GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

DOCUMENTO DE EJECUCIÓN DE VISITA DE MANTENIMIENTO FORTIGATE 601E

MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

Fecha:

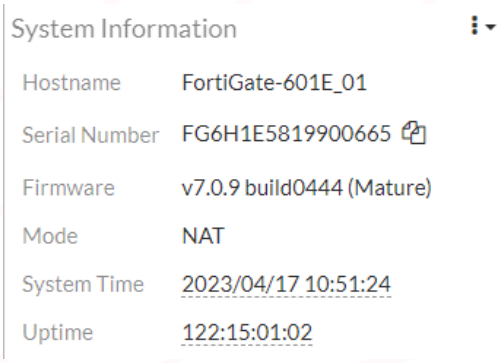
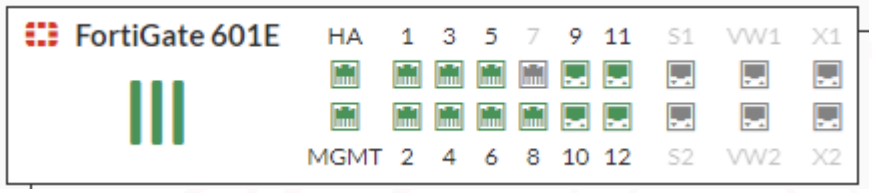
Abril 2023

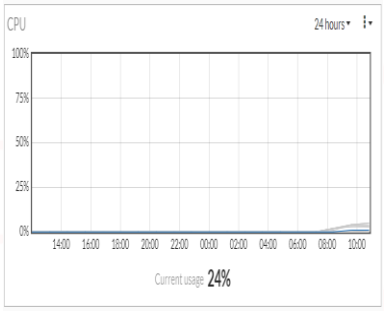
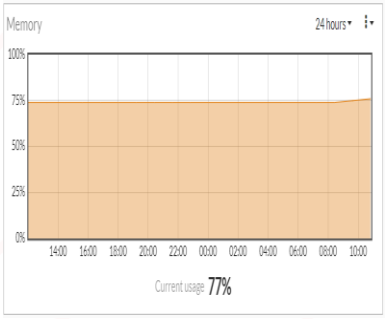
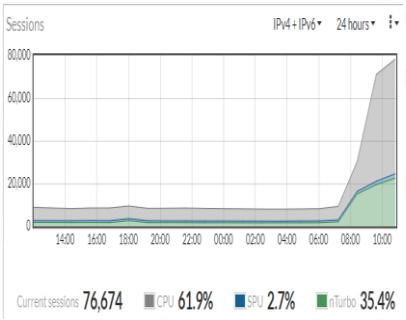
Gamma Ingenieros S.A.
U.E.N. Tecnología

Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147
Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

CLIENTE:	MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

Datos de la visita	
Nombre:	MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL
Contacto:	Oficina TIC- Ministerio de Agricultura y Desarrollo Rural
Correo:	tics@minagricultura.GOV.CO
Fecha:	17/04/2023
Ciudad:	Bogotá
Serial:	FG6H1E5819900665 - FG6H1ETB20907192
Ingeniero encargado:	John Sebastián Beltrán
Contacto:	3182861641

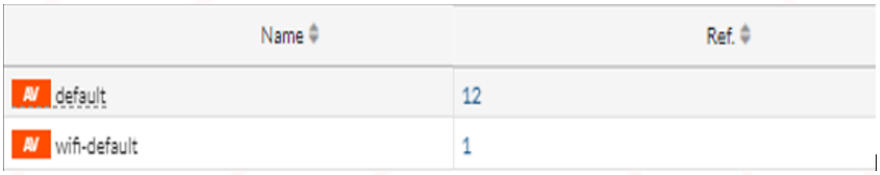
	Información Recolectada	Observaciones
1. Información básica del sistema		
1.1 Nombre del equipo, Versión de firmware, Serial del equipo, Configuración Fecha, hora y zona		
1.2 Referencia del equipo		

1.2 Estado de CPU	La imagen muestra que, durante el período de tiempo analizado, el uso de la CPU se mantuvo en un promedio del 24% Es importante tener en cuenta que el uso de la CPU puede variar dependiendo de muchos factores, como la cantidad de aplicaciones que se están ejecutando simultáneamente, la complejidad de estas aplicaciones y la cantidad de recursos que están disponibles en el sistema.	
1.3 Estado de memoria	La imagen sugiere que, durante el período de tiempo analizado, el uso promedio de la memoria se mantuvo alrededor del 77%. Lo cual nos indica que mantuvo un promedio normal y no alcanzado sus límites. Es importante tener en cuenta que el uso de la memoria puede fluctuar y alcanzar niveles más altos en momentos de alta carga o cuando se ejecutan aplicaciones que requieren una gran cantidad de recursos	
1.4 Total, de sesiones	En la imagen se puede evidenciar que el promedio de sesiones fue de 76,674 lo cual nos indica que hubo un número considerable de sesiones durante el periodo de tiempo analizado	

1.5	Nombre de Host	FortiGate-601E_01	
2. Licenciamiento			
2.1	Estado del licenciamiento	Hasta	Vigente hasta 2024/11/12
3. Interfaces			
3.1	Total de Interfaces en uso	13	HA, mgmt, port1, port2, port3, port4, port5,port6,port8, port9, port10, port11, port12
3.2	Total de Interfaces libres	7	Port7, S1, S2, VW1, VW2, X1, X2
3.3	Total Subinterfaces Vlan	10	• VLAN_INTERNET • VLAN_LACP_INSIDE • VLAN 200 - Mesa_Ayuda • VLAN16 - SEDES • VLAN_BK_NUTANIX • VLAN_SERVER_ANT • VLAN_SEVER_NUE • DMZ_F5-VLAN130 • DMZ_INT-VLAN34
3.4	Prevención de Botnet y C&C en interfaz con rol WAN	Disable	No se encuentra habilitado la característica
4. System DNS			
4.1	DNS Primario	172.20.50.222	
4.2	DNS Secundario	172.20.50.1	
4.3	Dominio local	minagricultura.gov.co	
5. Accesos Administrativos			
5.1	Ping	14	• LACP_INT, • VLAN_INTERNET, • LACP_INSIDE, • VLAN_LACP_INSIDE, • fortilink, • VLAN 200-Mesa_Ayuda, • VLAN16-SEDES, • LACP_SERVIDORES,

			• VLAN_BK_NUTANIX, • VLAN_SERVER_ANT, • VLAN_SEVER_NUE, • DMZ_F5-VLAN130, • DMZ_INT-VLAN34, • Mgmt
5.2	SSH	1	Mgmt
5.3	HTTP	1	Mgmt
5.4	HTTPS	1	Mgmt
5.5	TELNET	N/A	
6. System settings			
6.1	HTTP Port	80	
6.2	HTTPS Port	10443	
6.3	SSH Port	1022	
6.4	Telnet Port	23	
6.5	Redirect to https Option	On	
6.6	Idle Timeout	5	
6.7	Password policy	Admin	
6.8	Lenguage	English	
6.9	Theme	Jade	
6.10	Inspection Mode	N/A	
6.11	Virtual Domains	Off	
7. Conectores Security Fabric			
7.1	Forti Connectors (FSSO ...)	On	
7.2	FortiAnalyzer logging	On	
7.3	FortiAP/Fortiswitch	Off	
7.4	Cloud Logging	On	
7.5	FortiManager	On	
7.6	Forticlient EMS	Off	
7.7	Fortiweb/Forticache	Off	

8. Antivirus

8.1	Perfiles de antivirus	En la imagen podemos ver el nombre de cada antivirus que se tienen en el equipo más la cantidad de políticas en las que se encuentran.  	
8.2	Default	12	286, 579, 577, 365, 92, 66, 482, 278, 152, 150, 276, 277
8.3	Wifi-default	1	wifi-default
8.4	Uso de base de datos FortiSandbox	Off	
8.5	Virus Outbreak Prevention Database	Off	

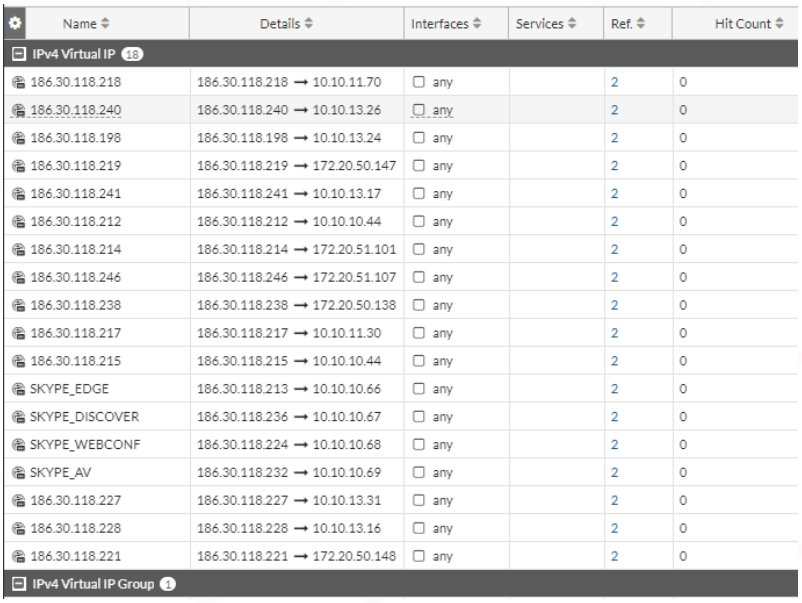
9. Políticas-root

9.1	Total de políticas	272	494,598,221,504,134,100,416,215,299,374,105,377,377,587,101,66,333,420,506,191,402,106,102,496,396,517,470,104,305,343,210,31,94,229,580,290,17,465,326,299,556,360,439,291,454,197,221,321,229,583,230,295,304,512,204,374,429,214,472,323,26,21,492,317,283,108,101,603,456,490,204,515,590,379,532,312,18,552,577,222,535,432,220,415,401,311,279,32,309,422,142,602,17,585,361,49,22,25,30,32,169,187,303,190,487,98,468,193,293,381,444,464,541,505,288,338,488,542,543,544,545,551,555,431,507,300,285,319,80,554,547,549,388,387,3,6,315,94,421,91,121,594,365,122,289,426,92,123,425,434,403,124,90,384,424,278,125,107,5,270,120,67,152,573,150,357,404,11,128,356,359,528,457,319,117,531,375,209,116,537,292,313,399,115,534,331,417,398,210,195,418,12,

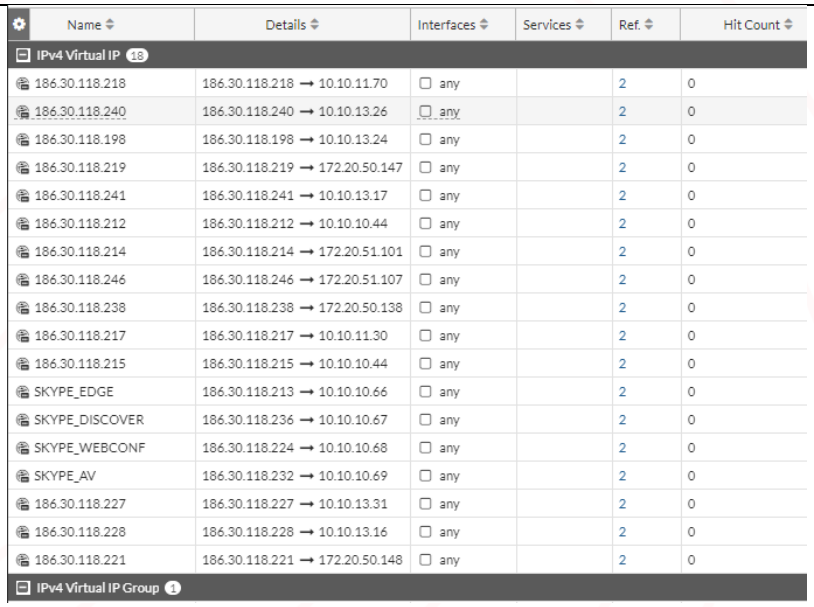
			8,349,372,437,33,232,97,208,61,385,171,210,276,460,41,500,270,62,433,222,5911,272,219,414,500,306,268,60,221,410,233,599,262,220,411,493,307,260,67,612,409,569,173,259,43,498,175,350,68,153,99,245,469,459,95,412,482,254,400,182,382,266,65,596,575,177,40,302,497,95,294,277,201, 88,7,588,485,481
9.2	políticas con cero tráficos	84	586,585,361,330,389,412,433,177,220,468,512,215,191,575,496,228,169,184,193,307,481,245,488,254,504,266,542,543,544,277,292,271,331,381,545,444,549,551,464,555,478,431,550,513,384,404,299,507,187,454,541,515,293,505,300,101,303,492,284,490,288,286,487,437,315,456,171,370,459,577,580,262,349,591,260,319,485,306,459,460,599,480,368,121,67
9.3	políticas deshabilitadas	85	586,585,361,330,389,307,481,245,488,254,504,266,542,412,277,543,292,433,177,271,544,331,220,468,381,545,512,215,444,551,549,191,464,555,575,496,478,431,384,169,228,550,513,184,193,299,507,404,586,585,361,330,389,307,481,245,488,254,504,266,542,412,277,543,292,433,177,271,544,331,220,468,381,545,512,215,444,551,549,191,464,555,575,496,478,431,384,169,228,550,513,184,193,299,507,404,67
9.4	Políticas (Source/destination ALL)	1	505
9.5	Políticas con (Services ALL)	139	94,98,99,589,58,66,285,586,585,361,330,389,307,481,245,488,254,504,266,542,412,277,543,292,433,177,271,544,331,220,468,381,545,512,215,444,551,549,191,464,555,575,496,478,431,384,169,228,550,513,184,193,299,507,404,68,67,84,90,88,62,410,411,401,60%,29,409,43,219,7,220,459,195,482,382,40,512,65,290,201,105,104,549,109,384,107,404,7,5,321,106,554,588,547,11,108,399,12,594,400,100,400,13,197,215,317,80,84,87,88,356,377,3,101,6,579,416,577,142,

	90,102,365,602,92,270,123,152,124,150,125,120,195,359,360,257,590,105,603

10. Virtual IP

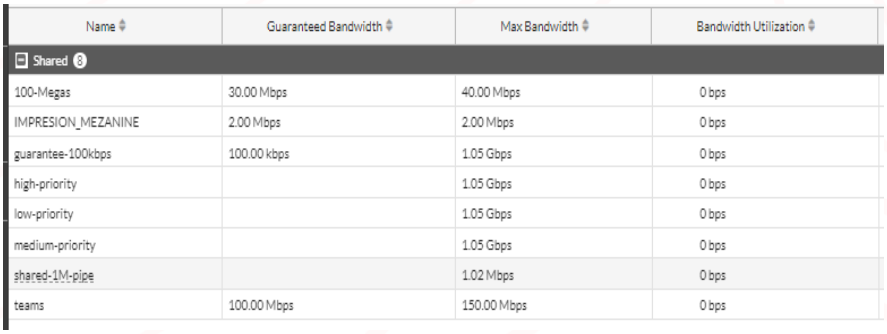
10.1 Total de Virtual IP	En la imagen podemos ver la cantidad de Virtual IP: 18 • Nombre • detalles • interfaz • Política 
10.2 Virtual IP con interfaz ANY:	En la imagen se puede observar un total de 18 interfaz en ANY

Name	Details	Interfaces	Services	Ref.	Hit Count
IPv4 Virtual IP 18					
186.30.118.218	186.30.118.218 → 10.10.11.70	any		2	0
186.30.118.240	186.30.118.240 → 10.10.13.26	any		2	0
186.30.118.198	186.30.118.198 → 10.10.13.24	any		2	0
186.30.118.219	186.30.118.219 → 172.20.50.147	any		2	0
186.30.118.241	186.30.118.241 → 10.10.13.17	any		2	0
186.30.118.212	186.30.118.212 → 10.10.10.44	any		2	0
186.30.118.214	186.30.118.214 → 172.20.51.101	any		2	0
186.30.118.246	186.30.118.246 → 172.20.51.107	any		2	0
186.30.118.238	186.30.118.238 → 172.20.50.138	any		2	0
186.30.118.217	186.30.118.217 → 10.10.11.30	any		2	0
186.30.118.215	186.30.118.215 → 10.10.10.44	any		2	0
SKYPE_EDGE	186.30.118.213 → 10.10.10.66	any		2	0
SKYPE_DISCOVER	186.30.118.236 → 10.10.10.67	any		2	0
SKYPE_WEBCONF	186.30.118.224 → 10.10.10.68	any		2	0
SKYPE_AV	186.30.118.232 → 10.10.10.69	any		2	0
186.30.118.227	186.30.118.227 → 10.10.13.31	any		2	0
186.30.118.228	186.30.118.228 → 10.10.13.16	any		2	0
186.30.118.221	186.30.118.221 → 172.20.50.148	any		2	0
IPv4 Virtual IP Group 1					

10.3 Virtual IP con 0 referencia:	 0

Name	Details	Interfaces	Services	Ref.	Hit Count
IPv4 Virtual IP 18					
186.30.118.218	186.30.118.218 → 10.10.11.70	any		2	0
186.30.118.240	186.30.118.240 → 10.10.13.26	any		2	0
186.30.118.198	186.30.118.198 → 10.10.13.24	any		2	0
186.30.118.219	186.30.118.219 → 172.20.50.147	any		2	0
186.30.118.241	186.30.118.241 → 10.10.13.17	any		2	0
186.30.118.212	186.30.118.212 → 10.10.10.44	any		2	0
186.30.118.214	186.30.118.214 → 172.20.51.101	any		2	0
186.30.118.246	186.30.118.246 → 172.20.51.107	any		2	0
186.30.118.238	186.30.118.238 → 172.20.50.138	any		2	0
186.30.118.217	186.30.118.217 → 10.10.11.30	any		2	0
186.30.118.215	186.30.118.215 → 10.10.10.44	any		2	0
SKYPE_EDGE	186.30.118.213 → 10.10.10.66	any		2	0
SKYPE_DISCOVER	186.30.118.236 → 10.10.10.67	any		2	0
SKYPE_WEBCONF	186.30.118.224 → 10.10.10.68	any		2	0
SKYPE_AV	186.30.118.232 → 10.10.10.69	any		2	0
186.30.118.227	186.30.118.227 → 10.10.13.31	any		2	0
186.30.118.228	186.30.118.228 → 10.10.13.16	any		2	0
186.30.118.221	186.30.118.221 → 172.20.50.148	any		2	0
IPv4 Virtual IP Group 1					

11. Traffic Shapers

11.1 Total de objetos de traffic shaper	Un total de 8. 

Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization
Shared 8			
100-Megas	30.00 Mbps	40.00 Mbps	0 bps
IMPRESION_MEZANINE	2.00 Mbps	2.00 Mbps	0 bps
guarantee-100kbps	100.00 kbps	1.05 Gbps	0 bps
high-priority		1.05 Gbps	0 bps
low-priority		1.05 Gbps	0 bps
medium-priority		1.05 Gbps	0 bps
shared-1M-pipe		1.02 Mbps	0 bps
teams	100.00 Mbps	150.00 Mbps	0 bps

11.2 Políticas de traffic Shaper	La única habilitada es la implícita

11.3 Objetos sin referencia

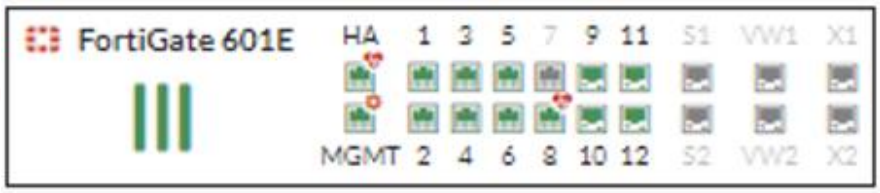
Un total de 5.

Name	Max Bandwidth	Ref.
Shared 5/8		
100-Megas	40.00 Mbps	0
guarantee-100kbps	1.05 Gbps	0
low-priority	1.05 Gbps	0
medium-priority	1.05 Gbps	0
shared-1M-pipe	1.02 Mbps	0

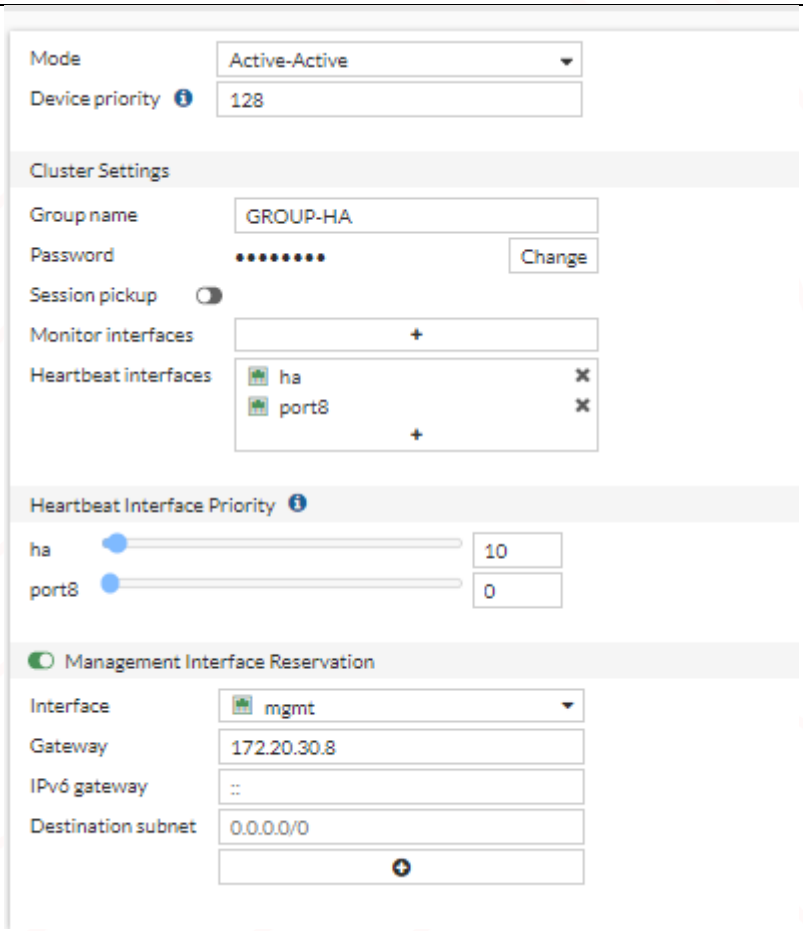
12. Configuración HA

12.1 Modo HA

Active-Active



12.2 Interfaces heartbeat



12.3 Checksum

OK	Checksum dc85319f8cb1f1f900b3db8cd439586c dc85319f8cb1f1f900b3db8cd439586c

12.4 Estado Master/Slave	OK	Hostname / Serial No. / Role FortiGate-601E_01 / FG6H1E5819900665 / Primary FortiGate-601E_02 / FG6H1ETB20907192 / Secondary
12.5 Simetría en Interface	N/A	

13. Condiciones eléctricas

13.1 conexión a tierra	N/A	
13.2 Tomas reguladas	N/A	
13.3 conexión a UPS	N/A	
13.4 ubicación	N/A	
13.5 Temperatura	N/A	

14. SitioS Web más visitados

En la imagen que se presenta se puede apreciar una lista de los sitios web con mayor cantidad de salidas a Internet. Esta información puede ser valiosa para entender el comportamiento de los usuarios en línea y para identificar patrones de uso de Internet en diferentes contextos.

Domain	Category	Bytes	Sessions	Bandwidth
icloud.com		1.20 MB	6.375	16.20 kbps
tiktokv.com		489.66 kB	2.380	0 bps
google.com		80.83 kB	485	11.03 kbps
live.com		104.98 kB	278	86.64 kbps
facebook.com	Social Networking	16.75 MB	86	101.48 kbps
doubleclick.net		14.60 kB	79	544 bps
youtube.com		8.38 kB	48	0 bps
netflix.com		7.05 kB	41	0 bps
fbcdn.net		92.92 MB	41	2.66 Mbps
googlevideo.com		5.18 kB	31	0 bps
172.217.28.106		3.78 kB	22	0 bps
twitter.com		3.51 MB	16	8.46 kbps
157.240.6.32		2.58 kB	15	0 bps
openx.net		1.72 kB	10	0 bps
oneclient.sfx.ms		4.04 kB	10	2.83 kbps
tiktokcdn.com		9.36 MB	9	0 bps
apple.com		2.00 kB	8	0 bps

15. Políticas con más uso

En la imagen se puede apreciar las políticas más utilizadas.

Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	Bandwidth
Navegacion funcionarios (152)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_INTERNET	152.08 GB	10.927	156.44 Mb...
ID_107 (107)	Firewall	VLAN_SERVER_NUE	VLAN_LACP_INSIDE (VLAN_INSIDE)	119.57 GB	2.157	260.42 kbps
398	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_SERVER_ANT	104.49 GB	12	3.05 kbps
MGMT_VEEAM_BKP_NUTANIX_VLAN_40 (318)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_BK_NUTANIX (VLAN_BK_NUTANIX)	15.49 GB	34	34.93 kbps
Inside_Outside_SMB (420)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_SERVER_NUE	11.16 GB	274	660.80 kbps
ID_66 (66)	Firewall	VLAN 16 - SEDES (sedes)	VLAN_INTERNET	9.42 GB	1.087	18.09 Mbps
ID_13 (13)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_SERVER_NUE	2.89 GB	29.615	2.04 Mbps
Navegacion_vip (150)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_INTERNET	1.86 GB	1.527	12.88 Mbps
ID_11 (11)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN 16 - SEDES (sedes)	1.52 GB	223	1.19 Mbps
ID_377 (377)	Firewall	VLAN_SERVER_NUE	VLAN_INTERNET	983.58 MB	4.162	223.62 kbps
RDP_ID_396 (396)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_SERVER_NUE	809.42 MB	42	70.97 kbps
ID_90 (90)	Firewall	VLAN_SERVER_ANT	VLAN_SERVER_NUE	604.55 MB	70	4.30 kbps
CONEXION_PLANTA_TELEFONICA_SELCOMP (305)	Firewall	VLAN_SERVER_NUE	VLAN_LACP_INSIDE (VLAN_INSIDE)	422.17 MB	8	324.13 kbps
Azure_Vlan_Nueva (21)	Firewall	AZURE	VLAN_SERVER_NUE	251.15 MB	907	106.19 kbps
ID_92 (92)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	VLAN_INTERNET	212.33 MB	12.009	2.21 Mbps
ID_414 (414)	Firewall	DMZ_INT-VLAN34	VLAN_SERVER_NUE	210.10 MB	179	240.46 kbps
SERVER-150-VLAN_40_NUTANIX (322)	Firewall	VLAN_SERVER_NUE	VLAN_BK_NUTANIX (VLAN_BK_NUTANIX)	195.48 MB	61	45.06 kbps
ID_43 (43)	Firewall	DMZ_INT-VLAN34	VLAN_SERVER_NUE	188.02 MB	49	3.94 kbps
Inside-Azure_Produccion (3)	Firewall	VLAN_LACP_INSIDE (VLAN_INSIDE)	AZURE	171.10 MB	10	84.22 kbps
ID_65 (65)	Firewall	VLAN 16 - SEDES (sedes)	VLAN_LACP_INSIDE (VLAN_INSIDE)	104.02 MB	260	2.72 kbps
VPN_Acceso_SRV_Mozart (232)	Firewall	SSL-VPN tunnel interface (ssl.root)	VLAN_SERVER_ANT	79.48 MB	1	24 bps
INNOVA_NAT (374)	Firewall	VLAN_INTERNET	DMZ_F5-VLAN130	73.46 MB	7	139.78 kbps

16. Políticas con más uso

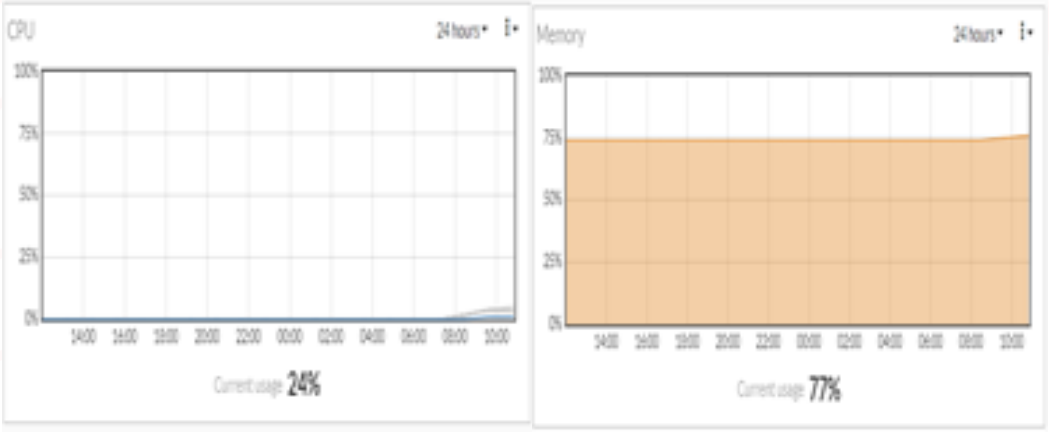
En la imagen se puede apreciar las aplicaciones más utilizadas.

Application	Category	Risk	Bytes	Sessions	Bandwidth
Github	Storage.Backup		85.41 GB	113	38.78 Mbps
Skype_Video	Collaboration		25.77 GB	103	52.61 Mbps
Microsoft.Outlook.Office.365	Email		22.16 GB	2.532	36.90 Mbps
ISAKMP	Network.Service		17.24 GB	7	364.04 kbps
HTTPS.BROWSER	Web.Client		3.32 GB	1.318	14.00 Mbps
Skype_Audio	Collaboration		3.28 GB	62	7.53 Mbps
YouTube	Video/Audio		2.19 GB	360	17.60 Mbps
Ping	Network.Service		985.93 MB	18	2.12 kbps
DTLS	Network.Service		504.62 MB	1	1.00 Mbps
STUN	Network.Service		428.56 MB	21	608.12 kbps
Skype_Data	Collaboration		390.64 MB	56	806.80 kbps
Microsoft.Office.Online	Collaboration		388.17 MB	734	9.63 Mbps
Microsoft.Teams	Collaboration		265.15 MB	1.526	531.61 kbps
WhatsApp_Web	Collaboration		217.72 MB	204	191.39 kbps
Microsoft.SharePoint	Collaboration		200.65 MB	248	504.71 kbps
Facebook	Social.Media		198.32 MB	292	7.81 Mbps
Microsoft.Office.365.Portal	Collaboration		177.56 MB	699	1.09 Mbps
Windows.Push.Notification	General.Interest		127.28 MB	896	38.30 kbps
Google.Services	General.Interest		124.28 MB	1.503	2.15 Mbps
Microsoft.Outlook	Email		117.41 MB	76	255.38 kbps
OneDrive	Storage.Backup		101.13 MB	302	1.56 Mbps
Twitter	Social.Media		84.40 MB	231	1.01 Mbps

17. Capturas de pantalla (CPU, Memoria, Sesiones, Licenciamiento.)

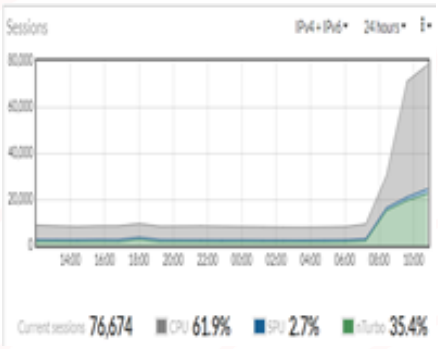
- **CPU – MEMORIA**

La imagen muestra que, durante el período de tiempo analizado, el uso de la memoria se mantuvo en un promedio del 48% y el uso de la CPU en un promedio del 4%. Es importante tener en cuenta que el uso de la memoria y la CPU puede variar dependiendo de muchos factores, como la cantidad de aplicaciones que se están ejecutando simultáneamente, la complejidad de estas aplicaciones y la cantidad de recursos que están disponibles en el sistema.



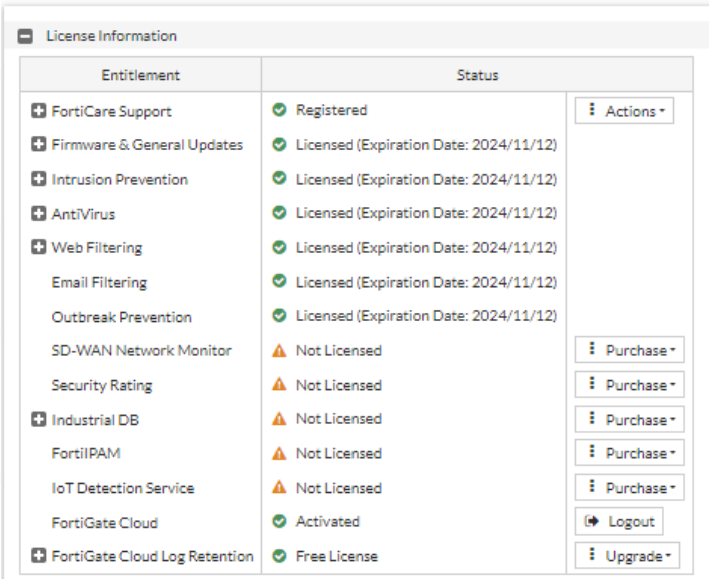
- **SESIONES**

En la imagen se puede evidenciar que el promedio de sesiones fue de 76,674, lo cual nos indica que hubo un número considerable de sesiones durante el periodo de tiempo analizado. Vemos pico en el horario de 12p.m lo cual puede variar dependiendo de muchos factores, como la cantidad de aplicaciones que se están ejecutando simultáneamente, la complejidad de estas aplicaciones y la cantidad de recursos que están disponibles en el sistema.



- **LICENCIAMIENTO**

La información presentada indica que la licencia del Fortigate (FG) está programada para expirar el 2024/11/12. Es importante destacar que el mantenimiento de la licencia es esencial para mantener el soporte técnico y las actualizaciones de seguridad del fabricante para el equipo Fortianalyzer. Por lo tanto, se debe renovar la licencia antes de la fecha de vencimiento para garantizar la continuidad del soporte técnico y el acceso a las últimas actualizaciones del software y las funcionalidades del equipo. Es recomendable estar al tanto de las fechas de expiración de las licencias para tomar las medidas necesarias y evitar problemas futuros.



16. Evidencias fotográficas (Fotos de ubicación de dispositivos, Ocupación de interfaces, fuentes de alimentación y polos a tierra).

- N/A

17. Recomendaciones

- Se recomienda que las VIP con interface ANY, ajustarlas a la interface por la cual se espera sea consumido el servicio. Esto con el fin de sesgar las zonas por las que se puede asociar los objetos vip en las políticas y prevenir brechas al publicar estos servicios por otras zonas.
  En general, se recomienda utilizar una dirección IP específica en lugar de una VIP con interfaz ANY siempre que sea posible, para minimizar los riesgos de seguridad y mejorar el rendimiento y el control.
- Según nos indica el funcionario de Ministerio de Agricultura estas políticas se encuentran en un periodo de desactivación por treinta (30) días iniciado. Desde el día 14 de abril hasta el día 14 de mayo, fecha en que serán eliminadas estas 84 políticas.

  586,585,361,330,389,412,433,177,220,468,512,215,191,575,496,228,169,184,193,307,481,245,488,254,504,266,542,543,544,277,292,271,331,381,545,444,549,551,464,555,478,431,550,513,384,404,299,507,187,454,541,515,293,505,300,101,303,492,284,490,288,286,487,437,315,456,171,370,459,577,580,262,349,591,260,319,485,306,459,460,599,480,368,121,67
- Según nos indica el funcionario de Ministerio de Agricultura estas políticas se encuentran en un periodo de desactivación por treinta (30) días iniciado. Desde el día 14 de abril hasta el día 14 de mayo, fecha en que serán eliminadas estas 85 políticas.

  586,585,361,330,389,307,481,245,488,254,504,266,542,412,277,543,292,433,177,271,544,331,220,468,381,545,512,215,444,551,549,191,464,555,575,496,478,431,384,169,228,550,513,184,193,299,507,404,586,585,361,330,389,307,481,245,488,254,504,266,542,412,277,543,292,433,177,271,544,331,220,468,381,545,512,215,444,551,549,191,464,555,575,496,478,431,384,169,228,550,513,184,193,299,507,404,67
- Se recomienda habilitar el perfil de antivirus en todas las políticas de entrada y salida de internet.
- A pesar de que el sistema es compatible con el español para la nomenclatura de los objetos evitar usar caracteres especiales comunes como: ñ, Ñ, á, é, í, ó, ú, Á, É, Í, Ó, Ú, debido a que es probable que en escenarios de actualización de firmware puedan ocasionar fallas en los objetos involucrados.
- Realizar copias de seguridad regulares: es importante realizar copias de seguridad regulares del Fortigate para proteger la información crítica almacenada en el dispositivo. Las copias de

seguridad deben almacenarse en un lugar seguro y accesible para facilitar la recuperación de datos en caso de una falla en el equipo.

- El equipo por sí solo no constituye una garantía de seguridad. Es fundamental su continua administración y análisis del tráfico que reporta, para efectuar mejoras a la implementación debido a las condiciones cambiantes de la red administrada.
- Se recomienda en lo posible mantener el dispositivo actualizado con la última versión más estable, para ello se debe revisar los release liberados por fabricante, analizando si pueden llegar a presentar fallas según la configuración existente. https://docs.fortinet.com/product/fortigate; actualmente se tiene una vulnerabilidad CVE-2023-25610 la cual se puede revisar en el siguiente boletín https://www.fortiguard.com/psirt/FG-IR-23-001, fabrica sugiere actualizar a 7.0.11.

Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147
Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454