

Network Security

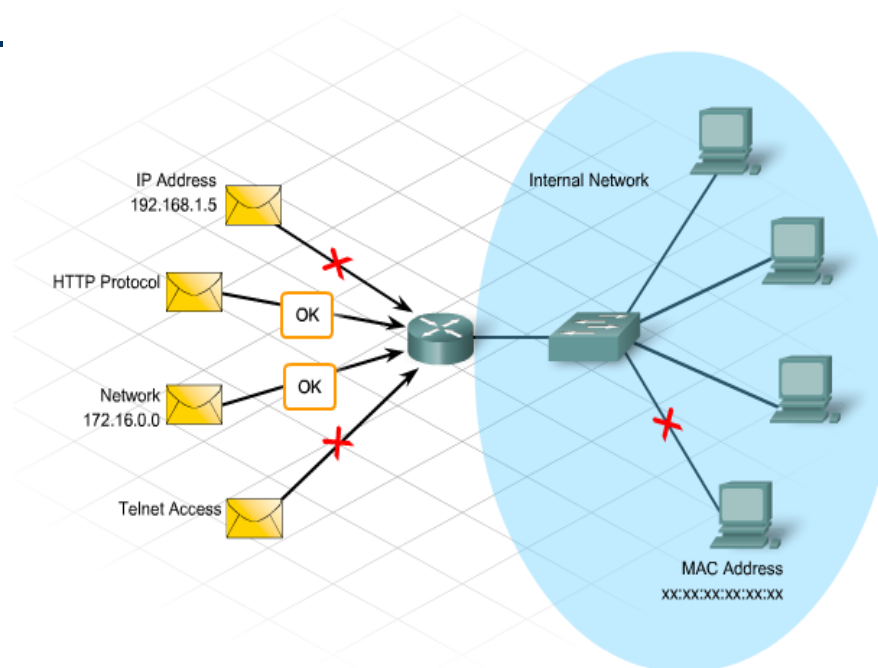
Lecture 5 Implementing Firewall Technologies

جامعة بابل
كلية تكنولوجيا المعلومات
قسم البرمجيات

الدكتور المهندس
الحارث عبدالكريم عبدالله

ACL Topology and Types

- Access Control List (ACL): An ordered list of permit and deny statements that can be applied on a device to effectively determine whether a packet will be permitted or denied access to the network.



ACL Topology and Types

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
Ethernet address	700-799
Transparent bridging (protocol type)	200-299
Transparent bridging (vendor code)	700-799
Extended transparent bridging	1100-1199
DECnet and extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Source-route bridging (protocol type)	200-299
Source-route bridging (vendor code)	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Standard VINES	1-100
Extended VINES	101-200
Simple VINES	201-300

Standard Numbered IP ACLs

```
Router(config)# access-list {1-99} {permit | deny} source-addr [source-mask]
```

- The first value specifies the ACL number
- The second value specifies whether to permit or deny the configured source IP address traffic
- The third value is the source IP address that must be matched
- The fourth value is the wildcard mask to be applied to the previously configured IP address to indicate the range
- All ACLs assume an implicit deny statement at the end of the ACL6+
- At least one permit statement should be included or all traffic will be dropped once that ACL is applied to an interface

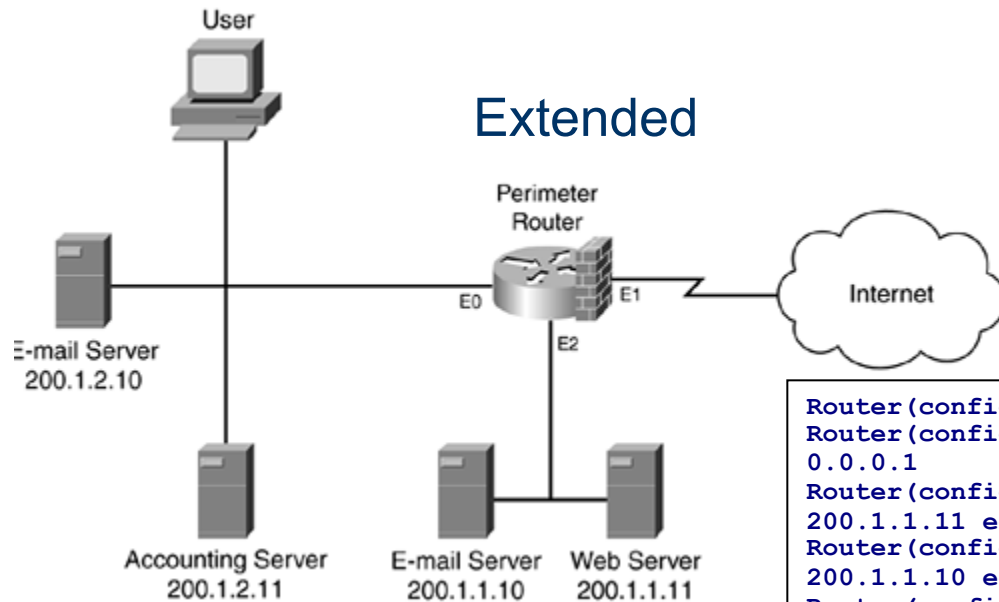
Extended Numbered IP ACLs

```
Router(config)# access-list {100-199} {permit | deny}  
protocol source-addr [source-mask] [operator operand]  
destination-addr [destination-mask] [operator operand]  
[established]
```

- The first value specifies the ACL number
- The second value specifies whether to permit or deny accordingly
- The third value indicates protocol type
- The source IP address and wildcard mask determine where traffic originates. The destination IP address and wildcard mask are used to indicate the final destination of the network traffic
- The command to apply the standard or extended numbered ACL:

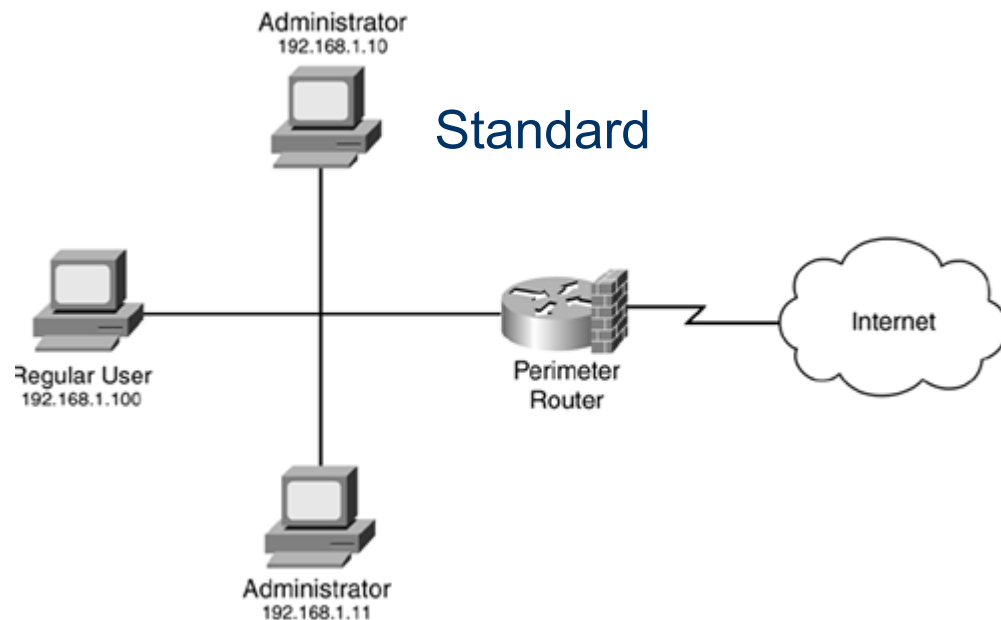
```
Router(config-if)# ip access-group number {in | out}
```

Named IP ACLs



```
Router(config)# ip access-list extended vachon1
Router(config-ext-nacl)# deny ip any 200.1.2.10
0.0.0.1
Router(config-ext-nacl)# permit tcp any host
200.1.1.11 eq 80
Router(config-ext-nacl)# permit tcp any host
200.1.1.10 eq 25
Router(config-ext-nacl)# permit tcp any eq 25 host
200.1.1.10 any established
Router(config-ext-nacl)# permit tcp any 200.1.2.0
0.0.0.255 established
Router(config-ext-nacl)# permit udp any eq 53
200.1.2.0 0.0.0.255
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# interface ethernet 1
Router(config-if)# ip access-group vachon1 in
Router(config-if)# exit
```

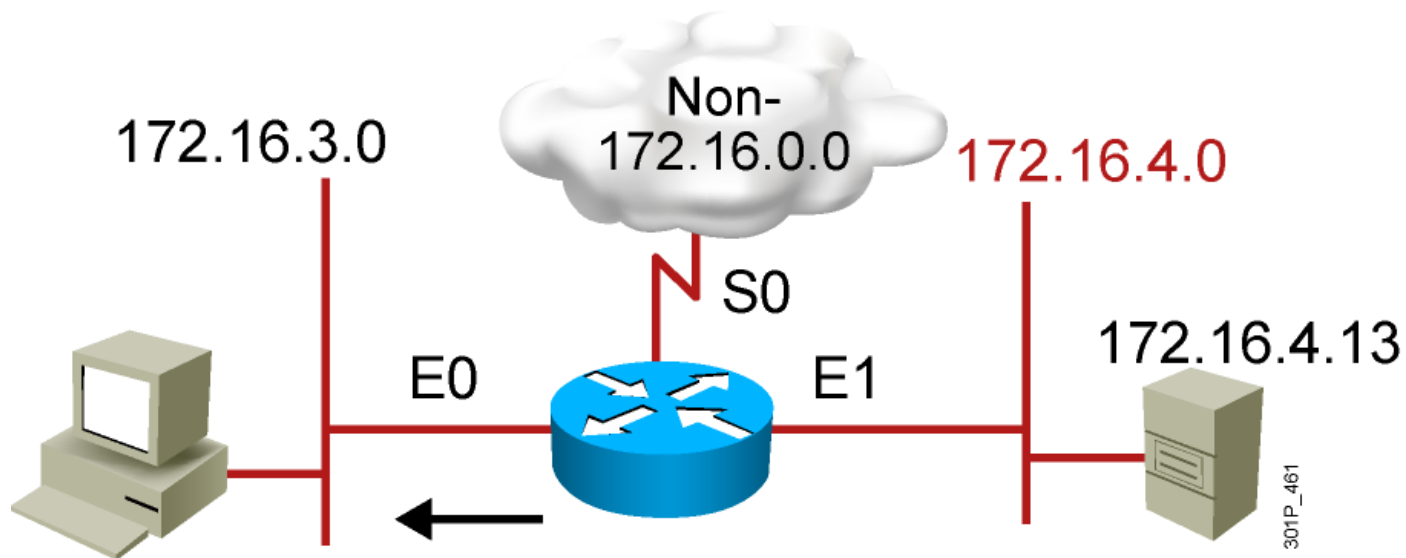
Named IP ACLs



```
Router(config)# ip access-list standard restrict_VTY
Router(config-std-nacl)# permit 192.168.1.10
Router(config-std-nacl)# permit 192.168.1.11
Router(config-std-nacl)# exit
Router(config)# line vty 0 4
Router(config-line)# access-class restrict_VTY in
```

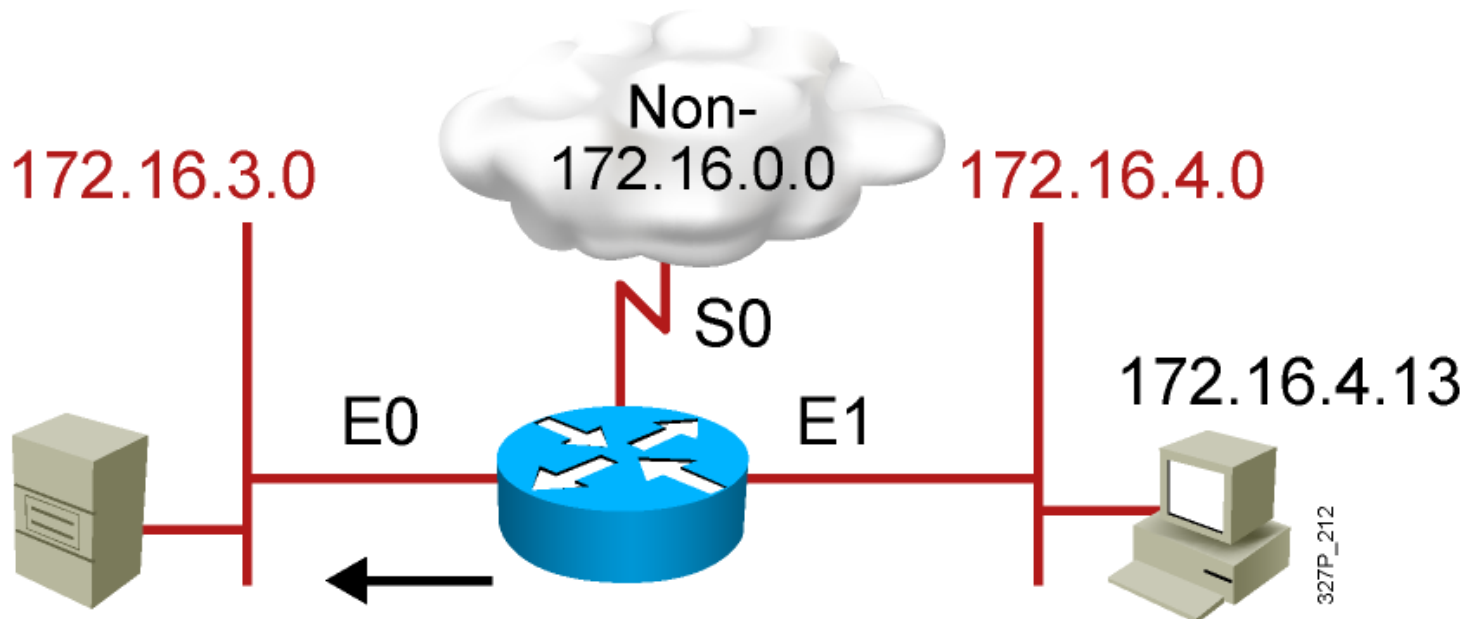
Example 1

Use a standard ACL to block all traffic from 172.16.4.0/24 network, but allow all other traffic.



Example 2

- Use an extended ACL to block all FTP traffic from 172.16.4.0/24 network, but allow all other traffic.



Advantage of ACLs

ACLs can be used to mitigate the following attacks:

- Mitigate IP address spoofing—inbound/outbound
- Mitigate Denial of service (DoS) TCP synchronizes (SYN) attacks—blocking external attacks
- Mitigate DoS TCP SYN attacks—using TCP intercept
- Mitigate DoS smurf attacks
- Filter Internet Control Message Protocol (ICMP) messages—inbound
- Filter ICMP messages—outbound
- Filter traceroute