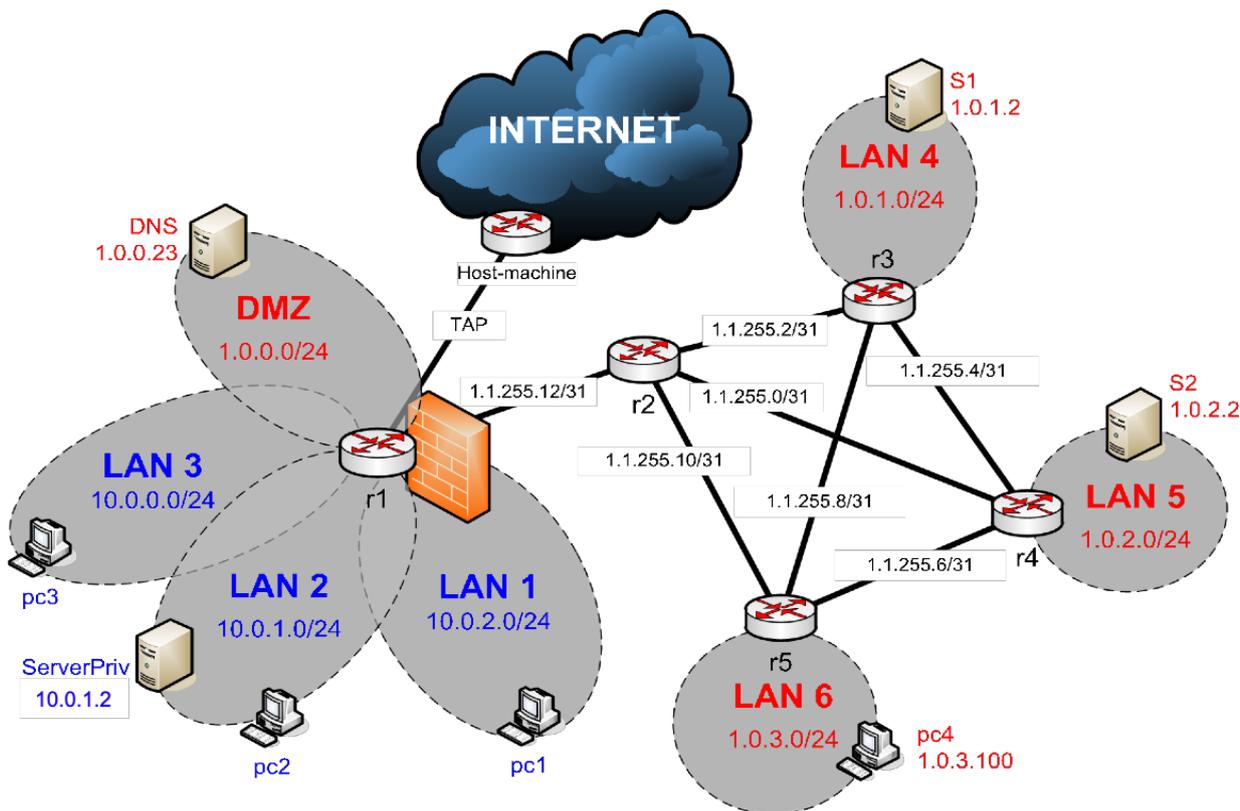


# Laboratorio di Configurazione e Gestione Reti Locali - 2019

## Descrizione progetto

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



## Preliminari

pc configurati con DHCP (LAN1-2-3 indirizzi privati e non routabili)

Server in DMZ e LAN 2 configurati con DHCP, binding statici.

Server in LAN 4, 5 configurati staticamente

PC in lan 5 configurato staticamente

Accesso public internet attraverso TAP (attenzione indirizzamento TAP)

ServerPriv: server HTTP (default virtual host)

## OSPF

Configurare routing dinamico con OSPF (NO advertising delle Lan con indirizzamento privato)

Propagare rotta di default.

## NAT

MASQUERADE per le LAN private

DNAT per serverPriv (HTTP, pagina di benvenuto)

Su r2 ricordarsi il MASQUERADE per le LAN che si vogliono instradare “fuori”

## Firewall su r1

1. Default su DROP
2. “sbloccare” i servizi in DMZ (HTTP, HTTPS, SSH, DNS, 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 private LAN1, LAN2 e LAN3
5. “sbloccare” il seguente traffico generato dalle LAN verso “fuori”: WEB, DNS, SSH, FTP, ICMP
6. “sbloccare” il seguente traffico indirizzato a r1: SSH, ICMP
7. “sbloccare” il traffico in uscita da r1 e il traffico in entrata solo se associato a “connessioni” iniziate localmente

## Server DNS

Il server chiamato DNS è autoritativo per la zona "esame.com" (impostare risoluzione di ns, S1, S2 www, seclogin)

Tutti i PC utilizzano il server "DNS" come resolver DNS. I router non serve che abbiano un server DNS impostato.

Il nome di questo server è "ns.esame.com"

Server DNS include anche un server web apache2 (lasciare pagina “it works”)

Il server DNS risolve la sua zona di competenza ed inoltra ad un resolver DNS esterno quello che non conosce

## SSH server

Configurare server SSH su r1 e i server e permettere accesso a utente “sysadmin”. Su r1 configurare accesso con chiave pubblica per utente sysadmin2 (e testarlo da pc4)

## Server HTTPS

Abilitare un virtual host <https://seclogin.esame.com> con una semplice pagina di benvenuto (creare chiavi e certificati con OpenSSL – non utilizzare certificati fatti in classe) accessibile mediante username/password (HTTP basic authentication).

Configurare questo virtual host sulla macchina DNS in DMZ

## File Server SAMBA

- 1) Accessibile solo dalle LAN (o da “fuori” con VPN, vedi dopo...)
- 2) Impostare un record A su server DNS (fs.esame.com)
- 3) Creare 2 cartelle condivise
  - a. 1 pubblica read only
  - b. 1 autenticata per l’utente cgrl in r/w
- 4) Modificare firewall se necessario

## VPN

Consentire l’accesso da “fuori” al file server SAMBA solo tramite VPN.

Configurazione della VPN libera.

Modificare firewall se necessario

Testare con PC4