Network Technology 2 –

Lennart Franked
email:lennart.franked@miun.se
Tel:060-148683

Informations- och Kommunikationssystem (IKS)
Mittuniversitetet

2014-04-23

Slides are based on Chapters 4 and 5 in Accessing the WAN[4].

Introduction

- Threats,
- Open versus Closed Networks.
- Security Policies.
- Attacks.
- Mitigation Techniques.
- Securing the Routers.
- Access Control Lists.
- Wildcard masks.

Threats

Threats over the years:

- 1985: Password guessing and code replication.
- 1990: Password cracking and war dialers.
- 1995: Viruses.
- 2000: Trojan horses.
- 2005: Worms.
- 2010:
- 2015: ?

Threats

Threats over the years:

- 1985: Password guessing and code replication.
- 1990: Password cracking and war dialers.
- 1995: Viruses.
- 2000: Trojan horses.
- 2005: Worms.
- 2010:
  - Piggybacking.
- 2015: ?

Threats

Threats over the years:

- 1985: Password guessing and code replication.
- 1990: Password cracking and war dialers.
- 1995: Viruses.
- 2000: Trojan horses.
- 2005: Worms.
- 2010:
  - Piggybacking.
  - Injection attacks.
- 2015: ?

Threats

Threats over the years:

- 1985: Password guessing and code replication.
- 1990: Password cracking and war dialers.
- 1995: Viruses.
- 2000: Trojan horses.
- 2005: Worms.
- 2010:
  - Piggybacking.
  - Injection attacks.
  - Denial-of-service.
- 2015: ?

Threats

Threats over the years:

- 1985: Password guessing and code replication.
- 1990: Password cracking and war dialers.
- 1995: Viruses.
- 2000: Trojan horses.
- 2005: Worms.
- 2010:
  - Piggybacking.
  - Injection attacks.
  - Denial-of-service.
  - Social Engineering (Phising).
- 2015: ?

Types of attackers

Attackers

- White hat, Black hat, Grey hat.
- Hacker versus Cracker.
- Phreaker.
- Spammer.
- Phiser.

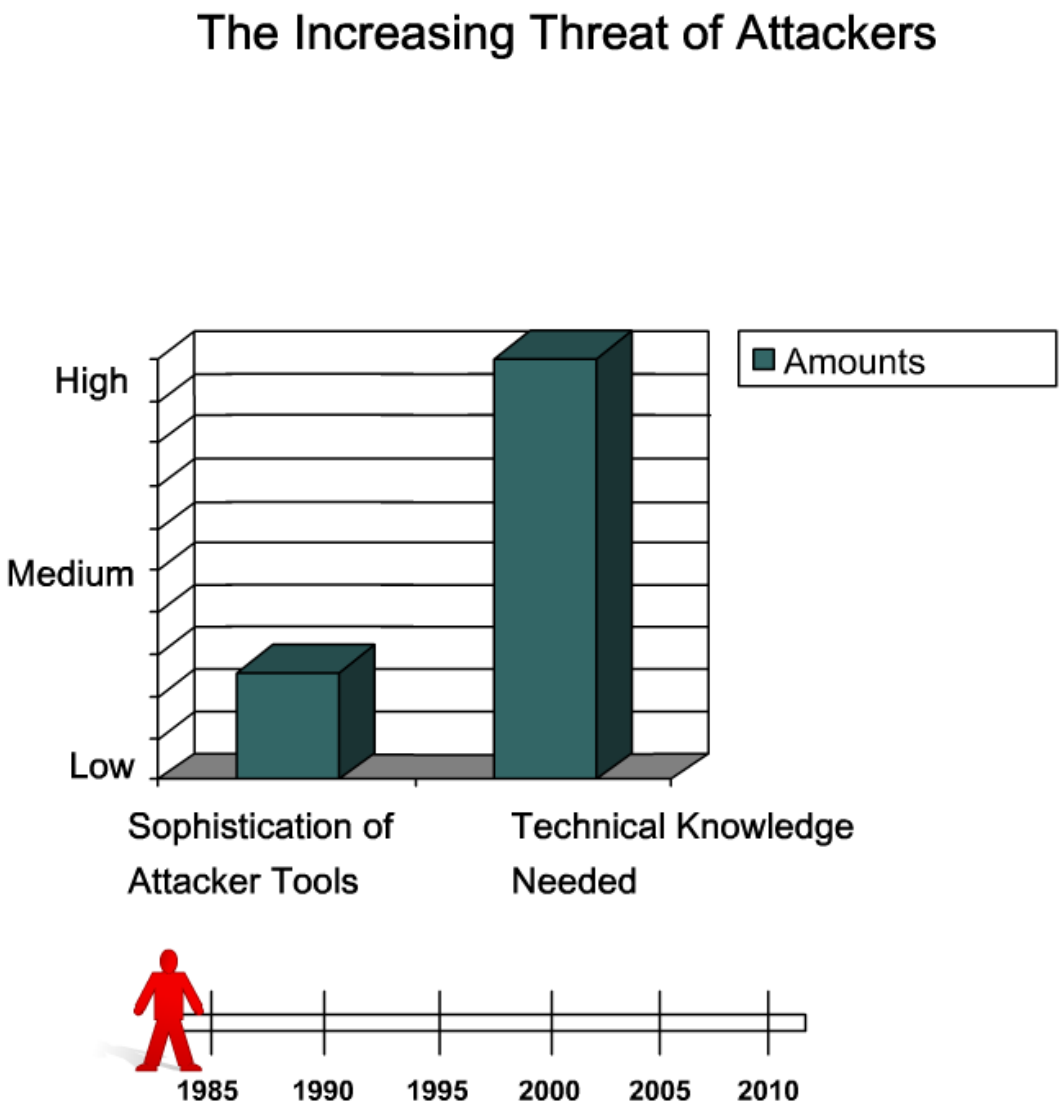

Figure 1 : Less technical knowledge is needed [4]

Common Security Threats

Common factors in Network Security

- Vulnerabilities.
- Threats.
- Attacks.

Vulnerabilities

Weaknesses

A vulnerability is a potential way in for an attacker.

- Technological weaknesses.
- Configuration weaknesses.
- Security policy weaknesses.
- Social weaknesses.

Weaknesses

Technological Weaknesses	Examples
TCP/IP protocol	HTTP, FTP, ICMP, SMTP, SNMP, SYN-floods
Operating System	Exploits are found at regular bases

Configuration Weaknesses	Examples
Unsecured user accounts	Sending sensitive information unencrypted
Weak passwords	Lack of knowledge
Mis-configured internet services	JavaScript enabled
Default settings	Forgot to change default settings of devices
Mis-configured network equipment	Accesslists, routing protocols

Weaknesses continued.

Policy Weaknesses	Examples
Lack of written security policy	Cannot be consistently applied
Corporate politics	Political arguments and battles makes policies difficult to implement.
Logical Access Controls are not applied	Inadequate monitoring and auditing allows misuse, attacks and waste of resources.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or the installation of unapproved applications creates security holes.
Lack of disaster recovery	Could result in chaos and confusion if the worse would happen.

Social Weaknesses	Examples
Staff not educated in basic security	Results in weak passwords, unsecured use of computers, network access and facilities, circumvent security
Disgruntled employees	Information leakage, sabotage, theft.

Threats to physical infrastructure

Four classes of physical threats:

- Hardware threats.
  - Theft or vandalism.
- Environmental threats.
  - Temperature extremes.
- Electrical threats.
  - Voltage spikes.
- Maintenance threats.
  - Poor handling of equipment.

Structured and Unstructured threats

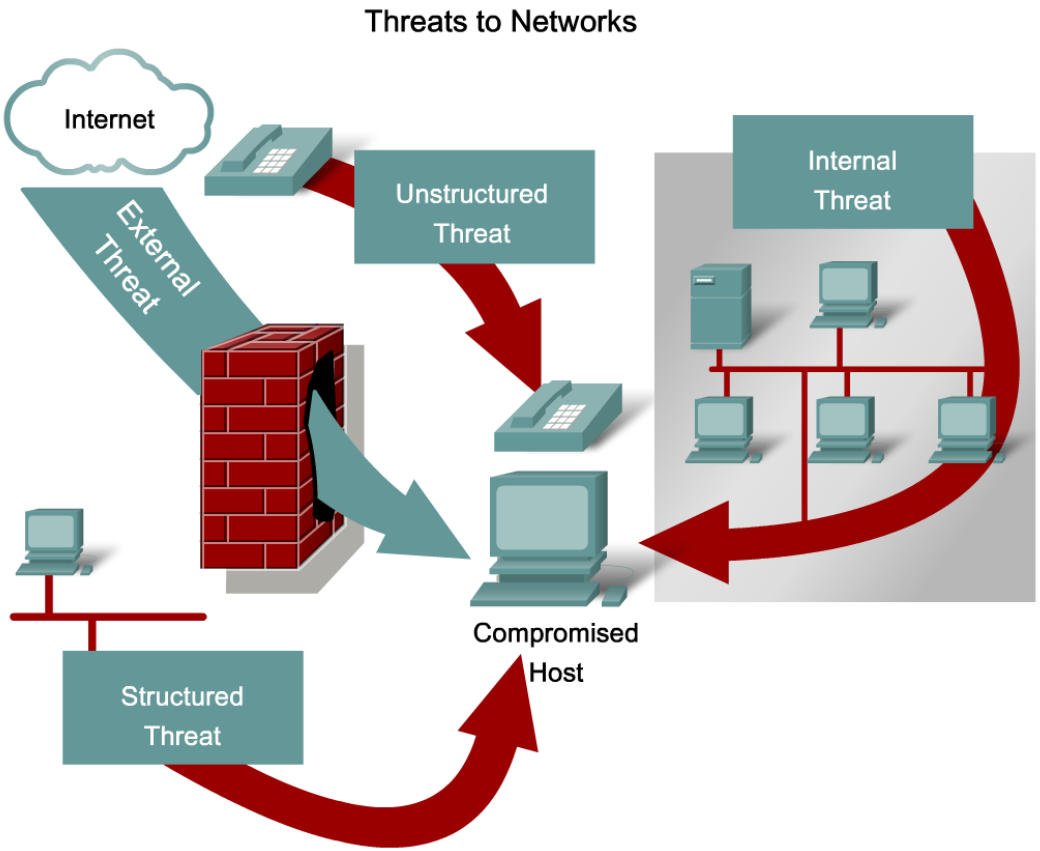

Figure 2 : Types of threats to networks [4]

Open versus Closed Networks

- Open – Open by default.
- Restrictive – Closed by default.

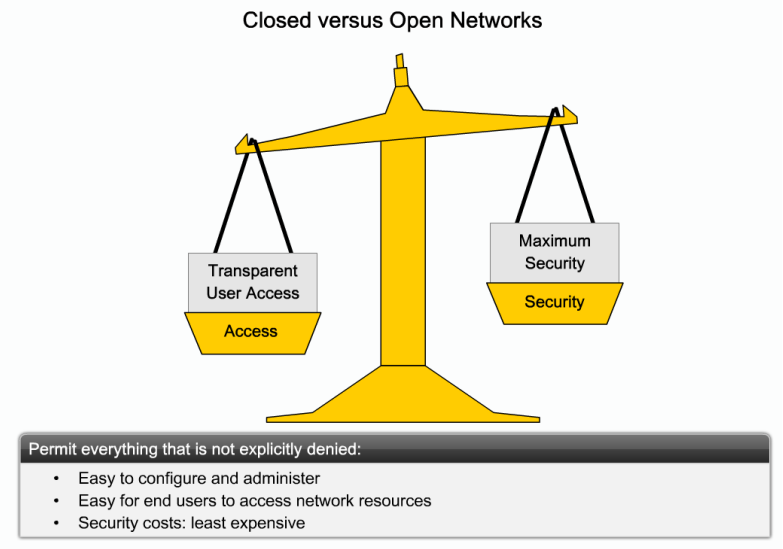

Figure 3 : Open versus Closed networks [4]

Open Networks

Advantages

- Easy to configure and administrate.
- Ease of access.

Disadvantages

- Easy to miss necessary restrictions.

Restricted Networks

Advantages

- Security.

Disadvantages

- Users will have problems accessing resources.
- Circumvent security.

Security Policies

Definition: Security policy

"Security policy is a formal statement of the rules by which people who are given access to an organisation's technology and information must abide" [1]

- Every organisation should have a security policy.
- Contains anything from how to use the company network wisely to a very long and explicit documentation about everything.
- ISO 27002 contains practical guidelines to create a security policy for an organisation.
- The SANS institure provides guidelines as well.

Components of a Security Policy

Examples of what a security policy should contain

- Statement of Authority and scope – Defines who is responsible for what.
- Acceptable use policy (AUP) – Defines acceptable use of equipment and services.
- Identification and authentication policy – Defines the technology used for authentication.
- Password policy – Defines how to create, protect and change passwords.
- Access policies – Policies on how to access and use the network.
- Incident-handling procedure – How to respond to security incidents.

Active and Passive Attacks

Passive Attack

"A "passive attack" attempts to learn or make use of information from a system but does not affect system resources of that system."[3]
Referred to as *non-invasive* in the course materials.

Active Attack

"An "active attack" attempts to alter system resources or affect their operation."[3]
Referred to as *invasive* in the course materials.

Attacks

Types of attacks

- Reconnaissance.
- Access.
- Denial-of-Service(DoS).
- Malicious code.

Reconnaissance

Definition

"Reconnaissance is the unauthorized discovery and mapping of systems, services or vulnerabilities."[4]

Reconnaissance attacks

- Passive and active attacks
- Following methods are usually used:
  - Internet information queries.
  - Ping sweeps.
  - Port scans.
  - Passive wiretapping "Packet sniffing".

Protection against reconnaissance attacks

Three methods for protection against passive attacks

- Limit physical access to networks (VLANs).
- Encryption.
- Enforce security policies.

Access

Definition

An attacker gains access to a system which that person should not have access to.

Access attacks

- Active attack.
- Passwords can be gained by either active or passive attacks.
- Key-logger, social engineering, vulnerabilities (Injection attacks), password attacks.

Protection against access attacks

Methods for protection against access attacks

- Limit physical access to devices.
- Encryption.
- Enforce security policies.

Man-in-the-Middle Attacks

Definition

"A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association."[3]

Man-in-the-Middle Attacks

MITM

- Active attack.
- Active Wiretapping.
- Social Engineering (such as Phishing).

Protection against MITM

- Authentication.
- Integrity check.

Denial-of-Service (DoS)

Definition

"The prevention of authorized access to a system resource or the delaying of system operations and functions."[3]

DoS

- Active attack.
- Flooding.
  - SYN-flood.
  - ICMP-flood.
- Physically disrupt services.
- Distributed Denial-of-Service (DDoS).

Protection against Denial-of-Service (DoS)

DoS

- Awareness – Keep yourself update about security vulnerabilities.
- Detection – Make sure that you are able to detect an ongoing attack.
- Prevention – Traffic rate limiting, deny specific type of data, Redundancy.
- Response – React effectively when an attack occur (Security policy).

[3]

Malicious Code

Worm

"A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume system resources destructively."[3]

Virus

"A self-replicating (and usually hidden) section of computer software (usually malicious logic) that propagates by infecting – i.e., inserting a copy of itself into and becoming part of – another program. A virus cannot run by itself; it requires that its host program be run to make the virus active."[3]

Trojan Horse

"A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program." [3]

Worm

- **The enabling vulnerability:** Installs itself using a known vulnerability.
- **Propagation mechanism:** Copies itself to the host and select a next target.
- **Payload:** Worms usually makes the host available to the attacker.

- Containment – Contain the spread of the worm.
- Inoculation – Remove the vulnerability.
- Quarantine – Find all infected machines.
- Treatment – Clean and patch these hosts as well.

Securing the Routers

Security problems on a router

- Compromising the access control can expose network configuration details.
- Compromising the routing table can reduce performance, deny network communication services.
- Misconfiguring a router traffic filter can expose internal network components to scans and attack.

Basic security

Common practise

- Physical security.
- Keep routers updated.
- Back-up router configurations and IOS.

Applying Cisco IOS Security Features

- Manage router security.
- Secure remote administrative access to routers.
- Log router activity.
- Secure vulnerable router services and interfaces.
- Secure routing protocols.
- Control and filter network traffic.

Manage router security

Strong passwords

- Do *not* write down passwords.
- Do *not* use dictionary words, phonenumbers, dates, names et cetera.
- Combine letters, number and special characters.
- Deliberately misspell a password (This is not good advise).
- Use long passwords.
  - A password of 16 characters minimum without any other requirement provides strong security.[2]
- Change passwords often.

Hash your passwords

Always store passwords hashed using:
`enable secret`, `service password encryption`

Hash algorithms

MD5 is *not* a strong encryption method.

Secure remote administrative access to routers

Access the router

Three ways to connect the router:

- Console.
- Telnet.
- SSH.

Disable unused ports

Initial steps

- Disable logins on AUX-port if it is not used.
- Set a exec-timeout on VTYs.
- Only allow SSH login.

Running SSH in IOS

Steps for setting up SSH

- Set a Hostname.
- Set a Domain name.
- Generate Asymmetric keys.
- Configure local authentication and vty.
- Configure SSH timeouts.

Log router activity

Logs

- If possible, send router logs to a dedicated syslog-server.
- Make sure that the timestamps are accurate.

Secure vulnerable router services and interfaces.

Disable unused services

Disable all services that isn't used on the router.

```
R1#auto secure
Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:1
Enter the interface name that is facing internet:Serial0/1/0
Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
(output omitted)
```

Figure 4 : Secure the router using auto secure [4]

Secure routing protocols.

Enable authentication for routing protocols

If using a routing protocol, make sure that authentication mode is enabled.

Definitions

Firewall

"An internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall)."[3]

Access Control Lists

"A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity." [3]

Access Control Lists when used with firewalls

ACLs

Allows us to create rules of what traffic to permit or block.

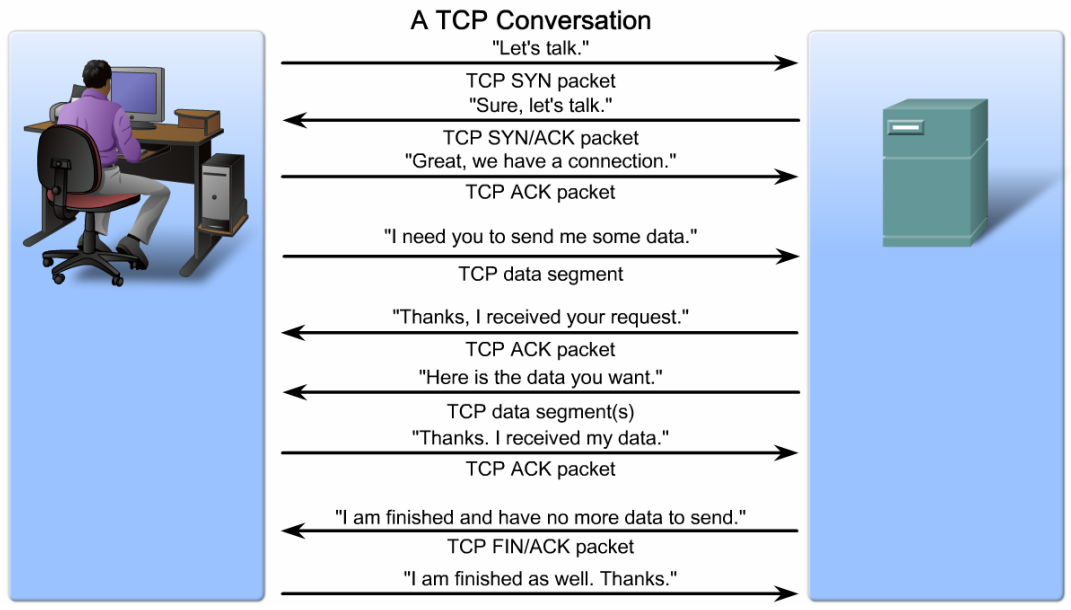

Figure 5 : Overview of a TCP conversation [4]

Port addresses

Table 1 : Port Numbers

Port Number Range	Port Group
0 to 1023	Well-known ports
1024 to 49151	Registered ports
49152 to 65535	Private and/or dynamic ports

Table 2 : Examples of Port Numbers

Type of Port	Port Number	Description
Well-known TCP ports	21	FTP
	22	SSH
	25	SMTP
	80	HTTP
	110	POP3
	143	IMAP
	443	HTTPS
Well-known UDP ports	96	TFTP
	520	RIP
Well-known TCP/UDP ports	53	DNS
	161	SNMP

Packet Filter

Packet filter firewalls

Packet filtering firewall can filter traffic based on:

- Packet L3 source and/or destination address.
- Packet L3 protocol.
- Packet L4 source and/or destination address.
- Packet L4 protocol.

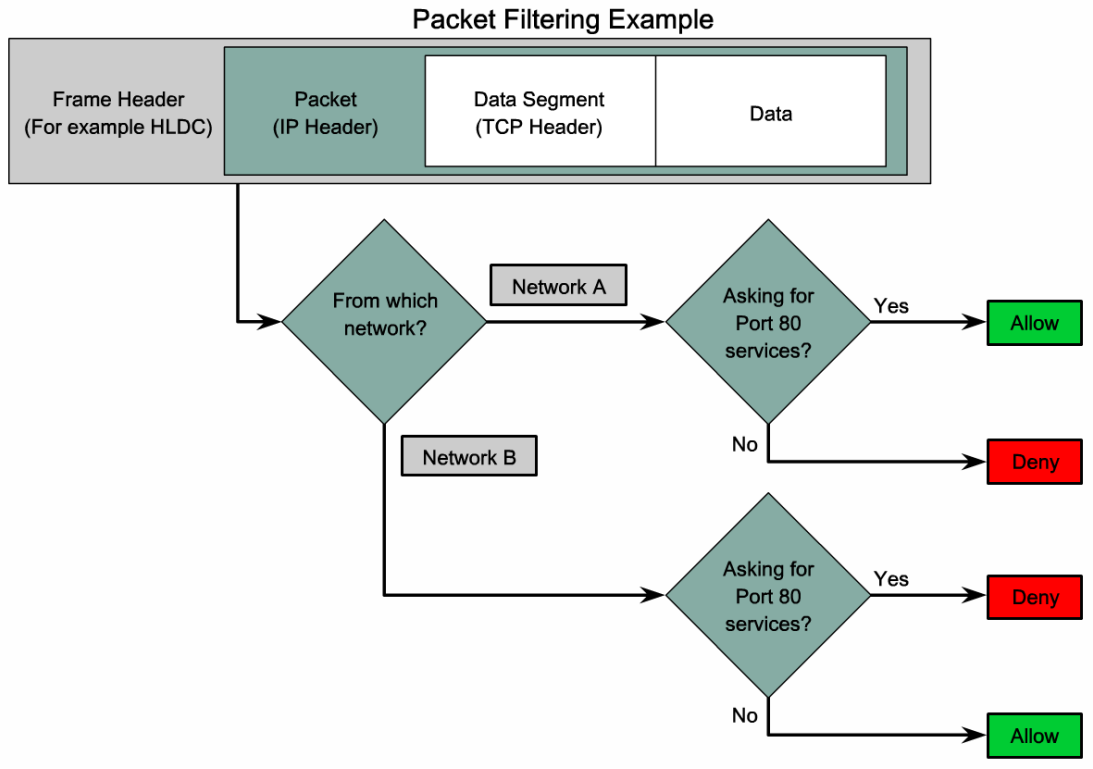

Figure 6 : Flow chart over a packet filtering firewall. [4]

ACL Overview

- Use an ACL on routers that are positioned between your internal and your external network.
- Use an ACL between two parts of your network to control traffic to these parts.
- Use an ACL for each network protocol running on the border router.

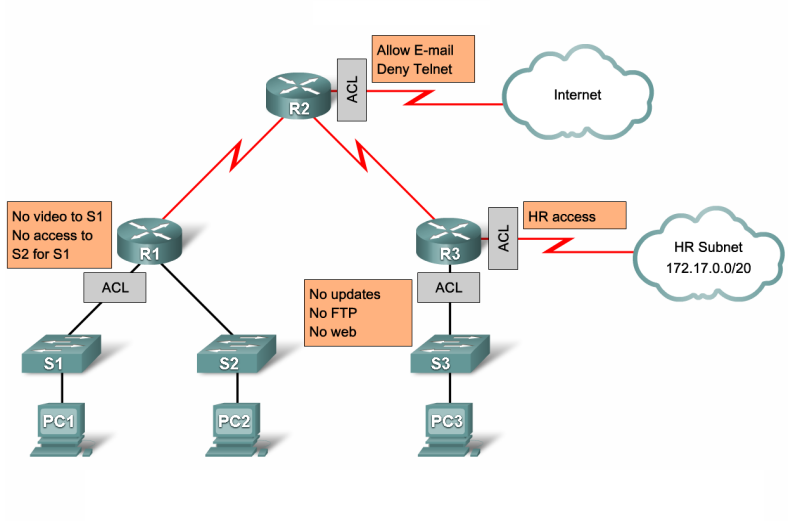

Figure 7 : An overview of how to use ACL. [4]

PID

One ACL per *protocol*, *interface* and *direction*.

- An ACL can be added to Inbound or Outbound.
- If a packet is permitted by the ACL, then it will be processed for routing.
- Outgoing packets are evaluated once the packet has been forwarded to the outgoing interface.
- Start with specific rules, and end with general rules.
- If no match it will by default deny the packet.

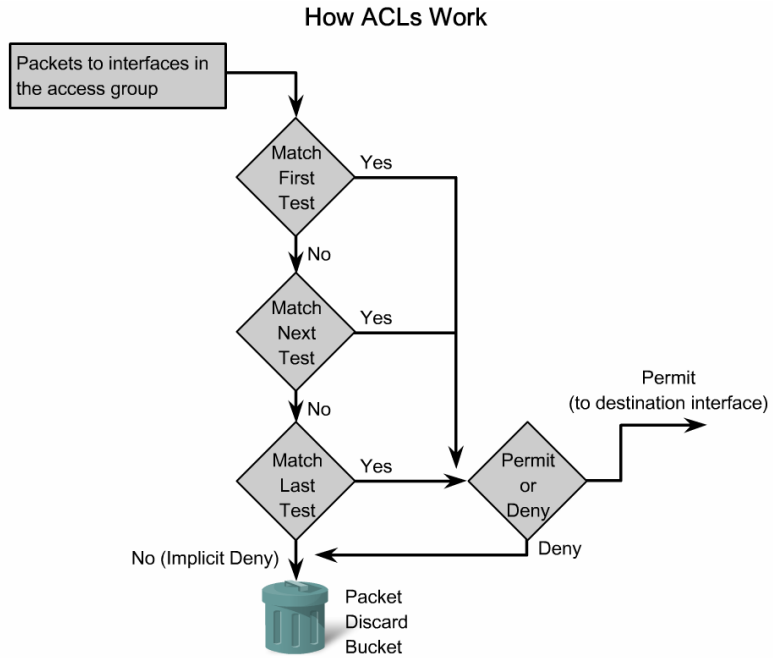

Figure 8 : ACL flow chart [4]

Types of ACLs on Cisco devices

Numbered ACLs

- 1-99 and 1300-1999: Standard IP ACL.
- 100-199 and 2000-2699: Extended IP ACL.
- Cannot add or delete entries within the ACL.

Named ACLs

- Give an ACL a name.
- Alphanumerical characters.
- Recommended to be written in capital letters.
- Possible to add and delete entries.

Types of ACLs on Cisco devices

Standard ACL

A standard ACL filter packets based on source IP only.

```
Router(config)# access-list 10 permit 10.14.14.1 0.0.0.255
Router(config)# ip access-list standard NETLAB
Router(config-std-nacl)# permit 10.14.14.1 0.0.0.255
```

Extended ACL

An extended ACL filters based on IP, Port, and L3 and L4 protocol.

```
Router(config)# access-list 103 permit tcp 10.14.14.1 0.0.0.255 any eq
80
Router(config)# ip access-list extended NETLAB
Router(config-ext-nacl)# permit tcp 10.14.14.1 0.0.0.255 any eq 80
```

Complex ACL

Table 3 : Complex ACL Categories [4]

Complex ACL	Description
Dynamic ACLs (lock-and-key)	Users who want to traverse the router are blocked until they use Telenet to connect to the router and are authenticated.
Reflexive ACLs	Allows outbound traffic and limits inbound traffic in response to sessions that originate inside the router.
Time-based ACLs	Allows for access control based on the time of day and the day of week.

Complex ACL

Dynamic ACL

```
Router(config)# username Gladstone password 0 Gander
Router(config)# access-list 101 permit src dst eq telnet
Router(config)# access-list 101 dynamic name timeout time permit ip src
dst
Router(config-if)# ip access-group 101 in
Router(config-line)#login
Router(config-line)# autocommand access-enable host timeout time
```

Reflexive ACL

Reflexive ACL

```
Router(config)# ip access-list extended name
Router(config-ext-nacl)# permit proto src dst reflect name – Outbound
interface
Router(config) ip access-list extended name
Router(config-ext-nacl)# evaluate name of reflect
Router(config-if)# ip access-group name of inbound filter in
Router(config-if)# ip access-group name of outbound filter out
```

Complex ACL

Complex ACL

```
Router(config)# time-range name
Router(config-time-range)# periodic days time
Router(config) ip access-list 101 permit proto src dst port time-range
name of time range
Router(config-if)# ip access-group 101 out
```

Wildcard masks

References

[1] B. Fraser. Site Security Handbook. RFC 2196 (Informational), September 1997. URL `http://www.ietf.org/rfc/rfc2196.txt`.

[2] Saranga Kommanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Christin Nicolas, Lorrie Faith Cranor, and Serge Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *CHI*, 2011. URL `http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf`.

[3] R. Shirey. Internet Security Glossary, Version 2. RFC 4949 (Informational), August 2007. URL `http://www.ietf.org/rfc/rfc4949.txt`.

[4] Bob Vachon and Rick Graziani. *Accessing the WAN : CCNA exploration companion guide*. Cisco Press, Indianapolis, Ind., 2008. ISBN 978-1-58713-205-6 (hardcover w/cd).