**ACL Lab**

**Requirement-1:** PC0 of Admin zone and all host of Finance zone cannot access SERVER-1.

Solution:

* Create a standard ACL in ISP router as per following.

**Numbered ACL**

conf t

access-list 10 deny host 192.168.50.21

access-list 10 deny 192.168.60.0 0.0.0.255

access-list 10 permit any

interface FastEthernet0/0

ip access-group 10 out

**Named ACL**

ip access-list standard DENY

deny host 192.168.50.21

deny 192.168.60.0 0.0.0.255

permit any

interface FastEthernet0/0

ip access-group DENY out

* Now check from the PC0 of Admin zone and Finance zone.

**Requirement-2:** From Technology zone 192.168.70.20 IP will not be able to communicate with SERVER-1.

* Create an extended ACL in BR router as per following.

**Numbered ACL**

conf t

access-list 101 deny ip host 192.168.70.20 10.10.10.0 0.0.0.255

access-list 101 permit ip any any

interface FastEthernet0/0.70

ip access-group 101 in

**Named ACL**

ip access-list extended DENY

deny ip host 192.168.70.20 10.10.10.0 0.0.0.255

permit ip any any

interface FastEthernet0/0.70

ip access-group DENY in

**Requirement-3:** From Technology zone 192.168.70.21 IP will not be able to communicate with SERVER-1 port 80 or http.

* Create an extended ACL in BR router as per following.

conf t

ip access-list extended DENY

12 deny tcp host 192.168.70.21 host 10.10.10.100 eq 80

**Requirement-4:** Technology zone and Finance Zone will not communicate with HR SERVER IP 192.168.50.12 via HTTP and HTTPS but ping should be reachable.

* Create an extended ACL in BR router as per following.

ip access-list extended DENY-HR

deny tcp 192.168.60.0 0.0.0.255 host 192.168.50.12 eq www

deny tcp 192.168.60.0 0.0.0.255 host 192.168.50.12 eq 443

deny tcp 192.168.70.0 0.0.0.255 host 192.168.50.12 eq 443

deny tcp 192.168.70.0 0.0.0.255 host 192.168.50.12 eq www

permit ip any any

interface FastEthernet0/0.50

ip access-group DENY-HR out