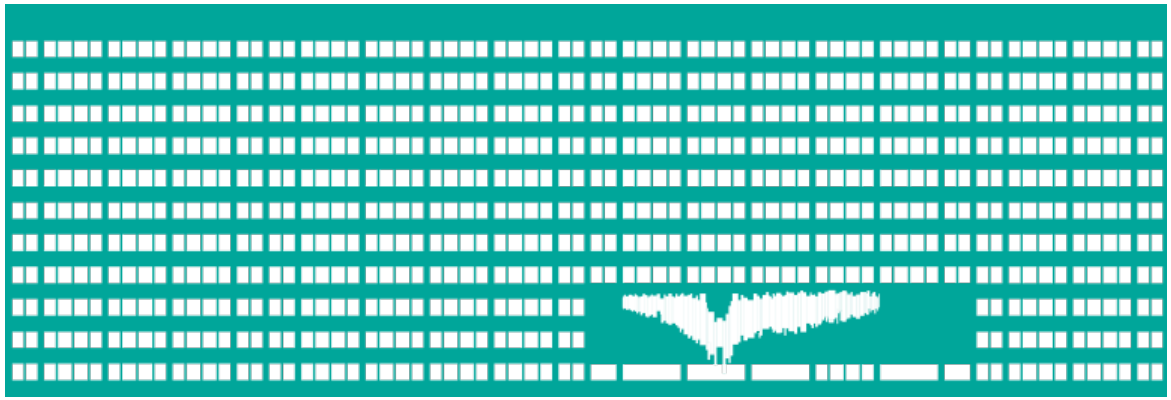
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Access Control Lists (ACL)



Computer networks
Seminar 12

ACL

- Packet filtering rules (stateless)
  - Based on layer header (2nd, 3rd and 4th layer)
  - Passing the rules from first to last
  - In the case of matched rule the rest is skipped
- Choosing the interface which ACL is stuck to.
  - Inbound interface – no need to route dropped packets
  - Outbound interface – uniform processing regardless of packet source
- Closing rule
  - Drop all – implicit; what is not allowed it is denied
  - Let all through – possible to be set manually, atypical
- **It is always needed to allow a backward direction** (SRC↔DST)!

ACL creation

- When creating ACL, we have to answer these question first:
  - To filter on incoming or outgoing traffic, from/to router?
  - Which router interface should be selected?
  - What protocols will be allowed, from where to where, what are their port numbers?
  - Is it better to deny something and allow the rest, or the opposite?

ACL – example 1

- Deny all traffic which is not addressed to VPN concentrator 40.0.0.1.

ACL – example 1

- Deny all traffic which is not addressed to VPN concentrator 40.0.0.1.

Out-going direction

Order	Allow/ deny	Protocol	Source IP	Source port	Destination IP	Destin. port
1	permit	IP	*		40.0.0.1	
2	deny	IP	*		*	

In-going direction

Order	Allow/ deny	Protocol	Source IP	Source port	Destination IP	Destin. port
1	permit	IP	40.0.0.1		*	
2	deny	IP	*		*	

ACL – example 2

- Allow DNS and HTTP(S) protocols to Internet

ACL – example 2

- Allow DNS and HTTP(S) protocols to Internet

Order	Permit/ deny	Protocol	Source IP	Source port	Destination IP	Destin. Port
1	permit	UDP	*	*	*	53
2	permit	TCP	*	*	*	53
3	permit	TCP	*	*	*	80
4	permit	TCP	*	*	*	443
5	deny	IP	*		*	

In-going direction

Order	Permit/ deny	Protocol	Source IP	Source port	Destination IP	Destin. Port
1	permit	UDP	*	53	*	*
2	permit	TCP	*	53	*	*
3	permit	TCP	*	80	*	*
4	permit	TCP	*	443	*	*
5	deny	IP	*		*	

Defining ACL entries on CISCO

- **access-list** <*ACL n.*> {**permit**|**deny**} <*protocol*> <source_*IP*> <*wildcard_mask*> [<source_*port*>] <destination_*IP*> <*wildcard_mask*> [<destination_*port*>] [protocol dependent parameters]
  - Wildcard mask says, which address bit should be ignored and which not
    - 0=compare, 1=ignore
    - „Inverse subnet mask“
  - TCP, UDP port: {**eq**|**gt**|**lt**} <port number>
  - Protocol dependent parameters
    - ICMP message types (**echo**, **echo-reply**, …)
    - If TCP session has to be already established (**established**)

Syntactic shortcuts

- **any**
  - any IP address + wildcard mask **255.255.255.255**
  - *
- **host X.X.X.X**
  - IP address X.X.X.X + wildcard mask **0.0.0.0**

- Example:
  - **`permit tcp host 158.196.100.100 any eq 80`**

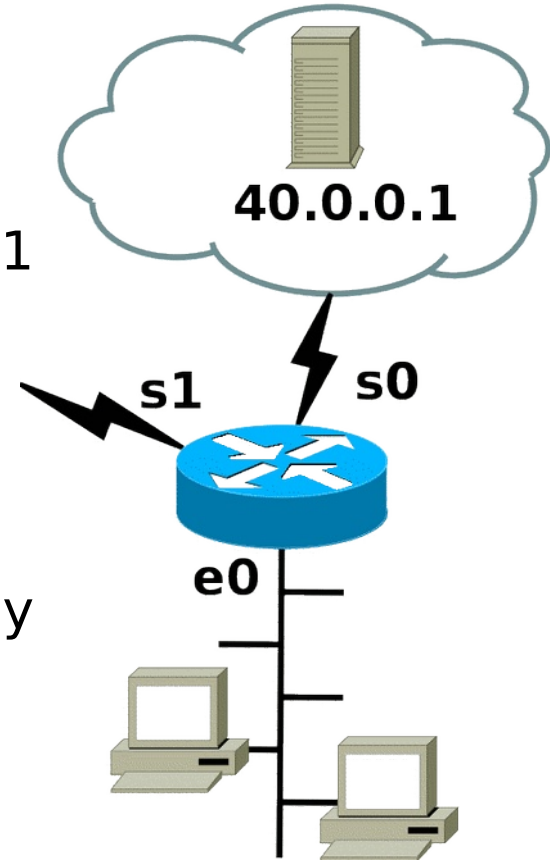
Assigning ACL to an interface

- **interface** *<interfae>*
  ip access-group *<acl n.>* {**in**|**out**}

- ACL is assigned to particular interface by identification number
  - **in** – filters the traffic coming to the inteface (entering the router)
  - **out** – filters the traffic going from interface (leaving the router)

ACL – example 1

- Deny all traffic which is not addressed to ISP proxy server 40.0.0.1.
  - Outgoing direction
    - access-list 101 permit ip any host 40.0.0.1
    - **interface e0**
      - **ip access-group 101 in**
  - Incoming direction
    - access-list 102 permit ip host 40.0.0.1 any
    - **interface e0**
      - **ip access-group 102 out**



ACL – example 2

- Allow DNS and HTTP(S) protocols to Internet
- Outgoing direction
  - `access-list 103 permit udp any any eq 53`
  - `access-list 103 permit tcp any any eq 53`
  - `access-list 103 permit tcp any any eq 80`
  - `access-list 103 permit tcp any any eq 443`
- Incoming direction
  - `access-list 104 permit udp any eq 53  any`
  - `access-list 104 permit tcp any eq 53  any established`
  - `access-list 104 permit tcp any eq 80  any established`
  - `access-list 104 permit tcp any eq 443 any established`

ACL – example 3

- Deny ICMP traffic for network 10.0.20.0/24 except usage of command ping to public network

ACL – example 3

- Deny ICMP traffic for network 10.0.20.0/24 except usage of command ping to public network
- Outgoing direction
  - `access-list 105 permit icmp 10.0.20.0 **0.0.0.255** any **echo**`
  - `access-list 105 deny icmp 10.0.20.0 **0.0.0.255** any`
  - `access-list 105 permit ip any any`
- Incoming direction
  - `access-list 106 permit icmp any 10.0.20.0 **0.0.0.255 echo-reply**`
  - `access-list 106 deny icmp any 10.0.20.0 **0.0.0.255**`
  - `access-list 106 permit ip any any`

ACL – example 4

- Allow the access from outside to POP3 servers in network 100.70.20.40/30 and to SMTP server 100.70.20.45

ACL – example 4

- Allow the access from outside to POP3 servers in network 100.70.20.40/30 and to SMTP server 100.70.20.45
- Outgoing direction
  - access-list 107 permit tcp 100.70.20.40 **0.0.0.3** eq 110 any **established**
  - access-list 107 permit tcp host 100.70.20.45 eq 25 any **established**
  - access-list 107 permit tcp host 100.70.20.45 any eq 25
  - (rules allowing the access to DNS servers should follow)
- Incoming direction
  - access-list 108 permit tcp any 100.70.20.40 **0.0.0.3** eq 110
  - access-list 108 permit tcp any host 100.70.20.45 eq 25
  - access-list 108 permit tcp any eq 25 host 100.70.20.45 **established**
    - (rules allowing the access to DNS servers should follow)

ACL – example 5+6

- Avoid the packets to leave private network 192.168.0.0/16

- Avoid faked packets of network 192.168.0.0/16 from the outside to enter private network (anti-spoofing filter)

ACL – example 5+6

- Avoid the packets to leave private network 192.168.0.0/16
  - (Just) outgoing direction
    - **access-list 109 deny ip 192.168.0.0 0.0.255.255 any**
    - access-list 109 permit ip any any
- Example 6
  - (Just) incoming direction
    - **access-list 110 deny ip 192.168.0.0 0.0.255.255 any**
    - access-list 110 permit ip any any