**Standard ACL**

**Part 1:**     **Plan an ACL Implementation**

**Step 1:**     **Investigate the current network configuration.**

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

**Step 2:**     **Evaluate two network policies and plan ACL implementations.**

a.     The following network policies are implemented on **R2**:

         The 192.168.11.0/24 network is not allowed access to the**WebServer** on the 192.168.20.0/24 network.

         All other access is permitted.

To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

b.    The following network policies are implemented on **R3**:

         The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.

         All other access is permitted.

To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

**Part 2:**     **Configure, Apply, and Verify a Standard ACL**

**Step 1:**     **Configure and apply a numbered standard ACL on R2.**

R2>enable

R2#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255

R2(config)#access-list 1 permit any

R2(config)#interface GigabitEthernet0/0

R2(config-if)#ip access-group 1 out

R2(config-if)#exit

R2(config)#exit

R2#

%SYS-5-CONFIG\_I: Configured from console by console

**Step 2:**     **Configure and apply a numbered standard ACL on R3.**

R3>enable

R3#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255

R3(config)#access-list 1 permit any

R3(config)#interface GigabitEthernet0/0

R3(config-if)#ip access-group 1 out

R3(config-if)#exit

R3(config)#exit

R3#

%SYS-5-CONFIG\_I: Configured from console by console

**Step 3:**     **Verify ACL configuration and functionality.**

R2>enable

R2#show access-list

Standard IP access list 1

 deny 192.168.11.0 0.0.0.255

 permit any

R2#show run

Building configuration...

Current configuration : 956 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R2

!

!

!

!

!

!

!

!

!

!

!

!

license udi pid CISCO1941/K9 sn FTX1524UE18

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

interface GigabitEthernet0/0

 ip address 192.168.20.1 255.255.255.0

 ip access-group 1 out

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 no ip address

 duplex auto

 speed auto

 shutdown

!

interface Serial0/0/0

 description Link to R1

 ip address 10.1.1.2 255.255.255.252

!

interface Serial0/0/1

 description Link to R3

 ip address 10.2.2.1 255.255.255.252

 clock rate 4000000

!

interface Vlan1

 no ip address

 shutdown

!

router eigrp 100

 passive-interface GigabitEthernet0/0

 network 192.168.20.0

 network 10.0.0.0

 no auto-summary

!

ip classless

!

!

access-list 1 deny 192.168.11.0 0.0.0.255

access-list 1 permit any

!

!

!

!

!

line con 0

 login

!

line aux 0

!

line vty 0 4

 login

!

!

!

end

R2#show ip interface gigabitethernet 0/0

GigabitEthernet0/0 is up, line protocol is up (connected)

 Internet address is 192.168.20.1/24

 Broadcast address is 255.255.255.255

 Address determined by setup command

 MTU is 1500 bytes

 Helper address is not set

 Directed broadcast forwarding is disabled

 Outgoing access list is 1

 Inbound access list is not set

 Proxy ARP is enabled

 Security level is default

 Split horizon is enabled

 ICMP redirects are always sent

 ICMP unreachables are always sent

 ICMP mask replies are never sent

 IP fast switching is disabled

 IP fast switching on the same interface is disabled

 IP Flow switching is disabled

 IP Fast switching turbo vector

 IP multicast fast switching is disabled

 IP multicast distributed fast switching is disabled

 Router Discovery is disabled

 IP output packet accounting is disabled

 IP access violation accounting is disabled

 TCP/IP header compression is disabled

 RTP/IP header compression is disabled

 Probe proxy name replies are disabled

 Policy routing is disabled

 Network address translation is disabled

 BGP Policy Mapping is disabled

 Input features: MCI Check

 WCCP Redirect outbound is disabled

 WCCP Redirect inbound is disabled

 WCCP Redirect exclude is disabled

R2#

**Extended ACL**

**Part 1:**     **Configure, Apply and Verify an Extended Numbered ACL**

**Step 1:**     **Configure an ACL to permit FTP and ICMP.**

 R1 > enable

 R1 # config terminal

R1(config)# access-list ?

R1(config)# access-list 100 ?

R1(config)# access-list 100 permit ?

R1(config)# access-list 100 permit tcp ?

R1(config)# access-list 100 permit tcp 172.22.34.64 ?

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

**Step 2:**     **Apply the ACL on the correct interface to filter traffic.**

R1(config)# interface gigabitEthernet 0/0

R1(config-if)# ip access-group 100 in

**Part 2:**     **Configure, Apply and Verify an Extended Named ACL**

**Step 1:**     **Configure an ACL to permit HTTP access and ICMP.**

 (R1 > enable R1 # config terminal)

or

R1 (config-if)# exit

R1(config)# ip access-list ?

R1(config)# ip access-list extended HTTP\_ONLY

R1(config-ext-nacl)# permit tcp 172.22.34.96 ?

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

**Step 2:**     **Apply the ACL on the correct interface to filter traffic.**

R1(config)# interface gigabitEthernet 0/1

R1(config-if)# ip access-group HTTP\_ONLY in

R1(config-if)# exit

R1(config)#exit

R1# show access-list

Extended IP access list 100

10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

Extended IP access list HTTP\_ONLY

10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

 R1# show run

 Building configuration...

Current configuration : 1069 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R1

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

license udi pid CISCO2911/K9 sn FTX15242FJ3

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0

ip address 172.22.34.65 255.255.255.224

ip access-group 100 in

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 172.22.34.97 255.255.255.240

ip access-group HTTP\_ONLY in

duplex auto

speed auto

!

interface GigabitEthernet0/2

ip address 172.22.34.1 255.255.255.192

duplex auto

speed auto

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

ip flow-export version 9

!

!

access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

ip access-list extended HTTP\_ONLY

permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end