Firewalls Fortinet

Disposem 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 interficies 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 interficies (xarxes).

Logs

Es pot 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.