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.

Addresses / Services

Podem definir adreces i serveis amb noms representatius per tal de facilitar la lectura de les regles.

Es poden gestionar des de Policy & Objects > Addresses o Services.

Sembla que aquests apartats apliquen únicament al FortiGate que hem accedit via URL, independentment del VDOM que haguem triat.

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.

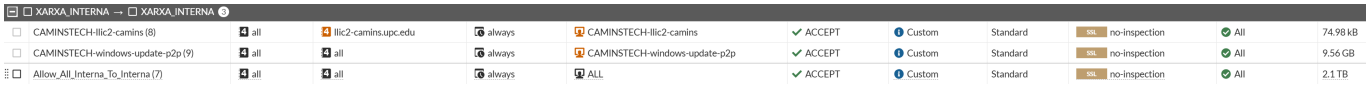
Per a cada regla, es pot restringir més l'àmbit d'aplicació, de manera que no necessàriament ha d'aplicar a totes les interficies (xarxes).

En l'exemple següent definim:

```
1. Regla que permet l'accés al servidor de llicències llic2-camins.
2. Regla que permet l'accés entre equips de les xarxes privades al servei de
Windows Update P2P.
3. Regla genèrica que permet l'accés entre equips de les xarxes privades.
```

És interessant consultar els logs de la 3a regla per veure coses que se'ns poden estar escapant i potser ens interessaria capar.

La situació final hauria de ser que la regla 3 tingués una política de DENY.



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 bloq de zona origen-destí 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.

Hem d'indicar l'equip sobre el que volem veure els logs (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.

Començarem filtrant per ID de la regla.

Seguirem filtrant, eliminant aquells protocols que ens generen molt tràffic i ens acaben ofuscant, com per exemple el servei de Windows Update Peer2Peer (port 7680). Podem filtrar-ho als logs o bé fer una regla amb més prioritat abans de la nostra regla genèrica de captura de logs.