# ACL & AAA Configuration Guides

## 1. ACL Demonstration

Observe ACL impact: view ACLs, remove ACL, and verify access.

### View Current ACL Configuration

|  |  |
| --- | --- |
| Prompt | Command |
| R1# | show access-lists |
| R1# | show run | include interface|access |

### Remove ACL from Interface

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface Serial0/0/0 |
| R1(config-if)# | no ip access-group 11 out |
| R1(config-if)# | exit |

### Delete ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | no access-list 11 |

### Verify Access Restoration

|  |  |
| --- | --- |
| Prompt | Command |
| PC1> | ping 192.168.30.12 |
| PC1> | ping 192.168.31.12 |

## 2. Numbered Standard IPv4 ACLs

Restrict specific source networks with numbered standard ACLs on R2 and R3.

### Configure and Apply ACL on R2

|  |  |
| --- | --- |
| Prompt | Command |
| 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 |

### Configure and Apply ACL on R3

|  |  |
| --- | --- |
| Prompt | Command |
| 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 |

### Verify ACLs

|  |  |
| --- | --- |
| Prompt | Command |
| R2# | show access-lists |
| R3# | show access-lists |

## 3. Named Standard IPv4 ACLs

Create and apply a named standard ACL to protect a file server.

### Configure Named ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ip access-list standard File\_Server\_Restrictions |
| R1(config-std-nacl)# | permit host 192.168.20.4 |
| R1(config-std-nacl)# | permit host 192.168.100.100 |
| R1(config-std-nacl)# | deny any |

### Apply Named ACL to Interface

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface FastEthernet0/1 |
| R1(config-if)# | ip access-group File\_Server\_Restrictions out |

### Verify Named ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1# | show access-lists |
| R1# | show ip interface FastEthernet0/1 |

## 4. Extended ACLs (Scenario 1)

Permit specific FTP and HTTP/ICMP traffic using extended ACLs.

### Configure Extended Numbered ACL

|  |  |
| --- | --- |
| Prompt | Command |
| 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 |

### Apply Numbered ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface GigabitEthernet0/0 |
| R1(config-if)# | ip access-group 100 in |

### Configure Extended Named ACL

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

### Apply Named ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface GigabitEthernet0/1 |
| R1(config-if)# | ip access-group HTTP\_ONLY in |

## 5. IP ACLs to Mitigate Attacks

Use ACLs to restrict management and service access on edge routers.

### Create Numbered IP ACL 120 on R1

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | access-list 120 permit udp any host 192.168.1.3 eq 53 |
| R1(config)# | access-list 120 permit tcp any host 192.168.1.3 eq smtp |
| R1(config)# | access-list 120 permit tcp any host 192.168.1.3 eq ftp |
| R1(config)# | access-list 120 deny tcp any host 192.168.1.3 eq 443 |
| R1(config)# | access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22 |

### Apply ACL 120 on R1

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface Serial0/0/0 |
| R1(config-if)# | ip access-group 120 in |
| R1(config-if)# | exit |

### Modify ACL 120 for ICMP

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ip access-list extended 120 |
| R1(config-ext-nacl)# | permit icmp any any echo-reply |
| R1(config-ext-nacl)# | permit icmp any any unreachable |
| R1(config-ext-nacl)# | deny icmp any any |
| R1(config-ext-nacl)# | permit ip any any |

### Secure R3 Edge Router

|  |  |
| --- | --- |
| Prompt | Command |
| R3(config)# | access-list 110 permit ip any any |

## 6. Local AAA for Console and VTY Access

Configure local AAA authentication for console and SSH on R1.

### Configure Local User

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | username Admin1 secret admin1pa55 |

### Enable AAA for Console

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | aaa new-model |
| R1(config)# | aaa authentication login default local |
| R1(config)# | line console 0 |
| R1(config-line)# | login authentication default |

### Configure SSH Authentication

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ip domain-name netsec.com |
| R1(config)# | crypto key generate rsa modulus 1024 |
| R1(config)# | aaa authentication login SSH-LOGIN local |
| R1(config)# | line vty 0 4 |
| R1(config-line)# | login authentication SSH-LOGIN |
| R1(config-line)# | transport input ssh |

## 7. Server-Based AAA with TACACS+ and RADIUS

Configure TACACS+ on R2 and RADIUS on R3 with backup local accounts.

### Backup Local Users

|  |  |
| --- | --- |
| Prompt | Command |
| R2(config)# | username Admin2 secret admin2pa55 |
| R3(config)# | username Admin3 secret admin3pa55 |

### Configure TACACS+ on R2

|  |  |
| --- | --- |
| Prompt | Command |
| R2(config)# | tacacs-server host 192.168.2.2 |
| R2(config)# | tacacs-server key tacacspa55 |
| R2(config)# | aaa new-model |
| R2(config)# | aaa authentication login default group tacacs+ local |
| R2(config)# | line console 0 |
| R2(config-line)# | login authentication default |

### Configure RADIUS on R3

|  |  |
| --- | --- |
| Prompt | Command |
| R3(config)# | radius-server host 192.168.3.2 |
| R3(config)# | radius-server key radiuspa55 |
| R3(config)# | aaa new-model |
| R3(config)# | aaa authentication login default group radius local |
| R3(config)# | line console 0 |
| R3(config-line)# | login authentication default |