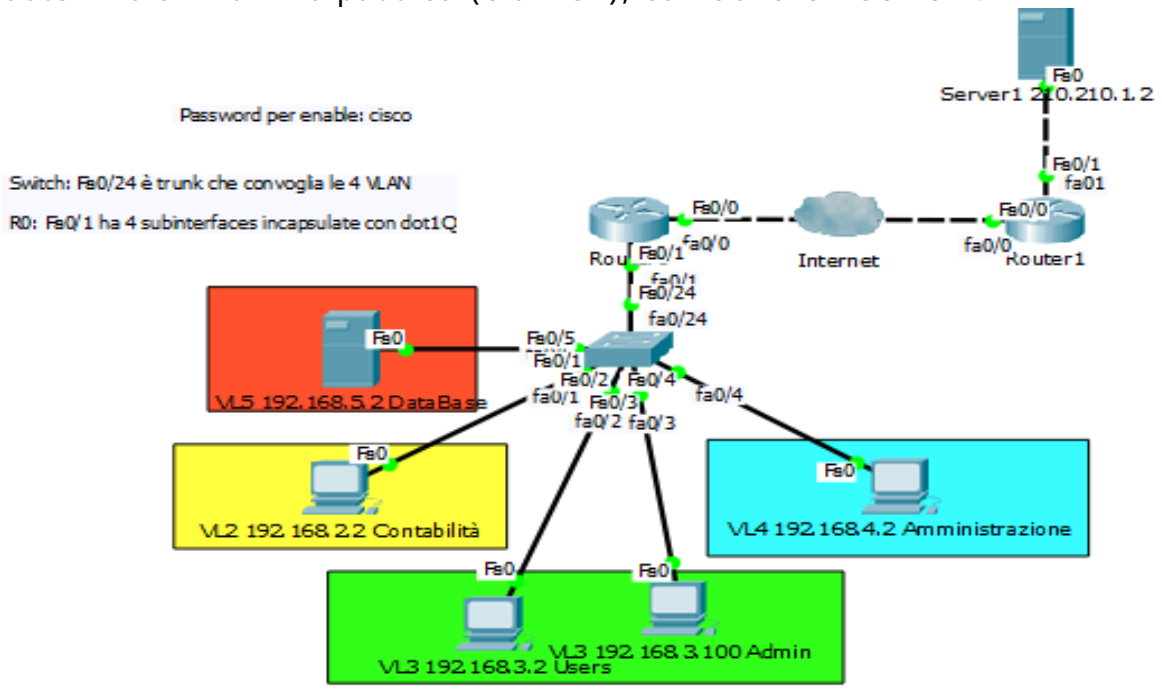
Esercitazione: ACL di tipo standard ed extended.

ACL

Obiettivi:

- Utilizzare le liste ACL standard e estese
- Configurare l'accesso dalle VLAN, escluso il database server, alla rete esterna (Internet), con ACL standard, per il NAT.
- Simulare l'hackeraggio del Router1 (ISP) per accedere alle VLAN.
- Vietare l'accesso alle VLAN dall'esterno, con ACL extended per il traffico in entrata al Router0.
- Apprendere le regole pratiche di implementazione ACL

La rete aziendale è suddivisa in 4 VLAN. Le porte dello switch sono configurate come access per le VLAN 2-5, la porta verso il Router0 è di tipo trunk.
Router0 ha 5 subinterfaces configurate sulla porta Fa0/1.
Router1 ha un indirizzo pubblico (è un ISP), come anche il Server1.



Le ACL extended possono controllare maggiormente il traffico che quelli standard, ma funzionano molto più lentamente perche devono andare a vedere dentro il pacchetto, a differenza delle ACL standard, dove si controlla solo il campo Source Address. *(Ora che la IOS Cisco è arrivata alla versione 12.4, la gestione delle ACL è molto più agile di come era prima).*
Le regole:
- Non è possibile associare più di una ACL per interfaccia, per protocollo, per la direzione (in o out).
- ACL non agisce sul traffico generato dal router stesso.
- Alla fine di ogni ACL c'è una regola invisibile "DENY ANY"
Per filtrare gli indirizzi nell'ACL, si usa wildcard mask. E' una mask riversiva.
Si prende 255.255.255.255 e si sottrae la netmask.
Esempio: 255.255.255.255 - 255.255.255.0 = 0.0.0.255.

CONFIGURAZIONE

R0 **ip access-list standard FOR-NAT**
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255
permit 192.168.4.0 0.0.0.255
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload

R1 (ISP) è stato hackerato oppure qualcuno si è introdotto tra R0 e R1 (Man-in-the-Middle). Il malintenzionato potrebbe inserire un percorso per arrivare alle reti interne LAN. Può anche non conoscere gli indirizzi delle LAN, ma visto che quasi ogni rete aziendale usa indirizzi 192.168.x.x, inserirà sul R1 un percorso tipo

ip route 192.168.0.0 255.255.0.0 210.210.0.2 */in cui sono incluse tutte le ns LAN*

TEST: **ping 192.168.5.2** /4.2 /3.2 va a buon fine, le LAN diventano accessibili

R0

Provvediamo, e creiamo le ACL, che potremmo mettere o in ingresso o in uscita al R0, scegliamo in ingresso perchè l'attacco verrà fatto dall'esterno, da Internet. Possiamo indicare un solo protocollo, ma vogliamo vietare l'accesso su tutti i protocolli

```
ip access-list extended FROM-OUTSIDE
deny ip any 192.168.2.0 0.0.0.255
deny ip any 192.168.3.0 0.0.0.255
deny ip any 192.168.4.0 0.0.0.255
deny ip any 192.168.5.0 0.0.0.255
!
ip access-group FROM-OUTSIDE in
```

PROVA: Verifica accesso dai PC in Internet: ping 210.210.1.2 e non va! Il motivo è seguente:

Alla fine di ogni ACL c'è una regola <u>invisibile</u> "DENY ANY"

Cosa fare? Aggiungiamo una regola di permesso:

ip access-list extended FROM-OUTSIDE

permit ip any host 210.210.0.2 *//permesso per tutti i protocolli da qualsiasi indirizzo all'IP del R0*

Vediamo le ACL su R0 e teniamo conto della regola invisibile detta sopra ***deny any any*** :

```
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255
permit 192.168.4.0 0.0.0.255
deny any any
```

```
ip access-list extended FROM-OUTSIDE
deny ip any 192.168.2.0 0.0.0.255
deny ip any 192.168.3.0 0.0.0.255
deny ip any 192.168.4.0 0.0.0.255
deny ip any 192.168.5.0 0.0.0.255
permit ip any host 210.210.0.2
deny any any
```

La ACL **FROM-OUTSIDE** non è configurata in modo ottimale. E' molto più ragionevole permettere una lista mentre il resto verrà vietato per default.

Quindi, 1) eliminiamo la lista FROM-OUTSIDE e 2) indichiamo una sola regola:

```
no ip access-list extended FROM-OUTSIDE   // eliminiamo la lista FROM-OUTSIDE
ip access-list extended FROM-OUTSIDE      // la ricreiamo
permit ip any host 210.210.0.2            // indichiamo una sola regola
```

PROVA:

ping da PC a Internet (cioè, server) *ping 210.210.1.2* e <u>va bene</u>

ping dal R1 ai PC *ping 192.168.3.2* <u>non va, i PC sono protetti dall'accesso esterno.</u>

Conclusione: con una sola ACL abbiamo messo in sicurezza la ns rete locale, cioè, dall'accesso esterno.