ACCESS CONTROL LIST

Vediamo come si realizza un Firewall su un router. Come sappiamo per configurare un firewall si devono definire le regole che regolano il traffico in entrata (**in** – inbound) e/o in uscita (**out** -outbound). Questo avviene, come sappiamo, inserendo queste regole in una lista: l'ACL. Ma su quale router bisogna intervenire per filtrare il traffico in ingresso e/o in uscita? La risposta è… dipende. Innanzitutto, dobbiamo dire che le regole (ACE Access Control Entry) vanno inserite nella lista con un 'certo' ordine. Infatti, il router appena incontra una regola su un determinato filtro, la esegue. Quindi se, ad esempio, diciamo che possono entrare tutti gli IP ad eccezione di un determinato IP, se le regole le inseriamo nell'ordine:

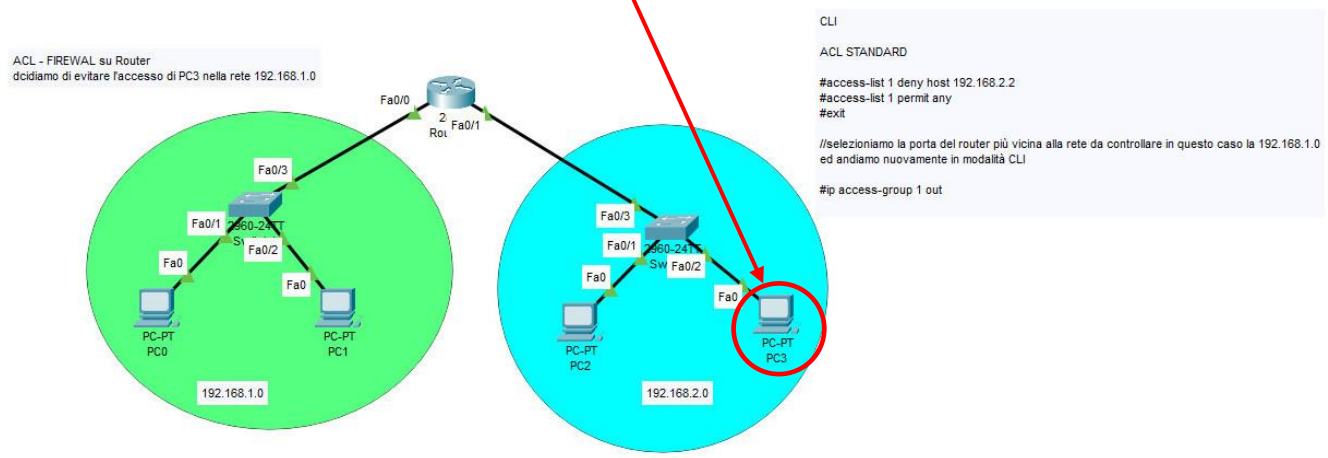
1) entrano tutti gli IP

2) non entra un determinato IP,

quando l'IP che non deve entrare si presenta al router, il router esegue per prima cosa la prima regola (e quindi lo fa entrare). Le regole, in questo caso, devono essere invertite. Infine, dobbiamo decidere su quale Router (e/o su quale porta) definire le regole. Se usiamo ACL standard, si deve configurare il router e la porta più vicina alla rete da proteggere. Acl standard, infatti, le regole contengono solo le definizioni del dispositivo, rete, porta… da filtrare ed in caso configuriamo il router/porta più vicina alla rete che contiene il dispositivo da filtrare, lo escluderemmo anche da reti ove il suo accesso è consentito. Se usiamo l'ACL esteso, siccome, in questo caso, le regole contengono sia le informazioni del dispositivo, rete, porta… da filtrare ma anche della rete da proteggere, le configuriamo, di norma, sul router e porta più vicino ai dispositivi mittenti.

ACL STANDARD – FIREWALL

Supponiamo di voler inibire l'ingresso del PC3 (IP: 192.168.2.2) della rete 192.168.2.0, nella rete 192.168.1.0:



Creiamo l'ACL 1 sul Router, andiamo in CLI:

Router>enable

Router#configure terminal
Router(config-if)#access-list 1 deny host 192.168.2.2
Router(config)#access-list 1 permit any
Router(config)#exit
Router#

Visualizziamo le ACL create

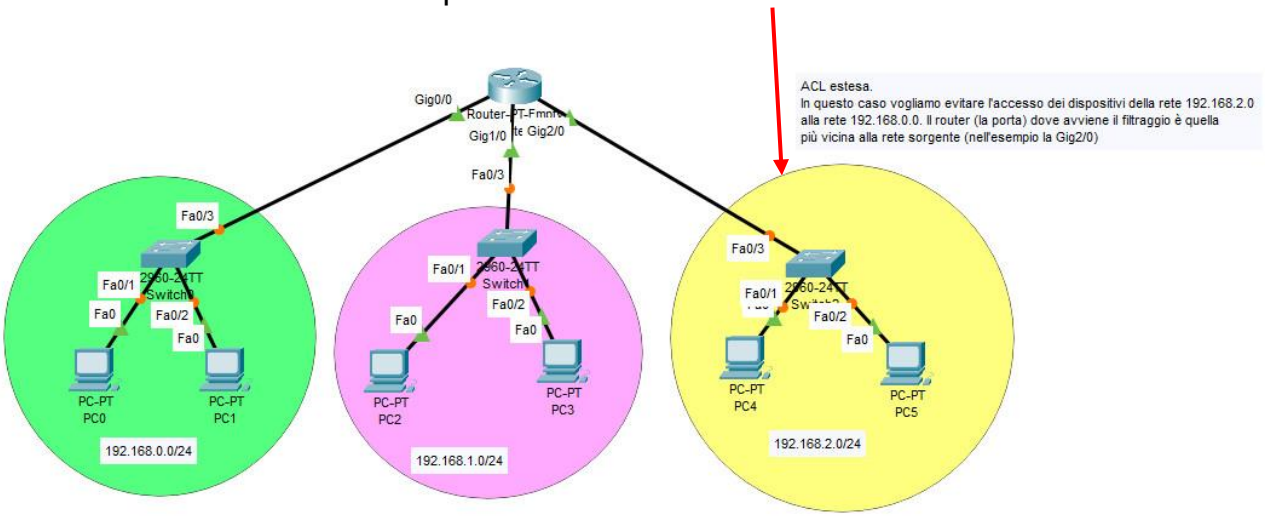
%SYS-5-CONFIG_I: Configured from console by console
show access-list
Standard IP access list 1
10 deny host 192.168.2.2
20 permit any

Definiamo la porta del router su cui devono essere applicate le regole

Router#
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#

ACL ESTESA – FIREWAL

Vogliamo inibire l'accesso di tutti i dispositivi della rete 192.168.2.0 alla rete 192.168.0.0



Router(config)#access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.0.0 0.0.0.255
Router(config)#access-list 101 permit ip any any
Router(config)#

Definiamo la porta del router su cui devono essere applicate le regole

Router(config)#
Router(config)#interface GigabitEthernet2/0
Router(config-if)#ip access-group 101 in

Router(config-if)#exit
Router#

N.B. In rosso i comandi che devono essere scritti da noi

Analizziamo l'istruzione:

#access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list: comando per realizzare una ACL; siccome possono essere realizzate più ACL con regole diverse, queste devono essere numerate.

101: numero di ACL (per le estese >99, per le standard da 1 a 99)

Deny: indica la condizione (nega) – ***permit*** (consenti) – su come devono essere trattati i pacchetti.

Ip: protocollo/servizio/dispositivo (***host***) (altri protocolli tcp, udp, icmp…..)

192.168.2.0: indirizzo ip su cui deve essere applicata la condizione

0.0.0.255: WildCard Mask – tratteremo nel capitolo successivo

Analogamente gli atri due parametri che indicano la rete di destinazione su cui applicare le condizioni dell'ACL.

WILDCARD MASK.

La ***WILDCARD MASK***, analogamente alla subnet mask, è formata da un quartetto di numeri binari, ognuno di 8 bit (1 byte), che consente di esaminare quale parte dell'IP deve essere considerata o meno in una regola nell'ACL. Possiamo affermare che la WildCard Mask funziona allo 'incontrario' della subnet mask: se gli 1 nella subnet mask indicano quali sono i bit che indicano il net-id, nella WildCard Mask indicano quali bit NON devono essere controllati nell'ACL. Ad esempio, la wildcard mask 0.0.0.255 indica che i primi tre byte devono essere controllati dalla regola, mentre l'ultimo byte no.

Per esempio, l'istruzione **deny ip** 192.168.0.0 **0.0.0.255** indica che deve essere **negato** l'accesso agli IP che hanno i primi tre byte uguali a 192.168.0….

Così la regola: permit ip 192.168.1.100 **0.0.0.127 (che corrisponde a 00000000.00000000.00000000.01111111)** indica che deve essere **permesso** l'accesso agli IP **192.168.1.1NN (NN qualunque).**

Altro esempio. Supponiamo di voler negare l'accesso agli host di indirizzo 192.168.1.**4**, 192.168.1.**5**, 192.168.1.**6**, 192.168.1.**7**. Siccome:

192	168	1	4, 5, 6, 7
11000000	10100000	00000001	00000100 (4+0) 4
11000000	10100000	00000001	00000101 (4+1) 5
11000000	10100000	00000001	00000110 (4+2) 6
11000000	10100000	00000001	00000111 (4+3) 7

Si può notare che le cifre **nere** sono sempre uguali, mentre le **rosse** variano da 00 a 11, la WldCard Mask che risolve il nostro problema è 0.0.0.3 (00000000.00000000.00000000.00000011). da cui: **deny ip 192.168.1.4 0.0.0.3.**

Per maggiori informazioni: Configurazione degli ACL di indirizzi IP più utilizzati - Cisco