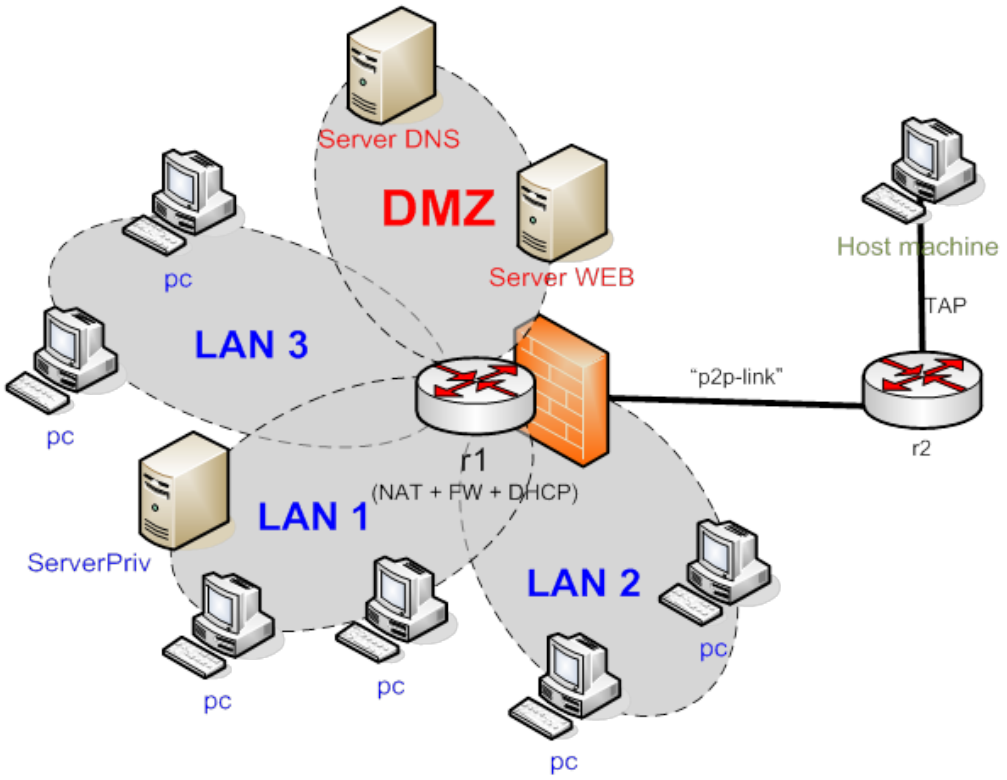
Laboratorio di Configurazione e Gestione Reti Locali 2018

Descrizione progetto

Il progetto richiede l'emulazione su piattaforma netkit dell'architettura mostrata in figura:



Indirizzamento

LAN1: 10.0.0.0/24
LAN2: 10.0.1.0/24
LAN3: 10.0.2.0/24
DMZ: 160.80.103.0/24
p2p-link: 2.34.1.228/31

pc configurati con DHCP
Server configurati con DHCP ma binding statici
Accesso public internet attraverso TAP (attenzione indirizzamento TAP)

NAT

MASQUERADE per le LAN private

DNAT per serverPriv (SSH e HTTP)

Firewall su r1

1. default su DROP
2. “sbloccare” i servizi in DMZ (ICMP compreso)
3. “sbloccare“ (tutto) il traffico tra DMZ e LAN1, LAN2 e LAN3 solo se iniziato dalle LAN
4. “sbloccare” il traffico tra le tre LAN
5. “sbloccare” il seguente traffico generato dalle LAN verso “internet”: WEB, DNS, SSH, FTP, ICMP
6. “sbloccare” il seguente traffico indirizzato a r1: SSH e ICMP
7. ***NOTA: Garantire il funzionamento del DNAT verso ServerPriv***

Server DNS

1 livello. Scegliere il dominio. Configurare un DN per tutti i server.
DNS è anche resolver per i PC configurati in DHCP. Far in modo che le query per nomi “esterni” siano inoltrate ad altri server DNS

SSH server

Configurare server SSH su tutti i router e i server. Creare un account “sysadmin” sulle macchine con server SSH e configurare accesso con chiave pubblica

Server WEB

Creare un virtual host HTTPS (scegliere nome, creare i certificati).

ServerPriv

Server WEB apache di default.

OpenVPN

Configurare r1 come server VPN. Configurare hostmachine come client VPN. Configurare il firewall in modo che sia possibile dal client VPN di raggiungere la porta TCP 9000 su ServerPriv solo dalla VPN (usare nc per emulare un server TCP su porta 9000).