Extended ACLs

CyberQuince

Standard vs Extended ACLs

Standard ACL: only filters traffic based on source IP

```
Router(config-std-nacl)# deny host 10.0.0.1
```

Standard vs Extended ACLs

Standard ACL: only filters traffic based on source IP

```
Router(config-std-nacl)# deny host 10.0.0.1
```

Extended ACL: filters traffic based on protocol, source and destination IP, and port number

```
Router(config-ext-nacl)# deny icmp host 10.0.0.1 host 10.0.0.2
```

Standard vs Extended ACLs

Standard ACL: only filters traffic based on source IP

```
Router(config-std-nacl)# deny host 10.0.0.1
```

Extended ACL: filters traffic based on protocol, source and destination IP, and port number

```
Router(config-ext-nacl)# deny icmp host 10.0.0.1 host 10.0.0.2
```

source

Standard vs Extended ACLs

Standard ACL: only filters traffic based on source IP

```
Router(config-std-nacl)# deny host 10.0.0.1
```

Extended ACL: filters traffic based on protocol, source and destination IP, and port number

```
Router(config-ext-nacl)# deny icmp host 10.0.0.1 host 10.0.0.2
```

source destination

Standard vs Extended ACLs

```
Router(config-ext-nacl)# deny ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
```

Blocking Traffic Based on Port Numbers

Blocking only Telnet connections:

```
Router(config-ext-nacl)# deny tcp host 10.0.0.1 host 10.0.0.2 eq telnet
```

Blocking Traffic Based on Port Numbers

Blocking only Telnet connections:

```
Router(config-ext-nacl)# deny tcp host 10.0.0.1 host 10.0.0.2 eq telnet
```

or

```
Router(config-ext-nacl)# deny tcp host 10.0.0.1 host 10.0.0.2 eq 23
```

Blocking Traffic Based on Port Numbers

Default TCP protocols:

```
Router(config-ext-nacl)#deny tcp host 10.0.0.1 host 10.0.0.2 eq ?
  <0-65535>  Port number
  domain     Domain Name Service (DNS, 53)
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
```

Blocking Traffic Based on Port Numbers

Default UDP protocols:

```
Router(config-ext-nacl)#deny udp host 10.0.0.1 host 10.0.0.2 eq ?
  <0-65535>      Port number
  bootpc         Bootstrap Protocol (BOOTP) client (68)
  bootps         Bootstrap Protocol (BOOTP) server (67)
  domain         Domain Name Service (DNS, 53)
  isakmp         Internet Security Association and Key Management Protocol (500)
  non500-isakmp  Internet Security Association and Key Management Protocol
                 (4500)
  snmp           Simple Network Management Protocol (161)
  tftp           Trivial File Transfer Protocol (69)
```

Extended ACLs

CyberQuince