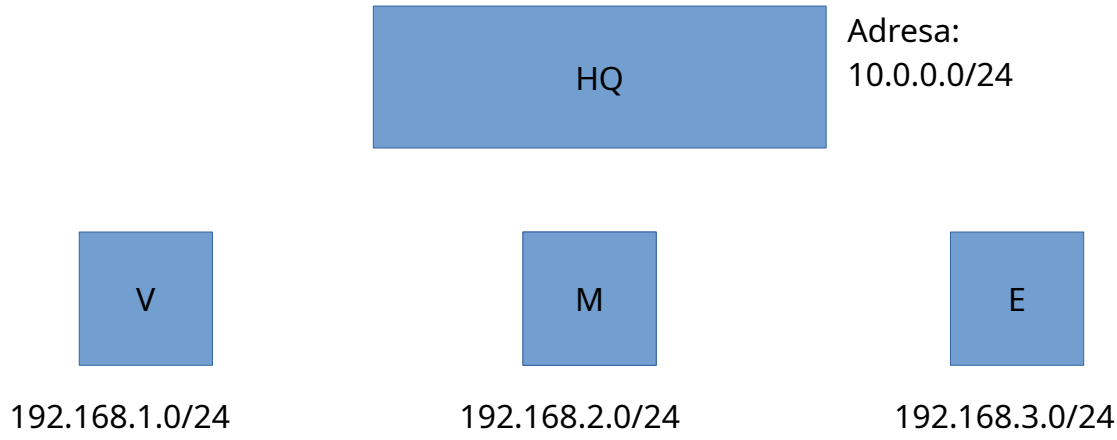
O organizatie pe numele: Eu, Gigel si Costel SRL

Are 3 puncte de lucru conectate la un HQ



Angajare pe post de IT → Primul task: Configurarea politicilor de acces ale organizatiei intre sediile acesteia.

Cerinte:

~~1. Toti angajatii din cladirea V au dreptul sa navigheze doar pe web securizat, in rest nimic altceva.~~

~~2. Tuturor angajatilor din cladirea M li le acorda dreptul de a naviga si pe web nesecurizat, pe langa web securizat, dar nimic altceva~~

~~3. Angajatilor din cladirea E le este total interzis sa dea PING-uri~~

~~4. Angajatii din HQ au toate drepturile posibile, mai putin sa transfere fisiere prin FTP.~~

~~5. Toata lumea are dreptul sa foloseasca doar Google DNS (8.8.8.8) pentru interogari DNS, nimic altceva nu se permite in zona DNS.~~

Firewall documentativ → valorile de configurare sunt doar trecute intr-un document. Nu produc efecte reale.

Rezolvare:

Nr. cerinta	Nr. regula	Sursa	Destinatia	Protocol L4	Protocol L5	Port	Actiune
1	1	192.168.1.0/24	0.0.0.0/0	TCP	HTTPS	443	ACCEPT
	2			*	*	*	REJECT
2	1	192.168.2.0/24	0.0.0.0/0	TCP	HTTPS	443	ACCEPT
	2			TCP	HTTP	80	ACCEPT
	3			*	*	*	REJECT
3	1	192.168.3.0/24	0.0.0.0/0	-	L3: ICMP	-	REJECT
4	1	10.0.0.0/24	0.0.0.0/0	TCP	FTP	20, 21	REJECT
	2			*	*	*	ACCEPT
5	1	0.0.0.0/0	8.8.8.8/32	UDP, TCP	DNS	53	ACCEPT
	2		0.0.0.0/0	UDP, TCP	DNS	53	REJECT

Firewall poate fi de 2 tipuri:

→ PERMISIV: blocam explicit ce ne intereseaza, in rest lasam tot.
→ RESTRICTIV: blocam implicit tot, si doar acceptam ce ne intereseaza.

Exemplu: ordinea regulilor:

```
192.168.0.3      TCP   SMTPS   465   ACCEPT
192.168.0.0/24   TCP   SMTPS   465   REJECT
```

In Linux si in Cisco IOS conteaza ORDINEA regulilor.
Daca un pachet face MATCH pe o regula, se valideaza acea regula – NU SE MAI CAUTA MAI JOS

Niciodata nu faceti asa:

```
192.168.0.0/24   TCP   SMTPS   465   REJECT
192.168.0.3      TCP   SMTPS   465   ACCEPT
```

Regulile mai EXPLICITE SE PUN MAI SUS, lasand loc regulilor mai GENERALE mai jos.

Dupa ce tabelul de firewall este gata, asa cum este el, trebuie EFICIENTIZAT.
Mutam regulile mai explicite sus, lasand alea generale mai jos si VERIFICAM SA NU AVEM CONFLICTE.

Tabel final eficientizat:

Nr. cerinta	Nr. regula	Sursa	Destinatia	Protocol L4	Protocol L5	Port	Actiune
(nu mai conteaza :-))	1	192.168.1.0/24	0.0.0.0/0	TCP	HTTPS	443	ACCEPT
	2	192.168.2.0/24	0.0.0.0/0	TCP	HTTPS	443	ACCEPT
	3	192.168.2.0/24	0.0.0.0/0	TCP	HTTP	80	ACCEPT
	4	192.168.3.0/24	0.0.0.0/0	-	L3: ICMP	-	REJECT
	5	10.0.0.0/24	0.0.0.0/0	TCP	FTP	20, 21	REJECT
	6	0.0.0.0/0	8.8.8.8/32	UDP, TCP	DNS	53	ACCEPT
	7	0.0.0.0/0	0.0.0.0/0	UDP, TCP	DNS	53	REJECT
	8	192.168.1.0/24	0.0.0.0/0	*	*	*	REJECT
	9	192.168.2.0/24	0.0.0.0/0	*	*	*	REJECT
	10	10.0.0.0/24	0.0.0.0/0	*	*	*	ACCEPT