UNIÓN TEMPORAL **UT HC-WX SEGURIDAD 2025**

Heimcore | WEXLER

ASSESSMENT
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI



INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI
ASSESSMENT INFRAESTRUCTURA FORTINET

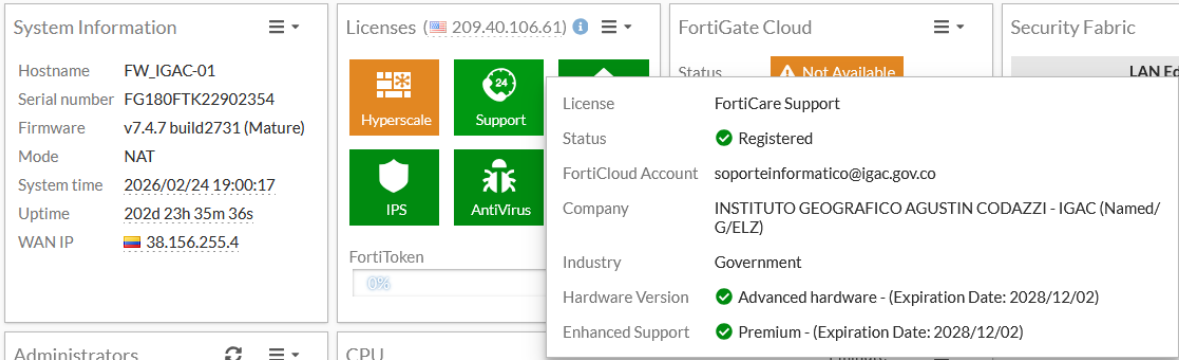
Tabla de Contenido

1 FortiGate 1800F 1-4
1.1 Firmware 1-4
1.2 Performance 1-4
1.3 Interfaces 1-5
1.4 1-6
1.5 Políticas 1-6
1.6 Objetos 1-9
1.6.1 Address y Services: 1-9
1.6.2 VIP: 1-9
1.6.3 Traffic Shaping: 1-10
1.7 Configuraciones generales 1-11
1.8 Security Fabric 1-12
1.9 VPN IPSEC 1-12
1.10 Seguridad 1-13
1.10.1 VPN SSL: 1-13
1.10.2 Intrusion Prevention: 1-16
1.10.3 Equipos e IPs comprometidas: 1-17
2 FortiAnalyzer 400E 2-18
2.1 Firmware 2-19
2.2 Dispositivos asociados 2-19
2.3 Performance 2-19
3 FortiManager 200G 3-20
3.1 Firmware 3-20
3.2 Configuraciones generales 3-21
4 SDWAN 4-22
4.1 Firmware 4-22

4.2 Puertos de gestión 4-22
4.3 Consumo de RAM 4-23
4.4 Conectividad con Sede y BGP 4-24
5 Aprobación 5-25

1 FortiGate 1800F

A nivel de licenciamiento se valida que se cuenta con vigencia hasta el 02 de diciembre de 2028.

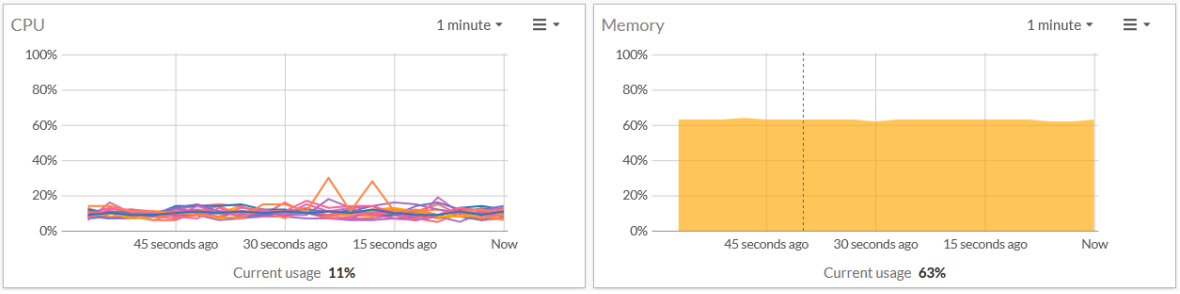


1.1 Firmware

Teniendo en cuenta que por mejoras en el nivel de seguridad Fortinet ha liberado nuevas versiones de Firmware se recomienda realizar la actualización a la versión 7.4.11 lo más pronto posible bajo una ventana de mantenimiento.

Ya se encuentra liberada la versión de firmware 7.6.X sin embargo aún no recomendamos pasar a esta versión teniendo en cuenta que aún tiene varios bugs importantes por corregir.

1.2 Performance

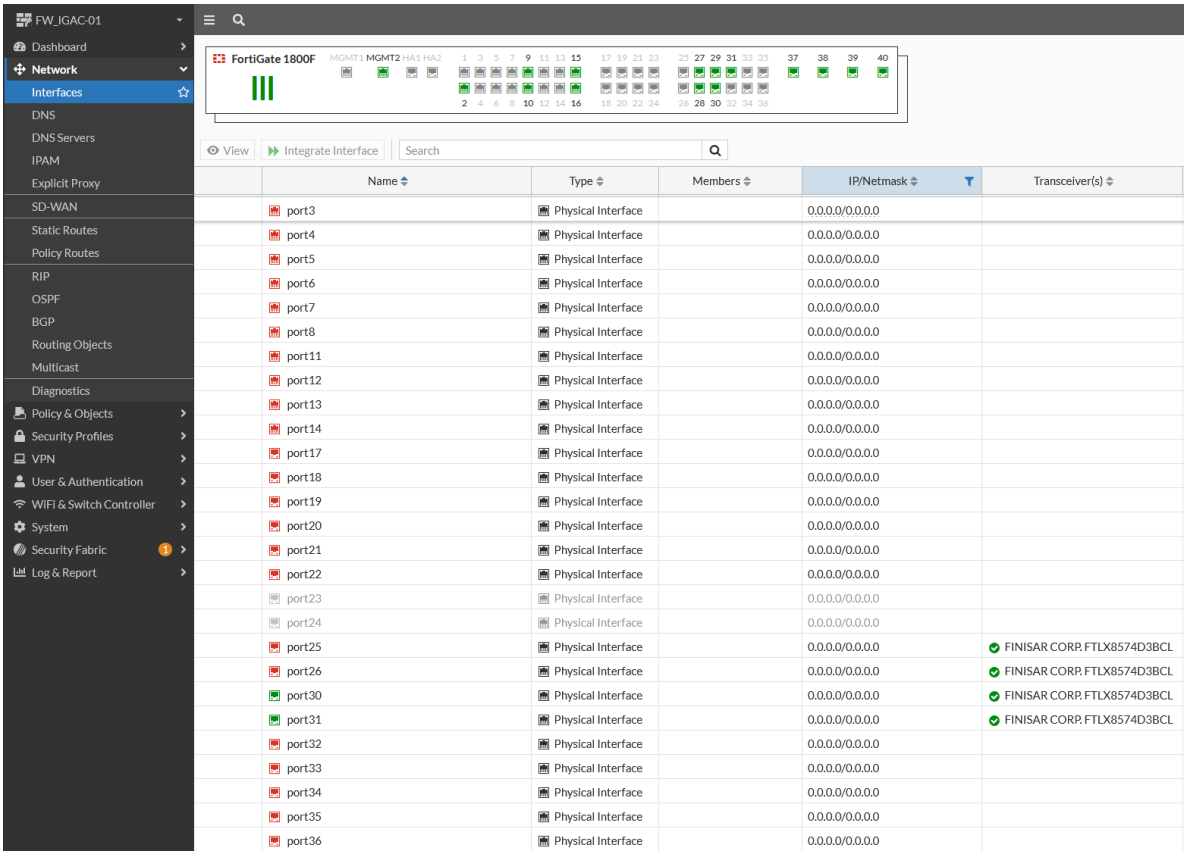


El equipo se encuentra en la versión de Firmware 7.4.7, bajo esta versión no se han detectado problemas de inestabilidad de consumo a nivel de procesamiento y memoria

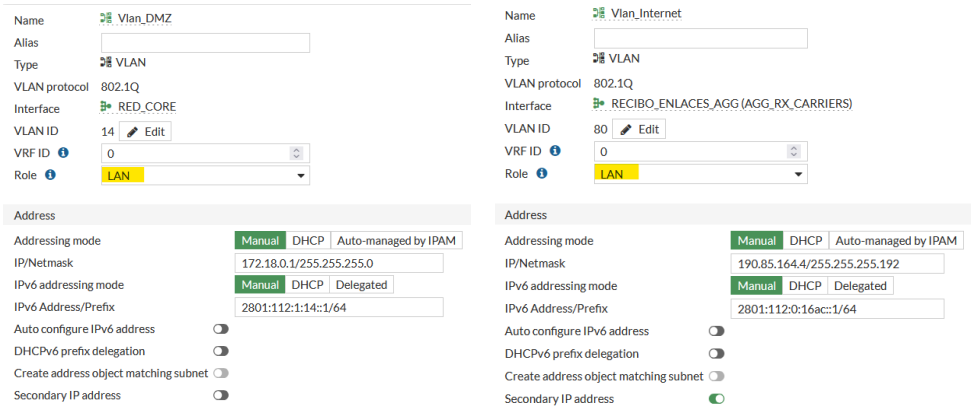
RAM, aunque si es importante informar que el equipo cuenta con consumo de memoria RAM por encima del 60% y esto se debe a la carga a nivel de tráfico y validaciones sobre este que se ha adicionado en el último año, es importante revisar constantemente que este consumo no llegue ni supere el 75% ya que el equipo podría entrar en modo Conservación, lo que podría ocasionar que se bloquee todo el tráfico.

1.3 Interfaces

Se recomienda deshabilitar las interfaces que no se estén utilizando.



Se recomienda categorizar los roles de las interfaces es especial para aquellas que son WAN y DMZ ya que esto agrega o elimina características a la interfaz lo que permite darle un trato especial a cada tipo de tráfico.



1.4 Políticas

Hay 258 políticas cuyo origen está establecido como ALL y 319 cuyo destino está establecido como ALL también, teniendo en cuenta que la información a mostrar es extensa se anexa a este documento un archivo de Excel llamado “Políticas Origen o Destino ALL.xlsx” que compila estas políticas.

Es muy importante delimitar todas reglas lo máximo posible con el fin de solo permitir el acceso a los servicios y recursos estrictamente necesarios inclusive si el origen son los equipos de los administradores, esto teniendo en cuenta que no se está exento de adquirir un malware en nuestros equipos con lo cual estaríamos facilitando el trabajo a los atacantes para acceder a nuestros recursos sin restricciones.

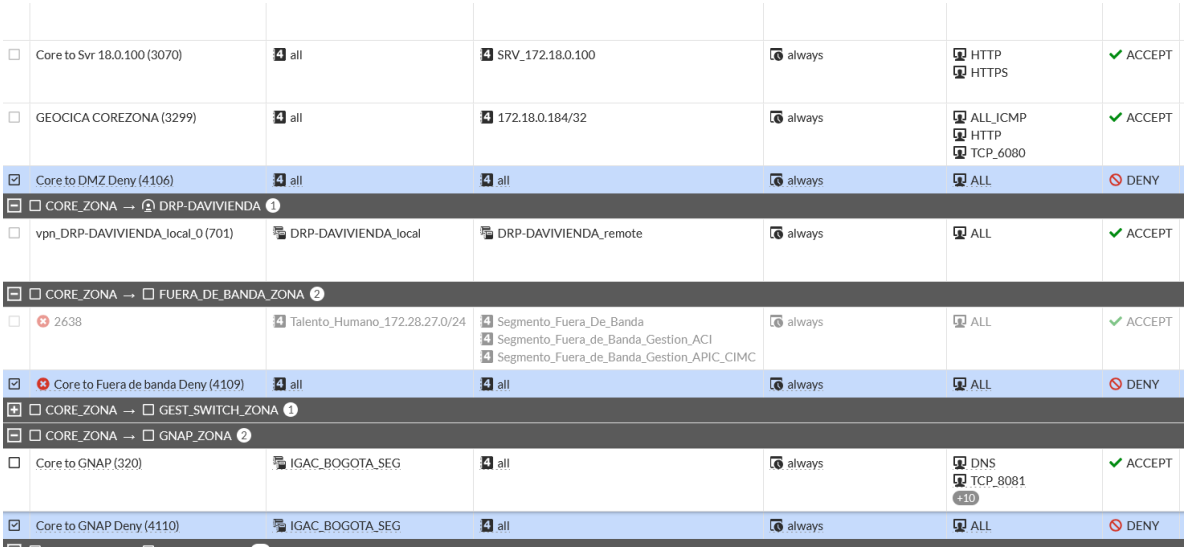
Para los orígenes que se requiera que muchos equipos tengan acceso se recomienda por lo menos hacer la limitación con el objeto u objetos que contengan las redes que exclusivamente deberían tener acceso.

Algunas de estas políticas se encuentran al final del grupo de par de interfaces y tienen tráfico, estas reglas no deben existir ya que en posiciones superiores a ellas

deberían existir las reglas que cubran el trafico que debería estar permitido con el fin de poder eliminarlas.

	Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log	Bytes
					TCP_135-139_wi... +1					SSL certificate-inspection IPS IGAC_Server		
☐	Analisis DNA to Granja (1694)	DNA-CLUSTER DNA-ENTERPRISE	GRANJA_172.19.0.0/24	always	ALL	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	0 B
☐	Analisisis Lan_VDI_citrix_to_Granja (3806)	LAN_VDI_CITRIX_	all	always	HTTP HTTPS +2	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	18.3 GB
☐	HC - 01 - VDIs_to_WSUS (4070)	administradores_VDI_Citrix Cloud_coneectors_citrix LAN_VDI_CITRIX_	srv_172.19.0.18 WSUSCFGPRD02_172.19.0.140...	always	TCP_8530	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	0 B
☐	HC - 02 - VDIs_to_DA (4071)	LAN_VDI_CITRIX_ VDI_Server_Gestion	DCPRD01_172.19.0.10 DCPRD02_172.19.0.11 DCPRD03_172.19.0.12	always	TCP_88 TCP_49668 +4	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	629.71 GB
☐	HC - 09 - VDIs_to_DA (4081)	administradores_VDI_Citrix Cloud_coneectors_citrix LAN_VDI_CITRIX_	DCPRD01_172.19.0.10 DCPRD02_172.19.0.11 DCPRD03_172.19.0.12	always	MMS PING RDP	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	0 B
☐	HC - 04 - VDI_to_Srv_LIC_Argis (4073)	LAN_VDI_CITRIX_	srv_172.19.0.222 srv_172.19.0.224	always	TCP_27000_27009	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	1.88 GB
☐	HC - 06 - VDI_to_Srv_LIC_ERDAS (4077)	LAN_VDI_CITRIX_	sgcclmprd02_172.19.0.44 SRV_172.19.0.43	always	TCP_28000 TCP_5093 TCP_5842	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	365.81 MB
☐	HC - 11 - VDI_to_Srv_SIGIPOSTGRESPR (4083)	juan.angel LAN_VDI_CITRIX_	172.19.0.119	always	TCP_5432_POST...	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	742.49 GB
☐	Ticket 434252 (4878)	LAN_VDI_CITRIX_ VDI_Server_Gestion	172.19.0.149	always	TCP-1688	✔ ACCEPT		Disabled	Standard	AV AV_IGAC_P SSL certificate-inspection IPS IGAC_Server	All	0 B
☑	1696	all	all	always	ALL	✔ ACCEPT		Disabled	Standard	SSL no-inspection	All	228.53 GB

Al finalizar de algunos pares de interfaces existen políticas que deniegan el tráfico, aquí es importante aclarar que esa actividad ya la realiza la regla implícita (0), Sí debajo de estas reglas no hay mas reglas, no hay nada que bloquear, por tal motivo se recomienda eliminarlas.



☐	Core to Svr 18.0.100 (3070)	all	SRV_172.18.0.100	always	HTTP HTTPS	ACCEPT
☐	GEOCICA COREZONA (3299)	all	172.18.0.184/32	always	ALL_ICMP HTTP TCP_6080	ACCEPT
☑	Core to DMZ Deny (4106)	all	all	always	ALL	DENY
☐	CORE_ZONA → DRP-DAVIVIENDA 1					
☐	vpn_DRP-DAVIVIENDA_local_0 (701)	DRP-DAVIVIENDA_local	DRP-DAVIVIENDA_remote	always	ALL	ACCEPT
☐	CORE_ZONA → FUERA_DE_BANDA_ZONA 2					
☐	2638	Talento_Humano_172.28.27.0/24	Segmento_Fuera_De_Banda Segmento_Fuera_de_Banda_Gestion_ACI Segmento_Fuera_de_Banda_Gestion_APIC_CIMC	always	ALL	ACCEPT
☑	Core to Fuera de banda Deny (4109)	all	all	always	ALL	DENY
☐	CORE_ZONA → GEST_SWITCH_ZONA 1					
☐	CORE_ZONA → GNAP_ZONA 2					
☐	Core to GNAP (320)	IGAC_BOGOTA_SEG	all	always	DNS TCP_8081 +10	ACCEPT
☑	Core to GNAP Deny (4110)	IGAC_BOGOTA_SEG	all	always	ALL	DENY

Por otro lado, a pesar de estar en su mayoría bajo excelentes parámetros de delimitación, hay 384 políticas que están permitiendo todos los servicios y que pueden significar un riesgo para la seguridad de la infraestructura sobre todo los que se relacionan a continuación que

tienen como origen y destino el objeto ALL, prácticamente permiten todo tráfico. Estas políticas se pueden evidenciar en el archivo de Excel anexo llamado “Politicas Servicios All.xlsx”

Algunas políticas ALL se encuentran no en la parte inferior de la sesión de par de interfaces, lo que no permite que hagan match las políticas ya configuradas que se encuentran más abajo que posiblemente gestionen parte del acceso que está pasando por esas ALL.

Existen 709 políticas que no han tenido tráfico desde el 05 de agosto del 2025 (fecha del último reinicio del Firewall) lo que acumula un total de 203 días a la fecha en los que no han sido usadas y esto se podría ser ocasionado porque lo hay dispositivos que ya no existan en esas interfaces que ya no requieran comunicación, o también podría ser porque hay políticas encima que ya dan acceso a los recursos relacionado en ellas y por ende no podrían llegar a hacer match, estas políticas se encuentran relacionadas en el archivo de Excel anexo llamado “Politicas con 0 consumo.xlsx”.

En cuanto a políticas sin perfiles de seguridad encontramos que existen 1053 sin embargo aquí hay que tener especial cuidado en escoger las que realmente requieren establecerle perfiles de seguridad ya que el consumo de memoria RAM del equipo está ya por el 63%, entre más perfiles se habiliten más consumo habrá lo que podría llegar a ocasionar inestabilidad en el equipo, estas políticas se encuentran relacionadas en el archivo de Excel anexo llamado “Politicas sin perfiles de seguridad.xlsx.

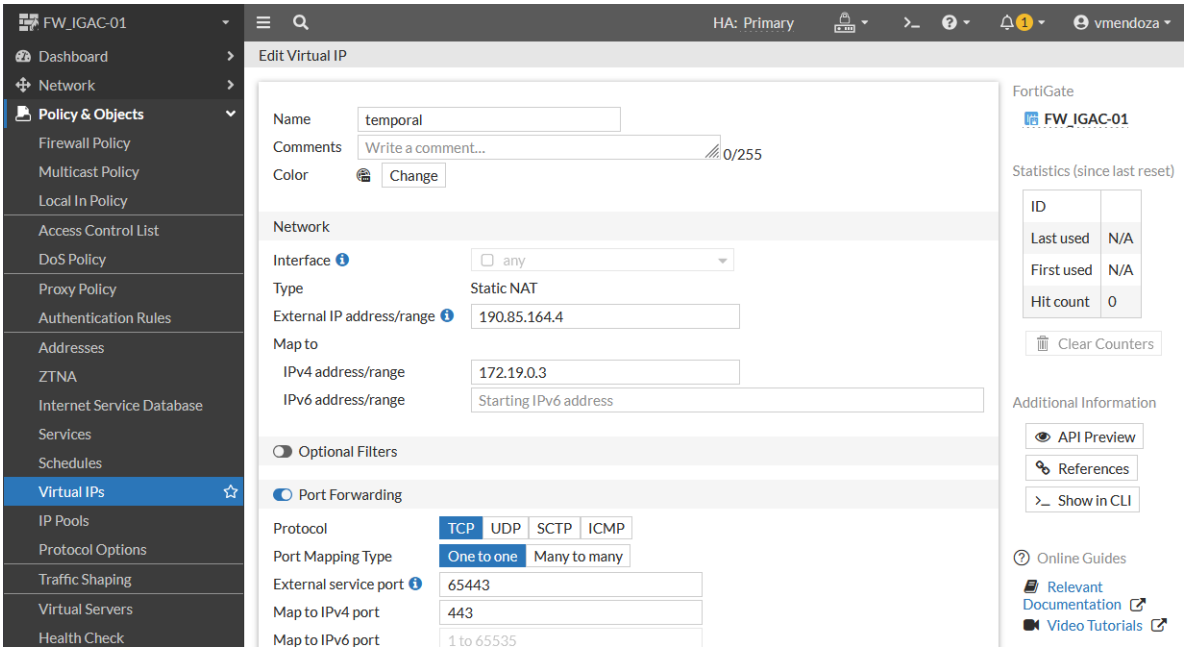
1.5 Objetos

1.5.1 Address y Services:

No se encontraron objetos de este tipo que no se estuvieran utilizando a excepción de los que vienen predeterminados en la máquina que se suelen conservar.

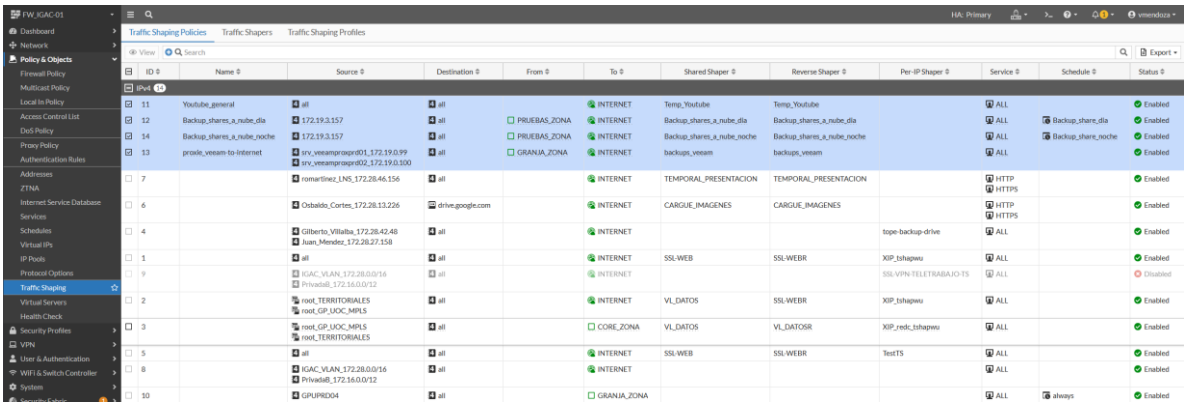
1.5.2 VIP:

El único objeto de tipo Virtual IP que no ha sido usado es el llamado “temporal”.



1.5.3 Traffic Shaping:

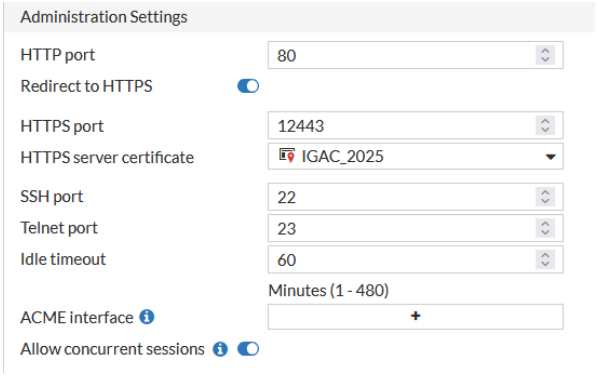
En la actualidad se están usando solamente 4 políticas de Traffic Shaping, las demás aunque están asociadas a políticas no han tenido tráfico.



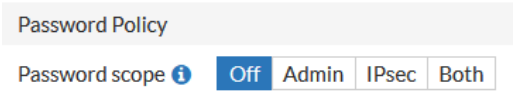
	ID	Name	Source	Destination	From	To
IPv4 14						
☑	11	Youtube_general	all	all		INTERNET
☑	12	Backup_shares_a_nube_dia	172.19.3.157	all	PRUEBAS_ZONA	INTERNET
☑	14	Backup_shares_a_nube_noche	172.19.3.157	all	PRUEBAS_ZONA	INTERNET
☑	13	proxie_veeam-to-internet	srv_veeamproxprd01_172.19.0.99 srv_veeamproxprd02_172.19.0.100	all	GRANJA_ZONA	INTERNET

1.6 Configuraciones generales

Se recomienda modificar los puertos de acceso administrativo HTTP y SSH que vienen por defecto.



Es importante habilitar la política de contraseñas para exigir características como tamaño mínimo, exigir caracteres especiales, tiempo de expiración de la contraseña y el evitar el reúso de contraseñas antiguas.

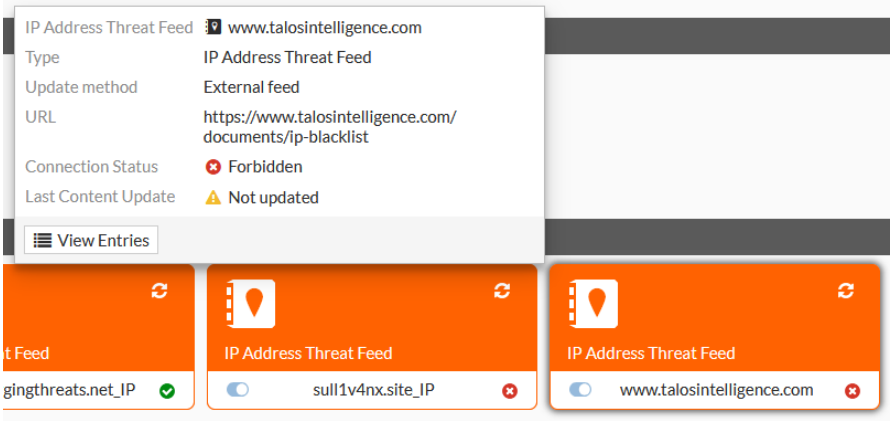


Se recomienda realizar una depuración de los certificados digitales que se encuentran expirados, ya sea para cambiarlos por los mas recientes o eliminar los que ya no son funcionales.

IGAC2019_SSL	C = CO, ST = Bogota, L = Bogota, O = Instituto Geograf...	DCIGAC-CAPRD01-CA	Expired	2021/09/30 15:45:26
SSL-IGAC	CN = 132.255.20.132, emailAddress = lfiorenzano@ig...	ROOTCA	Expired	2018/12/26 16:03:22
SSL_INSPECTION_CA	C = CO, ST = Bogota, L = Bogota, O = Instituto Geograf...	DCIGAC-CAPRD01-CA	Expired	2021/07/31 11:16:29

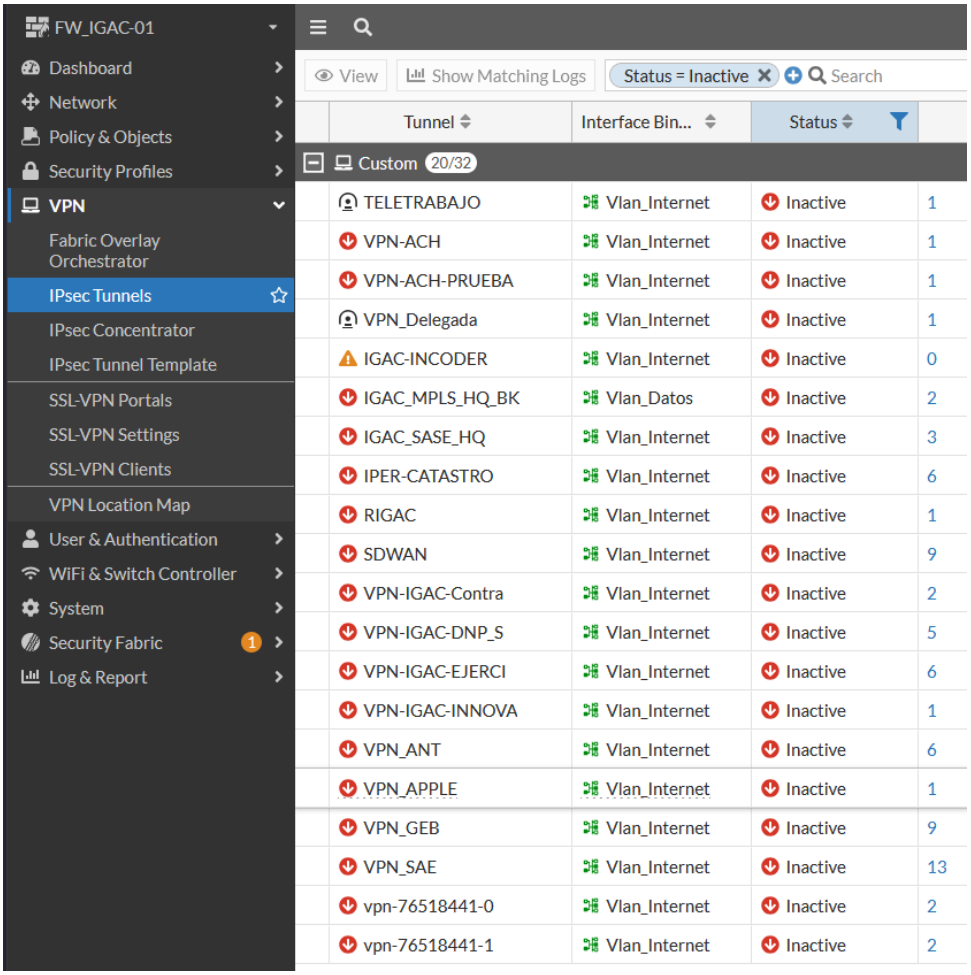
1.7 Security Fabric

Dos de los recursos externos de direcciones maliciosas no está funcionando debido a que al parecer el dominio ya no existe, se recomienda validar el origen para actualizarlo o en su debido caso eliminar este recurso.



1.8 VPN IPSEC

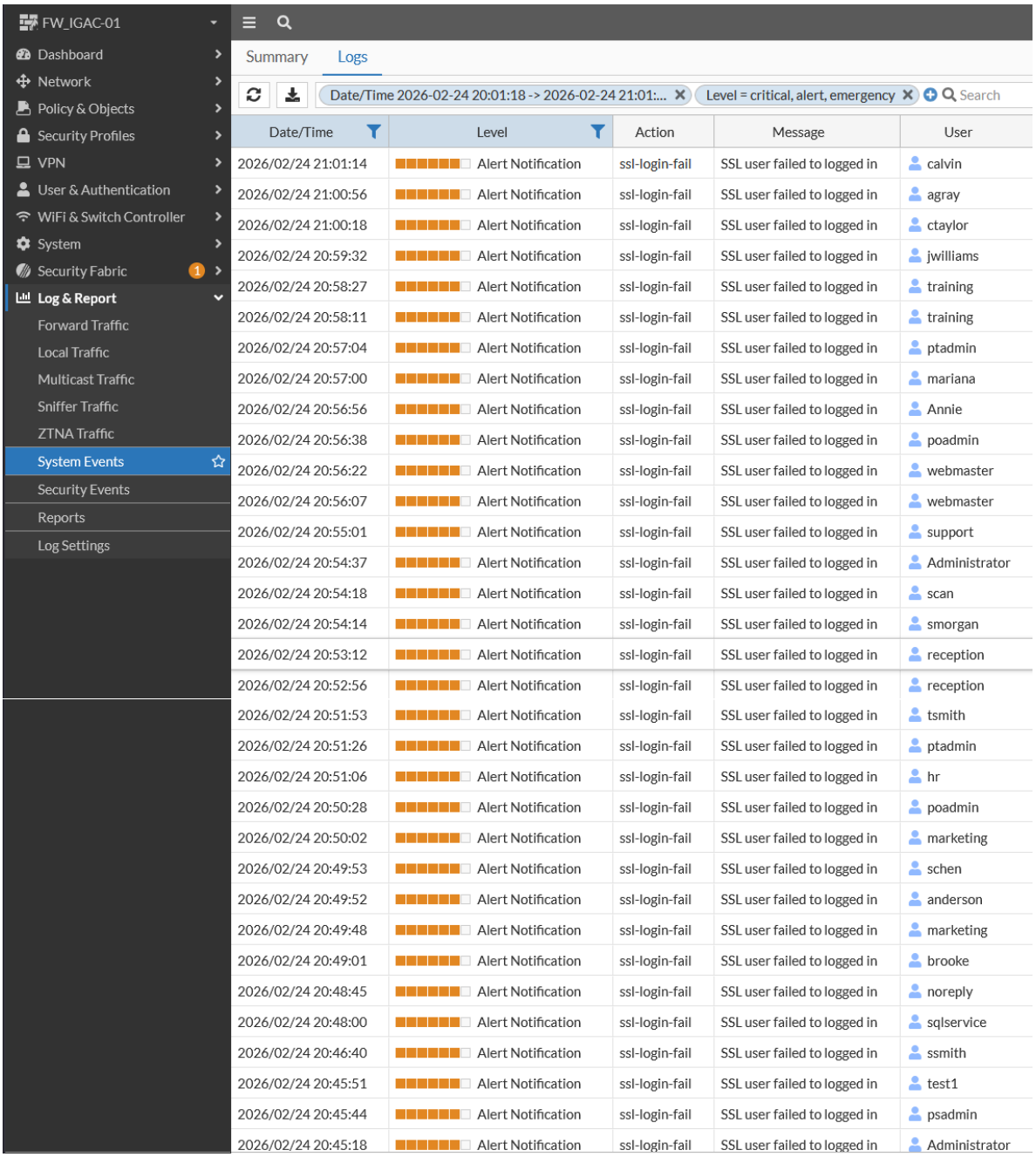
Existen actualmente 20 Túneles IPSEC que no se encuentran establecidos, de estos se recomienda que si no se necesitan se podrían eliminar para evitar posibles conflictos de enrutamiento.



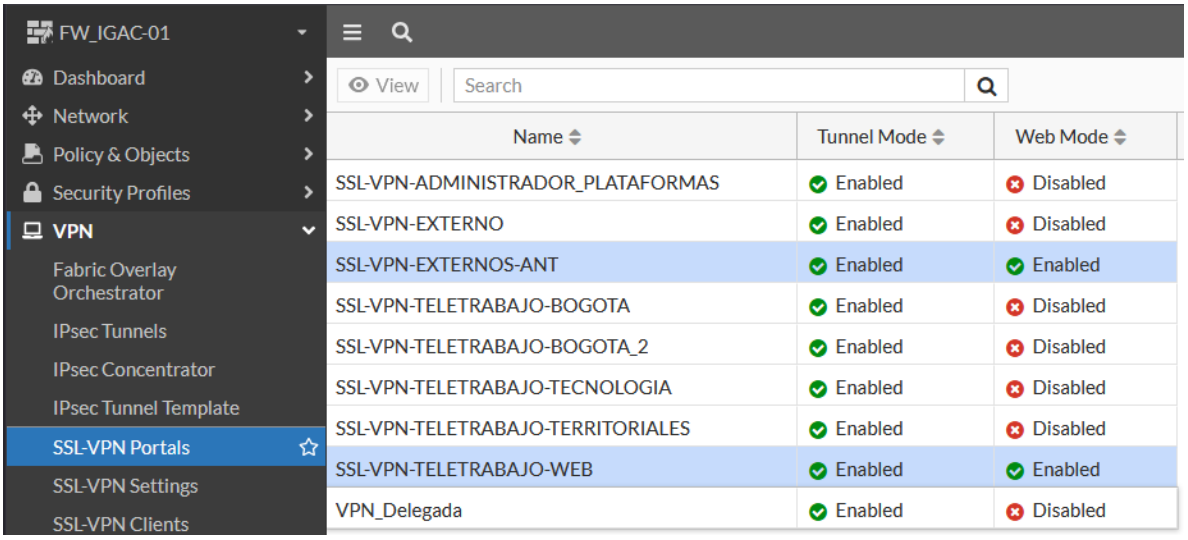
1.9 Seguridad

1.9.1 VPN SSL:

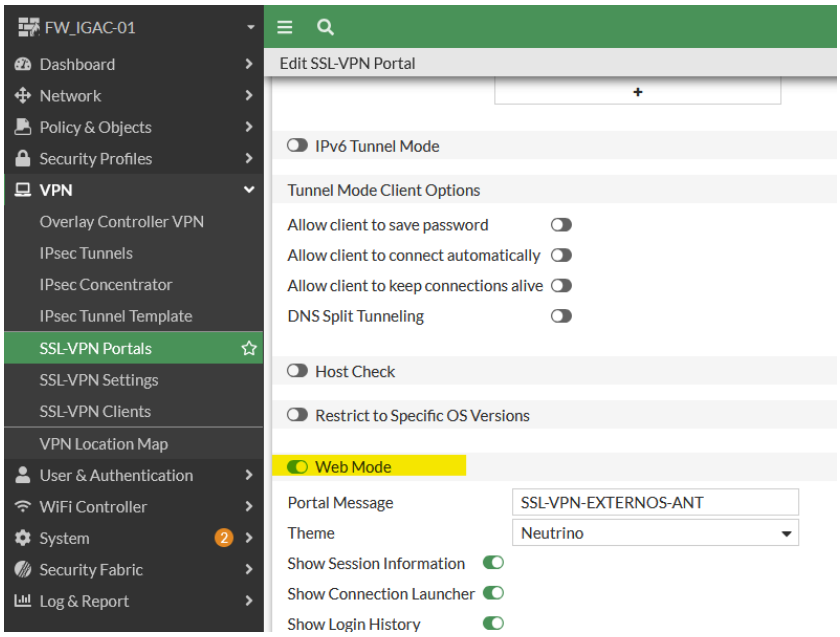
A nivel de VPN SSL se identifica que hay ataques continuos con cuentas de usuarios aleatorias con el fin de adivinar la contraseña, se recomienda usar un segundo factor de autenticación para proteger estas cuentas de usuario.



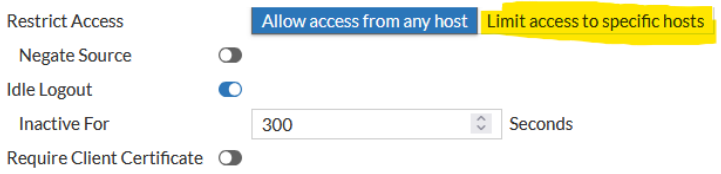
Esto ocurre porque hay dos portales SSL-VPN-EXTERNOS-ANT Y SSL-VPN-TELETRABAJO-WEB que tienen habilitada la opción de “Web Mode” que es normalmente atacada y puede presentar problema de vulnerabilidades a futuro.



Si es posible deshabilitar el modo Web en los portales de VPN para permitir solo conexiones desde la aplicación de FortiClient VPN y así contrarrestar estos ataques.



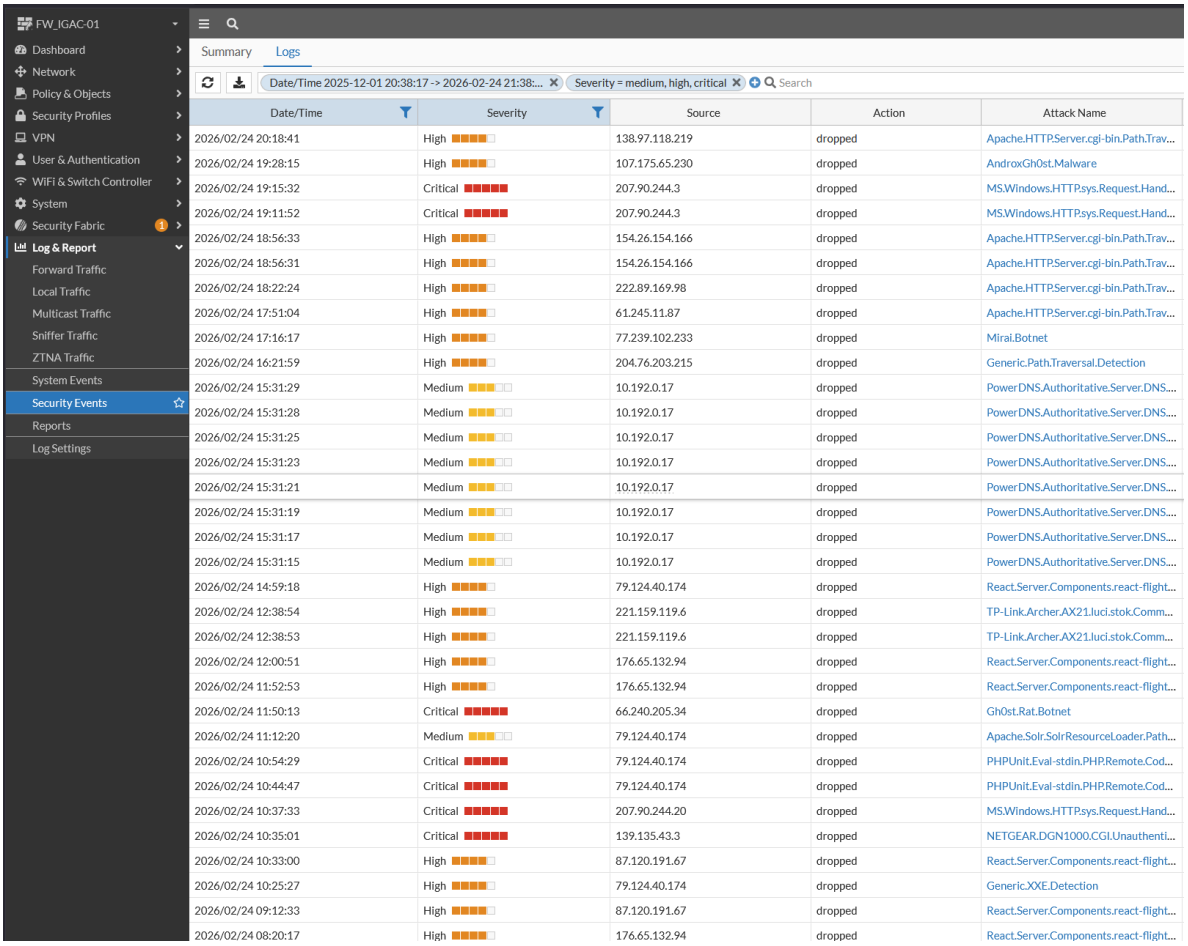
Se recomienda también la limitación geográfica para alcanzar este servicio, posiblemente que sea únicamente desde direcciones IP de Colombia.



A nivel general la postura de seguridad es buena sin embargo es prioritario cerrar la brecha de la VPN SSL bajo el "WEB Mode" y cerrar las políticas que aún faltan, aunque no son las más críticas si se les debe dar un manejo para que permitir que todo el trafico y todos los servicios puedan pasar sin ninguna restricción.

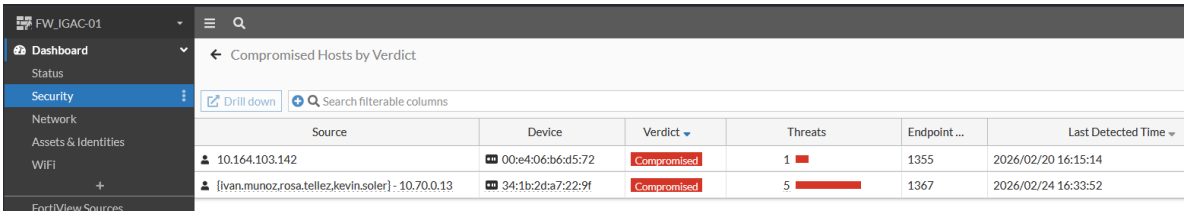
1.9.2 Intrusion Prevention:

En los últimos 3 meses se han identificado mas de 500 ataques de intrusión sin embargo todos fueron dropeados

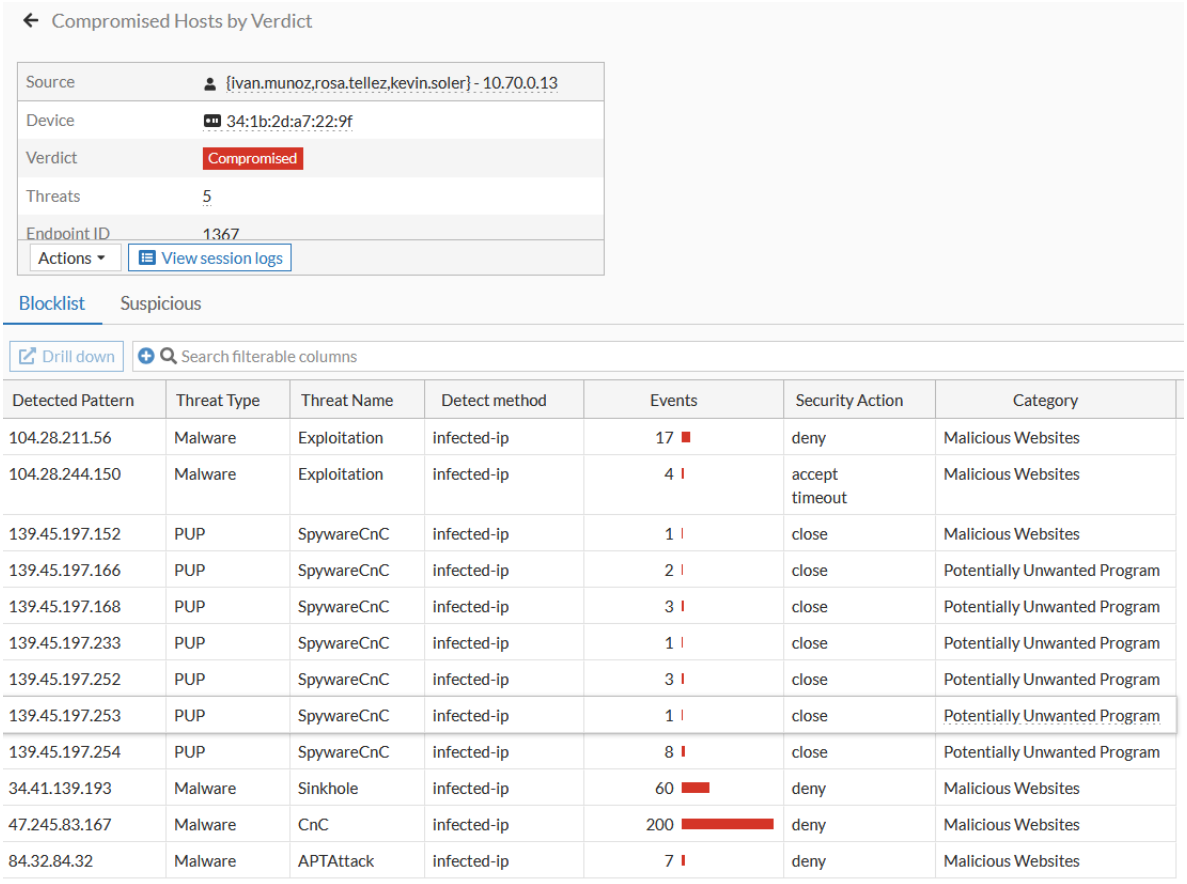


1.9.3 Equipos e IPs comprometidas:

En los últimos 7 días se han identificado dos dispositivos comprometidos



El sensor identificó que han visitado sitios categorizados como maliciosos y el equipo con IP 10.70.0.13 cuenta con un software potencialmente no deseado.



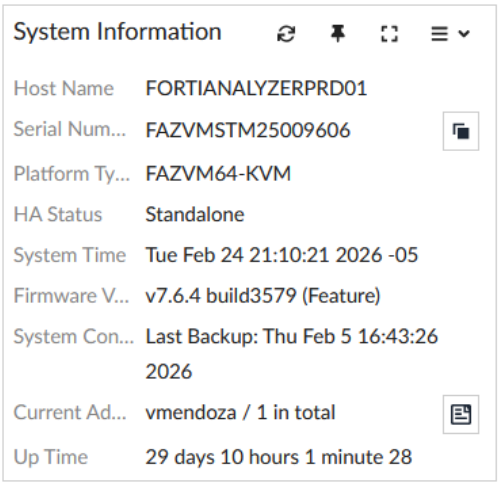
Detected Pattern	Threat Type	Threat Name	Detect method	Events	Security Action	Category
104.28.211.56	Malware	Exploitation	infected-ip	17	deny	Malicious Websites
104.28.244.150	Malware	Exploitation	infected-ip	4	accept timeout	Malicious Websites
139.45.197.152	PUP	SpywareCnC	infected-ip	1	close	Malicious Websites
139.45.197.166	PUP	SpywareCnC	infected-ip	2	close	Potentially Unwanted Program
139.45.197.168	PUP	SpywareCnC	infected-ip	3	close	Potentially Unwanted Program
139.45.197.233	PUP	SpywareCnC	infected-ip	1	close	Potentially Unwanted Program
139.45.197.252	PUP	SpywareCnC	infected-ip	3	close	Potentially Unwanted Program
139.45.197.253	PUP	SpywareCnC	infected-ip	1	close	Potentially Unwanted Program
139.45.197.254	PUP	SpywareCnC	infected-ip	8	close	Potentially Unwanted Program
34.41.139.193	Malware	Sinkhole	infected-ip	60	deny	Malicious Websites
47.245.83.167	Malware	CnC	infected-ip	200	deny	Malicious Websites
84.32.84.32	Malware	APTAttack	infected-ip	7	deny	Malicious Websites

2 FortiAnalyzer 400E

El equipo FortiAnalyzer a nivel general se encuentra bien configurado sin embargo es importante tener en cuenta los siguientes aspectos:

2.1 Firmware

El equipo se encuentra en la versión de Firmware 7.6.4, ya se encuentra disponible la versión 7.6.6 a la cual se recomienda subir ya que debemos garantizar la total compatibilidad con la versión del FortiGate 7.4.11 a la que se va a subir.

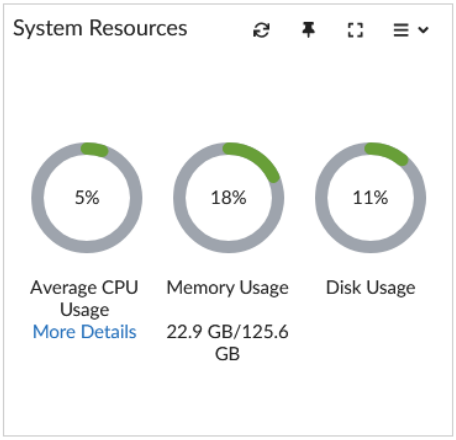


2.2 Dispositivos asociados

Se podrían agregar los dispositivos FortiGate/FortiWIFI remotos para tener de manera centralizada los logs de estos equipos y poder realizar análisis de los eventos que ocurren y que son identificados a través de ellos sin embargo es importante tener en cuenta que esto elevaría considerablemente el uso de almacenamiento lo que podría reducir considerablemente el tiempo de retención de logs de los equipos que ya se encuentran asociados.

2.3 Performance

El uso de recursos es bastante bajo en cuanto a RAM y CPU, ya a nivel de almacenamiento se están consumiendo el 51% de los logs, al agregar los equipos remotos se estaría consumiendo mas capacidad por ende habría que validar si se envían todos los logs o solamente los de seguridad para aquellas políticas importantes.

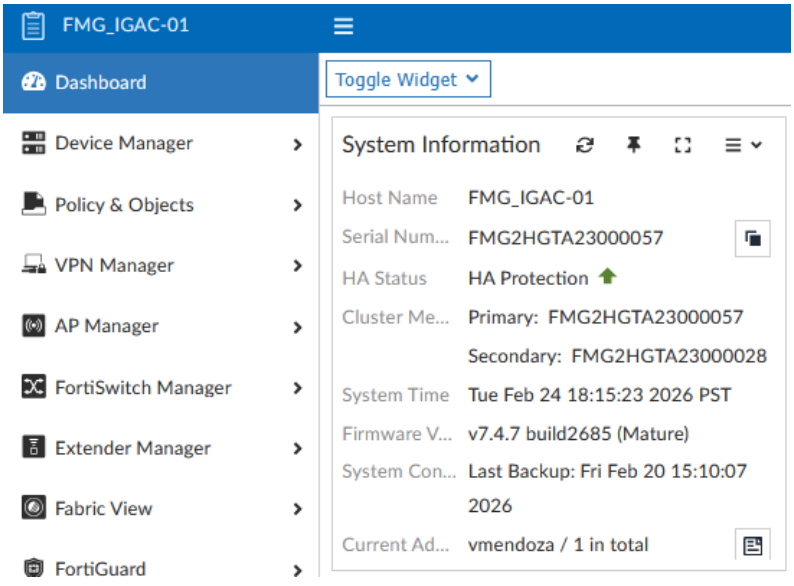


3 FortiManager 200G

El equipo FortiManager a nivel general se encuentra bien configurado sin embargo es importante tener en cuenta los siguientes aspectos:

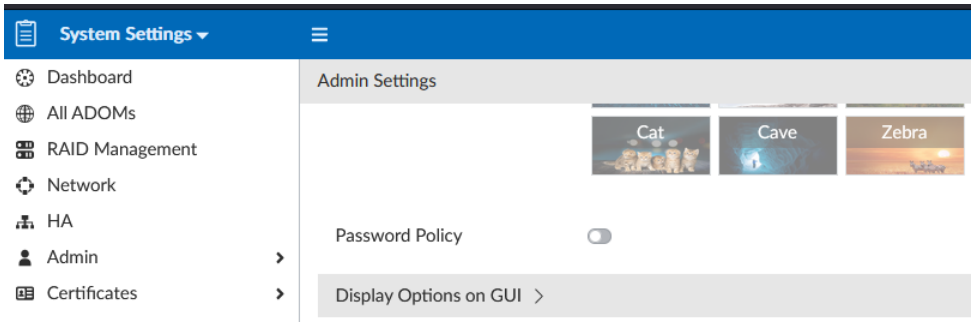
3.1 Firmware

El equipo se encuentra en la versión de Firmware 7.4.7, ya se encuentra disponible la versión 7.4.10 a la cual se recomienda subir ya que es más que obligatorio que el FortiManager que gestiona los FortiGate tenga completa compatibilidad con los equipos. Esta actualización de deberá realizar antes de actualizar los FortiGate.



3.2 Configuraciones generales

Teniendo en cuenta que este equipo administrara la configuración de los demás dispositivos de Fortinet, es muy importante habilitar la política de contraseñas para exigir características como tamaño mínimo, exigir caracteres especiales, tiempo de expiración de la contraseña y el evitar el reúso de contraseñas antiguas.



4 SDWAN

Se valida que todos los equipos de las sedes se encuentran operativos y funcionando correctamente, sin embargo, hay que tener en cuenta las siguientes consideraciones:

4.1 Firmware

14 equipos se encuentran en la versión de firmware 7.4.7 y se deberían actualizar a la versión 7.4.11 para quedar alineados con los demás equipos del ecosistema Fortinet.

SERIAL	NOMBRE EQUIPO	VERSION FIRMWARE
FWF61FTK20000780	FortiWiFi-61F-Armenia	7.4.7
FWF61FTK20000442	FortiWiFi-61F-Neiva	7.4.7
FWF61FTK20000181	FortiWiFi-61F-Barranquilla	7.4.7
FWF61FTK20000898	FortiWiFi-61F-Manizales	7.4.7
FWF61FTK20000502	FortiWiFi-61F-Pereira	7.4.7
FWF61FTK20000566	FortiWiFi-61F-Sta Marta	7.4.7
FWF61FTK20000509	FortiWiFi-61F-Cúcuta	7.4.7
FWF61FTK20000411	FortiWiFi-61F-Popayan	7.4.7
FWF61FTK20000950	FortiWiFi-61F-Monteria	7.4.7
FWF61FTK20000400	FortiWiFi-61F-Valledupar	7.4.7
FWF61FTK20000304	FortiWiFi-61F-Florencia	7.4.7
FWF61FTK20000904	FortiWiFi-61F-Bucaramanga	7.4.7
FGT90GTK24003020	FortiGate-90G-Cali	7.4.7
FGT90GTK24003626	FortiGate-90G-Villavicencio	7.4.7

4.2 Puertos de gestión

14 equipos tienen establecido el puerto de gestión 443 y los 7 restantes tienen el puerto 10443, se recomienda estandarizar este parámetro.

SERIAL	NOMBRE EQUIPO	Puert
FGT90GTK24009733	FortiGate-90G_Tunja	10443
FWF61FTK20000780	FortiWiFi-61F-Armenia	443
FWF61FTK20000442	FortiWiFi-61F-Neiva	443
FWF61FTK20000181	FortiWiFi-61F-Barranquilla	443
FWF61FTK20000898	FortiWiFi-61F-Manizales	443
FWF61FTK20000502	FortiWiFi-61F-Pereira	443
FGT90GTK24009993	FortiGate-90G-Cartagena	10443
FGT90GTK24009935	FortiGate-90G-Ibague	10443
FWF61FTK20000566	FortiWiFi-61F-Sta Marta	443
FWF61FTK20000509	FortiWiFi-61F-Cúcuta	443
FWF61FTK20000411	FortiWiFi-61F-Popayan	443
FWF61FTK20000950	FortiWiFi-61F-Monteria	443
FWF61FTK20000400	FortiWiFi-61F-Valledupar	443
FWF61FTK20000304	FortiWiFi-61F-Florencia	443
FGT90GTK24009753	FortiGate-90G_Pasto	10443
FWF61FTK20000904	FortiWiFi-61F-Bucaramanga	443
FGT90GTK24003020	FortiGate-90G-Cali	443
FGT90GTK24003626	FortiGate-90G-Villavicencio	443
FGT90GTK24009489	FortiGate-90G_Guajira	10443
FGT90GTK24009592	FortiGate-90G_Sincelejo	10443
FGT90GTK24009729	FortiGate-90G_Yopal	10443

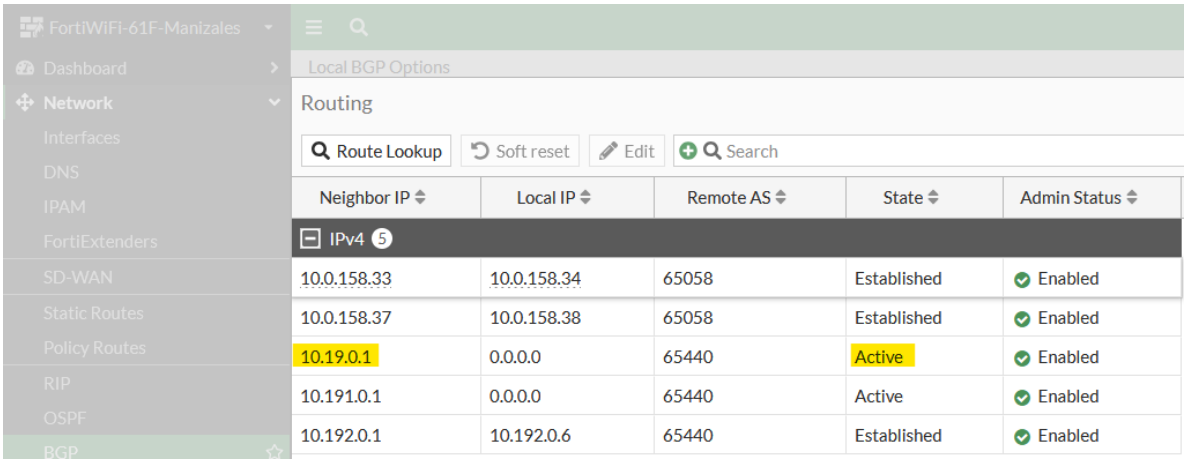
4.3 Consumo de RAM

Los equipos antiguos FortiWIFI 61F debido a la estricta configuración para validación del tráfico basada en perfiles de seguridad ha llevado a los equipos a consumir RAM por encima del 70% acercándose mucho al límite crítico de 75%, lo que puede ocasionar que el equipo se bloquee y no permita el flujo del tráfico, es importante evitar sobrecargarlos para no llevarlo al límite y evitar problemas de conectividad en las sedes. Se podrían mantener así como se encuentran a nivel de configuración, pero tener presente que agregar mas validaciones podría afectar la estabilidad del sistema.

SERIAL	NOMBRE EQUIPO	RAM
FGT90GTK24009733	FortiGate-90G_Tunja	30%
FWF61FTK20000780	FortiWiFi-61F-Armenia	69%
FWF61FTK20000442	FortiWiFi-61F-Neiva	72%
FWF61FTK20000181	FortiWiFi-61F-Barranquilla	72%
FWF61FTK20000898	FortiWiFi-61F-Manizales	71%
FWF61FTK20000502	FortiWiFi-61F-Pereira	70%
FGT90GTK24009993	FortiGate-90G-Cartagena	30%
FGT90GTK24009935	FortiGate-90G-Ibague	30%
FWF61FTK20000566	FortiWiFi-61F-Sta Marta	71%
FWF61FTK20000509	FortiWiFi-61F-Cúcuta	71%
FWF61FTK20000411	FortiWiFi-61F-Popayan	72%
FWF61FTK20000950	FortiWiFi-61F-Monteria	69%
FWF61FTK20000400	FortiWiFi-61F-Valledupar	71%
FWF61FTK20000304	FortiWiFi-61F-Florencia	72%
FGT90GTK24009753	FortiGate-90G_Pasto	30%
FWF61FTK20000904	FortiWiFi-61F-Bucaramanga	71%
FGT90GTK24003020	FortiGate-90G-Cali	26%
FGT90GTK24003626	FortiGate-90G-Villavicencio	26%
FGT90GTK24009489	FortiGate-90G_Guajira	29%
FGT90GTK24009592	FortiGate-90G_Sincelejo	30%
FGT90GTK24009729	FortiGate-90G_Yopal	30%

4.4 Conectividad con Sede y BGP

Todos los equipos tienen conectividad hacia la sede principal por el canal MPLS y la VPN sobre el canal de Internet y están enrutando el tráfico correctamente a excepción del equipo de Manizales que al parecer por motivo del ISP no tiene conexión por MPLS con la sede principal, por lo cual la comunicación se está realizando por el canal secundario conformado por la VPN IPSEC sobre el canal de Internet, se recomienda validar con el ISP.

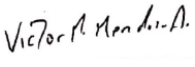


5 Aprobación

A continuación, se firma este documento como muestra de aceptación por parte del cliente que la información contenida en el mismo corresponde (informe).

En calidad de representantes autorizados por cada una de las partes y en acuerdo con todo lo descrito en este documento, Firman:

Por Instituto Geográfico Agustín Codazzi		
Nombre	**Firma**	**Fecha**

Por Heimcore		
Nombre	**Firma**	**Fecha**
Victor Manuel Mendoza Anaya		24/02/2026