IP1 VLAN 20 de ISP2 - vCMP Producción Nodo 1 GYE
		IP2 VLAN 20 de ISP2 - vCMP Producción Nodo 2 GYE
		IP3 VLAN 20 de ISP2 - vCMP Producción Nodo 1 UIO
		IP4 VLAN 20 de ISP2 - FLOTANTE vCMP Producción
VLAN81 ISP 2	4	IP1 VLAN 81 de ISP2 - vCMP Producción Nodo 1 GYE
		IP2 VLAN 81 de ISP2 - vCMP Producción Nodo 2 GYE
		IP3 VLAN 81 de ISP2 - vCMP Producción Nodo 1 UIO
		IP4 VLAN 81 de ISP2 - FLOTANTE vCMP Producción
VLAN40 ISP 3	4	IP1 VLAN 40 de ISP3 - vCMP Producción Nodo 1 GYE
		IP2 VLAN 40 de ISP3 - vCMP Producción Nodo 2 GYE
		IP3 VLAN 40 de ISP3 - vCMP Producción Nodo 1 UIO
		IP4 VLAN 40 de ISP3 - FLOTANTE vCMP Producción
VLAN82 ISP 3	4	IP1 VLAN 82 de ISP3 - vCMP Producción Nodo 1 GYE
		IP2 VLAN 82 de ISP3 - vCMP Producción Nodo 2 GYE
		IP3 VLAN 82 de ISP3 - vCMP Producción Nodo 1 UIO
		IP4 VLAN 82 de ISP3 - FLOTANTE vCMP Producción
VLAN4094 DMZ	4	IP1 VLAN 4094 de DMZ - vCMP Producción Nodo 1 GYE
		IP2 VLAN 4094 de DMZ - vCMP Producción Nodo 2 GYE
		IP3 VLAN 4094 de DMZ - vCMP Producción Nodo 1 UIO
		IP4 VLAN 4094 de DMZ - FLOTANTE vCMP Producción
VLAN4092 MGMT	8	IP1 VLAN 4092 Administración - Equipo Físico Nodo 1 GYE
		IP2 VLAN 4092 Administración - Equipo Físico Nodo 2 GYE
		IP3 VLAN 4092 Administración - Equipo Físico Nodo 1 UIO
		IP4 VLAN 4092 Administración - vCMP Producción Nodo 1 GYE
		IP5 VLAN 4092 Administración - vCMP Producción Nodo 2 GYE
		IP6 VLAN 4092 Administración - vCMP Producción Nodo 1 UIO
		IP7 VLAN 4092 Administración - vCMP PreProducción Nodo 1 GYE
		IP8 VLAN 4092 Administración - vCMP PreProducción Nodo 2 GYE
VLAN4093 SYNC	5	IP1 VLAN 4093 Sincronización - vCMP Producción Nodo 1 GYE
		IP2 VLAN 4093 Sincronización - vCMP Producción Nodo 2 GYE
		IP3 VLAN 4093 Sincronización - vCMP Producción Nodo 1 UIO
		IP4 VLAN 4093 Sincronización - vCMP PreProducción Nodo 1 GYE

		IP5 VLAN 4093 Sincronización - vCMP PreProducción Nodo 2 GYE
VLAN25 DMZ Preproducción	3	IP1 VLAN 25 DMZ Preproducción - vCMP PreProducción Nodo 1 GYE
		IP2 VLAN 25 DMZ Preproducción - vCMP PreProducción Nodo 2 GYE
		IP3 VLAN 25 DMZ Preproducción - FLOTANTE vCMP PreProducción
VLAN11 Internet Preproducción	3	IP1 VLAN 11 ISP1 Internet Preproducción - vCMP PreProduccipon Nodo 1 GYE
		IP2 VLAN 11 ISP1 Internet Preproducción - vCMP PreProduccipon Nodo 2 GYE
		IP3 VLAN 11 ISP1 Internet Preproducción - FLOTANTE vCMP PreProduccipon

En las subredes a través de las cuales cursa el tráfico de los servicios correspondientes a las aplicaciones publicadas, se define una IP denominada “flotante”. Esta IP, alterna entre los nodos que conforman un “traffic group” y se aplica sobre el nodo que se encuentre activo. En caso que el nodo activo tenga inconvenientes y la operación conmute hacia uno de los nodos en standby, la IP flotante se mueve hacia el nuevo nodo activo. Con esta IP se mantienen operativos los servicios que atiende la arquitectura de balanceo. En este caso, las subredes que mantienen una IP flotante son las que manejan el tráfico de Internet y el tráfico hacia la DMZ que es donde se encuentran los servidores de las apliaciones publicadas.

Otro factor importante para la configuración de red en los equipos balanceadores, es el de establecer el enrutamiento de los flujos de tráfico a través de los gateways de las distintas subredes. Esto se realiza con la finalidad de que el tráfico hacia redes internas o externas tomen las subinterfaces que correspondan de acuerdo

a la puerta de enlace conveniente. A continuación un ejemplo de la configuración de las rutas:

Tabla 8.
Ejemplos de rutas estáticas

Nombre	Destino	Máscara de Red	Tipo de Recurso	Recurso
Tacacs	192.168.11.30	255.255.255.255	Gateway	172.16.1.1
Directorio Activo	192.168.10.1	255.255.255.255	Gateway	192.168.1.1
Red Interna	192.168.0.0	255.255.0.0	Gateway	192.168.1.1
Red Internet	Default IPv4		Pool	Pool Gateway

2.1.5 SERVIDORES VIRTUALES

Los servidores virtuales o “virtual servers” son las instancias que se definen a nivel del módulo LTM para que las peticiones que se originan desde internet alcancen los servidores correspondientes a las aplicaciones que son requeridas por los clientes de la institución.

Para la configuración de estas instancias debemos tener claro de qué manera se relacionan las configuraciones que se establecen a nivel de los módulos GTM y LTM. Esto es clave dado que representan las configuraciones principales para la exposición y balanceo de los recursos asociados a cada aplicación.

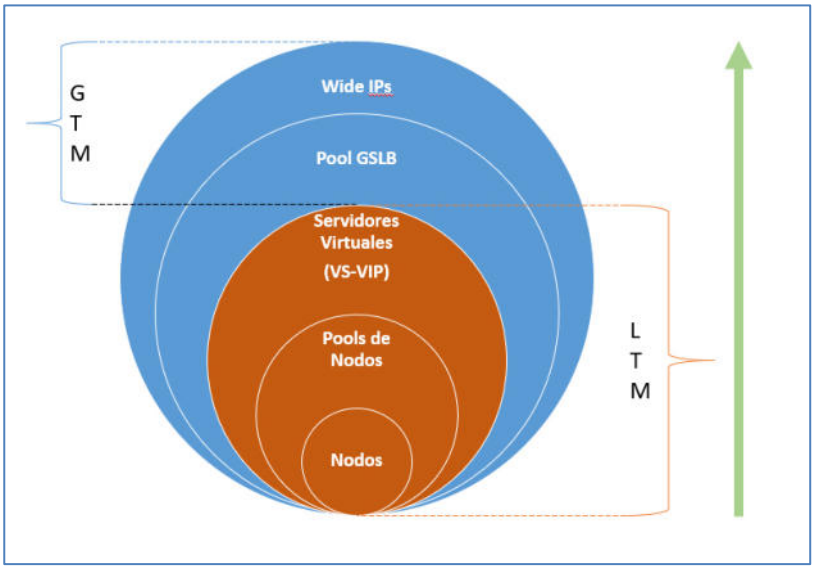


Figura 2.4 Relación GTM y LTM
Fuente: El Autor

En la Figura 2.4 se ilustra el orden en que se interrelacionan las configuraciones aplicadas desde el módulo LTM y que luego se vinculan a la parametrización en el módulo GTM. El orden en que se establece la configuración va desde los nodos hasta los Wide IPs tal como se ilustra con la flecha verde de la Figura 2.4. A continuación una descripción de cada uno de estos elementos [4]:

- Nodos: Los nodos son una configuración lógica que representan a los servidores finales o cargas donde se alojan las aplicaciones, el dato requerido para la configuración de estos elementos es su dirección IP y el puerto que van a publicar para responder las peticiones que serán direccionadas por el balanceador.

- Pools de Nodos: Los Pools de Nodos es una configuración requerida para agrupar los nodos que van a responder a un determinado servicio. En estos Pools se declaran, los nodos que conformarán el pool y el puerto del servicio al que responderán.
- Servidores Virtuales (VS-VIP): Los servidores virtuales son configuraciones lógicas en el sistema a las que se les define básicamente una IP Virtual (VIP) y un Pool de Nodos. La función de los servidores virtuales es la de enmascarcar con la IP Virtual, la IP real de los nodos finales que responden a los servicios.
- Pool GSLB: Los pools de servidor global de balanceo de cargas (Global Server Load Balancing) son utilizados a nivel del módulo GTM para agrupar los virtual servers creados en el módulo LTM y poderlos asociar a un nombre de dominio desde el mundo.
- Wide IP: Los Wide IPs son básicamente registros DNS de tipo A que responden a las peticiones DNS provenientes desde internet con la IP Pública asociada a los virtual servers configurados dentro del Pool GSLB que contiene.

Las peticiones de DNS que provienen desde el mundo son respondidas a través de los nodos de escucha o Listeners que se configuran en el módulo GTM.

Dentro de los servidores virtuales se establecen configuraciones para ayudar al sistema en la toma de decisiones creando un contexto y direccionando el tráfico de red hacia la mejor opción posible. Estas dos configuraciones son los Health Monitors (“Monitores de Salud”) y los iRules (“Reglas Inteligentes):

- Health Monitors (“Monitores de Salud”): Los Monitores de Salud como su nombre lo indica son sensores que ayudan a definir un estado y se aplican sobre los nodos o sobre los pools de nodos con la finalidad de que el sistema LTM pueda determinar si estos elementos lógicos se encuentran disponibles o no por lo tanto decide en base al estado de estos elementos si redireccionan tráfico de red a dichos nodos. Los monitores configurados en este proyecto son los de ICMP a nivel de nodos y de servicio o puerto a nivel del pool de nodos.

Status Indicator	Description
Green circle 	The object is available. This icon indicates that the BIG-IP system services traffic destined for this object. For BIG-IP APM sessions, this icon indicates that the session is established.
Blue square 	The availability of the object is unknown. For example, this status can occur when the object is not configured for service checking, the IP address of the object is misconfigured, or the object is disconnected from the network. For BIG-IP APM sessions, this icon indicates that the session is pending and not yet established. Note: Pool members and nodes with a status of unknown are eligible to receive client requests.
Yellow triangle 	The object is not currently available, but might become available later with no user intervention. For example, an object that has reached its configured connection limit might show a yellow status and then switch to a green status when the number of connections falls below the configured limit.
Red diamond 	The object is unavailable. This icon indicates that the BIG-IP system cannot service traffic destined for this object. For example, this status can occur when a node fails service checking because it has become unavailable. This status requires user intervention to restore the object status to green.
Black circle 	A user has actively disabled an available object.
Black diamond 	A user has actively disabled an unavailable object.
Gray icons 	A parent object has disabled the object or the object is enabled but unavailable because of another disabled object.
Black Square 	The availability of the object is unknown and the object is disabled.

Figura 2.5 Indicadores de estado de los nodos
Fuente: https://support.f5.com/csp/article/K12213214

En la Figura 2.5 se ilustran los estados que pueden adquirir los nodos desde la perspectiva de los equipos balanceadores.

- iRules (“Reglas Inteligentes”): Las iRules son reglas que permiten crear funcionalidades diversas para la toma de decisiones en los sistemas BIG-IP LTM. Estas reglas siguen la sintaxis de la industria denominada Tcl (“Tool Command Language”). Para este proyecto se crearon iRules con el objetivo de tomar una acción sobre los portales más visitados cuando están fuera de servicio y cuando son accedidos a través de puertos inseguros. En el primer caso se carga un archivo html con un mensaje de mantenimiento cuando los

miembros que conforman el pool del portal no están disponibles, mientras que en el segundo caso pasamos de una conexión http a https al momento que se recibe la URL a través del puerto inseguro aplicando una redirección a la URL segura.

2.1.6 TRADUCCIÓN DE DIRECCIONES DE RED

La traducción de direcciones de red es un apartado importante dentro de la configuración de la infraestructura dado que permite establecer los entes que de manera aislada requieren establecer conexiones por fuera de la configuración indicada anteriormente y relacionada con los servidores virtuales. En este proyecto se identificaron implementaciones que demandan conexiones a través de puertos dinámicos tales como los puertos que se utilizan en la comunicación vía protocolo SIP. También se identificó servicios que demandan generar tráfico saliente para un propósito específico como es el envío de correos masivos o la navegación a internet.

Para estos casos se utilizó lo que se conoce como NAT (“Network Address Translation”) o SNAT (“Secure Network Address Translation”), funcionalidades de red que permiten al sistema enmascarar una IP Privada con una IP Pública. La diferencia entre estas dos funcionalidades dentro del sistema BIG-IP es que

NAT permite una traducción 1 a 1 y no discrimina puertos de conexión, mientras que la SNAT establece conexiones a puertos específicos y permite crear contextos de 1 a 1, 1 a N ó N a N. Para el servicio de telefonía a través de protocolo SIP se utilizó la funcionalidad de NAT dada su naturaleza de manejar puertos dinámicos y para la navegación a internet y envío de correos masivos se utilizó la configuración a través de SNAT.

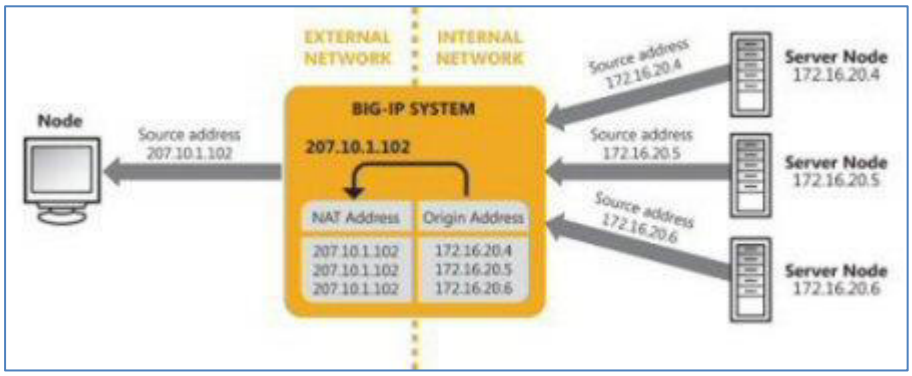


Figura 2.6 Ejemplo de SNAT con múltiples conexiones salientes
Fuente: https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-5-1/17.html

2.2. REEMPLAZO DE LOS EQUIPOS EN PRODUCCIÓN

Para el reemplazo de los equipos de la infraestructura anterior, por los nuevos componentes, se planificaron tres ventanas de mantenimiento. La primera ventana consistía en romper el clúster configurado entre los equipos F5 4000s, retirar el nodo secundario de los mismos y colocar en lugar de dicho componente el nodo secundario de la nueva

infraestructura de F5 i7800. Esta tarea demandó seis horas de trabajo más dos días de afinamiento.

Una vez sincronizado el nodo secundario con todas las configuraciones de los nodos que se encontraban en producción, se procedió a ejecutar la segunda ventana de trabajo que implicaba reemplazar las nodos correspondientes al nodo primario del centro de datos en la ciudad de Guayaquil y al nodo de contingencia ubicado en el centro de datos de la ciudad de Quito. Así mismo esta tarea demandó seis horas de trabajo y dos días de afinamiento de los componentes. Cabe indicar que desde la primera ventana de mantenimiento el cliente fue advertido de que el esquema de continuidad y contingencia se lo manejaría manualmente hasta que los tres nuevos nodos del mismo modelo (es decir los i7800) se encuentren operativos y formando el clúster respectivo. En ese sentido la tercera ventana de mantenimiento persiguió el objetivo de sincronizar los tres nuevos nodos a través de sus instancias virtuales de producción para restablecer el esquema de alta disponibilidad y contingencia geo-redundante.

Luego de la tercera ventana de mantenimiento los tres nodos entraban oficialmente a operar en producción manteniendo las exigencias de la infraestructura del cliente en cuanto a sincronización de la configuración, disponibilidad (Alta Disponibilidad en el centro de datos

principal) y contingencia (esquema Geo-Redundante con el centro de datos alterno).

2.3. CONFIGURACIÓN DE MÓDULOS DE SEGURIDAD

Los módulos que permiten a los sistemas balanceadores de F5 BIG-IP agregar capas de seguridad sobre el tráfico que pasa a través de ellos son los módulos, APM, AFM y ASM.

2.3.1. MÓDULO APM

Para este proyecto el módulo de APM (Access Policy Manager) fue activado con la finalidad de proveer acceso remoto a los funcionarios de la institución financiera a sus estaciones de trabajo que se encuentran en oficina. Sobre este módulo se establecieron los siguientes parámetros:

- Directorio Activo: Esta integración es necesaria para la validación de credenciales de los usuarios que se autentican en el portal y requieren establecer una conexión VPN-SSL,
- Servidor RADIUS: Esta integración fue necesaria aplicarla para validar el segundo factor de autenticación utilizado en el proceso de login de los usuarios.
- Autenticación LDAP: Esta integración es utilizada para identificar que los usuarios que están intentando autenticarse en la plataforma corresponden al grupo de seguridad que en

directorio activo está autorizado para realizar este tipo de interacción.

2.3.2. MÓDULOS AFM Y ASM

Los módulos AFM (Advanced Firewall Manager) y ASM (Application Security Manager) corresponden a los módulos que brinda la protecciones a nivel de capa 3 (de red) y de capa 7 (de aplicación). Estos módulos se configuraron para proteger dos canales transaccionales de la institución financiera contra ataques de Denegación de Servicio e identificación de interacciones a través de Bots.

Las protecciones a nivel de capa 3 y capa 7 que se habilitaron para la prevención de ataques de denegación de servicios fueron las siguientes:

- TCP/UDP (capa 3): Engloba todos los posibles ataques a través de los protocolos de red TCP y UDP, entre ellos tenemos los ataques de tipo “Flood” que como su nombre lo indica son ataques que inundan los servicios con peticiones no válidads. También ataques asociados a una malformación en la cabecera IPv6, IPv4 o del mismo TCP que podrían generar un error en la respuesta de los servicios.

- DNS (capa 7): Son protecciones contra ataques asociados a peticiones sobre el protocolo DNS tales como peticiones de registros A, PTR, NS, NX que podrían ser generados por entes maliciosos y direccionados a los servicios más importantes de la entidad financiera.
- HTTP (Capa 7): Sobre este protocolo se activó un sensor de peticiones que en el momento que sobrepasen una línea base que el sistema debe aprender tomará una acción de bloqueo o de comprobación de que existe interacción humana del lado del cliente.

Cabe indicar que estas protecciones se activan al inicio en modo aprendizaje por lo menos por treinta días para que el sistema pueda establecer líneas bases asociadas al comportamiento del tráfico que tiene la entidad financiera.

2.4. CONFIGURACIÓN DE PERFILES DE ANALÍTICA

Dentro de las configuraciones de monitoreo del sistema se establecen perfiles para monitorear el performance de los componentes que conforman la infraestructura. Los perfiles pueden ir desde lo más específico como los nodos que conforman una granja de servidores para una determinada aplicación hasta un dashboard donde se pueda apreciar el performance del vCMP como tal.

Para este proyecto se estableció el dashboard general en donde se puede apreciar el performance del nodo que se encuentra operando como principal el cual será utilizado para la emisión de reportes periódicos hacia los mandos interesados en conocer el estado de este componente crítico.

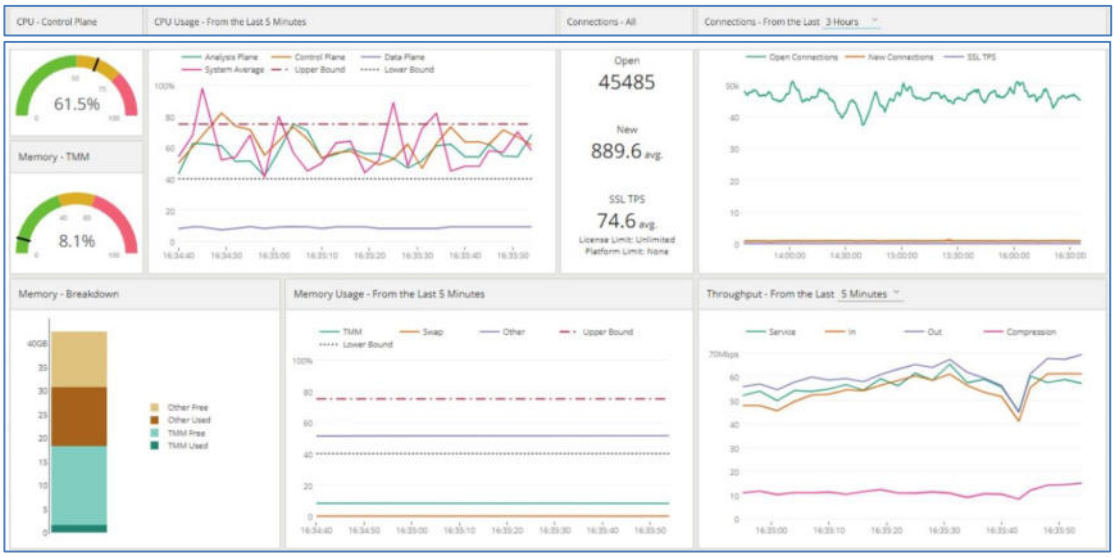


Figura 2.7 Dashboard de Performance vCMP Producción
Fuente: Equipos de Entidad Financiera

En la figura 2.7 se aprecia el Dashboard configurado para tener visibilidad del consumo de CPU, Memoria y de conexiones que cursan a través del sistema de balanceo de cargas. La gráfica muestra que el consumo de CPU está al 61.5% y memoria al 8.1%. Con respecto a las conexiones activas se tienen alrededor de 45 mil conexiones activas, con un promedio de 890 nuevas conexiones. Sobre las transacciones por segundo de conexiones SSL se tienen un promedio

de 74.6. Salvo por el consumo de CPU, las demás métricas no despiertan preocupación alguna ya que están por debajo de las capacidades propias de la infraestructura. El tráfico total que en ese instante soporta la infraestructura está por debajo de los 70Mbps.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 CUMPLIMIENTO DE OBJETIVOS DE DISPONIBILIDAD

De acuerdo a los alcances establecidos al inicio del proyecto los objetivos que corresponden a la disponibilidad fueron los siguientes:

- Alta Disponibilidad y Geo-Redundancia: Este objetivo fue abordado de manera íntegra con la instalación y sincronización de los 3 nodos (2 en el centro de datos de Guayaquil y 1 en el centro de datos de Quito) y la configuración de clúster de los vCMPs en ambiente de Producción.

- Migración de funcionalidades y configuraciones a la nueva Infraestructura: Este objetivo se cumplió con la instalación del Nodo 2 de la nueva Infraestructura y la carga del archivo de configuraciones en el vCMP de Producción. Las pruebas de que efectivamente no había afectaciones en Producción se realizaron durante la primera ventana de trabajo y los días de funcionamiento que se mantuvo el nodo 2 i7800, incluso en las siguientes ventanas este nodo pasó a ser la fuente de sincronización primaria de los vCMPs en los nodos 1 y 3.

- Configuración de instancias virtuales independientes: Este objetivo se cumplió al crear en cada nodo del centro de datos de Guayaquil dos vCMPs, uno para el ambiente de Producción y el segundo para el ambiente de Preproducción. Este alcance es importante en la disponibilidad de la infraestructura ya que la intención de la organización fue la de mitigar los riesgos de indisponibilidad asociados a cambios producto de pruebas en los ambientes productivos.

- Actualización del firmware a la última versión estable y recomendada por fabricante: Este objetivo persigue mantener estable la plataforma según las recomendaciones del fabricante.

Se instaló la versión de más reciente y estable tanto en los nodos físicos como en los nodos virtuales.

- Integración con la consola de administración centralizada de reportería modelo F5 BIG-IQ: Este objetivo no pudo cumplirse tal como se lo planteó dado que se presentaron problemas de estabilidad en la herramienta BIG-IQ. Como medida compensatoria se establecieron los dashboards de estadísticas relacionadas al performance de los nodos físicos y virtuales.

En resumen los objetivos de disponibilidad se cumplieron de acuerdo a lo que se estableció como alcance inicial en el acta de constitución del proyecto a excepción del relacionado con la herramienta BIG-IQ que se decidió revisarla posteriormente.

3.2. CUMPLIMIENTO DE OBJETIVOS DE SEGURIDAD

En el alcance inicial del proyecto no se establecieron alcances específicos orientados a la seguridad, sin embargo la misma se vio implícita en los siguientes alcances:

- Instalación de Licenciamiento F5 BEST Bundle con el addon de AWAF: Este objetivo es básico para el funcionamiento de la plataforma ya que incluye el licenciamiento de todos los módulos que se activaron en el sistema. Lo relacionado a la seguridad tiene

que ver con los módulos APM, AFM y ASM sobre los cuales se activaron las políticas de seguridad correspondientes. En el caso de APM, se aplicaron las políticas relacionadas al conexión por VPN-SSL en donde se establece un perfilamiento de la conexión de los usuarios. Por otro lado los módulos AFM y ASM fueron los módulos sobre los cuales se aplicaron políticas de protección de antidenegación de servicios tanto en capa de red como en la capa de aplicación en modo monitoreo.

- Configuración de funcionalidades de control de acceso, para mantener la segregación de funciones en la administración del sistema entre las áreas respectivas: Este objetivo está relacionado con la seguridad dado que se refiere a los privilegios establecidos para cada usuario administrador del sistema. Se configuraron los usuarios con sus respectivos roles de acuerdo a su ámbito de acción. Las áreas involucradas y que demandaron acceso al sistema fueron Auditoría, Tecnología y Seguridad.

En resumen dentro del alcance establecido en el acta de constitución del proyecto se abarcaron los aspectos de la seguridad en los módulos correspondientes (APM, ASM, AFM), así como lo relacionado a la administración de usuarios y sus roles y perfiles.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Las soluciones de balanceo de carga de aplicaciones, definitivamente juegan un rol fundamental en la infraestructura tecnológica de las organizaciones que cuentan con esquemas de alta disponibilidad y en donde los tiempos de restauración de los servicios se acortan debido a las exigencias de sus clientes y de los organismos de control.

Las entidades financieras en el Ecuador son reguladas por la Superintendencia de Bancos, la cual, dentro de sus Normas de Control Para las Entidades del Sector Financiero Público y Privado, Título IX de la Gestión y Administración de Riesgo [5], establece lineamientos para que las entidades reguladas implementen procedimientos y controles relacionados a la continuidad del negocio, la seguridad en los canales electrónicos y el manejo de ambientes aislados con la debida segregación. Con la implementación de este proyecto se reforzaron estas tres aristas dado que la solución mantiene un esquema de alta disponibilidad y georedundancia, habilita seguridades a nivel de aplicaciones y permite la separación de ambientes a través de sus instancias virtuales.

Adicionalmente, el proyecto se desarrolló adoptando los principios de la gestión de proyectos establecidos en el PMBOK del PMI y con un enfoque predictivo. Se definió un alcance a través de la correspondiente Acta de Constitución, se estableció un cronograma y los controles de cambios fueron acordados entre las partes hasta el cierre final del mismo. Finalmente, se establecieron los respectivos compromisos posterior al cierre del proyecto, es decir en el ciclo operativo de la solución, para atender las novedades que se presentaron en determinados puntos del alcance establecido en el Acta de Constitución del Proyecto.

Podemos concluir que el proyecto cubrió las expectativas principales que se planteó la entidad financiera tales como:

1. La renovación de la infraestructura tecnológica cuyo anuncio de fin de venta por parte del fabricante fue publicado en Abril del 2017 [6] y en consecuencia con las fechas de fin de soporte, se planificó dicha renovación.
2. Adicionalmente, la expectativa de mantener ambientes segregados de prueba y producción ahora son posibles debido a la funcionalidad de virtualización, la infraestructura quedó lista con la instancia configurada a pesar que no fue posible implementar este ambiente al 100% debido que la infraestructura sobre la cual las cargas de trabajo (servidores) debían desplegrase no se encontraba disponible.
3. Las configuraciones de Seguridad para proteger los servicios publicados se aplicaron en modo monitoreo lo cual permitió tener visibilidad de los ataques de denegación de servicio tanto a nivel de red como a nivel de aplicaciones. Sin embargo, dado que era necesario establecer una línea base con un aprendizaje de por lo menos un mes se acordó aplicar el bloqueo de las conexiones anómalas en lo posterior.
4. Con respecto al monitoreo de la plataforma se aplicó la respectiva integración con los servidores SNMP que ya contaba la entidad financiera y se implementaron Dashboards de estado de los vCMPs para tener un detalle del número de conexiones simultáneas, TPSs, Throughput y niveles de usabilidad de CPU y memoria.

RECOMENDACIONES

A pesar que un proyecto tecnológico logre las expectativas trazadas, sean de manera total o parcial, el cierre del mismo traslada la solución tecnológica al proceso operativo del área responsable. Dicha área debe adoptar un procedimiento de gestión y mejora continua para obtener el mayor provecho de la solución o proceso derivado del proyecto entregado.

Siguiendo el ciclo PDCA o ciclo de Deming [7] se plantean las siguientes recomendaciones:

1. Planificar:
    a. Recolectar las novedades presentadas sobre los alcances que fueron revisados, definir las implicaciones técnicas y levantar un cronograma de actividades con responsables y fechas de compromiso. Dentro de los alcances revisados y que quedaron pendientes de seguimiento están los siguientes:
        i. Configuración de Servicios en ambiente de Preproducción
        ii. Integración con sistema BiG-IQ
        iii. Habilitación de configuraciones de Seguridad en modo Prevención
        iv. Adición de más servicios en el monitoreo AntiDDoS y de AntiBots.

2. Hacer:
    a. Una vez levantadas las implicaciones técnicas y actividades de los 4 ítems indicados como pendientes de revisión, ejecutar el cronograma relevado. Según las definiciones en la Gestión de Proyectos de la entidad financiera, sería necesario por cada ítem levantar un proyecto independiente o en su defecto validar la relación entre ellos para tratar más de uno en un mismo proyecto. Es recomendable que por cada proyecto se realice un KickOff para que tanto Patrocinadores, Líderes, Gestor y miembros del equipo del proyecto estén al tanto de las actividades y su nivel de participación en el mismo.

3. Revisar:
    a. Una vez culminadas las actividades de los respectivos proyectos, realizar la validación respectiva de los alcances planteados. Adicionalmente establecer dentro del flujo de liberación de aplicaciones que requieran ser publicadas al internet procedimientos para que las configuraciones en los ambientes previos y de producción se realicen a nivel de los balanceadores de carga del perímetro. También, en dicho flujo se debe de considerar la habilitación de las protecciones de seguridad que la plataforma provee. No olvidar considerar las

pantallas de monitoreo configurables tanto a nivel de nodos como en el sistema BIG-IQ. A nivel general, estar muy pendientes de las alertas que la plataforma está emitiendo constantemente y analizarlas de forma periódica para tomar acciones correctivas o de mejora de manera anticipada.

4. Actuar
    a. En base a los indicadores del apartado anterior, tomar acción de las novedades encontradas y plantear proactivamente la planificación y ejecución de mejoras sobre el sistema administrado. Tomar en consideración las observaciones que emitan los entes reguladores y las áreas de cumplimiento como Auditoría Interna, Seguridad y Riesgos.

BIBLIOGRAFÍA

[1] F5 Networks, https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf, fecha de consulta septiembre 2020

[2] F5 Networks, https://www.f5.com/pdf/products/big-ip-modules-ds.pdf, fecha de consulta septiembre 2020

[3] F5 Networks – AskF5 – Resource Provisioning, https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-essentials-11-6-0/7.html, fecha de consulta septiembre 2020

[4] F5 Networks – AskF5 – BIG-IP Local Traffic Management: Basics, https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-basics-13-0-0.html, fecha de consulta septiembre 2020

[5] Superintendencia de Bancos, https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2019/05/L1_IX_cap_V.pdf, fecha de consulta diciembre 2020

[6] End of Sale announcement for BIG-IP 2000, 4000, 5000, 7000, and 10000 series appliances, https://support.f5.com/csp/article/K55590970**,** fecha de consulta diciembre 2020.

[7] Jorge Jimeno Bernal, Ciclo PDCA (Planificar, Hacer, Verficar y Actuar), https://www.pdcahome.com/5202/ciclo-pdca/, fecha de consulta diciembre 2020.