



Servicio Gestionado de Conectividad y Seguridad – Colombia Más

Cliente: ALCALDIA PAIPA

Periodo Evaluado: 01 de mayo – 31 de mayo / 2026

Servicio: Internet Seguro Premium

Elaborado por: Colombia Más

1. Resumen

Durante el periodo evaluado, el servicio de **Internet Seguro** prestado por Colombia Más operó de manera **estable, controlada y segura**, garantizando la continuidad de las operaciones del cliente, el uso eficiente del ancho de banda y la protección frente a amenazas provenientes de internet.

El tráfico fue monitoreado permanentemente a través de la plataforma de seguridad **FortiGate**, permitiendo identificar patrones de consumo, priorizar aplicaciones críticas y bloquear amenazas de seguridad sin afectar la experiencia del usuario final.

2. Descripción del Servicio Internet Seguro

El servicio de Internet Seguro integra **conectividad de datos** con **seguridad perimetral avanzada**, permitiendo al cliente:

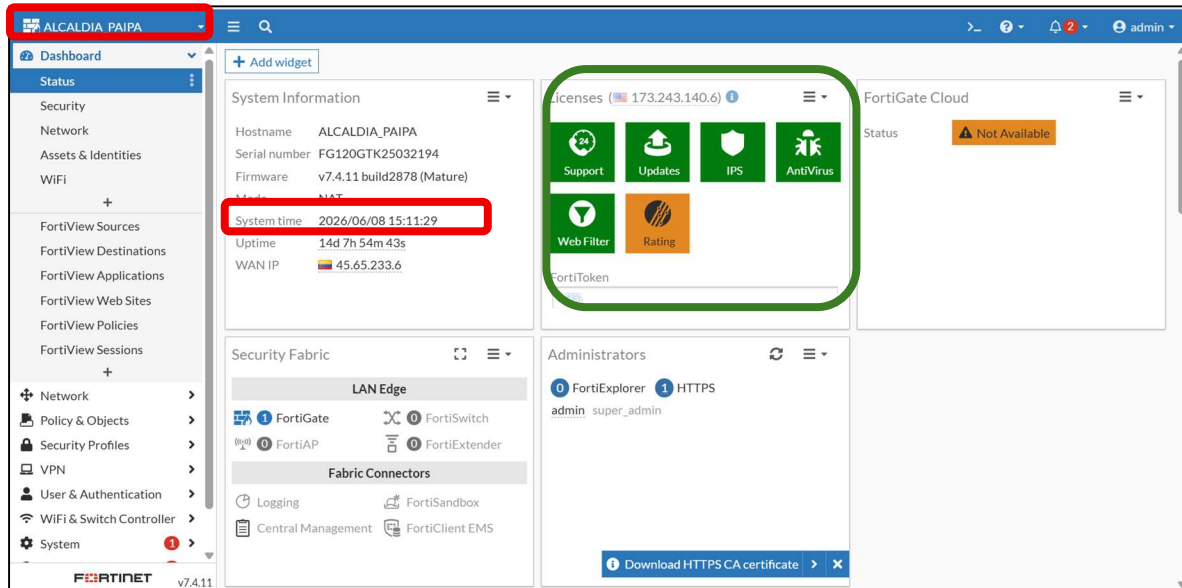
- Navegar de forma protegida
- Controlar el uso del ancho de banda
- Mitigar riesgos de ciberseguridad
- Obtener visibilidad real del tráfico de red

Componentes principales:

- Enlace de internet
- Firewall FortiGate
- Políticas de seguridad
- Monitoreo y reportes periódicos

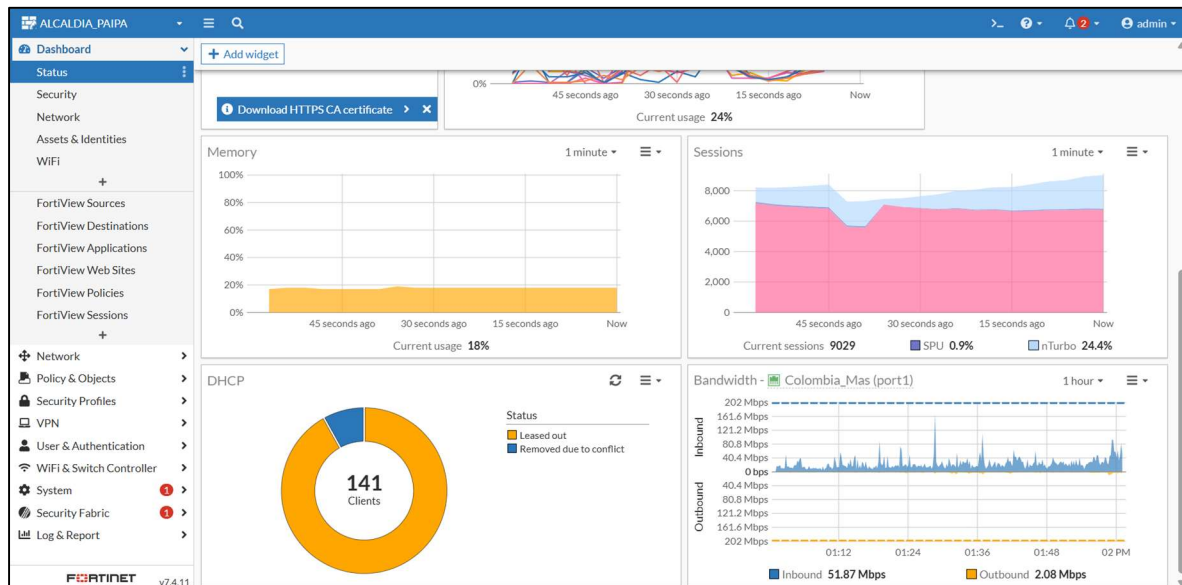


3. Estado General del Firewall FortiGate



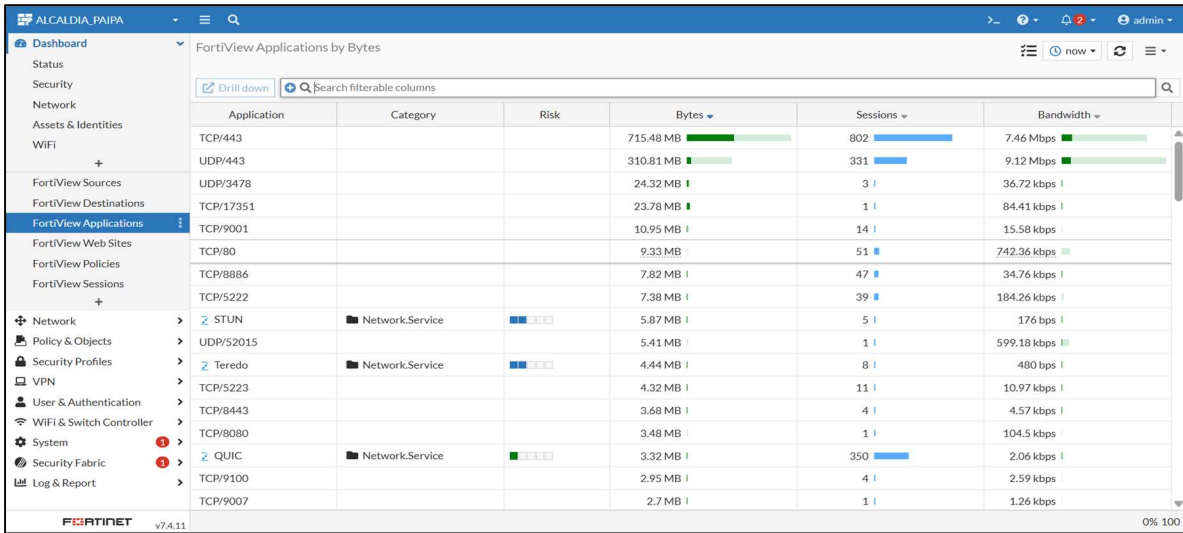
En la imagen anterior se evidencian aspectos generales del firewall instalado, como el nombre del host, serial del equipo, versión actual de firmware, fecha de vencimiento de licenciamiento, estado actual de CPU la cual es importante para establecer el desempeño de la red.

4. Consumo de Ancho de Banda, memoria y sesiones



Durante el monitoreo del tráfico de red realizado a través del firewall FortiGate, se identificaron la cantidad de recurso de memoria para el procesamiento de datos, la cantidad de sesiones en la red a nivel general de LAN y hacia internet, además de la cantidad de host en línea a través de sesiones de DHCP y un promedio de 1 hora de consumo de ancho de banda.

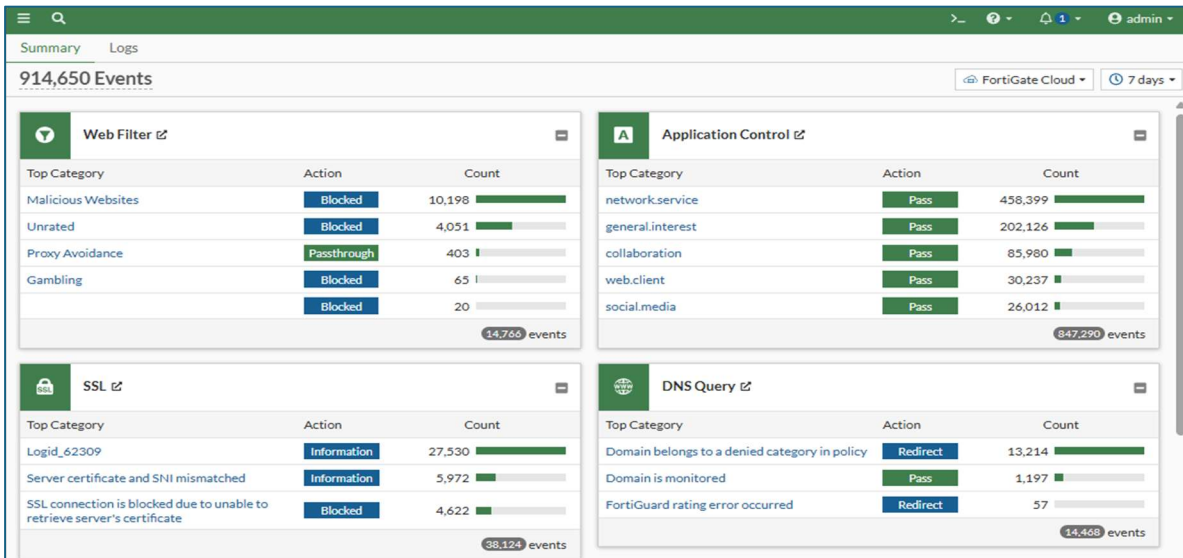
5. Aplicaciones con Mayor Consumo



Application	Category	Risk	Bytes	Sessions	Bandwidth
TCP/443			715.48 MB	802	7.46 Mbps
UDP/443			310.81 MB	331	9.12 Mbps
UDP/3478			24.32 MB	3	36.72 kbps
TCP/17351			23.78 MB	1	84.41 kbps
TCP/9001			10.95 MB	14	15.58 kbps
TCP/80			9.33 MB	51	742.36 kbps
TCP/8886			7.82 MB	47	34.76 kbps
TCP/5222			7.38 MB	39	184.26 kbps
TCP/STUN	Network.Service		5.87 MB	5	176 bps
UDP/52015			5.41 MB	1	599.18 kbps
TCP/Teredo	Network.Service		4.44 MB	8	480 bps
TCP/5223			4.32 MB	11	10.97 kbps
TCP/8443			3.68 MB	4	4.57 kbps
TCP/8080			3.48 MB	1	104.5 kbps
TCP/QUIC	Network.Service		3.32 MB	350	2.06 kbps
TCP/9100			2.95 MB	4	2.59 kbps
TCP/9007			2.7 MB	1	1.26 kbps

Durante el monitoreo del tráfico de red realizado a través del firewall FortiGate, se identificaron las aplicaciones que generan mayor consumo de ancho de banda dentro de la red. El análisis permitió determinar qué servicios y plataformas concentran la mayor cantidad de tráfico

6. Seguridad: Amenazas Detectadas y Bloqueadas



Top Category	Action	Count
Malicious Websites	Blocked	10,198
Unrated	Blocked	4,051
Proxy Avoidance	Passthrough	403
Gambling	Blocked	65
	Blocked	20
14,766 events		

Top Category	Action	Count
network.service	Pass	458,399
general.interest	Pass	202,126
collaboration	Pass	85,980
web.client	Pass	30,237
social.media	Pass	26,012
847,290 events		

Top Category	Action	Count
Logid_62309	Information	27,530
Server certificate and SNI mismatched	Information	5,972
SSL connection is blocked due to unable to retrieve server's certificate	Blocked	4,622
38,124 events		

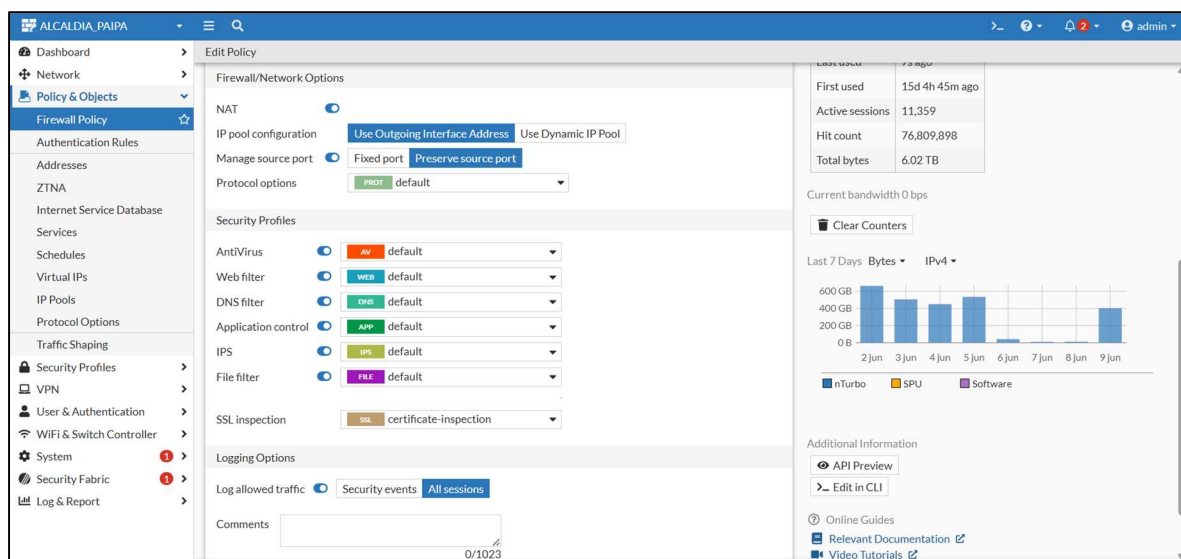
Top Category	Action	Count
Domain belongs to a denied category in policy	Redirect	13,214
Domain is monitored	Pass	1,197
FortiGuard rating error occurred	Redirect	57
14,468 events		

7. Políticas de Seguridad Aplicadas

El servicio de Internet Seguro cuenta con:

- Políticas de firewall activas y actualizadas
- Perfiles de seguridad habilitados:
 - Antivirus
 - Filtrado web
 - Control de aplicaciones
 - Prevención de intrusiones (IPS)

Estas políticas están aplicadas a nivel de WAN, prueba de ello:



Estas políticas garantizan un equilibrio entre **seguridad y rendimiento**.

Como resultado de estas reglas encontramos:

Durante el monitoreo de navegación web mediante el módulo de Web Filter del firewall FortiGate, se identificaron las categorías de sitios más consultadas por los usuarios. Este análisis permite determinar los patrones de navegación dentro de la red y aplicar políticas de control que garanticen un acceso seguro y acorde con las políticas de uso establecidas por la organización.

ALCALDIA PAIPA

Summary Logs

Search Web Filter Memory Details

Date/Time	User	Source	Action	URL	Category	Initiator	Sent / Received
2026/06/09 12:03:56		172.30.2.164	Blocked	http://208.91.112.55/service/tr069servlet			145 B / 0 B
2026/06/09 12:03:56		172.30.2.230	Blocked	http://qup.f360.cn/cloudquery.php			2.07 kB / 0 B
2026/06/09 12:03:56		172.30.2.22	Blocked	http://detectportal.firefox.com/canonical.html			324 B / 0 B
2026/06/09 12:03:56		172.30.2.77	Blocked	https://logs.ads.vungle.com/			517 B / 0 B
2026/06/09 12:03:56		172.30.2.96	Blocked	http://detectportal.firefox.com/success.txt?ipv4			341 B / 0 B
2026/06/09 12:03:56		172.30.2.230	Blocked	http://qup.f360.cn/cloudquery.php			1.99 kB / 0 B
2026/06/09 12:03:56		172.30.2.85	Blocked	http://detectportal.firefox.com/canonical.html			324 B / 0 B
2026/06/09 12:03:56		172.30.2.85	Blocked	http://detectportal.firefox.com/canonical.html			324 B / 0 B
2026/06/09 12:03:56		172.30.7.12	Blocked	http://www.msftncsl.com/connecttest.txt			147 B / 0 B
2026/06/09 12:03:56		172.30.2.162	Blocked	https://clients2.google.com/			1.82 kB / 0 B
2026/06/09 12:03:56		172.30.2.162	Blocked	https://beacons2.gvt2.com/			1.76 kB / 0 B
2026/06/09 12:03:56		172.30.2.162	Blocked	https://beacons3.gvt2.com/			1.76 kB / 0 B
2026/06/09 12:03:56		172.30.2.77	Blocked	https://media-bog2-2.cdn.whatsapp.net/			1.81 kB / 0 B
2026/06/09 12:03:56		172.30.7.9	Blocked	http://s.cloud.360safe.com/scan			556 B / 0 B
2026/06/09 12:03:56		172.30.2.77	Blocked	https://mmg.whatsapp.net/			1.79 kB / 0 B
2026/06/09 12:03:56		172.30.2.77	Blocked	https://logs.ads.vungle.com/			517 B / 0 B
2026/06/09 12:03:56		172.30.7.12	Blocked	https://ssl.gstatic.com/			1.76 kB / 0 B
2026/06/09 12:03:56		172.30.2.162	Blocked	https://beacons2.gvt2.com/			1.76 kB / 0 B

FortiGate v7.4.11 0% 500+

A través de la inspección y validación de certificados SSL realizada por el firewall FortiGate, se verificó la autenticidad y confiabilidad de las conexiones seguras establecidas por los usuarios. Este proceso permite identificar certificados inválidos, expirados o potencialmente riesgosos, contribuyendo a fortalecer la seguridad de las comunicaciones cifradas dentro de la red.

ALCALDIA PAIPA

Summary Logs

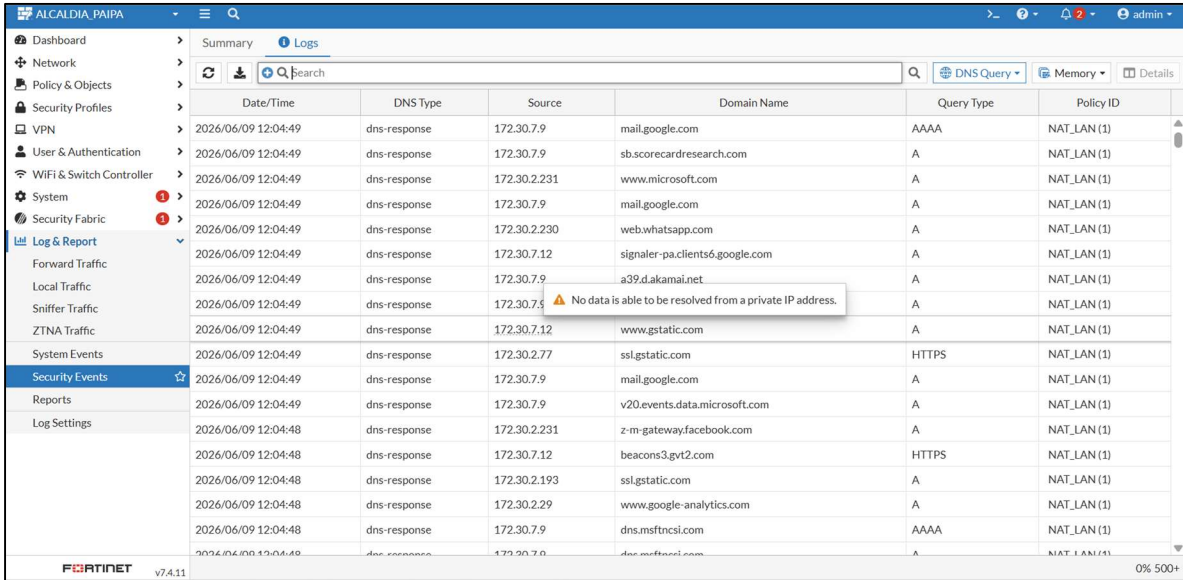
Search SSL Memory Details

Date/Time	Action	Service	Source	Source Interface	Destination	Destination Interface
2026/06/09 12:04:27	Information	SSL	172.30.2.70	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.245	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.245	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.147	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.77	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.49	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.85	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.49	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.19	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.245	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.49	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.7.10	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.85	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.85	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.7.12	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.7.12	LAN (lan)	208.91.112.55	Colombia_Mas (port1)
2026/06/09 12:04:27	Information	SSL	172.30.2.85	LAN (lan)	208.91.112.55	Colombia_Mas (port1)

FortiGate v7.4.11 0% 500+

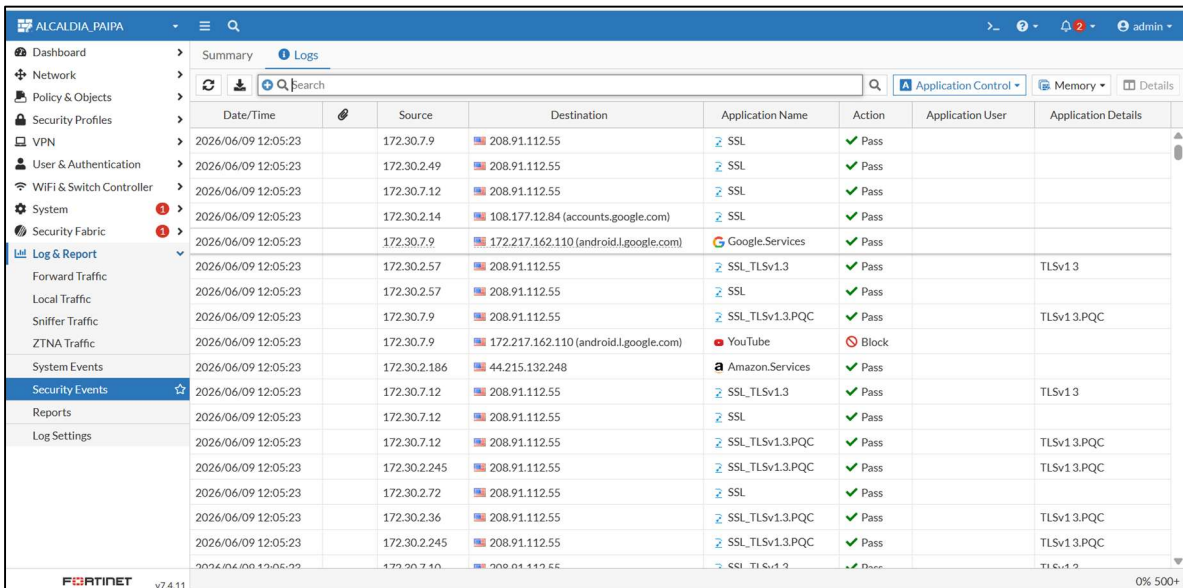
Mediante el análisis de consultas DNS registradas por el firewall FortiGate, se identificaron los dominios más consultados por los dispositivos de la red. Este monitoreo permite detectar

comportamientos anómalos, accesos a dominios potencialmente maliciosos y comprender los patrones de resolución de nombres utilizados por los usuarios y aplicaciones.



Date/Time	DNS Type	Source	Domain Name	Query Type	Policy ID
2026/06/09 12:04:49	dns-response	172.30.7.9	mail.google.com	AAAA	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.9	sb.scorecardresearch.com	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.2.231	www.microsoft.com	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.9	mail.google.com	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.2.230	web.whatsapp.com	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.12	signaler-pa.clients6.google.com	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.9	a39.d.akamai.net	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.9	No data is able to be resolved from a private IP address.	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.12	www.gstatic.com	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.2.77	ssl.gstatic.com	HTTPS	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.9	mail.google.com	A	NAT_LAN (1)
2026/06/09 12:04:49	dns-response	172.30.7.9	v20.events.data.microsoft.com	A	NAT_LAN (1)
2026/06/09 12:04:48	dns-response	172.30.2.231	z-m-gateway.facebook.com	A	NAT_LAN (1)
2026/06/09 12:04:48	dns-response	172.30.7.12	beacons3.gvt2.com	HTTPS	NAT_LAN (1)
2026/06/09 12:04:48	dns-response	172.30.2.193	ssl.gstatic.com	A	NAT_LAN (1)
2026/06/09 12:04:48	dns-response	172.30.2.29	www.google-analytics.com	A	NAT_LAN (1)
2026/06/09 12:04:48	dns-response	172.30.7.9	dns.msftncsl.com	AAAA	NAT_LAN (1)

El análisis realizado mediante el módulo de Application Control del firewall FortiGate permitió identificar las aplicaciones utilizadas dentro de la red y su nivel de consumo de recursos. Esta información facilita la implementación de políticas de control y priorización del tráfico, contribuyendo a optimizar el rendimiento de la red y mejorar la seguridad al limitar el uso de aplicaciones no autorizadas.



Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
2026/06/09 12:05:23	172.30.7.9	208.91.112.55	SSL	✓ Pass		
2026/06/09 12:05:23	172.30.2.49	208.91.112.55	SSL	✓ Pass		
2026/06/09 12:05:23	172.30.7.12	208.91.112.55	SSL	✓ Pass		
2026/06/09 12:05:23	172.30.2.14	108.177.12.84 (accounts.google.com)	SSL	✓ Pass		
2026/06/09 12:05:23	172.30.7.9	172.217.162.110 (android.l.google.com)	Google.Services	✓ Pass		
2026/06/09 12:05:23	172.30.2.57	208.91.112.55	SSL_TLSv1.3	✓ Pass		TLSv1.3
2026/06/09 12:05:23	172.30.2.57	208.91.112.55	SSL	✓ Pass		
2026/06/09 12:05:23	172.30.7.9	208.91.112.55	SSL_TLSv1.3.PQC	✓ Pass		TLSv1.3.PQC
2026/06/09 12:05:23	172.30.7.9	172.217.162.110 (android.l.google.com)	YouTube	✗ Block		
2026/06/09 12:05:23	172.30.2.186	44.215.132.248	Amazon.Services	✓ Pass		
2026/06/09 12:05:23	172.30.7.12	208.91.112.55	SSL_TLSv1.3	✓ Pass		TLSv1.3
2026/06/09 12:05:23	172.30.7.12	208.91.112.55	SSL	✓ Pass		
2026/06/09 12:05:23	172.30.7.12	208.91.112.55	SSL_TLSv1.3.PQC	✓ Pass		TLSv1.3.PQC
2026/06/09 12:05:23	172.30.2.245	208.91.112.55	SSL_TLSv1.3.PQC	✓ Pass		TLSv1.3.PQC
2026/06/09 12:05:23	172.30.2.72	208.91.112.55	SSL	✓ Pass		
2026/06/09 12:05:23	172.30.2.36	208.91.112.55	SSL_TLSv1.3.PQC	✓ Pass		TLSv1.3.PQC
2026/06/09 12:05:23	172.30.2.245	208.91.112.55	SSL_TLSv1.3.PQC	✓ Pass		TLSv1.3.PQC



Adicionalmente se realiza un registro de todos los cambios realizados a manera general de entidad para tener un registro y control de cambios en el equipo.

Date/Time	Level	User	Message	Log Description
2026/06/09 12:05:55	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:05:44	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:05:35	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:05:24	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:05:14	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:05:04	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:04:54	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:04:44	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:04:34	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:04:25	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:04:15	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:04:05	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:03:54	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:03:44	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:03:35	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:03:25	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:03:14	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable
2026/06/09 12:03:04	Error		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable

Cordialmente,

ERIN SANTOS

Ing. Erin Santos
Ingeniero Colombia Mas