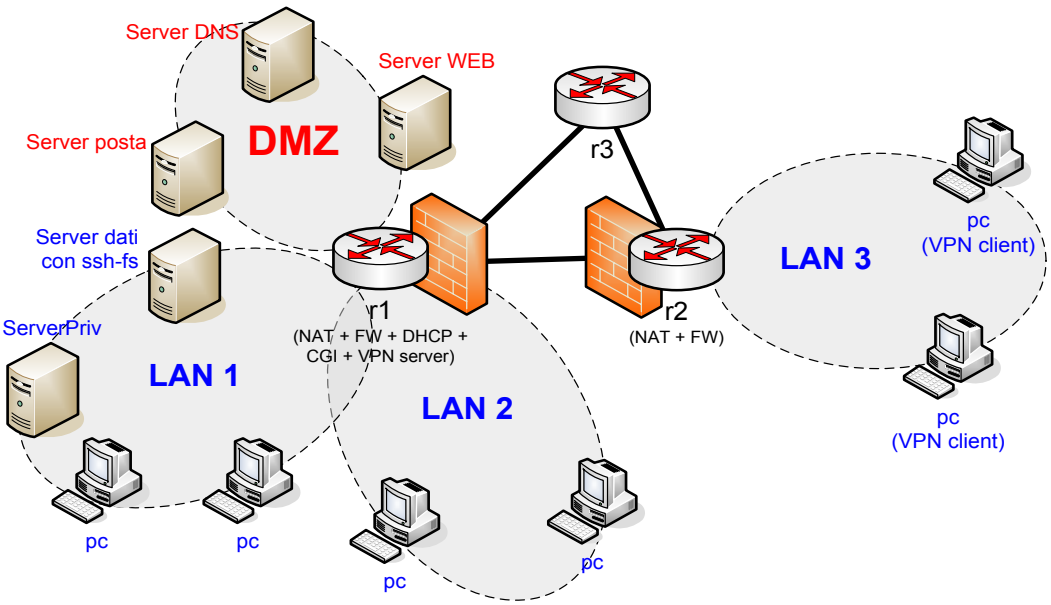
Laboratorio di Configurazione e Gestione Reti Locali 2014/2015

Descrizione progetto

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



Obbligatorio

1. Scegliere indirizzamento (LAN private nel range 172.16.0.0/16 e una /24 pubblica per la DMZ 1.0.0.0/24 e pubblici per collegamenti tra router nel range 11.4.3.0/24) e configurare routing. Inserire una TAP in r3 per l'accesso dalla macchina host
2. DHCP (scegliere se necessario inserire binding statici, configurare server DNS in DMZ) per le 3 LAN
3. Firewall r1
    a. default su DROP
    b. "sbloccare" i servizi in DMZ (ICMP compreso)
    c. "sbloccare" (tutto) il traffico tra DMZ e LAN1 e LAN2 solo se iniziato dalle LAN
    d. "sbloccare" il traffico tra LAN1 e LAN2
    e. "sbloccare" il seguente traffico generato da LAN1 e LAN2: WEB, SSH, FTP, ICMP
    f. "sbloccare" tutto il traffico iniziato da r2
    g. "sbloccare" il seguente traffico in ingresso a r1: SSH, WEB, VPN, ICMP (se configurata)
4. Firewall r2

    a. Default su DROP
    b. “Sbloccare” il traffico generato da LAN3: SSH, FTP, WEB, VPN, DNS, ICMP
    c. “Sbloccare” il traffico VPN verso r1 solo se iniziato da LAN3
    d. “Sbloccare” tutto il traffico generato da r2
    e. “Sbloccare” traffico SSH e ICMP in ingresso a r2
5. NAT (per le LAN private)
6. Server DNS (1 livello. Scegliere il dominio. DN per tutti i server)
7. Server WEB in DMZ: 2 virtual host (inventarsi i contenuti e i FQDN)
    a. non protetto
    b. server HTTPS (solo autenticazione server)
8. SSH server (autenticazione chiave pubblica) su tutti i router e i server. Creare un account “sysadmin” sulle macchine con server SSH.
9. Configurare OpenVPN per l’accesso remoto dei client dalla sede distaccata LAN3

Facoltativo (gruppi da 3: 2 punti – 3 < gruppi <= 5: 3 punti)

1. ServerPriv: server web con cartelle per utente protetto con TLS e accesso username e password. Bloccare accesso da “fuori” (permettere solo in VPN – se configurata)
2. Server di Posta
3. Server web protetto con username e password (accesso solo per utente sysadmin) su canale TLS che offra un CGI per:
    a. Generazione dinamica certificati OpenVPN per utenti registrati
    b. Attivazione/disattivazione di (alcune) regole FW
    c. Registrazione nuovi username password e creazione cartella per ServerPriv
4. Configurare il policy routing per la condivisione dei link di accesso su r1 (scegliete voi le politiche di condivisione) e/o per la differenziazione del traffico generato da LAN1 e LAN2 (scegliete voi le politiche)
5. OSPF tra i routers (NON propagare le LAN locali)