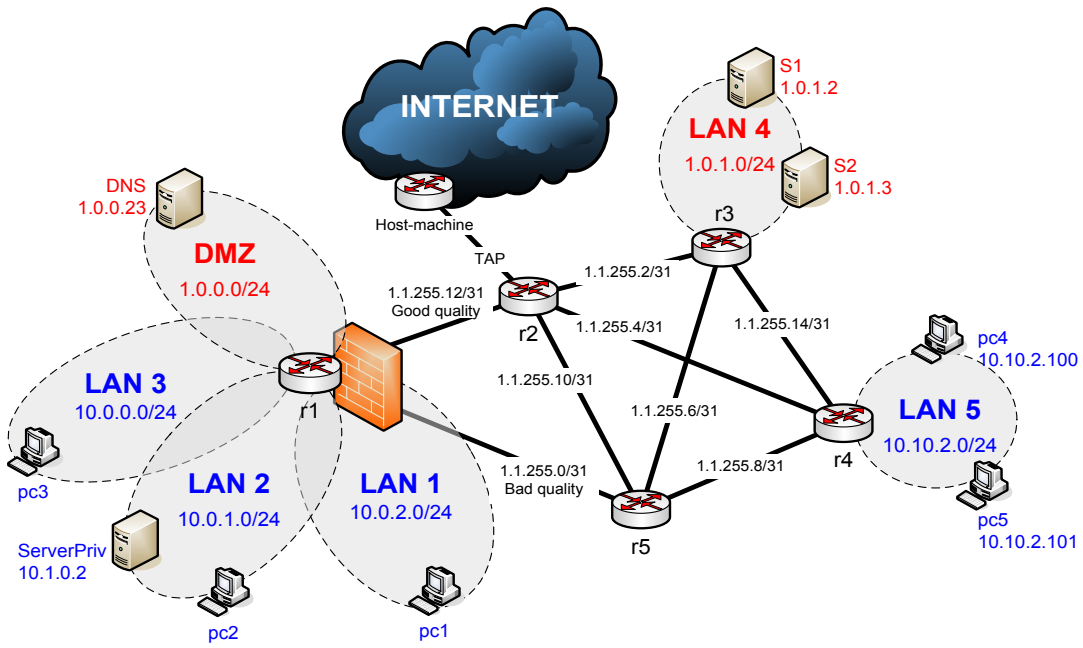
Laboratorio di Configurazione e Gestione Reti Locali - 2014

Descrizione progetto

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



Preliminari

pc configurati con DHCP (LAN1-2-3-5 indirizzi privati e non routabili)
Server in DMZ e LAN 2 configurati con DHCP, binding statici.
Server in LAN 4 configurati staticamente
Accesso public internet attraverso TAP (attenzione indirizzamento TAP)
ServerPriv: server HTTP (degault virtual host)

OSPF

Configuare routing dinamico con OSPF (NO advertising delle Lan con indirizzamento privato)
Propagare rotta di default.
IMPORTANTE: non fare advertisement della LAN tra r1 e r5. Questo link

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)
Tutte le macchine in LAN4, LAN5 utilizzano il server "DNS" come server 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”)

NOTA: le macchine in LAN1, LAN2 e LAN3 usano 8.8.8.8 come nameserver

SSH server

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

VPN

Configurare una VPN tra r1 e r4 (“connettere LAN1-2-3 e LAN5 in VPN)

Server HTTPS

Abilitare un virtual host https://seclogin.esame.com con una semplice pagina di ben venuto (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

Policy Routing

Considerare il link tra r1 e r5 come link BAD e il link tra r1 e r2 come link GOOD.
NOTA: il link tra r1 e r5 non viene propagato con OSPF.

Impostare policy routing su r1 in modo che:

1) traffico web da LAN1-2-3 in load balancing con sequenza: good, good, bad (i pacchetti di una connessione devono uscire dallo stesso linkl)
2) traffico generato da DMZ (eccetto ICMP): link good
3) traffico generato da LAN 1 2 3 (eccetto SSH): link bad
4) traffico SSH generato da LAN 1 2 3: link good
5) traffico ICMP: link bad
6) tutto il resto seguira la default propagata da ospf