

Firewall

Es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

El objetivo principal de los firewalls es controlar el tráfico de red y filtrar los paquetes de datos que entran y salen de una red. Esto ayuda a prevenir ataques cibernéticos y proteger la información confidencial.



Los orígenes del firewall se remontan a la década de los 80's, poco después de la aparición de Internet con la finalidad de proteger los datos de los usuarios.

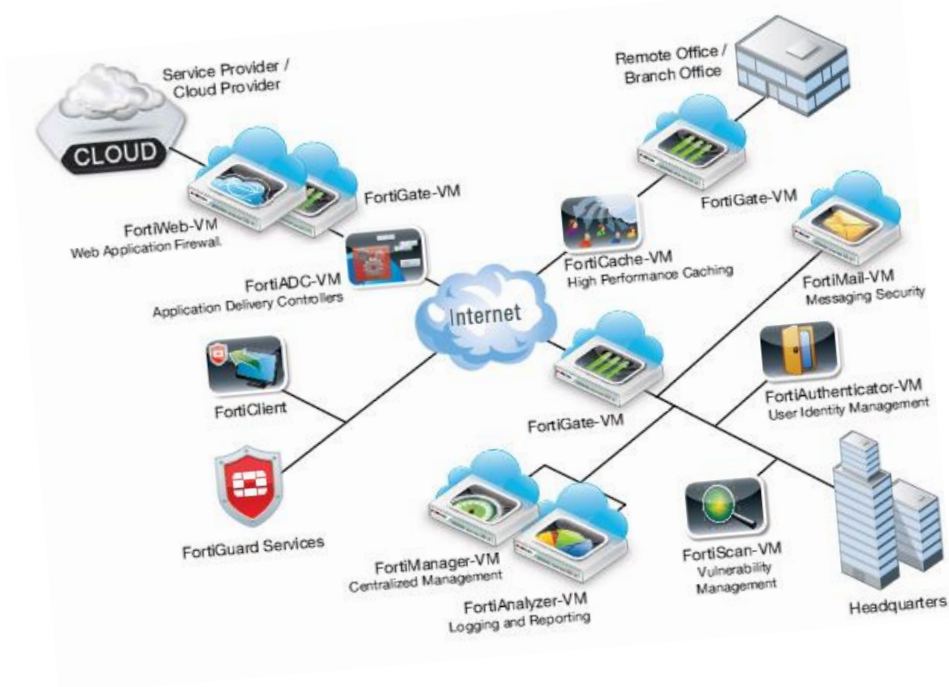
En 1989, Jeff Mogul de Digital Equipment Corp (DEC) propuso la primera versión de un firewall o filtro de paquetes. Esta propuesta sentó las bases para el desarrollo posterior de los firewalls.



Fortinet



Fue fundada en el año 2000 por Ken Xie, anterior presidente y Director Ejecutivo de NetScreen, partiendo de la idea de que los firewalls y las VPNs por si mismas no serían capaces de parar los ataques de nueva generación procedentes de Internet y dirigidos a contenidos y aplicaciones



Fortinet ofrece una serie de productos y servicios de ciberseguridad para ayudar a las organizaciones a proteger sus redes, puntos finales e infraestructura en la nube de amenazas avanzadas como malware, ransomware y ataques de phishing



Administración unificada de amenazas

Fortinet es considerado como pionero en el concepto de Administración unificada de amenazas (UTM), que unificó estas funciones en appliances únicos y altamente funcionales.



FortiGuard

Servicios e Investigación propios

Fortinet es el único proveedor de seguridad de red que cuenta con un equipo global de investigación y respuesta que monitoriza, de forma constante, el panorama de amenazas y proporciona a los clientes una protección en tiempo real frente a las últimas amenazas de Internet.

Los servicios de FortiGuard han sido diseñados para optimizar y maximizar la protección en la amplia gama de plataformas de seguridad de Fortinet. (IA y ML)



FortiGate



Chasis FG5000



FG3000



NGFW



UTM



FG200F



FORTISWITCH



FORTIAP



FORTIWiFi



FORTIWEB



FORTIMAIL



FORTIMANAGER



FORTIANALYZER

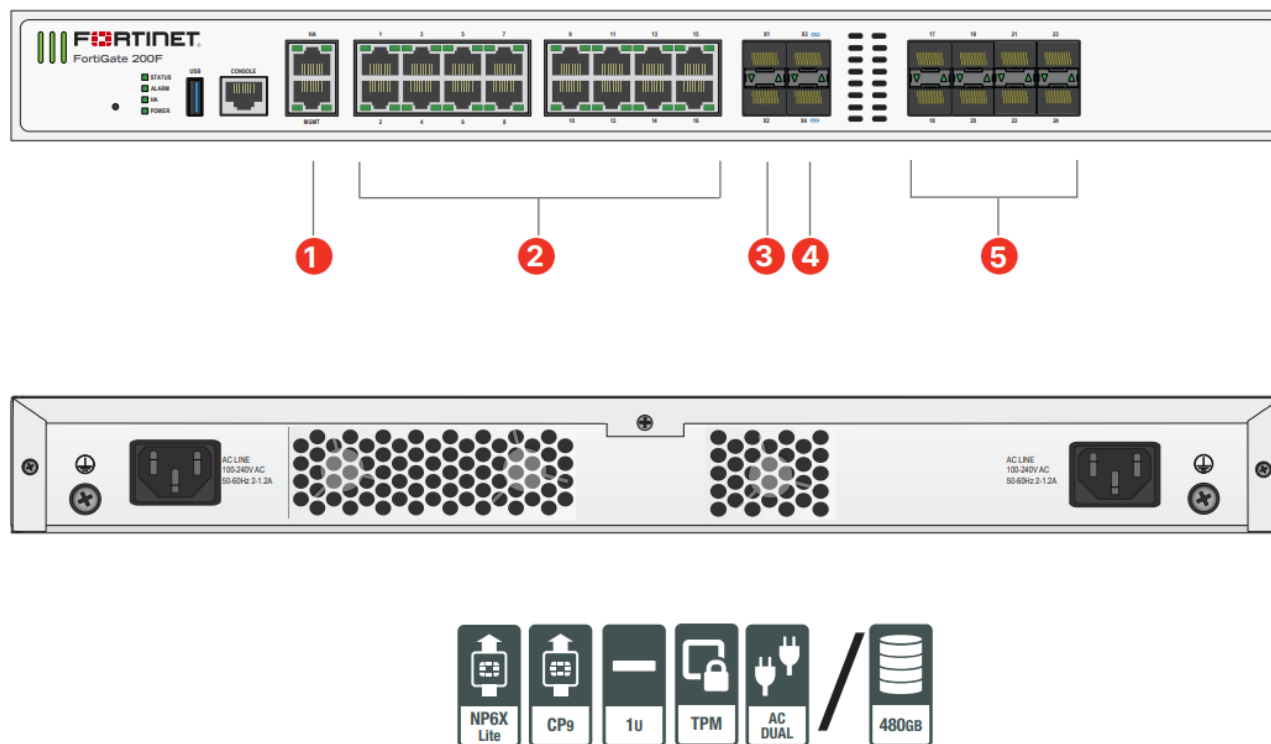


FortiGate



Hardware

FortiGate 200F Series



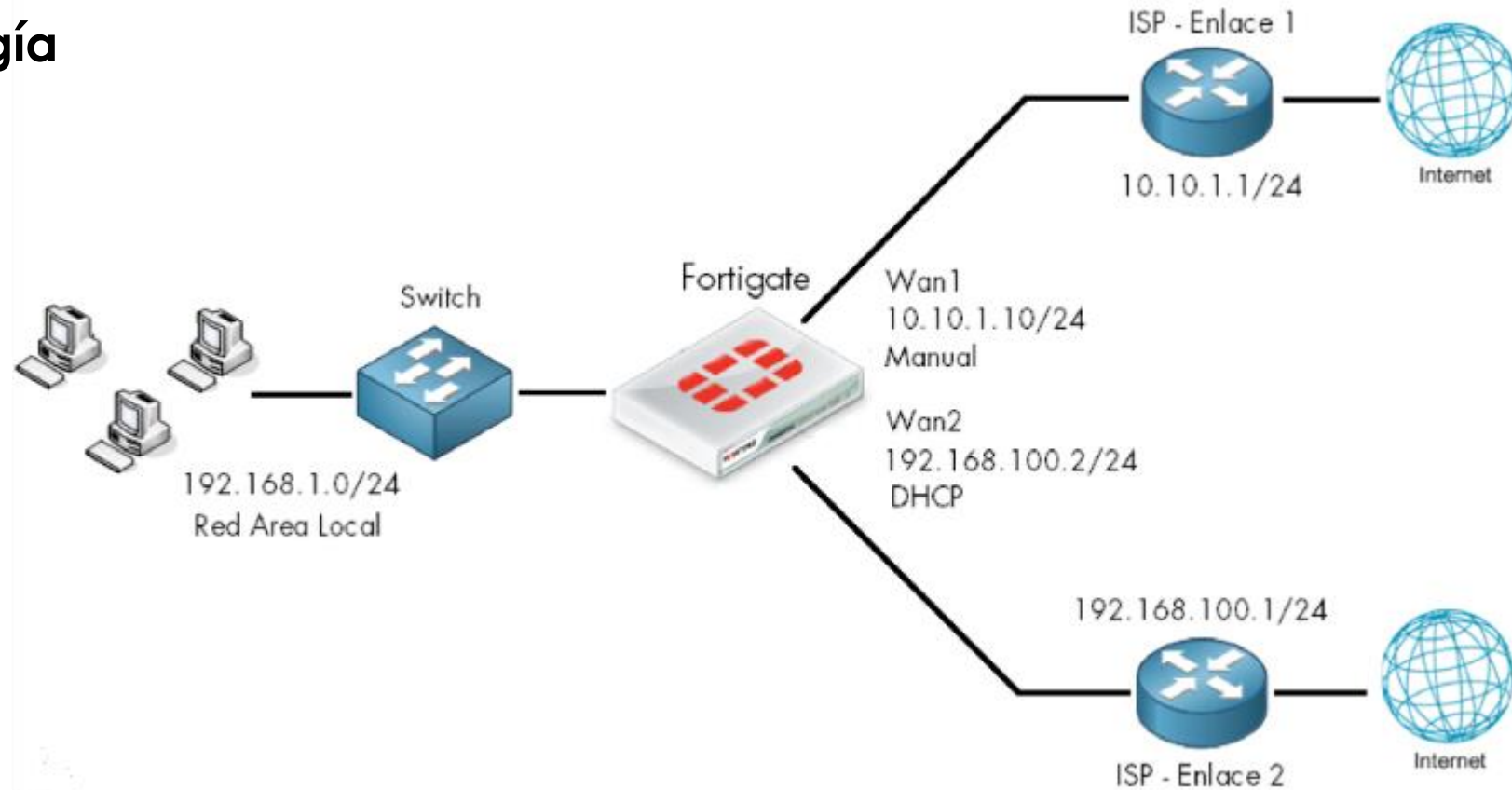
Interfaces

1. 2 x GE RJ45 HA/ MGMT Ports
2. 16 x GE RJ45 Ports
3. 2 x 10 GE SFP+ Slots
4. 2 x 10 GE SFP+ FortiLink Slots
5. 8 x GE SFP Slots

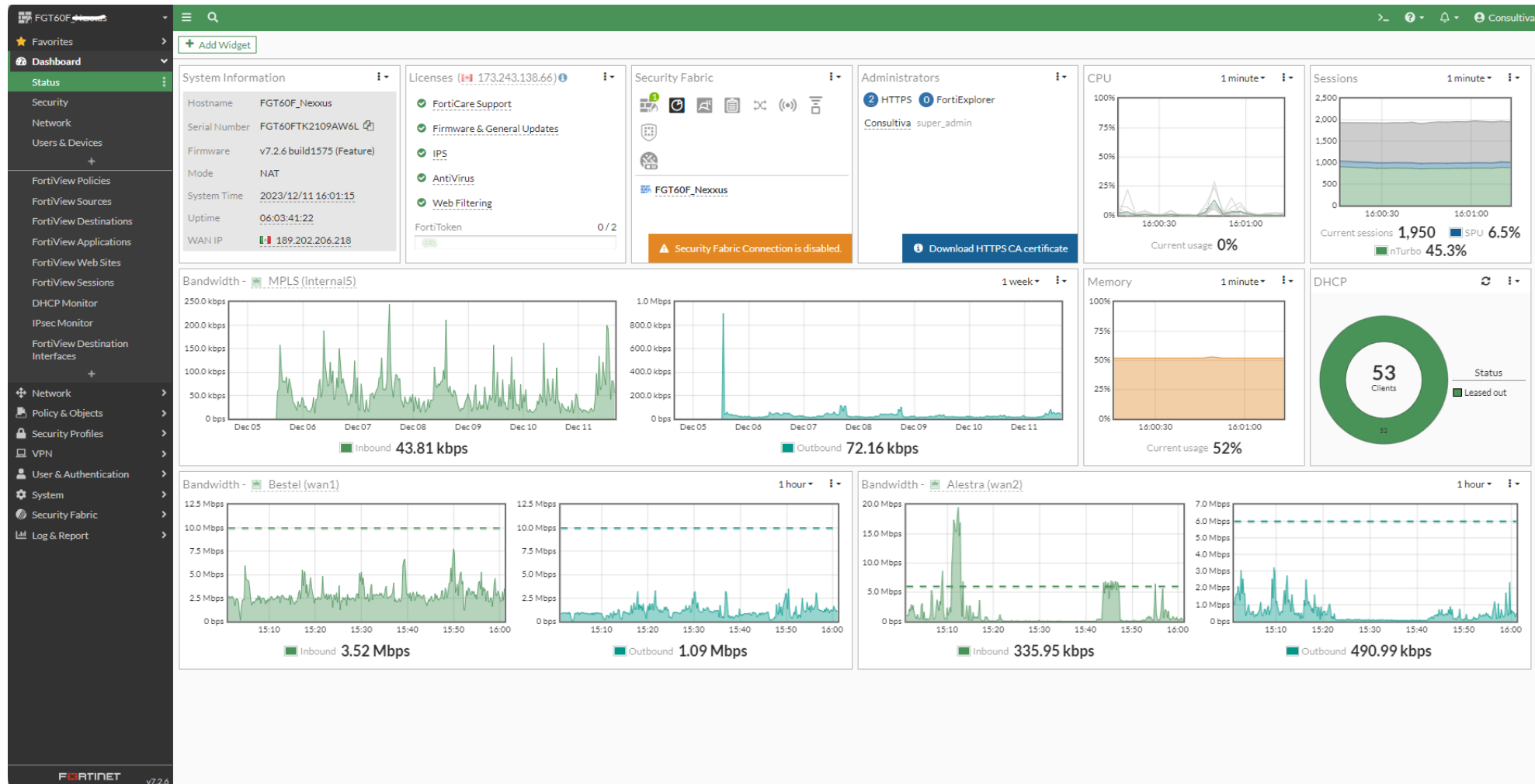


FortiGate

Topología



FortiGate - Dashboard



FortiGate - Interfaces

FGT60F

FortiGate 60F

INTERNAL

DMZ WAN1 WAN2

1

2

3

4

5

A

B

Create New

Edit

Delete

Integrate Interface

Search

Group By Type

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Hardware Switch							
Internal (internal)	Hardware Switch	internal1 internal2 internal3 internal4	172.17.40.252/255.255.255.224	PING HTTPS SSH SNMP	8	172.17.40.225-172.17.40.250	76
Physical Interface							
Alestra (wan2)	Physical Interface		200.188.7.254/255.255.255.252	PING HTTPS SNMP			12
b	Physical Interface		0.0.0.0/0.0.0.0				0
Bestel (wan1)	Physical Interface		189.202.206.218/255.255.255.248	PING HTTPS SNMP			10
conexión (a)	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS			0
MPLS (internal5)	Physical Interface		10.17.40.254/255.255.255.240	PING SNMP			5
Videoconferencia (dmz)	Physical Interface		10.90.23.254/255.255.255.248	HTTPS			6
SD-WAN Zone							
virtual-wan-link	SD-WAN Zone	Bestel (wan1) Alestra (wan2)	0.0.0.0/0.0.0.0				
Tunnel Interface							
NAT interface (nafroot)	Tunnel Interface		0.0.0.0/0.0.0.0				0

Security Rating Issues

14 | Updated: 16:04:14



