



# ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

## EQUIPO DE SEGURIDAD PERIMETAL

**2022**



## Contenido

FortiGate .....	3
Equipo de Seguridad Perimetral .....	4
Controles Aplicados.....	5
Antivirus .....	5
Web Filter.....	5
Controles Aplicados de Web Filter .....	6
Categoría de Web Filter .....	7
Control de Aplicaciones.....	8
Prevención de Intrusos.....	8



## FortiGate

FortiGate proporciona una convergencia perfecta que se puede escalar a cualquier ubicación: oficina remota, sucursal, campus, centro de datos y nube. Siempre hemos cumplido con el concepto de firewalls de malla híbrida con FortiManager para una administración unificada y una seguridad consistente en entornos híbridos complejos. El sistema operativo FortiOS de Fortinet proporciona visibilidad y seguridad profundas en una variedad de factores de forma.

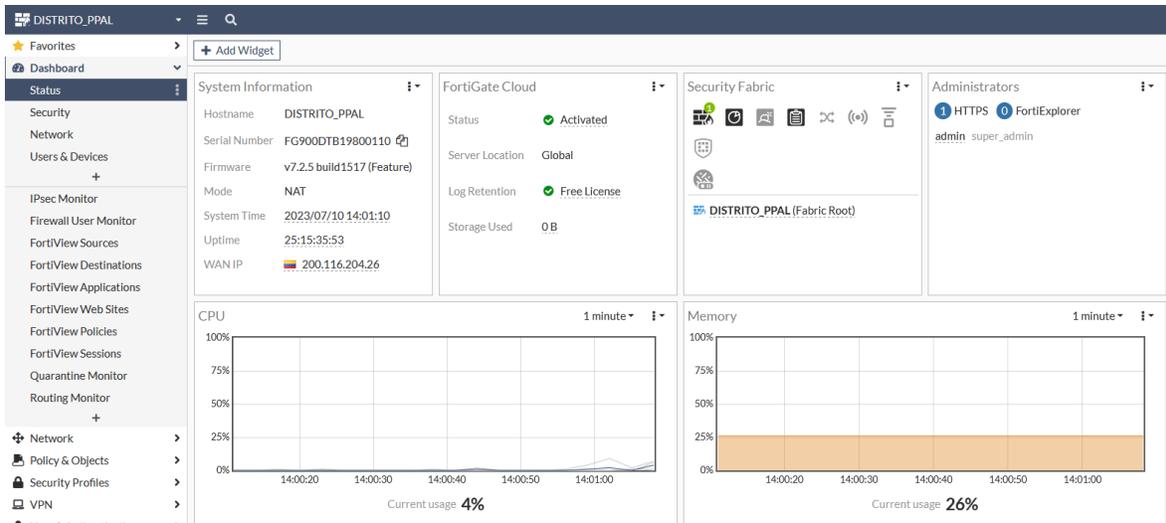
Los FortiGate NGFW proporcionan protección contra amenazas y descifrados líderes en la industria a escala con una arquitectura ASIC personalizada. También ofrecen redes seguras con funciones integradas como SD-WAN, conmutación e inalámbrica, y 5G. Haga converger sus soluciones de seguridad y punto de red en una consola de administración centralizada y fácil de usar potenciada por un único sistema operativo, FortiOS, y facilite la administración de TI.

Actualmente la entidad cuenta con firewall de la serie 900D para protección perimetral con licenciamiento de tipo UTP el cual tiene módulos de protección como:

- Web filtering
- DNS
- Anti-Spam
- IPS
- Application Control.



# Equipo de Seguridad Perimetral



Dashboard Firewall

License Information 2

Entitlement	Status	Actions
FortiCare Support	<span style="color: green;">✔</span> Registered	Actions
Firmware & General Updates	<span style="color: orange;">⚠</span> Expires Soon (Expiration Date: 2023/02/07)	Renew
Intrusion Prevention	<span style="color: orange;">⚠</span> Expires Soon (Expiration Date: 2023/02/07)	Renew
AntiVirus	<span style="color: orange;">⚠</span> Expires Soon (Expiration Date: 2023/02/07)	Renew
Web Filtering	<span style="color: orange;">⚠</span> Expires Soon (Expiration Date: 2023/02/07)	Renew
Email Filtering	<span style="color: orange;">⚠</span> Expires Soon (Expiration Date: 2023/02/07)	Renew
Outbreak Prevention	<span style="color: orange;">⚠</span> Expires Soon (Expiration Date: 2023/02/07)	Renew

Expiración de Licenciamiento



## Controles Aplicados

### Antivirus

Edit AntiVirus Profile

Name	AV_PROT_GRAL
Comments	Scan files and block viruses. 29/255
AntiVirus scan	<input checked="" type="checkbox"/> Block <input type="checkbox"/> Monitor
Feature set	<input type="checkbox"/> Flow-based <input checked="" type="checkbox"/> Proxy-based

Inspected Protocols

HTTP	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input checked="" type="checkbox"/>
MAPI	<input checked="" type="checkbox"/>
SSH	<input type="checkbox"/>

APT Protection Options

Content Disarm and Reconstruction	<input type="checkbox"/>
Treat Windows executables in email attachments as viruses	<input checked="" type="checkbox"/>
Include mobile malware protection	<input checked="" type="checkbox"/>
Quarantine	<input type="checkbox"/>

Virus Outbreak Prevention

Use FortiGuard outbreak prevention database	<input checked="" type="checkbox"/> Block <input type="checkbox"/> Monitor
Use external malware block list	<input type="checkbox"/>
Use EMS threat feed	<input type="checkbox"/>

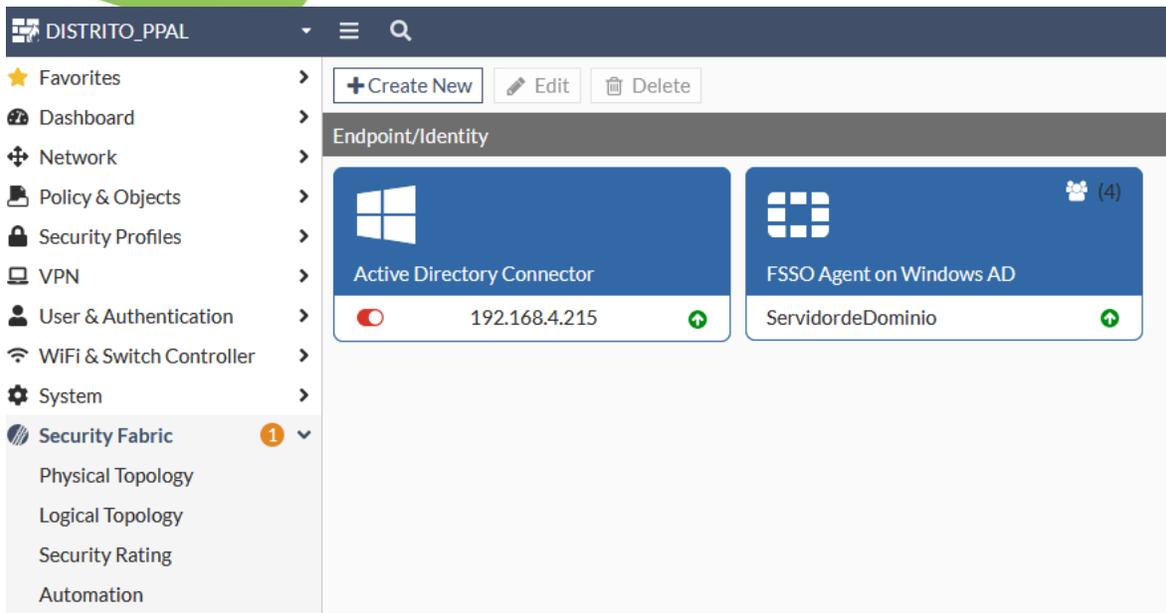
Aplicado sobre archivos descargado en la red

### Web Filter

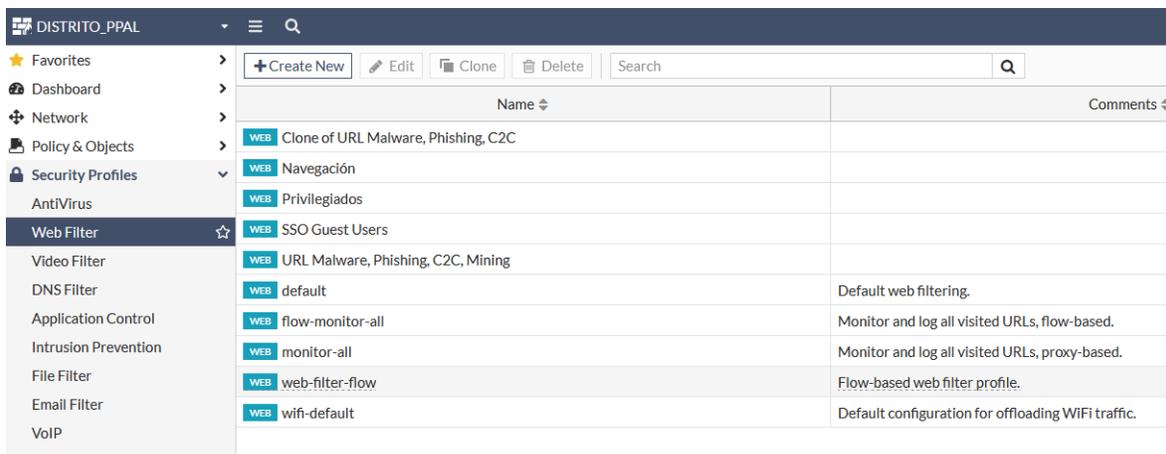
Existen 4 perfiles de navegación lo cuales son establecidos por el directorio

Conector FSSO

A continuación de detallan los grupos con distintos permisos de acceso para la navegación interna de los usuarios en la entidad



## Controles Aplicados de Web Filter



## Grupos de Web Filter

Para mas detalles de las categorías manejada por FortiGate para la protección y prevención de acceso a paginas potencialmente peligros podemos consultar su base de conocimiento en <https://www.fortiguard.com/webfilter/categories>



### Categoría de Web-Filter

- Potentially Liable:
- Drug Abuse
- Hacking
- Illegal or Unethical
- Discrimination
- Explicit Violence
- Extremist Groups
- Proxy Avoidance
- Plagiarism
- Child Abuse
- Adult/Mature Content:
- Alternative Beliefs
- Abortion
- Other Adult Materials
- Advocacy Organizations
- Gambling
- Nudity and Risque
- Pornography
- Dating
- Weapons (Sales)
- Marijuana
- Sex Education

Edit Web Filter Profile

Name: WCF\_NVA\_GRAL

Comments: Write a comment... 0/255

Feature set: Flow-based Proxy-based

FortiGuard Category Based Filter

Allow Monitor Block Warning Authenticate

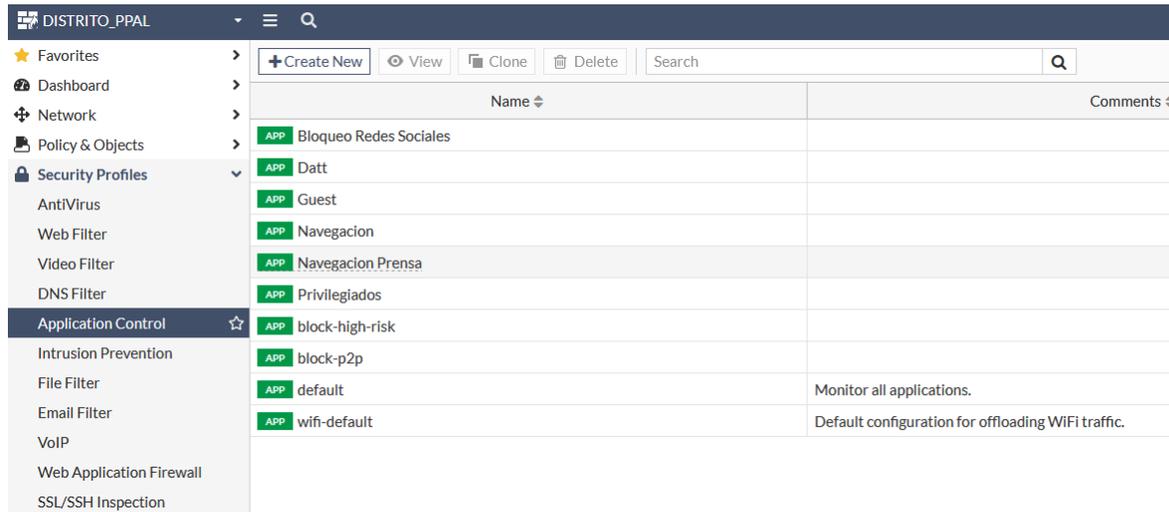
Name	Action
+ Potentially Liable 12	
+ Adult/Mature Content 15	
+ Bandwidth Consuming 6	
+ Security Risk 6	
+ General Interest - Personal 35	
+ General Interest - Business 16	
- Unrated 1	
Unrated	Allow

91

### Detalles Aplicado para la navegación general



## Control de Aplicaciones



The screenshot shows the Fortinet configuration interface for Application Control. The left sidebar lists various security features, with 'Application Control' selected. The main area displays a table of application control profiles.

Name	Comments
APP Bloqueo Redes Sociales	
APP Datt	
APP Guest	
APP Navegacion	
APP Navegacion Prensa	
APP Privilegiados	
APP block-high-risk	
APP block-p2p	
APP default	Monitor all applications.
APP wifi-default	Default configuration for offloading WiFi traffic.

## Control de Aplicaciones

## Prevención de Intrusos

A continuación se describe los controles aplicados para la navegación y protección hacia los clientes (PCs) en donde se bloquean más de 3150 IP maliciosas registradas en el FortiGuard de Fortinet



DISTRITO\_PPAL

- ★ Favorites
- Dashboard
- Network
- Policy & Objects
- Security Profiles
  - AntiVirus
  - Web Filter
  - Video Filter
  - DNS Filter
  - Application Control
  - Intrusion Prevention**
  - File Filter
  - Email Filter
  - VoIP
  - Web Application Firewall
  - SSL/SSH Inspection
  - Application Signatures
  - IPS Signatures

### Edit IPS Sensor

Name: PCs-Alcaldia

Comments: Write a comment... 0/255

Block malicious URLs

#### IPS Signatures and Filters

[+ Create New](#) [Edit](#) [Delete](#)

Details	Exempt IPs	Action	Packet Logging
TGT Client SEV <span style="color: yellow;">■</span> <span style="color: orange;">■</span> <span style="color: red;">■</span> SEV <span style="color: yellow;">■</span> <span style="color: orange;">■</span> <span style="color: red;">■</span> SEV <span style="color: red;">■</span> <span style="color: red;">■</span> <span style="color: red;">■</span> <a href="#">+2</a>		<input type="checkbox"/> Default	<input checked="" type="checkbox"/> Disabled

1

#### Botnet C&C

Scan Outgoing Connections to Botnet Sites

## Prevención de intrusos



### Add Signatures

Type: **Filter** Signature

Action: Default

Packet logging:  Enable  Disable

Status:  Enable  Disable  Default

Filter

- TGT Client
- SEV
- SEV
- SEV
- OS Linux
- OS MacOS
- OS Windows

Search

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 3,510					
2Wire.Wireless.Router.XSRF.Password.Reset	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Server Client	Linux	<input checked="" type="checkbox"/> Block	CVE-2007-4387
3ivx.MPEG4.File.Processing.Buffer.Overflow	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Client	Windows	<input checked="" type="checkbox"/> Block	CVE-2007-6401
7-Zip.RAR.Solid.Compression.Remote.Code.E...	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Server Client	Windows	<input checked="" type="checkbox"/> Block	CVE-2018-10115
A32S.Botnet	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Server Client	All	<input checked="" type="checkbox"/> Block	
AARC.Botnet	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Client	All	<input checked="" type="checkbox"/> Block	
ABBS.Audio.Media.Player.LST.Buffer.Overflow	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Server Client	Windows	<input checked="" type="checkbox"/> Block	
AOL.Desktop.RTX.Buffer.Overflow	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Client	Windows	<input checked="" type="checkbox"/> Block	
AOL.ICQ.ActiveX.Control.Remote.Code.Execu...	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Client	Windows	<input checked="" type="checkbox"/> Block	CVE-2006-5650
AOL.IWinAmpActiveX.Class.ConvertFile.Buff...	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Client	Windows	<input checked="" type="checkbox"/> Block	

0% 3,510

Return

### Firmas y filtros IPS