**ACL Extended**

**Part 2: Configure Devices and Verify Connectivity**

1. **Configure basic settings on R3**
   * 1. Enable SSH.

R3(config)# **ip domain-name cisco.com**

R3(config)# **crypto key generate rsa modulus 1024**

R3(config)# **line vty 0 4**

R3(config-line)# **login local**

R3(config-line)# **transport input ssh**

Enable web access

R1(config)# **ip http server**

R1(config)# **ip http authentication local**

R1(config)# **username admin privilege 15 secret class**

1. **Configure OSPF routing on R1, ISP and R3**

Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 is included for reference.

R1(config)# **router ospf 1**

R1(config-router)# **network 192.168.10.0 0.0.0.255 area 0**

R1(config-router)# **network 192.168.20.0 0.0.0.255 area 0**

R1(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

**Part 3: Configure and Verify Extended Numbered and Named ACLs**

1. **Configure a numbered extended ACL on R1 for security policy numbers 1 and 2**

Configure the ACL on R1. Use 100 for the ACL number.

R1(config)# **access-list 100 remark Allow Web & SSH Access**

R1(config)# **access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22**

R1(config)# **access-list 100 permit tcp any any eq 80**

Apply ACL 100 to the S0/0/0 interface.

R1(config)# **interface s0/0/0**

R1(config-if)# **ip access-group 100 out**

Verify ACL 100.

Open up a web browser on PC-A, and access <http://209.165.200.225> (the ISP router). It should be successful; troubleshoot, if not.

Establish an SSH connection from PC-A to R3 using 10.2.2.1 for the IP address. Log in with **admin** and **class** for your credentials. It should be successful; troubleshoot, if not.

From privileged EXEC mode prompt on R1, issue the **show access-lists** command.

R1# **show access-lists**

Extended IP access list 100

10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)

20 permit tcp any any eq www (111 matches)

1. **Configure a named extended ACL on R3 for security policy number 3.**

Configure the policy on R3. Name the ACL WEB-POLICY.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80**

Apply ACL WEB-POLICY to the S0/0/1 interface.

R3(config-ext-nacl)# **interface S0/0/1**

R3(config-if)# **ip access-group WEB-POLICY out**

Verify the ACL WEB-POLICY.

**Part 4: Modify and Verify Extended ACLs**

1. **Modify ACL 100 on R1**

Enter global configuration mode and modify the ACL on R1.

R1(config)# **ip access-list extended 100**

R1(config-ext-nacl)# **30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255**

R1(config-ext-nacl)# **end**

Issue the **show access-lists** command.

1. **Modify ACL WEB-POLICY on R3**

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255**

R3(config-ext-nacl)# **end**

Issue the **show access-lists** command to verify that the new line was added at the end of the ACL.

1. **Verify modified ACLs**