NON SPEGNERE IL PC A FINE ESAME

Corso di Sistemi Operativi e Reti

Modulo Reti

Prova di laboratorio 01 Luglio 2022

Durata Prova **90 minuti**

ISTRUZIONI

Lo svolgimento della prova consiste nello sviluppo e simulazione di una rete locale (Firewalling + Routing + Configurazione).

1. **Rinomina** la cartella chiamata "Cognome-Nome-Matricola" che hai trovato sul Desktop e in cui hai trovato questa traccia, sostituendo "Cognome" "Nome" e "Matricola" con i tuoi dati personali e lasciando i trattini;
2. Configura la topologia lasciando tutti i file necessari nella cartella di cui sopra.

Istruzioni per il confezionamento dei file di configurazione:

1. I domini di collisione dovranno essere elencati all'interno del file `CDs` già presente all'interno della cartella **Cognome-Nome-Matricola**.

```
## ESEMPIO DI CD ##
CD1
    network 10.0.0.0/24
    netmask 255.255.255.0
    broadcast 10.0.0.255

CD2
    network 10.0.7.0/30
    netmask 255.255.255.252
    broadcast 10.0.7.3

CDX
...

# Accorpamento RED
RED
    network 10.0.0.0/23
    netmask 255.255.254.0
    broadcast 10.0.1.255
```

2. La risposta ai quesiti deve essere scritta all'interno del file `Quesiti` situato all'interno della directory **Cognome-Nome-Matricola**. Il formato dovrà essere uguale a quello dell'esempio sottostante:

NON SPEGNERE IL PC A FINE ESAME

```
1.
2. comando -xaz
3. altroComando -x -a -z
```

3. Le rotte dell'intero progetto potranno essere specificate all'interno di un file dal nome **rotte.sh** debitamente commentato. Per semplificare, è possibile usare la notazione *networkAreaRed/22* per indicare, ad esempio, il network e la maschera di una determinata area o dominio di collisione (evitando dunque di riportare l'intero indirizzo del network del dominio) e *R1[eth0]* per indicare, ad esempio, l'indirizzo ip relativo alla scheda di rete *eth0* del router *R1.* La stessa convenzione può essere utilizzata anche nelle regole di firewalling se necessario e lo si ritiene opportuno.

Si noti che per ogni risposta è riportato il numero del quesito a cui ci si riferisce. Se non si vuole dare alcuna risposta ad una determinata domanda basta scrivere il numero del quesito e lasciare in bianco la riga.
Non è consentito l'uso di alcun altro tipo di materiale (appunti, esempi, libri, calcolatrice, dati trasferiti tramite USB).

N.B. Per il superamento della prova è necessario completare correttamente **i primi 3 punti** specificati all'interno della sezione **[REQUISITI].**

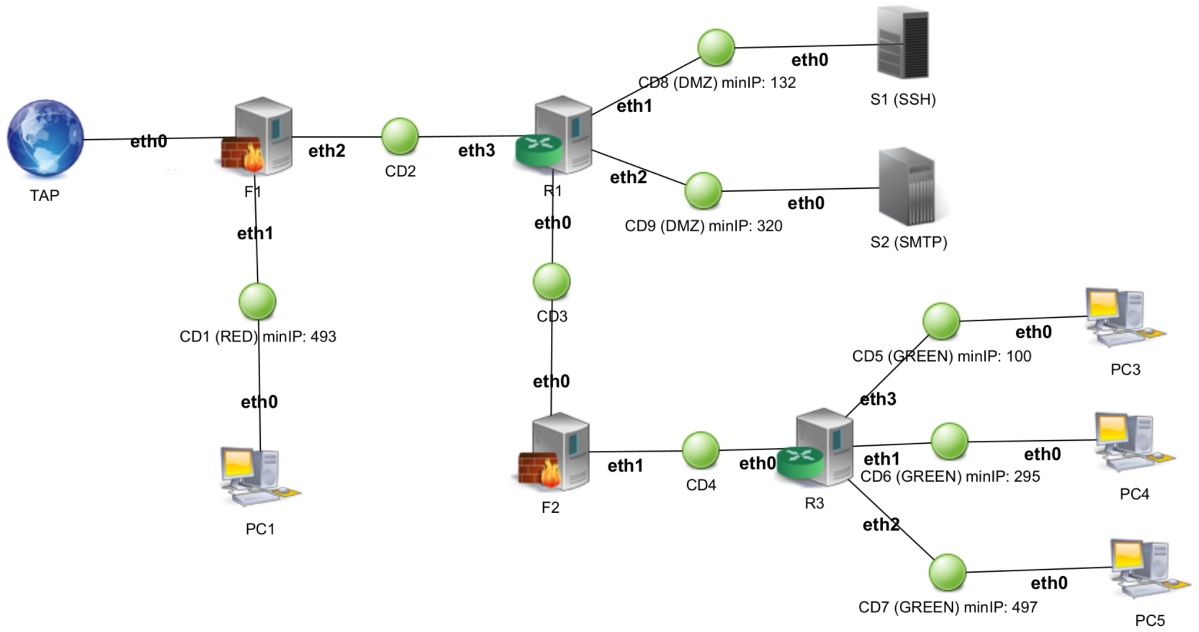
NON SPEGNERE IL PC A FINE ESAME

Quando finisci NON spegnere il PC.

SALVA SPESSO il tuo lavoro

ESERCIZIO 1 (22 punti)

Si ha a disposizione una rete di **`classe A`** (10.0.0.0/8). Si deve progettare/simulare una rete locale seguendo le specifiche riportate nella figura sottostante.



REQUISITI:

REQUISITI:

1. **(4pt)** È necessario accorpare i domini di collisione contigui della stessa tipologia (Green, Red o DMZ)
2. **(4pt)** È richiesto di minimizzare il più possibile lo spreco di indirizzi IP (**annotare sul foglio, per ogni dominio di collisione, gli indirizzi network, maschera e broadcast**)
3. **(3pt)** È necessario, in una prima fase, che tutta la rete sia completamente connessa e funzionante e che tutti gli host siano in grado di comunicare con tutti gli altri hosts (Es. I PC in CD1 devono poter raggiungere e pingare i PC di CD6 e viceversa)
4. **(8pt)** Successivamente applicare le seguenti regole di firewalling **(default policy DROP):**
    a. **(1pt)** L'area GREEN può aprire comunicazioni verso tutti; l'area RED può aprire nuove comunicazioni verso INTERNET e DMZ; l'area DMZ può ricevere nuove comunicazioni solo da INTERNET e da RED
    b. **(2pt)** L'area RED può avviare nuove richieste `icmp` (solo echo request) verso l'area GREEN

NON SPEGNERE IL PC A FINE ESAME

c. **(2pt)** INTERNET può contattare il firewall F2 tramite **ssh** sulla porta 22

d. **(3pt)** Natting:

   i. Tutti i server interni alle aree DMZ devono essere raggiungibili dall'esterno tramite l'indirizzo IP pubblico del firewall più esterno

   ii. Si scriva una regola per mascherare l'indirizzo ip sorgente di tutte le connessioni provenienti dall'interno della rete e dirette verso internet con uno dei seguenti indirizzi ip: `10.1.1.1`, `10.1.1.2` o `10.1.1.3`

   N.B.: La regola è da inserire nel firewall F1 e sarà F1 stesso a decidere con quale dei 3 possibili indirizzi ip mascherare la connessione.

5. **(1pt)** Scrivere il comando usato per ricavare il percorso seguito dai pacchetti sulla rete.
6. **(1pt)** Scrivere il comando per aprire un server in ascolto sulla porta 1234 sul computer locale.
7. **(1pt)** Scrivere il comando per trovare i server di posta elettronica associati al dominio **mat.unical.it**.

ESERCIZIO 2 (8 pt)

Si scriva uno script, in linguaggio Python o Perl, che conti *periodicamente* il numero di connessioni **TCP** attualmente attive (instaurate) sull'indirizzo ip assegnato alla scheda di rete dal nome "*enp1s0*" del computer locale su cui lo script è eseguito. Se il numero di connessioni stabilite è maggiore di 30, lo script imposta una regola di firewall che blocca tutte le connessioni per i prossimi 15 minuti. Allo scadere del timer, la regola di firewalling deve essere (eventualmente) eliminata e il controllo deve essere ripetuto.

Lo script deve effettuare il suddetto controllo con frequenza di 15 minuti e funzionerà nel seguente modo:

1. Conta il numero di connessioni "*numConnessioni*" attualmente attive sull'indirizzo ip assegnato ad *enp1s0;*
   1.1. *Se numConnessioni > 30* → blocco tutte le connessioni con regola di firewall;
   1.2. *Se numConnessioni <= 30* → rimuovo la regola di firewall inserita precedentemente (se non ho mai inserito la regola di firewall non effettuo alcuna operazione);
2. Aspetto 15 minuti e riparto dal punto 1.