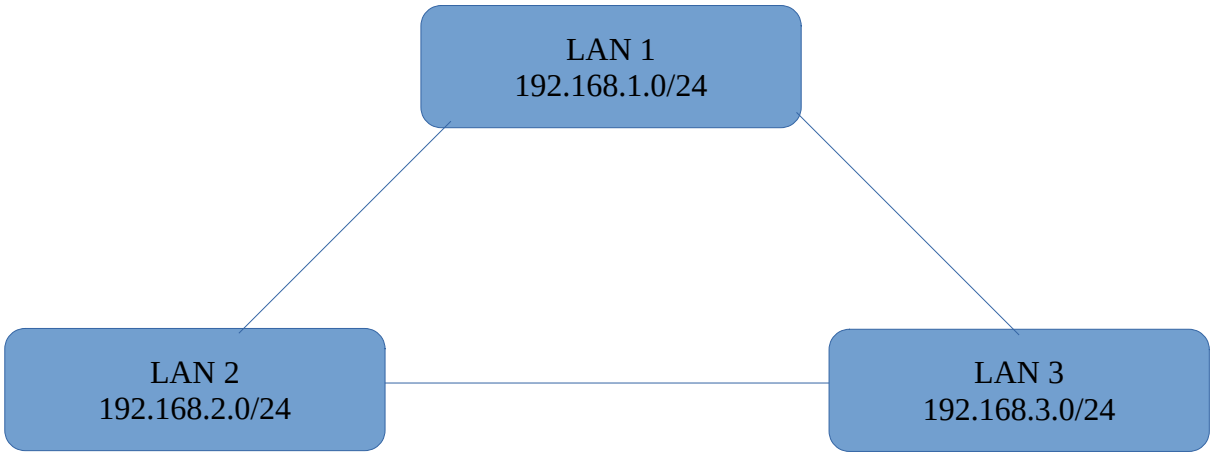
Dokumentacios Tuzfal



1. Engedjuk a Szekure Webbet akarhonan akarhova;
2. Blokajuk a Telnetet akarhonan akarhova;
3. Engedjuk LAN1-bol akarmilyen FTP akarhova
4. Engedjuk a 172.168.13.42-tol hozaferest akarhol a LAN-3ban SSH protokolon keresztul
5. Engedjuk a DNS trafikot csak LAN1-bol ere a cimre: 192.88.88.88
6. Blokajuk az Insecure Webbet LAN1 es LAN2 kozott, akarmeliyk direkcioban.
7. Engedjuk az ICMPt akarhonan akarhova
8. Blokajuk az Insecure SMTPt LAN1-bol es LAN2-bol akarhova;
9. Engedjuk az Incoming Mailt (Szekurizalva) IMAP-on keresztul akarhonan csak LAN1-ben;
10. Engedjuk a Szekurizalt Email kuldest LAN1-bol akarhova;

Keresz szam.	Szabaly szam.	Source	Destination	Protocol Layer #5	Protocol Layer #4	Nr. port Layer #4	Ops
1	1	*	*	HTTPS	TCP	443	ACCEPT
2	1	*	*	Telnet	TCP	23	REJECT
3	1	192.168.1.0/24	*	FTP	TCP	20,21	ACCEPT
4	1	172.168.13.42/32	192.168.3.0/24	SSH	TCP	22	ACCEPT
5	1	192.168.1.0/24	192.88.88.88/32	DNS	UDP,TCP	53	ACCEPT
	2	192.168.2.0/24	192.88.88.88/32				REJECT
	3	192.168.3.0/24	192.88.88.88/32				
6	1	192.168.1.0/24	192.168.2.0/24	HTTP	TCP	80	REJECT

	2	192.168.2.0/24	192.168.1.0/24				
7	1	*	*	(ICMP)			ACCEPT
8	1	192.168.1.0/24	*	SMTP	TCP	25	REJECT
	2	192.168.2.0/24					
9	1	*	192.168.1.0/24	IMAPS	TCP	993	ACCEPT
	2		192.168.2.0/24				REJECT
	3		192.168.3.0/24				
10	1	192.168.1.0/24	*	SMTPS	TCP	465	ACCEPT