

Data la topologia di rete allegata, si richiede di sviluppare un laboratorio netkit in accordo alle specifiche seguenti.

Determinare per tutti i domini di collisione, laddove mancanti, i seguenti valori:

- 1- N = Network (Ad esempio, 10.0.0.0 / 8).
- 2- NA = NetworkAddress (ad esempio 10.0.0.0).
- 3- BA = BroadcastAddress (ad esempio, 10.255.255.255).
- 4- UIP = Numero di IP utilizzabili.
- 5- R = Intervallo degli indirizzi IP usabili (esempio, 10.0.0.1-10.255.255.254)

Tenere presente che:

- I calcolatori rappresentano punti rete utente localizzati all'interno di un dato dominio di collisione;
- Gli hub (identificati con i pallini verdi) rappresentano i domini di collisione ed etichettati con il nome 'CDn' (n = 1, ...,).

Per ognuno dei domini di collisioni, vanno fissati i valori di cui ai punti 1-5;

- I router (identificati con l'etichetta Rn (n = 1,...)) rappresentano le interconnessioni tra i domini di collisione;

- I firewall (identificati con l'etichetta Fn (n = 1,...)) costituiscono i dispositivi di sicurezza presenti nel sistema.

Ogni firewall si comporta anche da router, e deve essere programmato con le regole di filtraggio opportune (vedi sotto);

- I server (identificati con l'etichetta Sn (n = 1,...)) rappresentano servizi offerti dalla rete e accessibili dall'esterno. Un server ha normalmente alcune porte di ascolto attive che devono essere raggiungibili opportunamente programmando i firewall.

- I server contrassegnati dall'identificativo SNatted (colorati in rosso) forniscono servizi soggetti a port forwarding da parte del proprio router più vicino, che deve essere considerato operante come router NAT.

Per questi server è necessario consentire l'erogazione del servizio mantenendo nascosta la reale macchina che lo fornisce.

Ogni server è etichettato con i servizi che deve erogare (indicando il nome simbolico del servizio stesso, e.g. 'https').

Più domini di collisione adiacenti formano delle 'aree', che possono essere di tipo DMZ, GREEN e RED.

Limitazioni generali sul traffico di rete (in ordine crescente di priorità):

- Le Green Area possono aprire connessioni destinate alle aree RED, DMZ e Internet;

- Le aree DMZ possono aprire connessioni destinate alle aree RED mentre queste ultime non possono aprire connessioni destinate alle altre reti, nè a Internet.

- Le aree 'DMZ' devono consentire i seguenti servizi (ANCHE se non è esplicitamente presente il server corrispondente), accessibili dalle sole aree RED:

- dns sulla porta 53
- smtp sulla porta 25
- ftp sulla porta 21
- msp sulla porta 18

- Per tutti i firewall la politica di default è DROP.