

Firewalls Fortinet

Disposen de dos firewalls FortiGate-200F:

```
KotelCamins01 .... VX .... xarxes locals servidors  
KotelCamins02 .... C3 .... xarxes privades UPC
```

Els dos equips estan connectats entre ells per tal de garantir HA, de manera que si un cau, l'altre agafa les seves xarxes i el servei no es veu afectat.

Accés a l'administració

Accedirem indistintament a qualsevol dels dos FortiGates (10.10.101.62 o 10.10.101.66). Credencials a Roques.

Un cop dins, a la part superior dreta podrem canviar el VDOM, el que ens donarà accés a la configuració d'un o altre firewall (CCPB-CPD / CCPB-XARXES).

Interfaces / Zones

Les Zones són agrupacions d'interfaces (xarxes), sobre les que després podrem aplicar regles.

Es poden gestionar des de Network > Interfaces.

Per exemple, en el cas de CCPB-CPD es defineix una zona XARXA_INTERNA que conté totes les interfícies de les xarxes privades UPC.

Regles

Es poden gestionar des de Policy & Objects > Firewall Policy

Les regles s'agrupen en funció de la zona d'origen i la zona de destí.

Per a cada regla, es pot restringir més l'àmbit d'aplicació, de manera que no necessàriament ha d'aplicar a totes les interfícies (xarxes).

Logs

Es poden consultar des de Log & Report > Forward Traffic

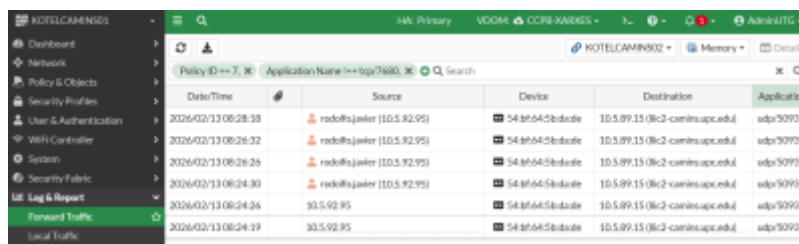
Aquí podrem veure els logs generats per les regles que tinguin el log habilitat. Es pot filtrar per múltiples camps.

Durant el procés de migració de PFSense a FortiGate és molt útil definir una darrera regla a cada zona-zona que permeti el tràfic i registri els logs. D'aquesta manera podem veure totes les

connexions que se'ns escapen del conjunt de regles que haguem definit.

S'ha de filtrar també per FortiGate (KotelCamins01 / 02), ja que tot i estar al VDOM que pertoqui en aquest cas l'apartat de logs pot mostrar informació de qualsevol dels dos.

Hi ha protocols que ens generaran molt tràfic que no ens aporta informació. Per exemple, en el cas de Windows Update hi ha un protocol Peer2Peer a través del port 7680 que permet que els equips es passin actualitzacions entre ells. Això ens pot inundar els logs i és recomanable anar-ho filtrant, ja sigui amb una regla de DENY o bé en la vista dels logs.



The screenshot shows the FortiGate log interface. The left sidebar has a menu with options like Dashboard, Network, Policy & Objects, Security Profiles, User & Authentication, VPN Controller, System, Security Fabric, Log & Report, and Forward Traffic. The main area displays a table of logs for Policy ID 7. The table has columns for DateTime, Source, Device, Destination, and Application. The logs show traffic from redolfsjavier (10.5.92.95) to KotelCamins02 (10.5.89.15) via 54.bh64.5bdcade, with the application identified as udp/5093.

DateTime	Source	Device	Destination	Application
2026/02/13 08:28:38	redolfsjavier (10.5.92.95)	54.bh64.5bdcade	10.5.89.15 (Rc2-camins.upc.edu)	udp/5093
2026/02/13 08:28:32	redolfsjavier (10.5.92.95)	54.bh64.5bdcade	10.5.89.15 (Rc2-camins.upc.edu)	udp/5093
2026/02/13 08:28:26	redolfsjavier (10.5.92.95)	54.bh64.5bdcade	10.5.89.15 (Rc2-camins.upc.edu)	udp/5093
2026/02/13 08:24:30	redolfsjavier (10.5.92.95)	54.bh64.5bdcade	10.5.89.15 (Rc2-camins.upc.edu)	udp/5093
2026/02/13 08:24:26	93.5.92.95	54.bh64.5bdcade	10.5.89.15 (Rc2-camins.upc.edu)	udp/5093
2026/02/13 08:24:19	93.5.92.95	54.bh64.5bdcade	10.5.89.15 (Rc2-camins.upc.edu)	udp/5093

From:

<https://wiki.caminstech.upc.edu/> - CaminsTECH Wiki

Permanent link:

<https://wiki.caminstech.upc.edu/doku.php?id=intranetfirewall-fortinet&rev=1770967853>

Last update: **2026/02/13 07:30**

