INFORME MENSUAL

Solución Balanceadores F5 para Superintendencia de Sociedades

CONFIDENCIAL

NGEEK Latam

Contact: consulting@ngeek.co
Document Information: v1.0
Publication Date: February 2024

NGEEK
Cra 16a # 79 – 05 Of 607
Bogotá, Colombia
www.ngeek.co
+57 3143554583
+57 3186113985

Revisión	Changes	Editor	Date
1.0	Base Version	Brian Mecon	30-OCT-2024

CONFIDENCIAL

Tabla de Contenido

CONFIDENCIAL 6

ACERCA DE ESTE DOCUMENTO 7

CONVENCIONES 7

INTRODUCCIÓN 8

OBJETIVOS ESPECÍFICOS 8

PLATAFORMA ACTUAL 9

INVENTARIO DE COMPONENTES 11

ANÁLISIS DE CAPACIDAD 11

ANÁLISIS DE PLATAFORMA ACTUAL 13

ANÁLISIS DE PLATAFORMA – HOST 13
Análisis de Plataforma – Host 1 13
Hostname 13
Modelo y Estatus 13
Estado de Soporte con el Fabricante 14
Performance – Consumo de CPU 15
Performance – Consumo de Memoria 15
Tabla Resumen de Consumo de Recursos 15
Análisis de Plataforma – Host 2 16
Hostname 16
Modelo y Estatus 16
Estado de Soporte con el Fabricante 17
Performance – Consumo de CPU 18
Performance – Consumo de Memoria 18
Tabla Resumen de Consumo de Recursos 18
ANÁLISIS DE PLATAFORMA – GUESTS (VIRTUAL EDITION LTM) 19
Análisis de Plataforma – Cluster Producción – Guest Virtual 1 19
Hostname 19
Modelo y Estatus 19
Licenciamiento y Aprovisionamiento 20
Performance – Consumo de CPU 20

CONFIDENCIAL

Performance – Consumo de Memoria 21
Performance – Conexiones Concurrentes 21
Performance – Throughput 21
Performance – TPS SSL 22
Tabla Resumen de Consumo de Recursos 22
Análisis de Plataforma – Cluster Producción – Guest Virtual 2 23
Hostname 23
Modelo y Estatus 23
Licenciamiento y Aprovisionamiento 24
Performance – Consumo de CPU 24
Performance – Consumo de Memoria 25
Performance – Conexiones Concurrentes 25

Performance – Throughput 25
Performance – TPS SSL 26
Tabla Resumen de Consumo de Recursos 26
Análisis de Plataforma – Cluster DMZ – Guest Virtual 1 27
Hostname 27
Modelo y Estatus 27
Licenciamiento y Aprovisionamiento 28
Performance – Consumo de CPU 28
Performance – Consumo de Memoria 29
Performance – Conexiones Concurrentes 29
Performance – Throughput 29
Performance – TPS SSL 30
Tabla Resumen de Consumo de Recursos 30
Análisis de Plataforma – Cluster DMZ – Guest Virtual 2 31
Hostname 31
Modelo y Estatus 31
Licenciamiento y Aprovisionamiento 32
Performance – Consumo de CPU 32
Performance – Consumo de Memoria 33
Performance – Conexiones Concurrentes 33
Performance – Throughput 33
Performance – TPS SSL 34
Tabla Resumen de Consumo de Recursos 34
Análisis de Plataforma – Cluster BackEnd – Guest Virtual 1 35
Hostname 35
Modelo y Estatus 35
Licenciamiento y Aprovisionamiento 36
Performance – Consumo de CPU 36
Performance – Consumo de Memoria 37
Performance – Conexiones Concurrentes 37
Performance – Throughput 37
Performance – TPS SSL 38
Tabla Resumen de Consumo de Recursos 38
Análisis de Plataforma – Cluster BackEnd – Guest Virtual 2 39
Hostname 39

CONFIDENCIAL

Modelo y Estatus 39
Licenciamiento y Aprovisionamiento 40
Performance – Consumo de CPU 40
Performance – Consumo de Memoria 41
Performance – Conexiones Concurrentes 41
Performance – Throughput 41
Performance – TPS SSL 42
Tabla Resumen de Consumo de Recursos 42
Análisis de Plataforma – Cluster Pruebas – Guest Virtual 1 43
Hostname 43
Modelo y Estatus 43
Licenciamiento y Aprovisionamiento 44
Performance – Consumo de CPU 44
Performance – Consumo de Memoria 45
Performance – Conexiones Concurrentes 45
Performance – Throughput 45
Performance – TPS SSL 46
Tabla Resumen de Consumo de Recursos 46
Análisis de Plataforma – Cluster Pruebas – Guest Virtual 2 47

Hostname 47
Modelo y Estatus 47
Licenciamiento y Aprovisionamiento 48
Performance – Consumo de CPU 48
Performance – Consumo de Memoria 49
Performance – Conexiones Concurrentes 49
Performance – Throughput 49
Performance – TPS SSL 50
Tabla Resumen de Consumo de Recursos 50

SEGUIMIENTO A OBJETOS CONFIGURADOS 51

ANÁLISIS DE VULNERABILIDADES 52

CONCLUSIONES & RECOMENDACIONES 57

CONFIDENCIAL

Confidencial

El material contenido en este documento es propiedad de **SUPERINTENDENCIA DE SOCIEDADES**. Este material incluye información que no debe ser discutida fuera de la organización y no puede ser duplicada para ningún efecto, lo cual significa que es de uso exclusivo del personal designado.

El sello de confidencialidad hace referencia a que esta información no puede ser reproducida ni revelada a terceros. Las normas y políticas de uso y manejo de la información especificada en el presente documento están sujetas a lo especificado en la cláusula de confidencialidad incluida en el contrato de servicios, previamente firmado entre **SUPERITENDENCIA DE SOCIEDADES** y **NGEEK S.A.S**.

CONFIDENCIAL

Acerca de este Documento

Convenciones

Las convenciones de estilo utilizadas en este documento se detallan en la tabla a continuación:

Convention	Use
Calibri	Texto.
Calibri Bold Italic	***Nombres de menús, comandos, botones y otros elementos de la interfaz de usuario.***
Calibri Italic 11pt	*Citas y términos especiales, la primera vez que aparecen.*
`Courier New Italic`	*`Lenguaje scripts`*
	Notas que ofrecen una explicación adicional o una pista sobre cómo superar un problema común.
	Advertencias que indican operaciones de usuario potencialmente dañinas y explican cómo evitarlas.
	Un ejemplo.

CONFIDENCIAL

Introducción

SUPERITENDENCIA DE SOCIEDADES actualmente cuenta con una solución de Balanceo de *F5 Networks*, cuya administración se encuentra a cargo del proveedor que elabora el presente documento: **NGEEK S.A.S**. El presente, tiene como fin entregar un reporte de la situación actual de la plataforma, indicando las actividades de gestión llevadas a cabo sobre esta solución, en el último mes cursado.

Objetivos Específicos

- ✓ Entender la plataforma actual y su inventario de componentes.
- ✓ Ejecución de análisis de capacidad actual respecto de su consumo.
- ✓ Análisis del comportamiento y consumo de la solución en la actualidad, respecto del comportamiento del tráfico y servicios.
- ✓ Seguimiento a Objetos de Trafico configurados y su comportamiento.
- ✓ Análisis de vulnerabilidades y su aplicación.
- ✓ Conclusiones y recomendaciones respecto de la información recopilada y el análisis realizado.

CONFIDENCIAL

Plataforma Actual

La solución de BIG-IP F5 en el **SUPERITENDENCIA DE SOCIEDADES**, está conformada por dos (2) chasis BIG-IP i5800 ubicados en el Datacenter Principal (Bogotá), los cuales cuentan cada uno con cuatro (4) Ambientes Virtual (vCMP Guest), que se encuentran en Alta Disponibilidad (HA) (Active-Standby). Estos ambientes (Clusters) son: Producción, DMZ, BackEnd y Pruebas. A continuación, las topologías tipo esquema, diagramando lo mencionado anteriormente.

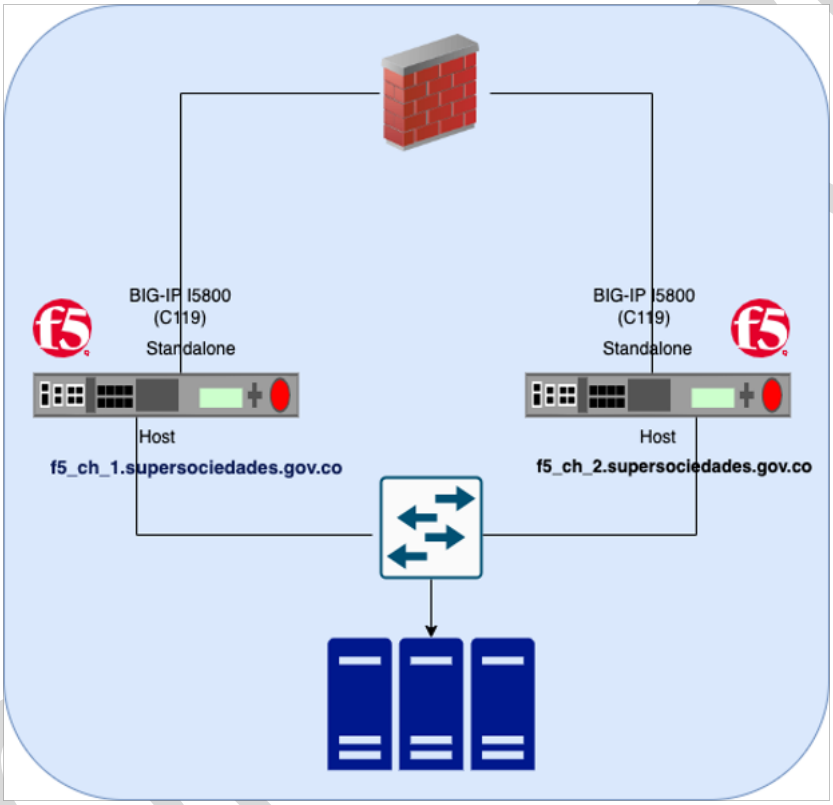


Figura No. 1 - Estado actual de la Solución F5 (Hardware)

COMERCIAL

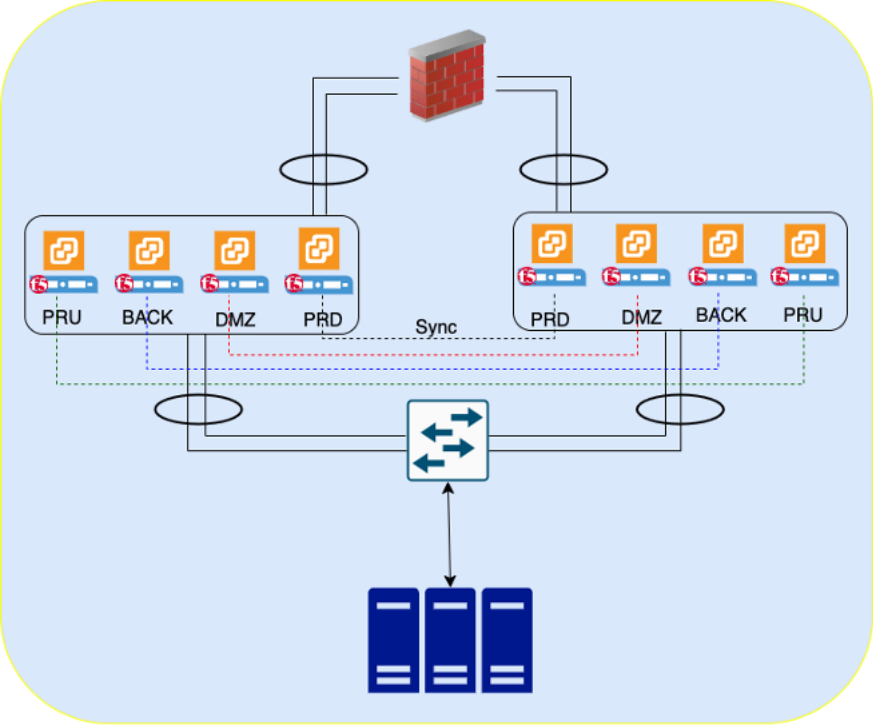


Figura No. 2 - Estado actual de la Solución F5 (vCMP

CONFIDENCIAL

Inventario de Componentes

Nombre del Host	Ciudad	Tipo	TMOS Version	S/N
f5_ch_1.supersociedades.gov.co	Bogotá	Chasis	15.1.7 Build 0.0.6	f5-ynfv-fjxk
f5_ch_2.supersociedades.gov.co	Bogotá	Chasis	15.1.7 Build 0.0.6	f5-mwpr-whrb
f5prod1.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A
f5prod2.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A
f5dmz1.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A
f5dmz2.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A
f5back1.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A
f5back2.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A
f5pru1.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A
f5pru2.supersociedades.gov.co	Bogotá	vCMP	15.1.7 Build 0.0.6	N/A

Tabla No. 1 - Inventario de Componentes – Solución F5Inventario de Componentes – Solución F5

Análisis de Capacidad

El chasis BIG-IP i5800 que se evidencia en la imagen a continuación, cuenta con las capacidades expuestas más abajo.



Figura No. 3 - F5 BIG-IP i5800 Chassis

CONFIDENCIAL

General	
Model Number	C119
Chassis 400 Level BOM	[No data available]
DAG Model ID	0
DAG Egress Model ID	0
BIOS Revision	OBJ-0645-xx BIOS: 5.20.030.0 ME: 6.0.50.1252 05/06/2019
FIPS Installed	[No data available]
Memory	
Physical Memory	47.11 GB
Total TMM RAM	522.0 MB
Total Linux Host RAM	47.11 GB
CPU	
Hardware Specifications	
Type	[No data available]
TMOS View	
Type	Intel(R) Xeon(R) CPU E5-1630 v4 @ 3.70GHz

Figura No. 4 - Modelo y Recursos de Computo Chasis BIG-IP i5800 -1

Virtualization (Maximum Number of vCMP® Guests):	N/A	8
Processor:	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor cores)	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor cores)
Memory:	48 GB DDR4	48 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD	1x 480 GB Enterprise Class SSD

Figura No. 5 - Modelo y Recursos de Computo Chasis BIG-IP i5800 -2

Specifications	i5800
Intelligent Traffic Processing:	L7 requests per second: 1.8M L4 connections per second: 800K L4 HTTP requests per second: 12M Maximum L4 concurrent connections: 40M Throughput: 60 Gbps/35 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 20K TPS (ECDSA P-256) RSA: 35K TPS (2K keys) 20 Gbps bulk encryption*

Figura No. 6 - Capacidad de Manejo de Trafico F5 BIG-IP i5800

Análisis de Plataforma Actual

***** NOTA: Es importante mencionar que, dado que la solución actualmente no almacena estadígrafos mayores a treinta (30) días calendario, las evidencias de consumo de recursos expuestos a continuación, igualmente no reflejan valores mayores a treinta (30)días de la fecha en la que fue elaborado el presente documento.***

Análisis de Plataforma – Host

Análisis de Plataforma – Host 1

Hostname

f5_ch_1.supersociedades.gov.co

Modelo y Estado

System	
Hostname	f5_ch_1.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-ynfv-fjxk
Blade S/N	[No data available]
Status	STANDALONE active for about 19 hours, 23 minutes
Uptime	19 hours, 25 minutes
Load Average	1.50, 1.39, 1.23
Physical Memory	47.11 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 8 Cores

Figura No. 7 - Información General de Chasif5_ch_1.supersociedades.gov.co

CONFIDENCIAL

Estado de Soporte con el Fabricante

```
BIG-IP i5800 Serial Number: f5-ynfv-fjxk
Name: f5_ch_1.supersociedades.gov.co
```

```
#-------------------------------------------------------------------
# F5 Product Information for ZBGMXVHD
#-------------------------------------------------------------------
 F5 Product         : F5-BIG-LTM-I5800 BIG-IP APPLIANCE: LOCAL TRAFFIC MANAGER I5800 (48G
 Usage              : Production
 Product Order Status  : Sales
 License Time Limit    : N/A
 Serial Number         : f5-ynfv-fjxk (C119)
  Mac Address          : 00:94:a1:15:0a:00
  Appliance Status     : Sales
#-------------------------------------------------------------------
# Service and Warranty Information
#-------------------------------------------------------------------
 Entitled Service      : 10-16-2018 - 10-28-2025 (F5-SVC-BIG-PRE-L1-3)
 Warranty End Date     : 08-09-2019
#-------------------------------------------------------------------
# Base Key for F5 Product BIG-IP v9.x for ZBGMXVHD
#-------------------------------------------------------------------
 Base RegKey         : BGMXVHD (Locked) BIG-IP
 F5 Platform         : C119
 First Activation Date : 10-16-2018
 Last Activation Date  : 10-29-2024
 License Time Limit    : N/A
 Mac Address           : 00:94:a1:15:0a:00
#-------------------------------------------------------------------
# License Modules for BGMXVHD (Locked) BIG-IP
#-------------------------------------------------------------------
 Serial Number       : PCDNAPJ (Active) LIC-PKG-BIG-LTM-I5800
 Serial Number       : XFYFVWK (Active) LIC-PKG-BIG-ROUTEMODS
#-------------------------------------------------------------------
# Hardware and Software Options
#-------------------------------------------------------------------
 Serial Number       : ZXFYFVWK (F5-ADD-BIG-ROUTING)
#-------------------------------------------------------------------

#-------------------------------------------------------------------
# Copyright © 1999-2024, F5 Networks, Inc.
# All rights reserved.
#
# F5 Document Created   : 2024-03-06 16:00:05 UTC
#-------------------------------------------------------------------
```

CONFIDENCIAL

Performance – Consumo de CPU

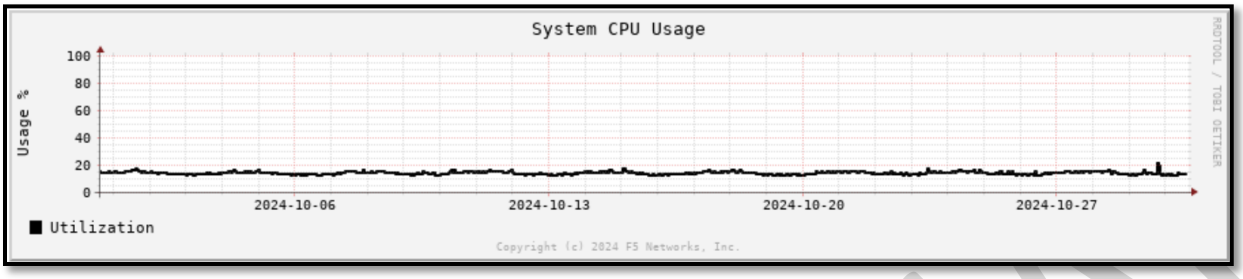


Figura No. 8 - Consumo CPU por Core f5_ch_1.supersociedades.gov.co últimos 30 días

Performance – Consumo de Memoria

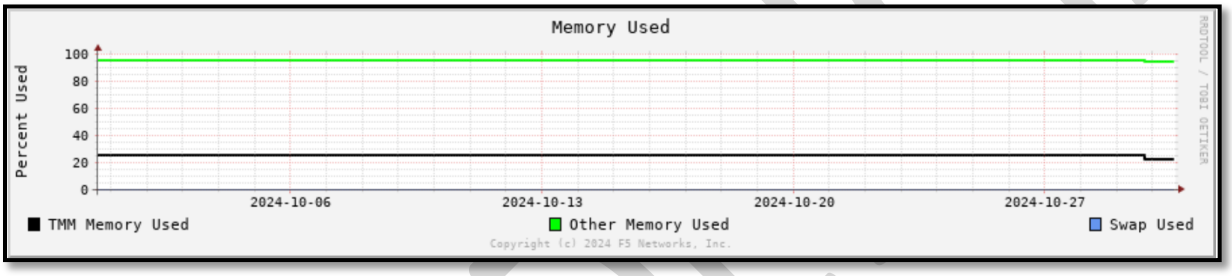


Figura No. 9 – Consumo Memoria f5_ch_1.supersociedades.gov.co últimos 30 días

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)
f5_ch_1.supersociedades.gov.co	20%	25%	95%	0%

- ✓ En los HOST/Chasis que permiten virtualizar, el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por todos los vCPU (8 vCPU) y los respectivos vCMP Guest (Máquinas Virtuales)
- ✓ En general los valores reflejados sobre el HOST/Chasis, son normales y muestran un consumo de recursos bajo.

CONFIDENCIAL

Análisis de Plataforma – Host 2

Hostname

f5_ch_2.supersociedades.gov.co

Modelo y Estatus

System	
Hostname	f5_ch_2.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-mwpr-whrb
Blade S/N	[No data available]
Status	STANDALONE active for about 22 hours, 10 minutes
Uptime	22 hours, 12 minutes
Load Average	2.32, 1.58, 1.32
Physical Memory	47.11 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 8 Cores

Figura No. 10 - Información General de f5_ch_2.supersociedades.gov.co

CONFIDENCIAL

Estado de Soporte con el Fabricante

```
BIG-IP i5800 Serial Number: f5-mwpr-whrb
Name: f5_ch_2.supersociedades.gov.co
```

```
#---------------------------------------------------------------
# F5 Product Information for ZVWCTDWK
#---------------------------------------------------------------
 F5 Product         : F5-BIG-LTM-I5800 BIG-IP APPLIANCE: LOCAL TRAFFIC MANAGER I5800 (48G
 Usage              : Production
 Product Order Status  : Sales
 License Time Limit    : N/A
 Serial Number       : f5-mwpr-whrb (C119)
  Mac Address        : 00:0a:49:fc:bb:00
  Appliance Status   : Sales
#---------------------------------------------------------------
# Service and Warranty Information
#---------------------------------------------------------------
 Entitled Service     : 10-16-2018 - 10-28-2025 (F5-SVC-BIG-PRE-L1-3)
 Warranty End Date    : 08-09-2019
#---------------------------------------------------------------
# Base Key for F5 Product BIG-IP v9.x for ZVWCTDWK
#---------------------------------------------------------------
 Base RegKey         : VWCTDWK (Locked) BIG-IP
 F5 Platform         : C119
 First Activation Date : 10-16-2018
 Last Activation Date  : 10-29-2024
 License Time Limit    : N/A
 Mac Address         : 00:0a:49:fc:bb:00
#---------------------------------------------------------------
# License Modules for VWCTDWK (Locked) BIG-IP
#---------------------------------------------------------------
 Serial Number       : KEABPOZ (Active) LIC-PKG-BIG-LTM-I5800
 Serial Number       : XTBIYLE (Active) LIC-PKG-BIG-ROUTEMODS
#---------------------------------------------------------------
# Hardware and Software Options
#---------------------------------------------------------------
 Serial Number       : ZXTBIYLE (F5-ADD-BIG-ROUTING)
#---------------------------------------------------------------

#---------------------------------------------------------------
# Copyright © 1999-2024, F5 Networks, Inc.
# All rights reserved.
#
# F5 Document Created   : 2024-03-06 16:00:08 UTC
#---------------------------------------------------------------
```

CONFIDENCIAL

Performance – Consumo de CPU

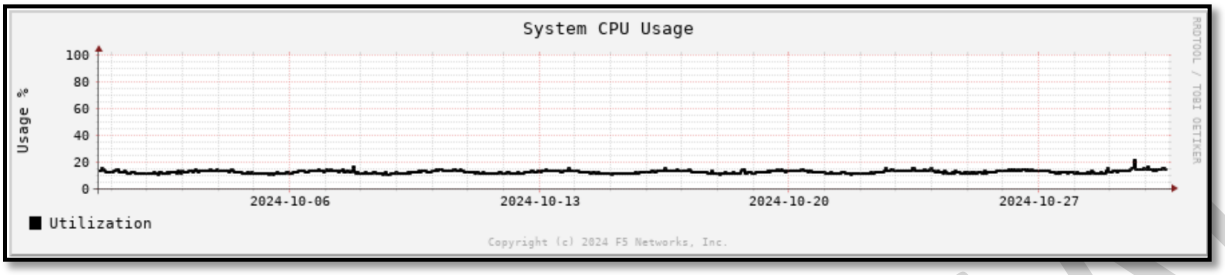


Figura No. 11 - Consumo CPU por Core f5_ch_2.supersociedades.gov.co últimos 30

Performance – Consumo de Memoria

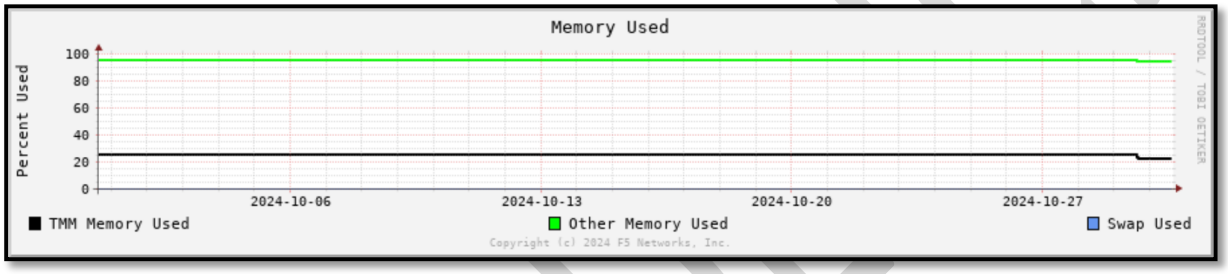


Figura No. 12 – Consumo Memoria f5_ch_2.supersociedades.gov.co últimos 30 días

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)
f5_ch_2.supersociedades.gov.co	21%	25%	95%	0%

- ✓ En los HOST/Chasis que permiten virtualizar, el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por todos los vCPU (8 vCPU) y los respectivos vCMP Guest (Máquinas Virtuales) futuros; y no refleja un consumo específicamente. Por tanto, es normal evidenciar una memoria Other alta.

CONFIDENCIAL

- ✓ En general los valores reflejados sobre el HOST/Chasis, son normales y muestran un consumo de recursos bajo.

Análisis de Plataforma – Guests (Virtual Edition LTM)

Análisis de Plataforma – Cluster Producción – Guest Virtual 1

Hostname

f5prod1.supersociedades.gov.co

Modelo y Estatus

System

Hostname	f5prod1.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-ynfv-fjxk
Blade S/N	[No data available]
Status	FAILOVER active for about 17 hours, 40 minutes
Uptime	19 hours, 3 minutes
Load Average	1.23, 0.55, 0.31
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 13 - Información General de f5prod1.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Nominal
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 14 - Licenciamiento y Aprovisionamiento f5prod1.supersociedades.gov.co

Performance – Consumo de CPU

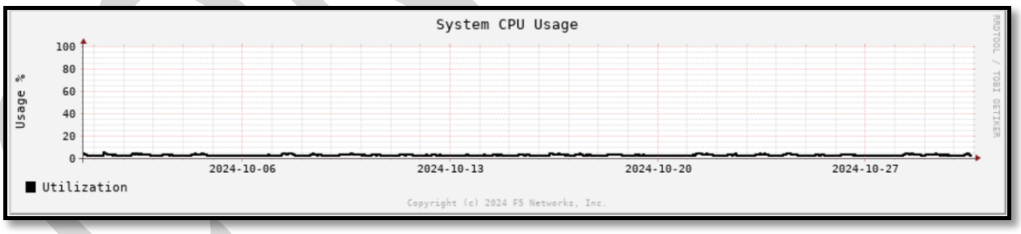


Figura No. 15 - Consumo CPU por Core f5prod1.supersociedades.gov.co (Producción) últimos 30 días

CONFIDENCIAL

Performance – Consumo de Memoria

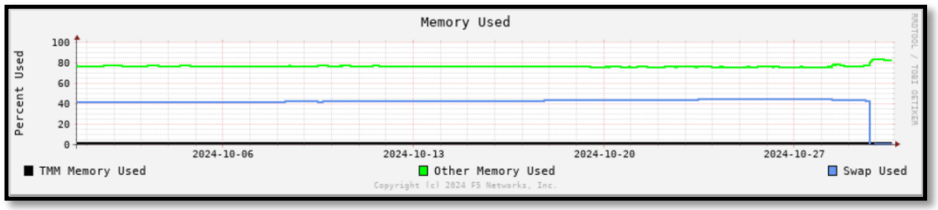


Figura No. 16 – Distribución de Consumo Memoria f5prod1.supersociedades.gov.co (Producción) últimos 30

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Performance – Conexiones Concurrentes

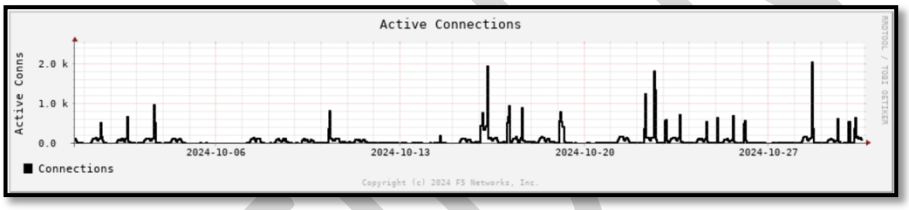


Figura No. 17 – Conexiones Activas f5prod1.supersociedades.gov.co (Producción) últimos 30 días – Equipo

Performance – Throughput

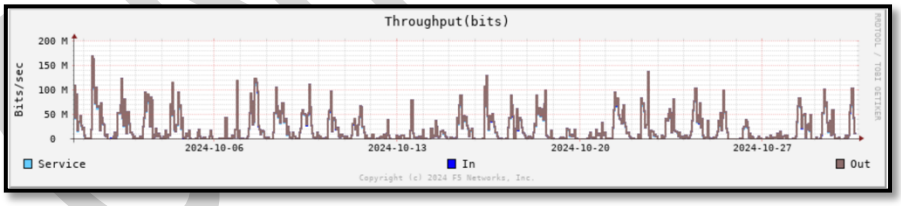


Figura No. 18 – Throughput f5prod1.supersociedades.gov.co (Producción) últimos 30 días – Equipo Standby

CONFIDENCIAL

Performance – TPS SSL

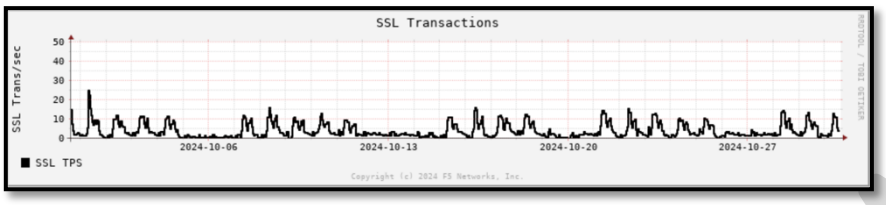


Figura No. 19 – Transacciones SSL f5prod1.supersociedades.gov.co (Producción) últimos 30 días – Equipo Standby

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico
f5prod1.supersociedades.gov.co	4%	0%	80%	15%	22

- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.
- ✓ A pesar de que es el equipo Activo del Cluster, el % de Consumo de MemoriaTMM es 0%.
- ✓ Las conexiones concurrentes en 2000 (valor pico), de un total de 40Mpermitido por un BIG-IP i5800, es un valor nulo/despreciable.
- ✓ El Ancho de Banda (Throughput) no es constante, pero ha llegado a ascender a un valor de 170Mbps en el último mes, de un total de 35Gbps soportado por este chasis, lo cual muestra que es un consumo mucho menor al soportado.

CONFIDENCIAL

Análisis de Plataforma – Cluster Producción – Guest Virtual 2

Hostname

f5prod2.supersociedades.gov.co

Modelo y Estado

System

Hostname	f5prod2.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-mwpr-whrb
Blade S/N	[No data available]
Status	FAILOVER standby for about 17 hours, 45 minutes
Uptime	20 hours, 48 minutes
Load Average	1.14, 0.42, 0.29
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 20 - Información General de f5prod2.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Nominal
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 21 - Licenciamiento y Aprovisionamiento f5prod2.supersociedades.gov.co

Performance – Consumo de CPU

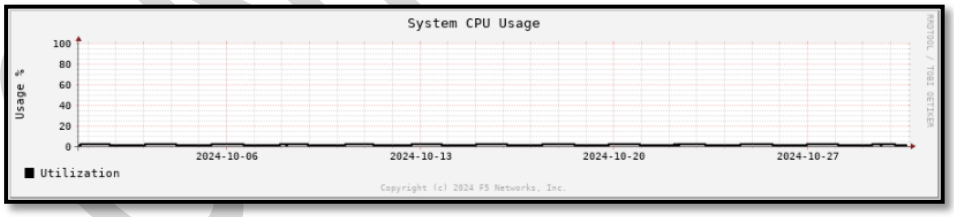


Figura No. 22 - Consumo CPU por Core f5prod2.supersociedades.gov.co (Producción) últimos 30 días

Performance – Consumo de Memoria

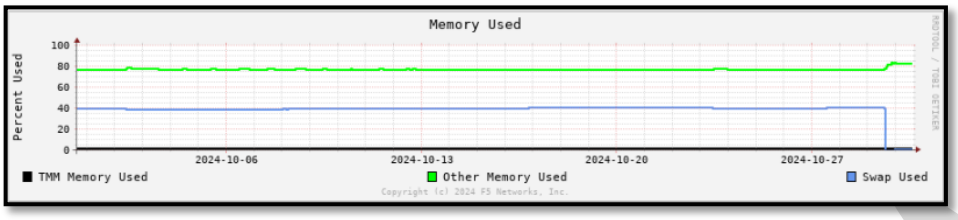


Figura No. 23 – Distribución de Consumo Memoria f5prod2.supersociedades.gov.co (Producción) últimos 30

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Performance – Conexiones Concurrentes

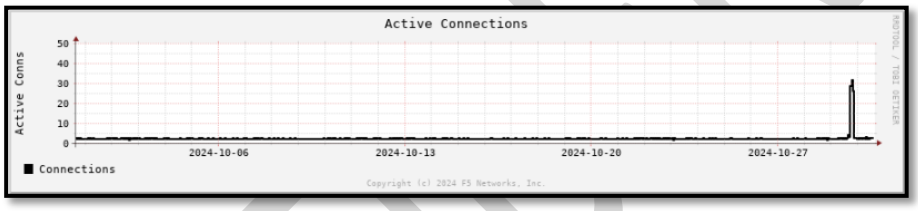


Figura No. 24 – Conexiones Activas f5prod2.supersociedades.gov.co (Producción) últimos 30 días – Equipo Standby

Performance – Throughput

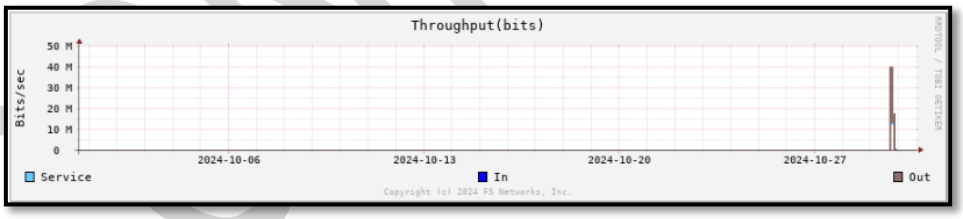


Figura No. 25 – Throughput f5prod2.supersociedades.gov.co (Producción) últimos 30 días – Equipo Standby

CONFIDENCIAL

Performance – TPS SSL

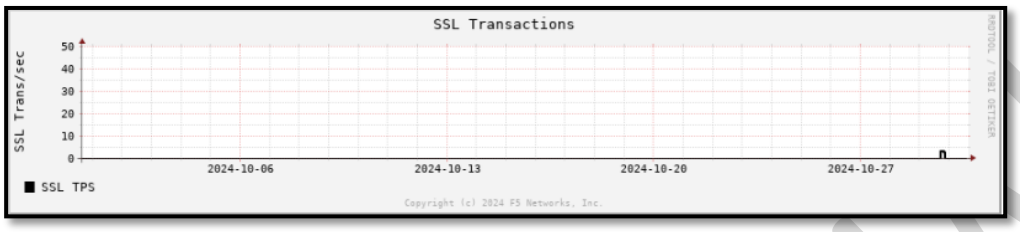


Figura No. 26 – Transacciones SSL f5prod2.supersociedades.gov.co (Producción) últimos 30 días – Equipo Standby

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico	SSL pico
f5prod2.supersociedades.gov.co	4%	0%	85%	40%	33	4

- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.
- ✓ Al ser el equipo Standby, el % de Memoria TMM es 0%.
- ✓ La memoria SWAP se ve un valor del 40% una vez se realizo el failover para la actualización del software.
- ✓ El promedio de conexiones de la mayor parte del mes fueron 3 mínimas, sin embargo, se observa un pico de 33 conexiones.

CONFIDENCIAL

Análisis de Plataforma – Cluster DMZ – Guest Virtual 1

Hostname

f5dmz1.supersociedades.gov.co

Modelo y Estatus

System	
Hostname	f5dmz1.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-ynfv-fjxk
Blade S/N	[No data available]
Status	FAILOVER active for about 17 hours, 38 minutes
Uptime	18 hours, 21 minutes
Load Average	0.80, 0.34, 0.27
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 27 - Información General de f5dmz1.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Nominal
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 28 - Licenciamiento y Aprovisionamiento f5dmz1.supersociedades.gov.co

Performance – Consumo de CPU

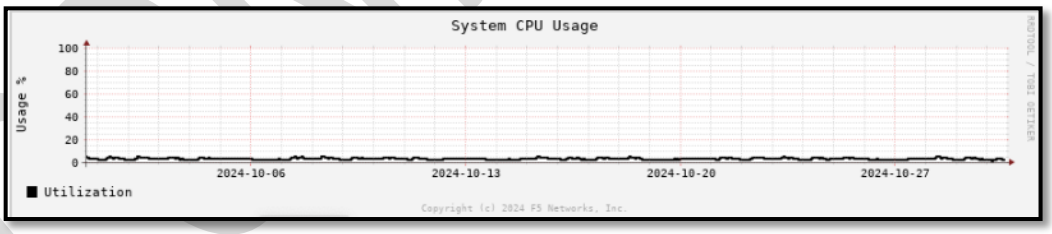


Figura No. 29 - Consumo CPU por Core f5dmz1.supersociedades.gov.co (DMZ) últimos 30 días

CONFIDENCIAL

Performance – Consumo de Memoria

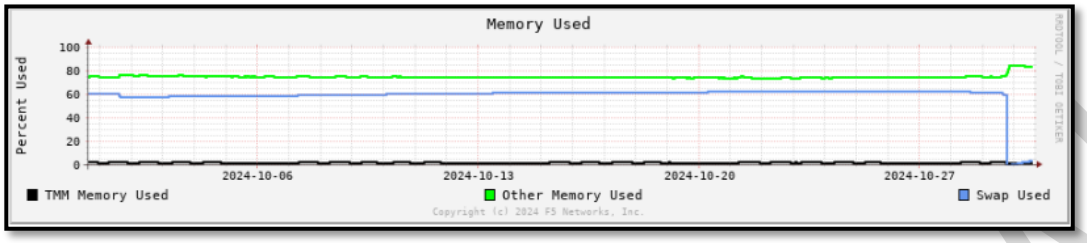


Figura No. 30 – Distribución de Consumo Memoria f5dmz1.supersociedades.gov.co (DMZ) últimos 30

Performance – Consumo de Memoria

Performance – Throughput

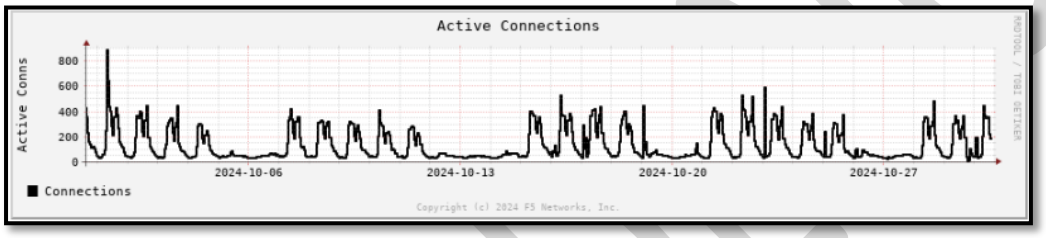


Figura No. 31 – Conexiones Activas f5dmz1.supersociedades.gov.co (DMZ) últimos 30 días – Equipo Activo

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Performance – Conexiones Concurrentes

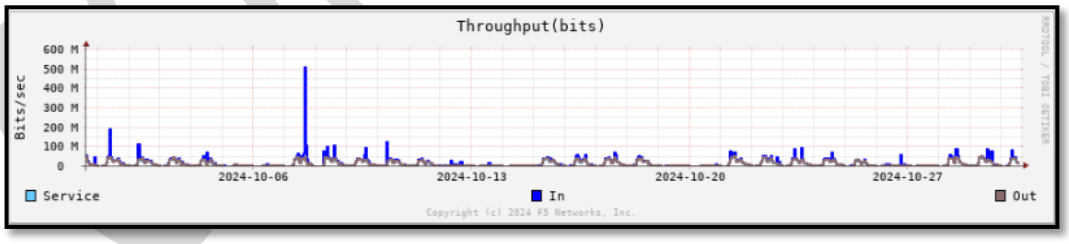


Figura No. 32 – Throughput f5dmz1.supersociedades.gov.co (DMZ) últimos 30 días – Equipo Activo

CONFIDENCIAL

Performance – TPS SSL

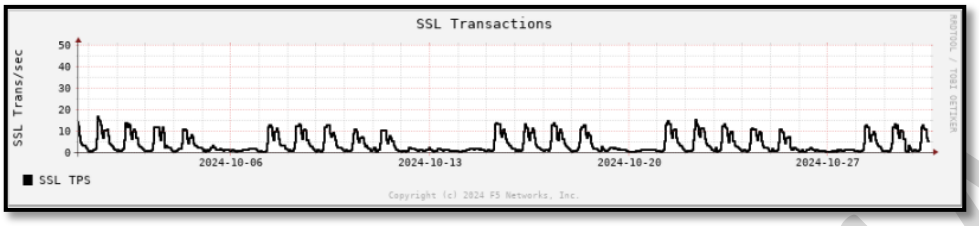


Figura No. 33 – Transacciones SSL f5dmz1.supersociedades.gov.co (DMZ) últimos 30 días – Equipo Activo

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico
f5dmz1.supersociedades.gov.co	4%	1%	85%	60%	850

- ✓ A pesar de que es el equipo Activo del Cluster, el % de Consumo de Memoria TMM es muy bajo (1%).
- ✓ Las conexiones concurrentes en 850 (valor pico), de un total de 40M permitido por un BIG-IP i5800, es un valor considerablemente bajo respecto de las capacidades totales del BIG-IP i5800.
- ✓ El Ancho de Banda (Throughput) no es constante, pero ha llegado a ascender a un valor de 510Mbps en el último mes, de un total de 35Gbps soportado por este chasis, lo cual muestra que es un consumo mucho menor al soportado.
- ✓ Este cluster maneja tráfico cifrado SSL, sin embargo, el valor de transacciones concurrentes SSL pico de 18 (TPS), es un valor mucho menor al máximo soportado por el equipo que es de 20K TPS.

CONFIDENCIAL

Análisis de Plataforma – Cluster DMZ – Guest Virtual 2

Hostname

f5dmz2.supersociedades.gov.co

Modelo y Estatus

System

Hostname	f5dmz2.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-mwpr-whrb
Blade S/N	[No data available]
Status	FAILOVER standby for about 17 hours, 43 minutes
Uptime	21 hours, 26 minutes
Load Average	0.88, 0.49, 0.34
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 34 - Información General de f5dmz2.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Nominal
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 35 - Licenciamiento y Aprovisionamiento f5dmz2.supersociedades.gov.co

Performance – Consumo de CPU

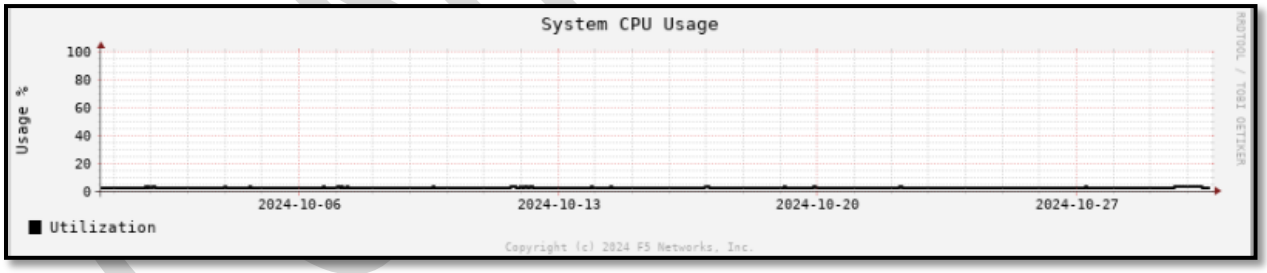


Figura No. 36 - Consumo CPU por Core f5dmz2.supersociedades.gov.co (DMZ) últimos 30 días

CONFIDENCIAL

Performance – Consumo de Memoria

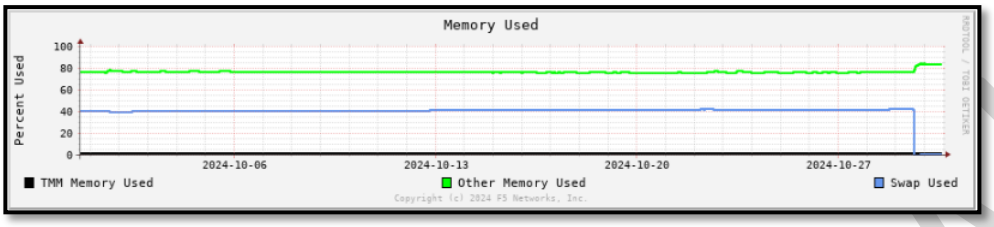


Figura No. 37 – Distribución de Consumo Memoria f5dmz2.supersociedades.gov.co (DMZ) últimos 30 días

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Performance – Conexiones Concurrentes

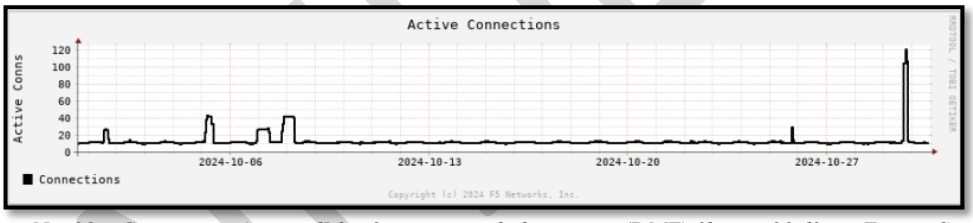


Figura No. 38 – Conexiones Activas f5dmz2.supersociedades.gov.co (DMZ) últimos 30 días – Equipo Standby

Performance – Throughput

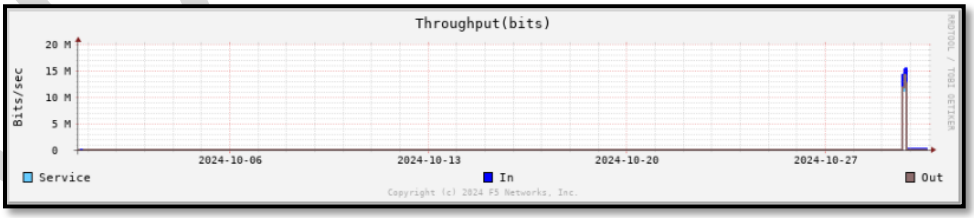


Figura No. 39 – Throughput f5dmz2.supersociedades.gov.co (DMZ) últimos 30 días – Equipo Standby

CONFIDENCIAL

Performance – TPS SSL

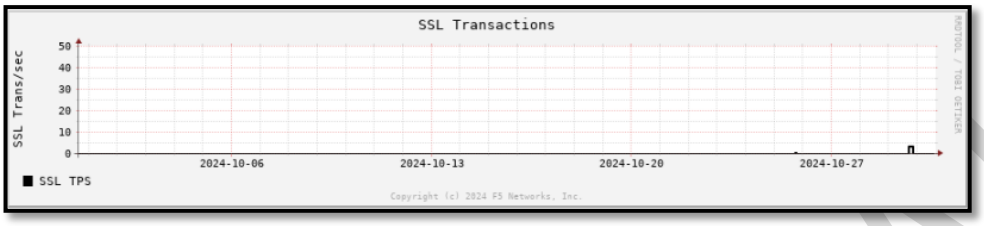


Figura No. 40 – Transacciones SSL f5dmz2.supersociedades.gov.co (DMZ) últimos 30 días – Equipo Standby

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico	SSL Pico
f5dmz2.supersociedades.gov.co	2%	2%	85%	42%	120	4

- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.
- ✓ Al ser el equipo Standby, el % de Memoria TMM es 2%.
- ✓ La memoria SWAP se ve del 42%, pero se entiende como un comportamiento habitual.
- ✓ El promedio de conexiones de la mayor parte del mes fueron 15 mínimas, sin embargo, se observa un pico de 120 conexiones.
- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.

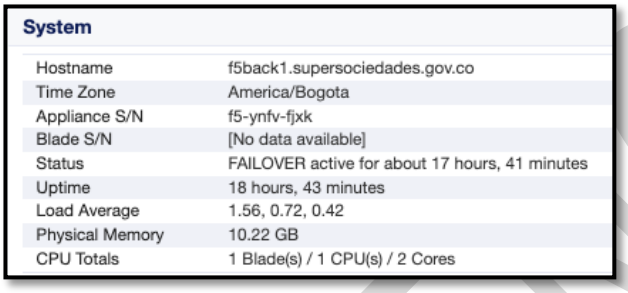
CONFIDENCIAL

Análisis de Plataforma – Cluster BackEnd – Guest Virtual 1

Hostname

f5back1.supersociedades.gov.co

Modelo y Estatus



System	
Hostname	f5back1.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-ynfv-fjxk
Blade S/N	[No data available]
Status	FAILOVER active for about 17 hours, 41 minutes
Uptime	18 hours, 43 minutes
Load Average	1.56, 0.72, 0.42
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 41 - Información General de f5back1.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Minimum
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 42 - Licenciamiento y Aprovisionamiento f5back1.supersociedades.gov.co

Performance – Consumo de CPU

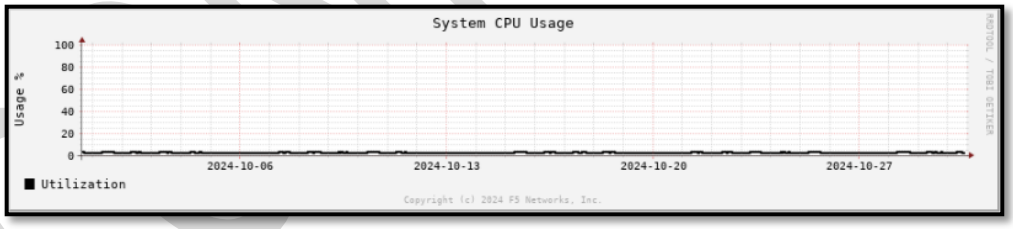


Figura No. 43 - Consumo CPU por Core f5back1.supersociedades.gov.co (BackEnd) últimos 30 días

Performance – Consumo de Memoria

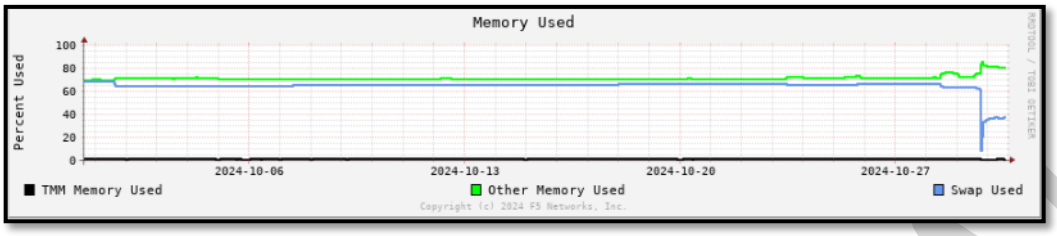


Figura No. 44 – Distribución de Consumo Memoria f5back1.supersociedades.gov.co (BackEnd) últimos 30

Performance – Conexiones Concurrentes

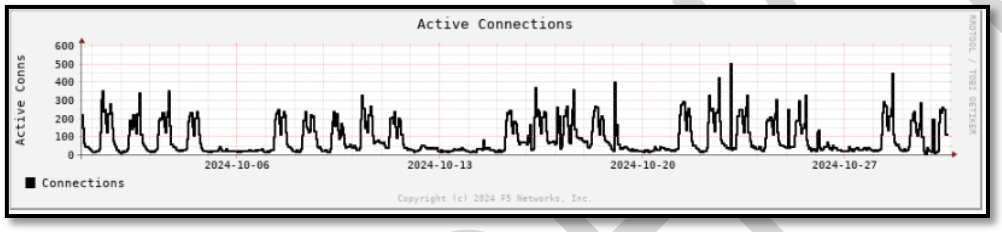


Figura No. 45 – Conexiones Activas f5back1.supersociedades.gov.co (BackEnd) últimos 30 días – Equipo Activo

Performance – Throughput

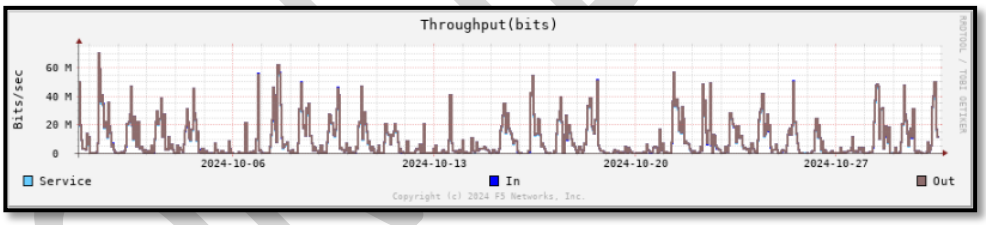


Figura No. 46 – Throughput f5back1.supersociedades.gov.co (BackEnd) últimos 30 días – Equipo Activo

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

CONFIDENCIAL

Performance – TPS SSL

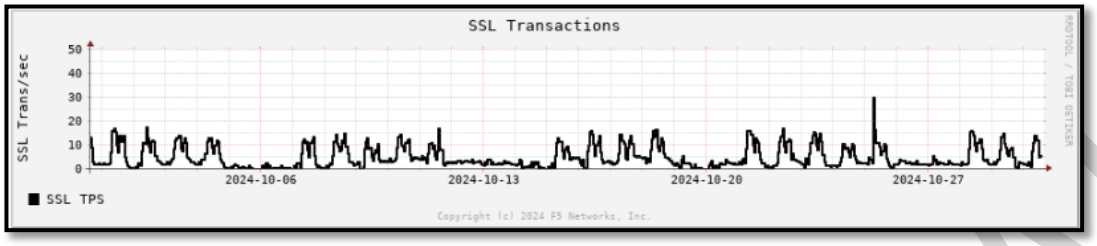


Figura No. 47 – Transacciones SSL f5back1.supersociedades.gov.co (BackEnd) últimos 30 días – Equipo Standby

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico
f5back1.supersociedades.gov.co	3%	2%	85%	65%	500

- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.
- ✓ A pesar de que el equipo Activo del Cluster, el % de Consumo de Memoria TMM es muy bajo (2%).
- ✓ Las conexiones concurrentes en 500 (valor pico), de un total de 40M permitido por un BIG-IP i5800, es un valor considerablemente bajo respecto de las capacidades totales del BIG-IP i5800.
- ✓ El Ancho de Banda (Throughput) no es constante, pero ha llegado a ascender a un valor de 70Mbps en el último mes, de un total de 35Gbps soportado por este chasis, lo cual muestra que es un consumo mucho menor al soportado.

CONFIDENCIAL

Análisis de Plataforma – Cluster BackEnd – Guest Virtual 2

Hostname

f5back2.supersociedades.gov.co

Modelo y Estatus

System	
Hostname	f5back2.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-mwpr-whrb
Blade S/N	[No data available]
Status	FAILOVER standby for about 17 hours, 52 minutes
Uptime	21 hours, 54 minutes
Load Average	0.30, 0.69, 0.52
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 48 - Información General de f5back2.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Minimum
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 49 - Licenciamiento y Aprovisionamiento f5back2.supersociedades.gov.co

Performance – Consumo de CPU

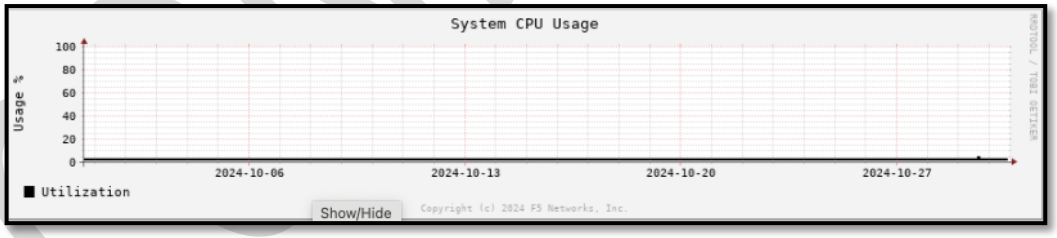


Figura No. 50 - Consumo CPU por Core f5back2.supersociedades.gov.co (BackEnd) últimos 30 días

Performance – Consumo de Memoria

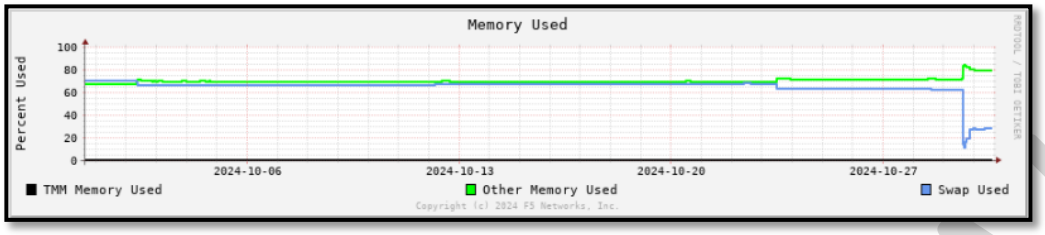


Figura No. 51 – Distribución de Consumo Memoria f5back2.supersociedades.gov.co (BackEnd) últimos 30

Performance – Conexiones Concurrentes

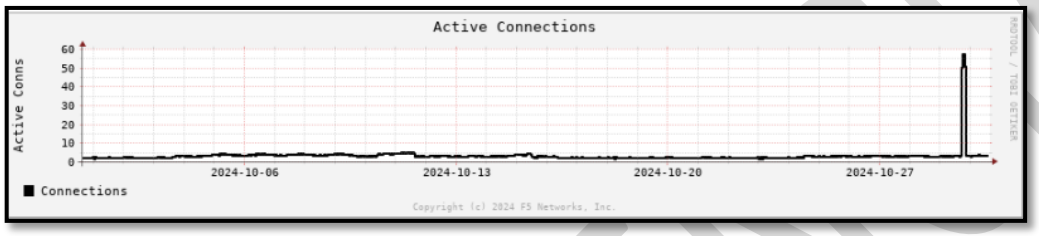


Figura No. 52 – Conexiones Activas f5back2.supersociedades.gov.co (BackEnd) últimos 30 días – Equipo Standby

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Performance – Throughput

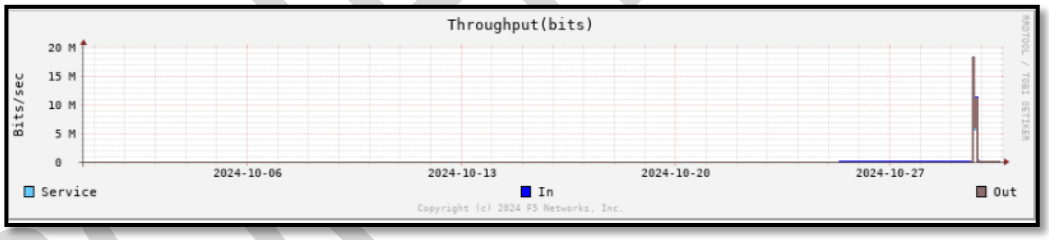


Figura No. 53 – Throughput f5back2.supersociedades.gov.co (BackEnd) últimos 30 días – Equipo Standby

CONFIDENCIAL

Performance – TPS SSL

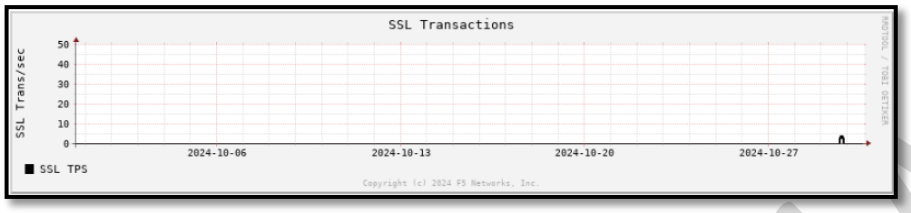


Figura No. 54 – Transacciones SSL f5back2.supersociedades.gov.co (BackEnd) últimos 30 días – Equipo Activo

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico
f5back2.supersociedades.gov.co	2%	1%	85%	65%	57

- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.
- ✓ Al ser el equipo Standby, el % de Memoria TMM es 1%.
- ✓ Las conexiones, al ser un equipo Standby son mínimas y se pueden entender como un valor despreciable.

CONFIDENCIAL

Análisis de Plataforma – Cluster Pruebas – Guest Virtual 1

Hostname

f5pru1.supersociedades.gov.co

Modelo y Estatus

System	
Hostname	f5pru1.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-ynfv-fjxk
Blade S/N	[No data available]
Status	FAILOVER active for about 17 hours, 41 minutes
Uptime	18 hours, 3 minutes
Load Average	0.97, 0.52, 0.35
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 55 - Información General de f5pru1.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Minimum
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 56 - Licenciamiento y Aprovisionamiento f5pru1.supersociedades.gov.co

Performance – Consumo de CPU

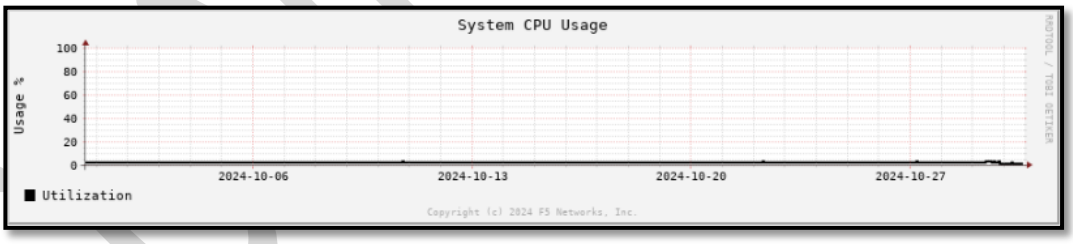


Figura No. 57 - Consumo CPU por Core f5pru1.supersociedades.gov.co (Pruebas) últimos 30 días

CONFIDENCIAL

Performance – Consumo de Memoria

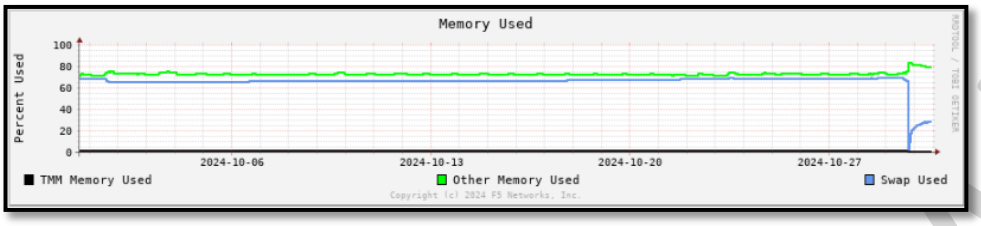


Figura No. 58 – Distribución de Consumo Memoria f5pru1.supersociedades.gov.co (Pruebas) últimos 30 días

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Performance – Conexiones Concurrentes

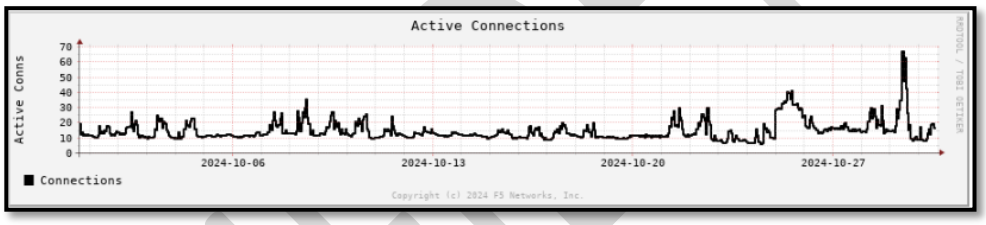


Figura No. 59 – Conexiones Activas f5pru1.supersociedades.gov.co (Pruebas) últimos 30 días – Equipo Activo

Performance – Throughput

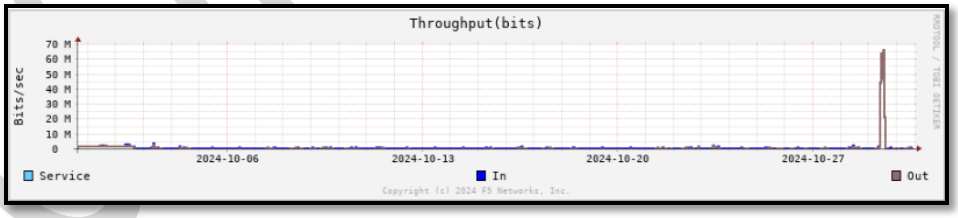


Figura No. 60 – Throughput f5pru1.supersociedades.gov.co (Pruebas) últimos 30 días – Equipo Standby

CONFIDENCIAL

Performance – TPS SSL

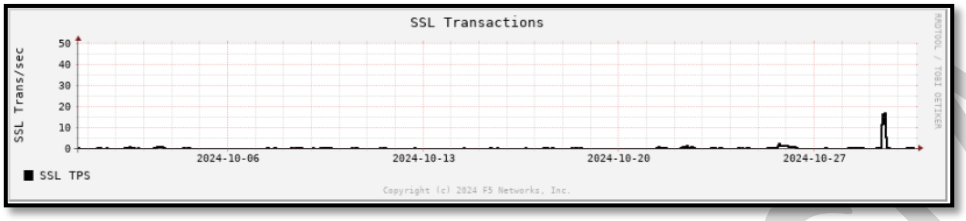


Figura No. 61 - Transacciones SSL f5pru1.supersociedades.gov.co (Pruebas) últimos 30 días – Equipo Standby

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico
f5pru1.supersociedades.gov.co	2%	1%	85%	65%	68

- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.
- ✓ A pesar que es el equipo Activo del Cluster, el % de Consumo de Memoria TMM es muy bajo (2%).
- ✓ Las conexiones concurrentes en 68 (valor pico), de un total de 40M permitido por un BIG-IP i5800, es un valor considerablemente bajo respecto de las capacidades totales del BIG-IP i5800.
- ✓ El Ancho de Banda (Throughput) no es constante, pero ha llegado a ascender a un valor de 65Mbps en el último mes, de un total de 35Gbps soportado por este chasis, lo cual muestra que es un consumo mucho menor al soportado.

CONFIDENCIAL

Análisis de Plataforma – Cluster Pruebas – Guest Virtual 2

Hostname

f5pru2.supersociedades.gov.co

Modelo y Estatus

System	
Hostname	f5pru2.supersociedades.gov.co
Time Zone	America/Bogota
Appliance S/N	f5-mwpr-whrb
Blade S/N	[No data available]
Status	FAILOVER standby for about 17 hours, 45 minutes
Uptime	21 hours, 8 minutes
Load Average	1.07, 0.45, 0.28
Physical Memory	10.22 GB
CPU Totals	1 Blade(s) / 1 CPU(s) / 2 Cores

Figura No. 62 - Información General de f5pru2.supersociedades.gov.co

CONFIDENCIAL

Licenciamiento y Aprovisionamiento

Licensing and Provisioning

Module / Feature	Licensed	Provisioned
Advanced Firewall (AFM)		
Application Acceleration Manager (AAM)		
Access Policy (APM)	X	
Access Policy Lite (APML)	X	
Application Security (ASM)		
Application Visibility and Reporting (AVR)	X	Minimum
Carrier Grade NAT (CGNAT)		
DDOS Protection (DOS)		
Enterprise Manager (EM)		
Fraud Protection Service (FPS)		
Global Traffic (DNS)		
iRules Language Extensions (iRulesLX)	X	
Link Controller (LC)		
Local Traffic (LTM)	X	Nominal
Policy Enforcement (PEM)		
SSL Orchestrator (SSLO)		
Secure Web Gateway (SWG)		
Traffic Accelerator Module (TAM)	X	
URLDB Minimal (URLDB)		
Virtual CMP (vCMP)	X	

Figura No. 63 - Licenciamiento y Aprovisionamiento f5pru2.supersociedades.gov.co

Performance – Consumo de CPU

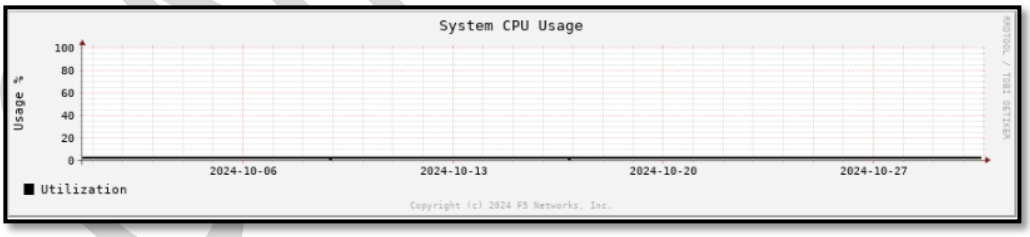


Figura No. 64 - Consumo CPU por Core f5pru2.supersociedades.gov.co (Pruebas) últimos 30 días

Performance – Consumo de Memoria

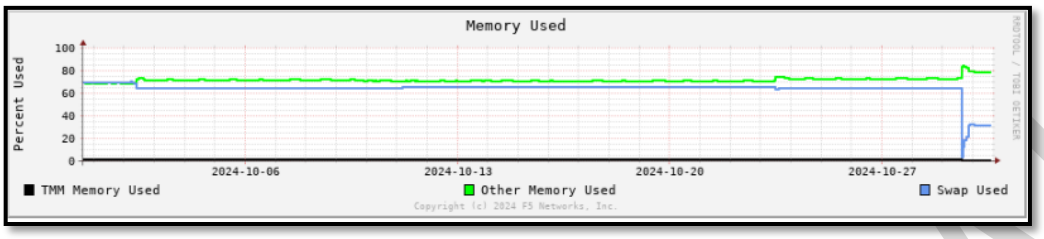


Figura No. 65 – Distribución de Consumo Memoria f5pru2.supersociedades.gov.co (Pruebas) últimos 30 días

TMM Memory: Es asignada por F5 para el procesamiento del tráfico balanceado.
Other Memory: Es la memoria asignada al HOST (Base Linux).
Swap Memory: espacio del disco utilizado como memoria, esta resulta dañina cuando sube demasiado.

Performance – Conexiones Concurrentes

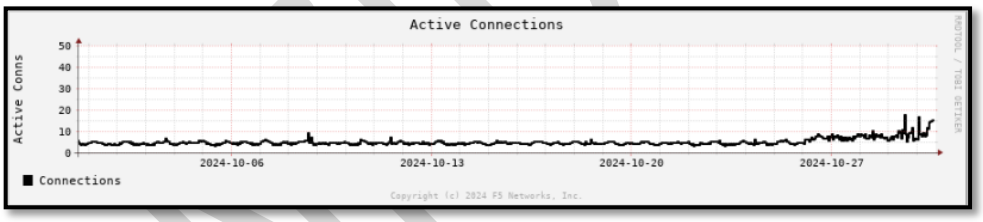


Figura No. 66 – Conexiones Activas f5pru2.supersociedades.gov.co (Pruebas) últimos 30 días – Equipo Standby

Performance – Throughput

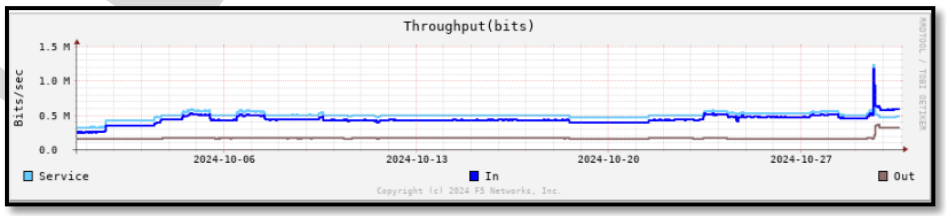


Figura No. 67 – Throughput f5pru2.supersociedades.gov.co (Pruebas) últimos 30 días – Equipo Standby

CONFIDENCIAL

Performance – TPS SSL

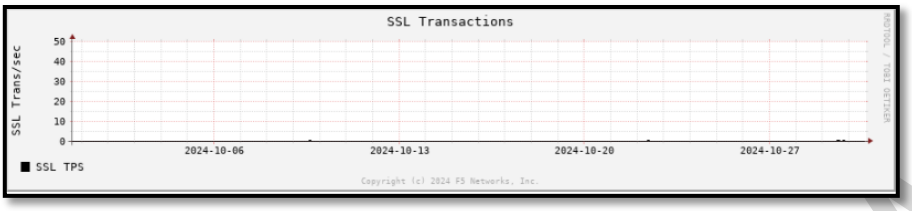


Figura No. 68 - Transacciones SSL f5pru2.supersociedades.gov.co (Pruebas) últimos 30 días – Equipo Standby

Tabla Resumen de Consumo de Recursos

Hostname	CPU pico (%)	TMM pico (%)	Other pico (%)	Swap pico (%)	Conexiones pico	SSL Pico
f5pru2.supersociedades.gov.co	2%	2%	85%	70%	18	1

- ✓ En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por En los vCMP Guest (Equipos Virtuales), el % de recursos de cómputo por Other Memory, refleja la memoria reservada para ser usada por el Base Linux, lo cual es normal ver un consumo alto.
- ✓ Al ser el equipo Standby, el % de Memoria TMM es 2%.
- ✓ Las conexiones, al ser un equipo Standby son mínimas y se pueden entender como un valor despreciable.

CONFIDENCIAL

Seguimiento a Objetos Configurados

A continuación, el seguimiento a Objetos de Tráfico configurados de todos los Clusters mencionados anteriormente.

Local Traffic Summary

Object Type	Total	Available	Unavailable	Offline	Unknown
Virtual Servers	14	9	0	4	1
Pools	20	14	0	6	0
Nodes	32	0	0	0	32

Figura No. 69 - Local Traffic Summary – Cluster - f5prod1.supersociedades.gov.co(Activo) - f5prod2.supersociedades.gov.co(Standby)

Local Traffic Summary

Object Type	Total	Available	Unavailable	Offline	Unknown
Virtual Servers	73	35	0	12 (3 Disabled)	23
Pools	85	70	0	15	0
Nodes	69	0	0	0	69

Figura No. 70 - Local Traffic Summary – Cluster DMZ - f5dmz1.supersociedades.gov.co(Activo) - f5dmz2.supersociedades.gov.co(Standby)

Local Traffic Summary

Object Type	Total	Available	Unavailable	Offline	Unknown
Virtual Servers	25	19	0	3	2 (1 Disabled)
Pools	23	17	0	6	0
Nodes	28	0	0	0	28

Figura No. 71 - Local Traffic Summary – Cluster - f5back1.supersociedades.gov.coBackEnd(Activo) - f5back2.supersociedades.gov.co(Standby)

Local Traffic Summary

Object Type	Total	Available	Unavailable	Offline	Unknown
Virtual Servers	64	54	0	3 (1 Disabled)	6
Pools	145	125	0	16	4
Nodes	61	0	0	0	61

Figura No. 72 - Local Traffic Summary – Cluster Pruebas - f5pru1.supersociedades.gov.co(Activo)- f5pru2.supersociedades.gov.co(Standby)

CONFIDENCIAL

Seguimiento sincronización de equipos

A continuación, se muestran los clusters sincronizados

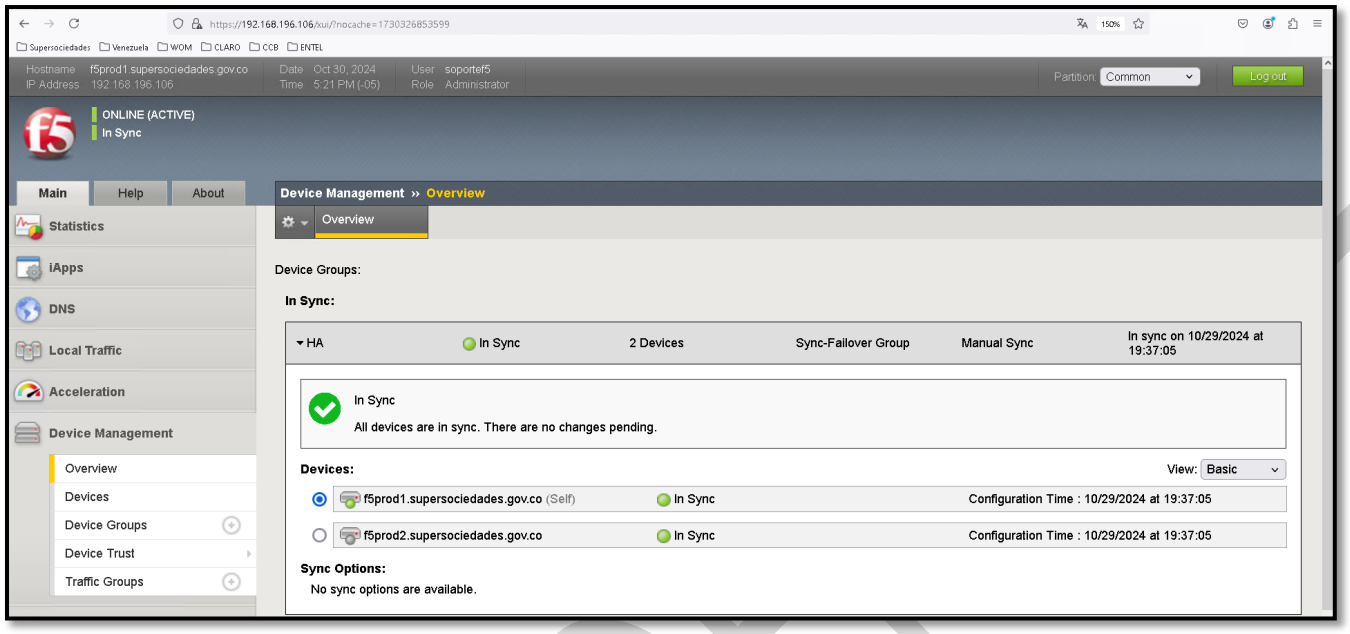


Figura No. 73 - Local Traffic Summary – Cluster - f5prod1.supersociedades.gov.co(Activo) - f5prod2.supersociedades.gov.co(Standby)

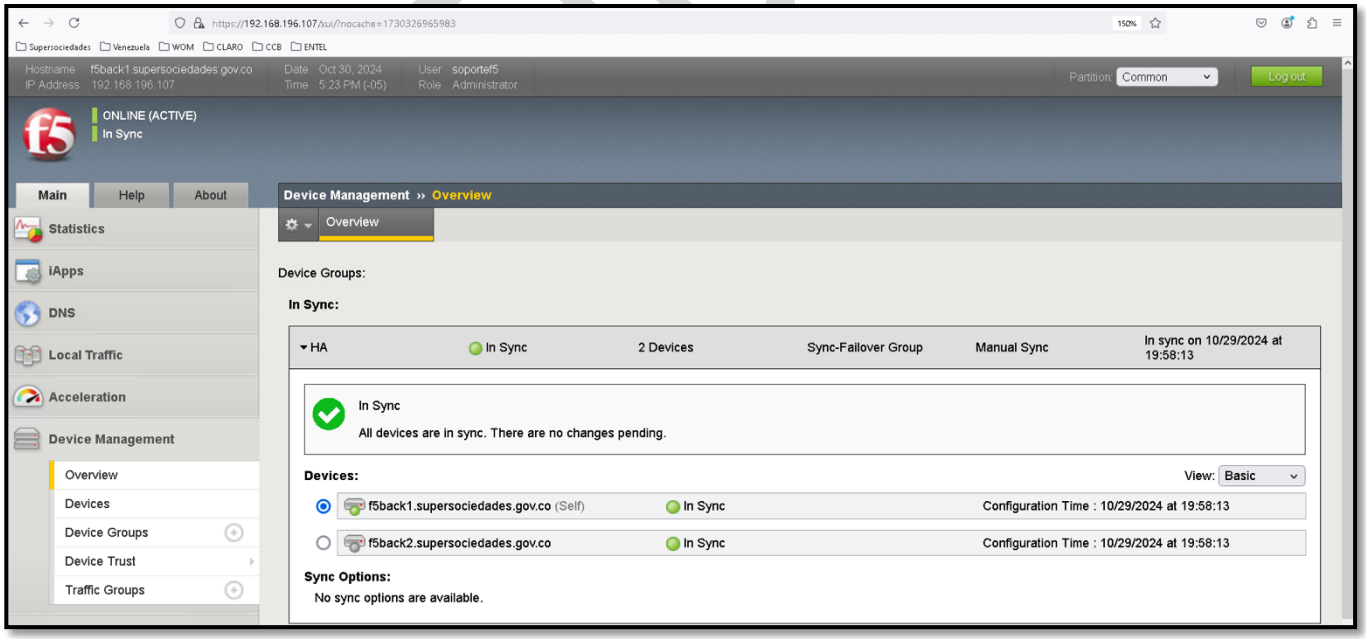


Figura No. 74 - Local Traffic Summary – Cluster - f5back1.supersociedades.gov.coBackEnd(Activo) - f5back2.supersociedades.gov.co(Standby)

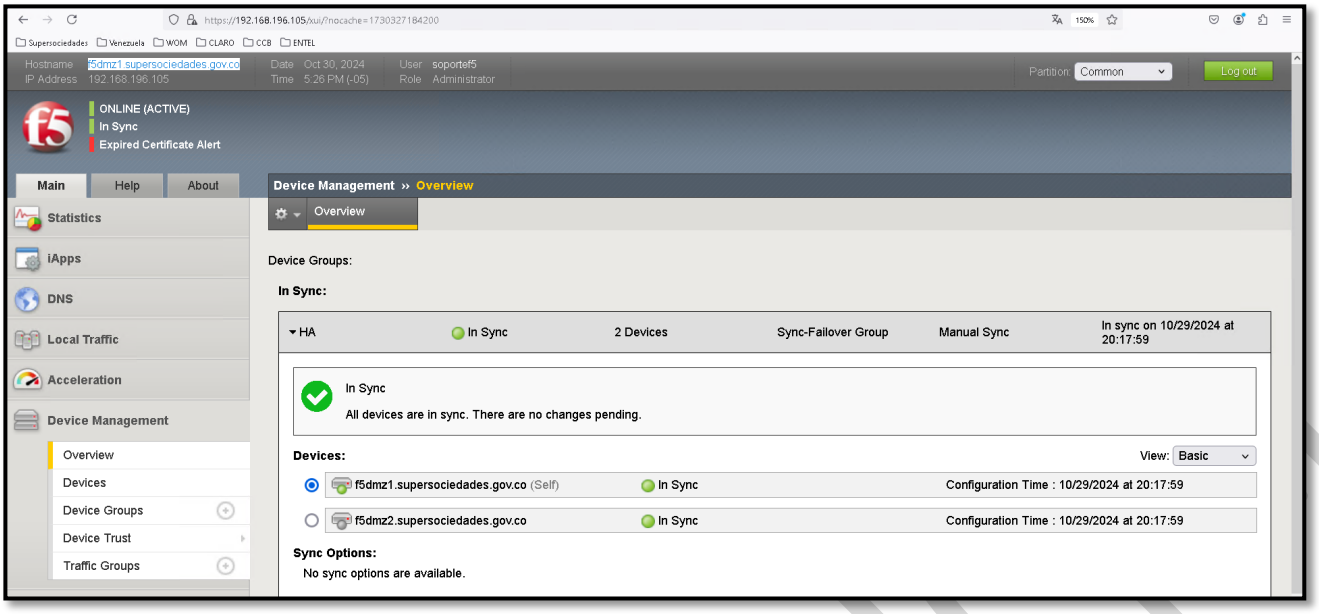


Figura No. 75 - Local Traffic Summary – Cluster DMZ - f5dmz1.supersociedades.gov.co(Activo) - f5dmz2.supersociedades.gov.co(Standby)

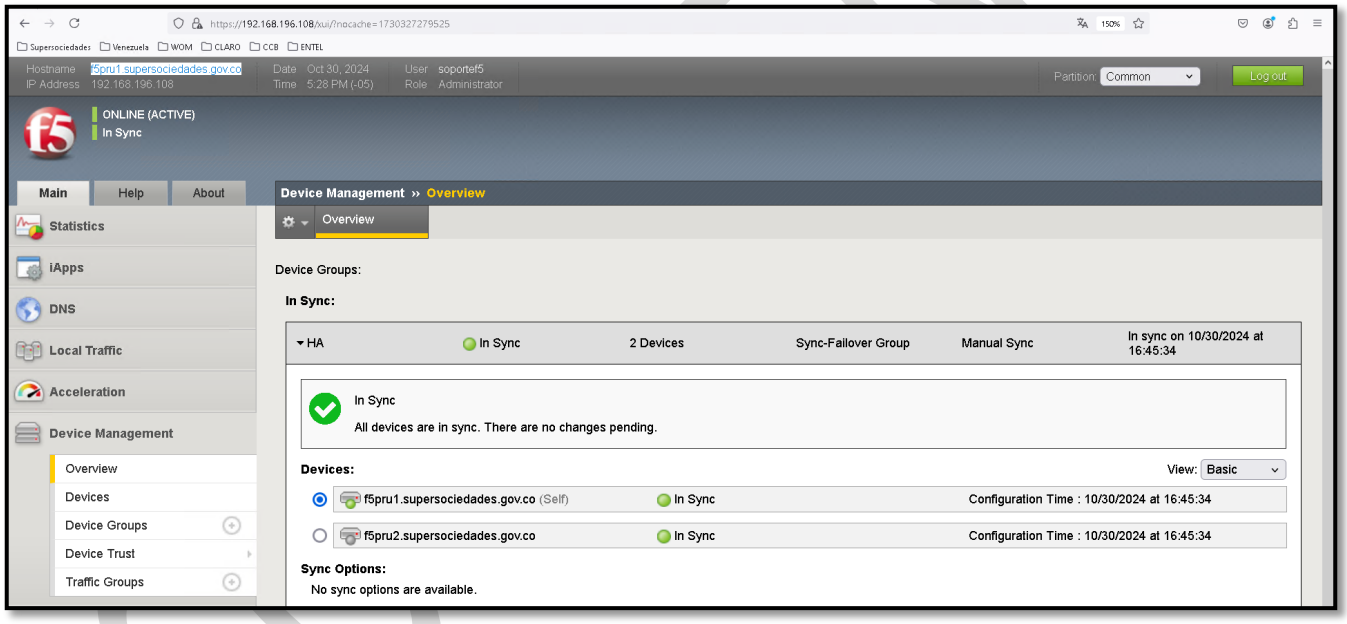


Figura No. 76 - Local Traffic Summary – Cluster Pruebas - f5pru1.supersociedades.gov.co(Activo)- f5pru2.supersociedades.gov.co(Standby)

Análisis de Vulnerabilidades

Categorización	Heuristic	Titulo	Descripción	Versión de Mitigación (Si aplica) o Recomendación
High	D000140061	BIG-IP monitors vulnerability	BIG-IP monitor functionality may allow an authenticated attacker with at least Manager role privileges to elevate their privileges and/or modify the configuration.	15.1.10.5, 16.1.5, 17.1.1.4
High	H487997	A modified default profile has been detected.	F5 recommends that you do not modify the default profiles unless directed to do so by an F5 Support employee, or as a result of installing a hotfix or an upgrade. The default profile types contain a recommended baseline from which an implementation starts. If you change the default profile values, the baseline settings may be difficult to recover.	None
Medium	D000137795	Potential Bug with Pools / Monitoring	After a pool member is forced offline on an active unit, a config sync is performed, and the pool member re-enabled on the active unit, the same pool member remains down on the standby unit.	None

CONFIDENCIAL

Categorización	Heuristic	Titulo	Descripción	Versión de Mitigación (Si aplica) o Recomendación
Medium	D014784	BIG-IP Cookie Persistence Encryption not enabled	This system uses cookie persistence profile without encryption. We recommend enabling encryption for improved security.	None
Medium	H647564	Required IP addresses for ConfigSync and device service clustering	For configuration synchronization (ConfigSync) and device service clustering (DSC) to function properly, you must have the ConfigSync IP and failover IPs properly configured. Self IP addresses for ConfigSync and failover must be defined and routable between device group members. To ensure the most stable network failover configuration for redundant systems, choose two channels for network failover communication. F5 considers it best practice to define two unicast addresses or a unicast and a multicast failover address for each device in the device group.	None

Tabla No. 2 - Vulnerabilidades Identificadas en el Cluster de Producción, de DMZ y de Pruebas

CONFIDENCIAL

Incidentes y solicitudes atendidas

El soporte inicio el 16 septiembre, actualmente no tenemos incumplimiento de SLAS a la fecha no se han presentado incidentes.

INC-3026
Supersociedades
Acompañamiento ejecución cambio RFC que incluye actividades en F5
Estado: Closed
1h
18-sept
Validación temas IPV6

INC-3080
Supersociedades
Asistencia configuración F5 aplicación Storm
Estado: Closed
2h
1-oct
Validación Assessment

INC-3189
Supersociedades
IPV6 para aplicativos y servicios Internet
Estado: Closed
1h
21-oct
Validación sesión.

INC-3054
Supersociedades
Aprobación comite de cambios RFC
Ejecucion de Assessment
Estado: Resolved
1h
23-oct
Permiso de conectividad, a los F5 vpn

INC-3054
Supersociedades
Ejecucion de Assessment
Estado: Resolved
8h
23-oct
Revision RFC de entrega

INC-3054
Supersociedades
Ejecucion de Assessment
Estado: Resolved
1h
30-oct
Re-licenciamiento para actualización del Service Check Date & versión de firmware 17.1.1.X.

INC-3234
Supersociedades
IPv6 - F5
Estado: Resolved
1h
30-oct
Total general: 8

CONFIDENCIAL

Conclusiones & Recomendaciones

Después de realizar el análisis de todos los recursos de la plataforma, se concluye:

Se recomienda actualizar el SO de la plataforma tan pronto el fabricante F5 libere la versión definitiva que contenga la mitigación de la vulnerabilidad critica BIG-IP monitors vulnerability CVE-2024-45844

Se recomienda no modificar los perfiles por defecto que tienen los equipos F5. Se recomienda crear perfiles heredados y sobre eso realizar los cambios y las customizaciones específicas.

A nivel del comportamiento de los equipos y sus recursos, estos presentan un comportamiento y consumo adecuado.

Se evidencia un tráfico y consumo de recursos de recursos estable, en los últimos días de estos últimos treinta (30) días.

Se evidencia que la los equipos han tenido cambios en sus estadísticas en los últimos 2 días, sin embargo es este comportamiento es normal debido al proceso de actualización realizado el día de ayer 29 de Octubre de 2024.

Se recomienda realizar la depuración de objetos que no se tengan en uso como por ejemplo certificados ssl, perfiles ssl, Virtual Servers, Pool Members, etc.

CONFIDENCIAL