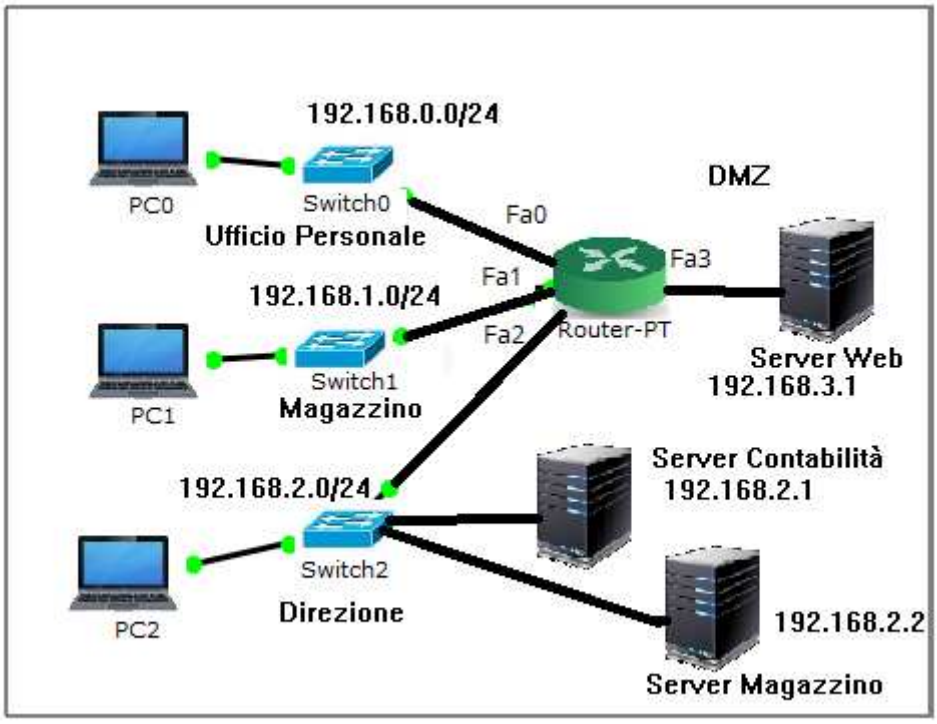
Access List per controllare il traffico interno di una rete

Si vogliono applicare alcune tipiche politiche di sicurezza per controllare il traffico interno di una rete aziendale.

Si considera la rete aziendale in figura con 3 uffici e una Zona Demilitarizzata (DMZ).



Rete con 3 uffici e una DMZ

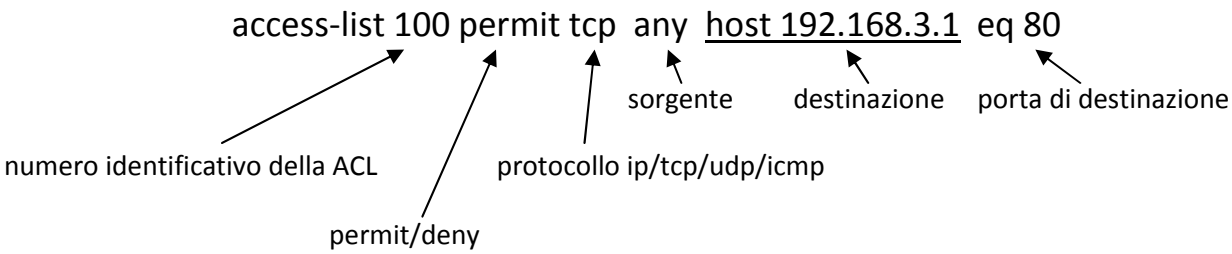
Le politiche di sicurezza che si vogliono appliacare sono le seguenti:

1) Nel SERVER WEB possono entrare tutti ma solo sulle Porte 80 e 443 (http e https)
2) Nel SERVER Magazzino possono entrare solo i pc del magazzino e il direttore
3) Nel SERVER Contabilità può entrare solo il direttore
4) Nell'Ufficio Personale non possono entrare i pc del magazzino

Nel formularle si deve cercare di essere chiari ed esaustivi in modo da indicare tutti quelli che possono entrare (white list) oppure tutti quelli che non possono entrare (black list).

Per ciascuna politica si definisce una Access Control List (ACL) e si specifica anche l'interfaccia del router dove si pensa di applicarla e la direzione del traffico da controllare (ingresso nel router oppure uscita).

Si ricorda brevemente la sintassi di una ACL di tipo Extended:



1) Nel SERVER WEB possono entrare tutti ma solo sulle Porte 80 e 443 (http e https)

R(config)# access-list 100 remark gestisce il traffico verso il server web

R(config)# access-list 100 permit tcp any host 192.168.3.1 eq 80

R(config)# access-list 100 permit tcp any host 192.168.3.1 eq 443

La ACL 100 viene applicata in uscita sull'interfaccia Fa3 del Router:

R(config)# interface Fa3

R(config-if)# ip access-group 100 out

Per verificare la corretta definizione della suddetta ACL si danno i seguenti comandi show:

R# show access-list

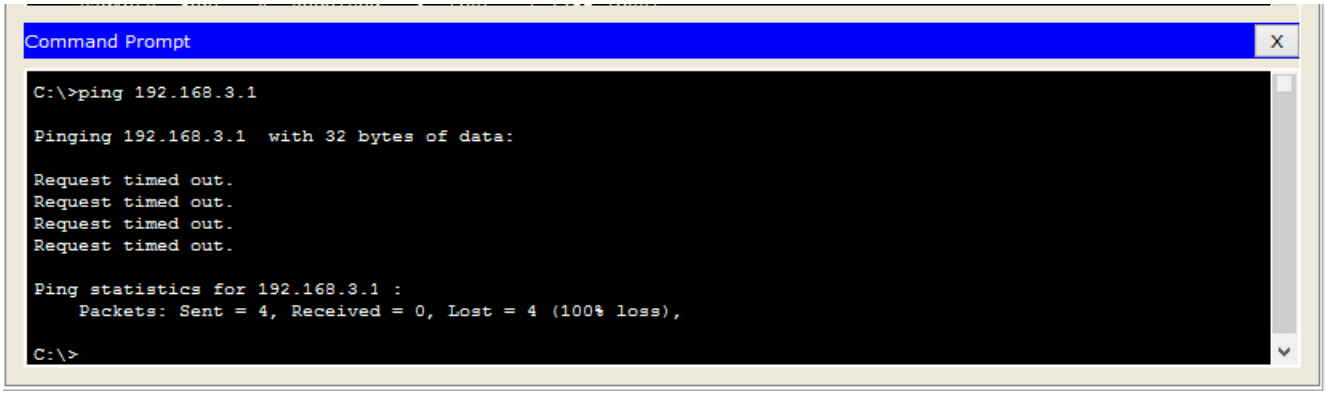
Extended IP access list 100
10 permit tcp any host 192.168.3.1 eq www
20 permit tcp any host 192.168.3.1 eq 443

R# show running-config

….
interface FastEthernet3
ip address 192.168.3.254 255.255.255.0
ip access-group 100 out
….

Si possono fare delle prove per verificare il corretto funzionamento della ACL: da uno dei pc degli uffici con il browser si prova con successo a connettersi a http://192.168.3.1 e a https://192.168.3.1

Si nota che invece il tentativo di fare ping al server web 192.168.3.1 dai pc degli uffici fallisce:



In effetti una ACL ha sempre una riga finale implicita che nega tutto il restante traffico:

access-list 100 deny ip any any

Se si intende variare la ACL 100 per consentire anche il passaggio del ping (protocollo icmp) allora si deve riscrivere l'intera ACL dopo aver cancellato quella precedente:

R(config)# no access-list 100

R(config)# access-list 100 remark gestisce il traffico verso il server web

R(config)# access-list 100 permit tcp any host 192.168.3.1 eq 80

R(config)# access-list 100 permit tcp any host 192.168.3.1 eq 443

R(config)# access-list 100 permit icmp any host 192.168.3.1

Si ricorda che l'ordine di scrittura delle righe è importante perché l'applicazione di una ACL prevede di partire dalla prima riga e di fermarsi appena si trova una riga che riguarda il pacchetto di cui decidere le sorti.

2) Nel SERVER Magazzino possono entrare solo i pc del magazzino e il direttore

R(config)# access-list 101 remark gestisce il traffico verso il server magazzino

R(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2 la rete 192.168.1.0/24

La wildcard mask 0.0.0.255 indica che il sorgente è una rete /24.

La ACL 101 viene applicata ai pacchetti in uscita dall'interfaccia Fa2:

R(config)# interface Fa2
R(config-if)# ip access-group 101 out

Ovviamente il pc del direttore si trova nella stessa rete del server magazzino e pertanto esso avrà sempre accesso libero a tale server senza passare per il router/firewall.

3) Nel SERVER Contabilità può entrare solo il direttore

Si pensa di creare una nuova ACL che impedisca il passaggio di pacchetti verso il server in questione:

R(config)# access-list 102 remark Gestisce il traffico verso il server contabilità
R(config)# access-list 102 deny ip any host 192.168.2.1

da applicare in uscita dall'interfaccia Fa2:

R(config)# interface Fa2
R(config-if)# ip access-group 102 out

Tuttavia questo non funziona perché in uscita dall'interfaccia Fa2 c'era già la ACL 101 e quindi la ACL 102 andrebbe a sostituire la 101. Allora si cancella la ACL 102

R(config)# no access-list 102

e si scrive un'unica ACL che comprenda le politiche 2 e 3:

R(config)# access-list 101 remark gestisce il traffico verso i server magazzino e contabilità

R(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2

R(config)# access-list 101 deny ip any host 192.168.2.1

da applicare ai pacchetti in uscita dall'interfaccia Fa2:

R(config)# interface Fa2

R(config-if)# ip access-group 101 out

Si nota che la ACL termina con un deny esplicito a cui va aggiunto il deny implicito "deny ip any any" e pertanto verrà negato tutto il traffico verso la rete della direzione ad eccezione di quello proveniente dai pc della rete del magazzino e diretto al server magazzino.

In particolare nessuno può raggiungere il pc del direttore, nemmeno i pacchetti provenienti dall'esterno in risposta ad una richiesta proveniente dal pc del direttore stesso! In pratica il pc del direttore non può uscire dalla sua rete!
Allora si potrebbe aggiungere alla ACL 101 una riga per consentire a tutti di raggiungere il pc del direttore (indirizzo ip 192.168.2.3):

access-list 101 permit ip any host 192.168.2.3

In definitiva la ACL 101 diventa la seguente:

R# show access-list

Extended IP access list 100
10 permit tcp any host 192.168.3.1 eq www
20 permit tcp any host 192.168.3.1 eq 443
30 permit icmp any host 192.168.3.1

Extended IP access list 101
10 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2
20 permit ip any host 192.168.2.3
30 deny ip any host 192.168.2.1

4) Nell'Ufficio Personale non possono entrare i pc del magazzino

Per questa richiesta si scrive la ACL 102 da applicare in ingresso all'interfaccia Fa1 del router in modo da troncare sul nascere i pacchetti del magazzino destinati all'ufficio personale:

R(config)# access-list 102 deny ip any 192.168.0.0 0.0.0.255

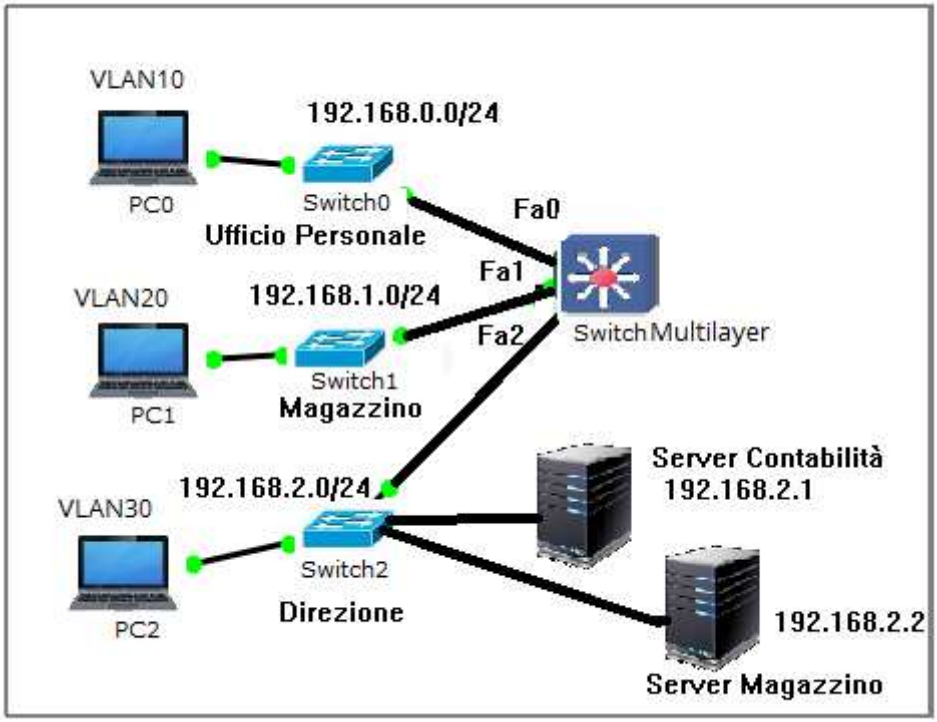
R(config)# interface Fa1
R(config-if)# ip access-group 102 in

Si noti che specificare come sorgente "any" rappresenta qualsiasi pc della rete magazzino, essendo tale ACL applicata in ingresso verso l'interfaccia Fa1.

Rete con switch multilayer

Le reti moderne di una certa complessità prevedono tante VLAN e uno switch multilayer per la gestione del traffico tra le stesse.

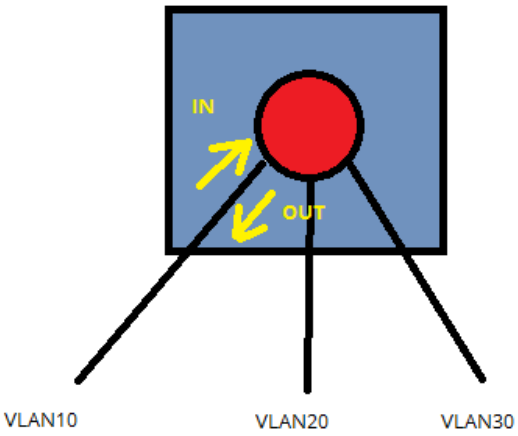
La figura mostra una rete composta da 3 VLAN corrispondenti ai 3 uffici dell'esempio precedente:



Rete con VLAN e switch multilayer

Per implementare le politiche di sicurezza dell'esempio precedente si scrivono le stesse ACL che andranno applicate alle interfacce virtuali (SVI = Switch Virtual Interface) dello switch multilayer.

Ogni VLAN ha la sua SVI. Nell'esempio trattato si avranno le seguenti SVI: Vlan10, Vlan20 e Vlan30 con rispettivamente gli indirizzi ip dei default gateway delle 3 VLAN: 192.168.0.254, 192.168.1.254 e 192.168.2.254.



Ingresso e Uscita dalla SVI di una VLAN

Una ACL applicata in direzione IN verso la SVI di una VLAN va a filtrare i pacchetti provenienti dai pc della VLAN in questione e diretti ad un'altra VLAN o ad una rete esterna.

Invece, una ACL applicata in direzione OUT sulla SVI di una VLAN va a filtrare i pacchetti diretti verso i pc della VLAN in questione.

Pertanto, la ACL 101 dell'esempio precedente si può applicare alla SVI della VLAN30 in direzione out:

Switch(config)# interface Vlan30

Switch(config-if)# ip access-group 101 out

e la ACL 102 dell'esempio precedente si può applicare alla SVI della VLAN 20 in direzione in:

Switch(config)# interface Vlan20

Switch(config-if)# ip access-group 102 in