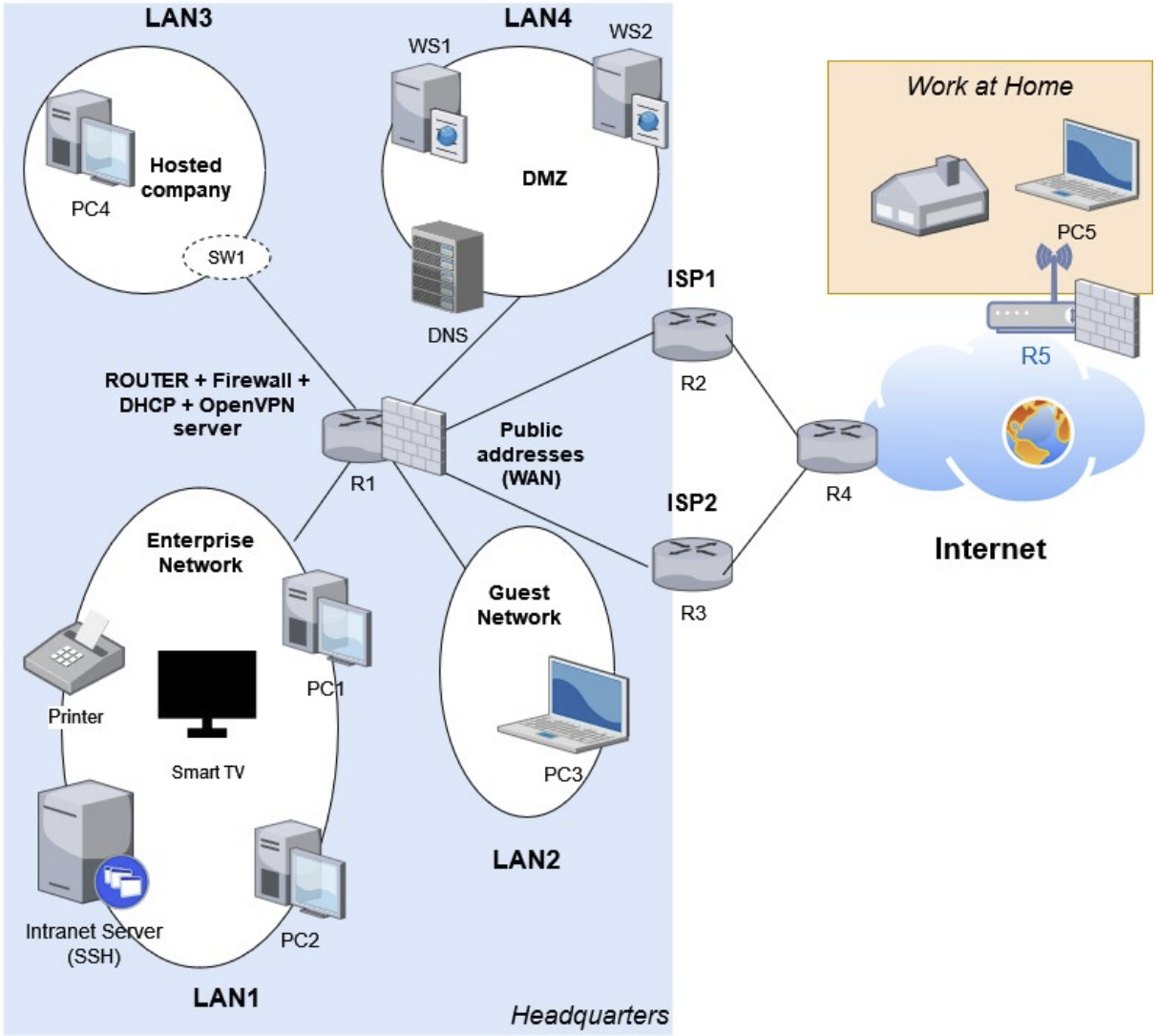
Laboratorio di Configurazione e Gestione Reti Locali 2022/2023 – 6 crediti

Descrizione progetto

Le configurazioni opzionali (opz) diventano obbligatorie in caso di lavoro in gruppo

Il progetto richiede l'emulazione su piattaforma Kathara della configurazione di rete e dei servizi di una piccola azienda collegata ad internet con l'architettura mostrata in figura:



La sede centrale dispone di due connessioni ad internet, tramite due ISP differenti. Solo attraverso ISP1 si potrà essere raggiunti, mentre la connessione attraverso ISP2 è solo "in uscita". Considerare ISP2 come "default via".
Dal committente viene richiesto quanto segue:

1. Definire tutte le sottoreti locali delle LAN utilizzando indirizzi locali e subnet /24
2. Definire le sottoreti per collegare tra loro R1, R2, R3 ed R4. Semplificare "Internet" con un'ulteriore sottorete tra R4 ed R5.

3. Assegnare un IP statico a tutti i router (Rx), sulle rispettive interfacce
4. Assegnare un IP statico a WS1, WS2, DNS, Printer, “Intranet Server” e “Smart TV”
5. Abilitare in R1 il servizio DHCP per assegnare indirizzi dinamici a PC1, PC2, PC3 e PC4
6. (opt) Far assegnare gli IP statici di Printer, “Intranet Server”, e “Smart TV” via DHCP con un match sul MAC address
7. Abilitare in R5 il servizio DHCP per assegnare indirizzo dinamico a PC5
8. Configurare le regole di routing su tutti i router
9. (opt) abilitare OSPF per propagare le regole di routing interne tra i router
10. Abilitare il servizio SSH su: “Intranet Server”, DNS, R1 ed R5. PC1 deve poter accedere a “Intranet Server” senza password.
11. Abilitare il servizio HTTP su: “Printer”, “Smart TV”
12. Abilitare il servizio HTTPS su WS1 e WS2, per servire la stessa coppia di pagine sicure in Virtual-Hosting https://www.azienda.net e https://www.hosted.net , con due due certificati differenti (WS1 e WS2 sono uno il mirror dell’altro)
13. (opt) Abilitare su WS1 e WS2 una pagina privata accessibile con auth di tipo digest, che fornisca l’elenco dei file al suo interno
14. (opz) Abilitare su DNS il servizio DNS per risolvere solo internamente alla rete aziendale printer.azienda.net, ssh.azienda.net (per raggiungere “Intranet Server”), tv.azienda.net e router.azienda.net (per raggiungere R1).
15. Per poter verificare il virtual hosting HTTPS, aggiungere le entry corrette in /etc/hosts di PC5, puntando all’IP pubblico di R1 (lato ISP1).
16. Abilitare il servizio OpenVPN su R1, configurando PC5 come client per poter accedere alla rete centrale dalla connessione di casa.
17. (opz) realizzare policy routing affinché il traffico uscente da LAN4 passi attraverso ISP1.
18. (opz) Realizzare LAN3 come VLAN, aggiungendo un elemento SW1 all’interno di LAN3 per staggare e taggare il traffico verso PC4.
19. Descrizione delle caratteristiche del firewall su R1:
    a. Consentire traffico in forward iniziato da LAN1 verso LAN 4 (DMZ), e viceversa solo traffico RELATED
    b. Consentire traffico in forward iniziato da LAN2 verso “Smart TV”, e viceversa solo traffico RELATED
    c. Consentire traffico in forward iniziato da LAN3 verso “Printer” e DNS, e viceversa solo traffico RELATED
    d. Consentire traffico in forward da LAN1, LAN2 e LAN3 verso internet (ISP2), e viceversa solo traffico RELATED
    e. Consentire traffico in forward da LAN4 verso internet, e viceversa solo traffico RELATED (se si fa policy routing al punto 17 usare ISP1, altrimenti ISP2)
    f. Consentire traffico in forward da Internet (via ISP1) a LAN4 per il servizio HTTPS (vedi punto 19.k)
    g. Consentire il traffico in ingresso (INPUT) per il servizio VPN da ISP1
    h. (opz) consentire in ingresso da ISP1 e ISP2 il ping con limite di 2 richieste al secondo
    i. Consentire il traffico in forward tra VPN e LAN1, in entrambe le direzioni
    j. Consentire il traffico in forward tra VPN e LAN 4, e viceversa solo traffico RELATED

    k. Redirezionare le richieste HTTPS da ISP1 verso WS1 o WS2 in modalità round robin
    l. Eseguire NAT (masquerade) per tutte le connessioni verso ISP1 ed ISP2
    m. Droppare in INPUT e FORWARD (tabella filter) tutto quanto non specificato
20. Descrizione delle caratteristiche del firewall su R5:
    a. Consentire traffico in forward iniziato dalla lan di PC5 verso internet, e viceversa solo traffico RELATED
    b. Eseguire NAT (masquerade) per tutte le connessioni verso internet
21. Descrizioni vincoli di QoS su R1
    a. Limitare uscita (tramite ISP2) per LAN2 e LAN3 a 10 Mbit/s
    b. Limitare ingresso (tramite ISP2) di tutta LAN2 a 10 Mbit/s
    c. Limitare ingresso (tramite ISP2) di tutta LAN3 a 10 Mbit/s
    d. (opz) Limitare l'uscita (verso ISP2) e l'ingresso complessivo di tutta LAN1 a 100 Mbit/s
    e. (opz) Limitare l'uscita (verso ISP2) e l'ingresso di tutte le macchine dentro LAN1 a 20 Mbit/s, con possibilità di usare la banda residua fino a 40 Mbit/s