TI III: Operating & Communication Systems

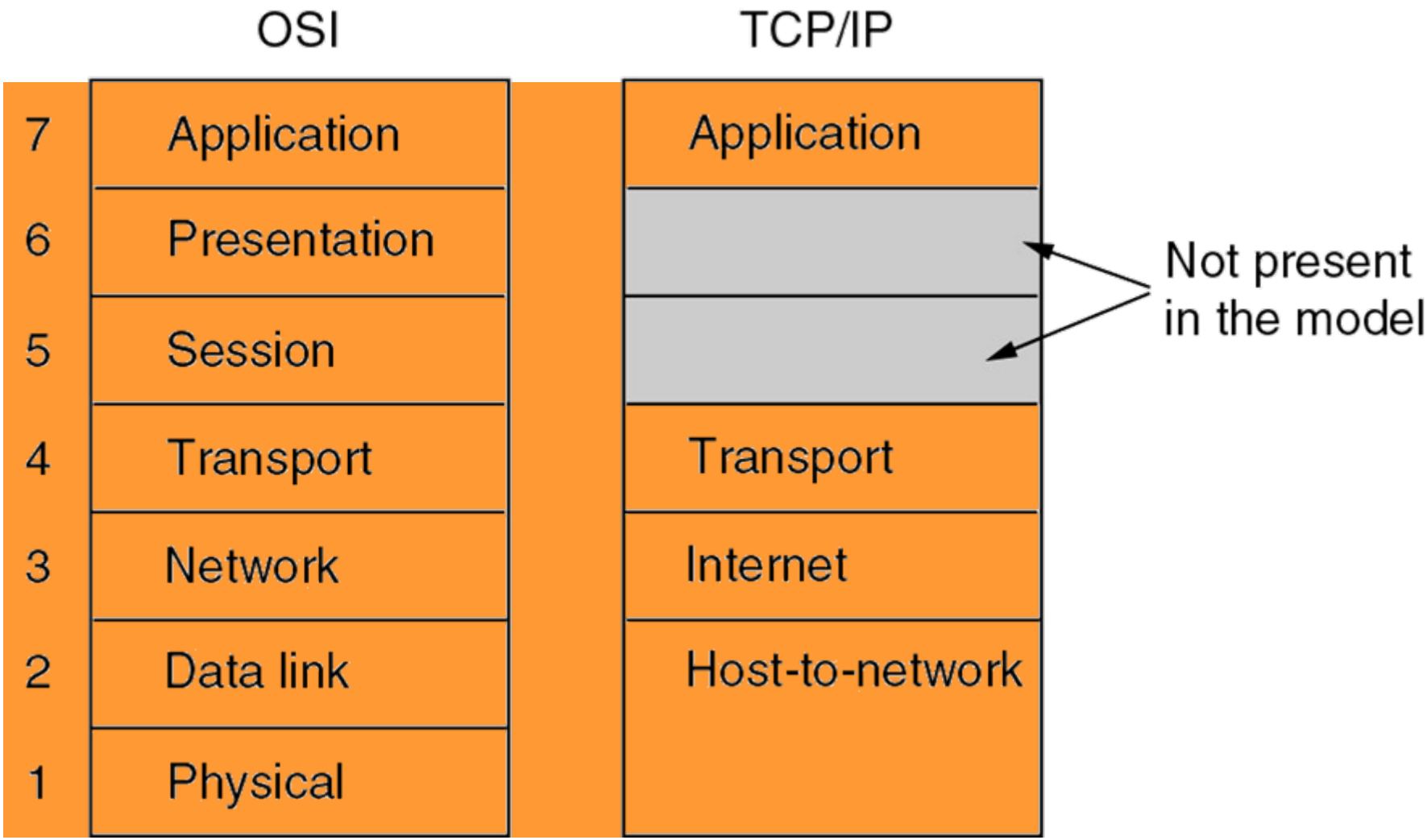
Security

Basic concepts & terms

Cryptology

Examples (Firewalls, VPNs, IPSec, PGP)

Content (2)


OSI
TCP/IP
7
Application
Application
6
Presentation
5
Session
Not present
in the model
4
Transport
Transport
3
Network
Internet
2
Data link
Host-to-network
1
Physical

What is a threat in a communication network?

- Abstract Definition
  - A *threat* in a communication network is any possible event or sequence of actions that might lead to a violation of one or more *security goals*
  - The actual realization of a threat is called an *attack*

- Examples
  - A hacker breaking into a corporate computer
  - Disclosure of emails in transit
  - Someone changing financial accounting data
  - A hacker temporarily shutting down a website
  - Someone using services or ordering goods in the name of others

Security goals technically defined

- Confidentiality
  - Data transmitted or stored should only be revealed to an intended audience
  - Confidentiality of entities is also referred to as anonymity
- Data Integrity
  - It should be possible to detect any modification of data
  - This requires to be able to identify the creator of some data
- Accountability
  - It should be possible to identify the entity responsible for any communication event
- Availability
  - Services should be available and function correctly
- Controlled Access
  - Only authorized entities should be able to access certain services or information

Threats technically defined

- Masquerade
  - An entity claims to be another entity
- Eavesdropping
  - An entity reads information it is not intended to read
- Authorization Violation
  - An entity uses a service or resources it is not intended to use
- Loss or Modification of (transmitted) Information
  - Data is being altered or destroyed
- Denial of Communication Acts (Repudiation)
  - An entity falsely denies its participation in a communication act
- Forgery of Information
  - An entity creates new information in the name of another entity
- Sabotage
  - Any action that aims to reduce the availability and / or correct functioning of services or systems

Threats and technical security goals

Technical Security Goals	General Threats						
	Masquer-ade	Eaves-dropping	Authori-sation Violation	Loss or Mo-dification of (transmitted) information	Denial of Communi-cation acts	Forgery of Infor-mation	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x
Controlled Access	x		x			x	

These threats are often combined in order to perform an attack!

Communications security: Some terminology

- Security Service
  - An abstract service that seeks to ensure a specific security property
  - A security service can be realized with the help of cryptographic algorithms and protocols as well as with conventional means
    - One can keep an electronic document on a USB stick confidential by storing it on the stick in an encrypted format as well as locking away the stick in a safe
    - Usually a combination of cryptographic and other means is most effective
- Cryptographic Algorithm
  - A mathematical transformation of input data (e.g. data, key) to output data
  - Cryptographic algorithms are used in cryptographic protocols
- Cryptographic Protocol
  - A series of steps and message exchanges between multiple entities in order to achieve a specific security objective

Security services – Overview

- Authentication
  - The most fundamental security service which ensures, that an entity has in fact the identity it claims to have
- Integrity
  - In some kind, the “small brother” of the authentication service, as it ensures, that data created by specific entities may not be modified without detection
- Confidentiality
  - The most popular security service, ensuring secrecy of protected data
- Access Control
  - Controls that each identity accesses only those services and information it is entitled to
- Non Repudiation
  - Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred

Cryptology – Definition and terminology

- Cryptology
  - Science concerned with communications in secure and usually secret form
  - The term is derived from the Greek kryptós (hidden) and lógos (word)
  - Cryptology encompasses
    - Cryptography (gráphein = to write): the study of the principles and techniques by which information can be concealed in ciphertext and later revealed by legitimate users employing a secret key
    - Cryptanalysis (analýein = to loosen, to untie): the science (and art) of recovering information from ciphers without knowledge of the key
- Cipher
  - Method of transforming a message (plaintext) to conceal its meaning
  - Also used as synonym for the concealed ciphertext
  - Ciphers are one class of cryptographic algorithms
  - The transformation usually takes the message and a (secret) key as input

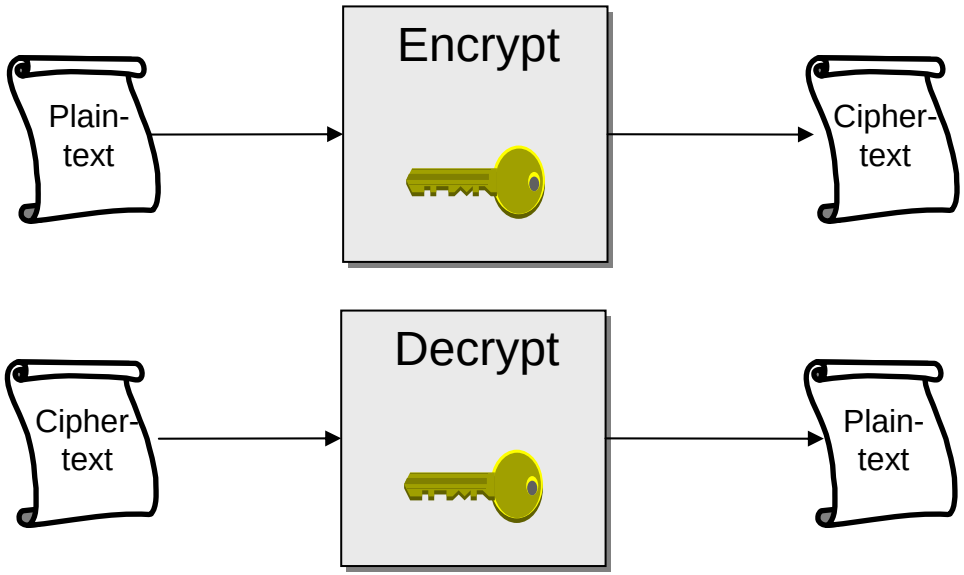
(Source: Encyclopaedia Britannica)

Cryptographic algorithms

- For network security two main applications of cryptographic algorithms are of principal interest
  - *Encryption of data*: transforms plaintext data into ciphertext in order to conceal its meaning
  - *Signing of data*: computes a check value or digital signature to a given plain- or ciphertext that can be verified by some or all entities being able to access the signed data
  - Some cryptographic algorithms can be used for both purposes, some are only secure and / or efficient for one of them.
- Principal categories of cryptographic algorithms
  - *Symmetric cryptography* using 1 key for en-/decryption or signing/checking
  - *Asymmetric cryptography* using 2 different keys for en-/decryption or signing/checking
  - Cryptographic *hash functions* using 0 keys (the “key” is not a separate input but “appended” to or “mixed” with the data).

Symmetric encryption

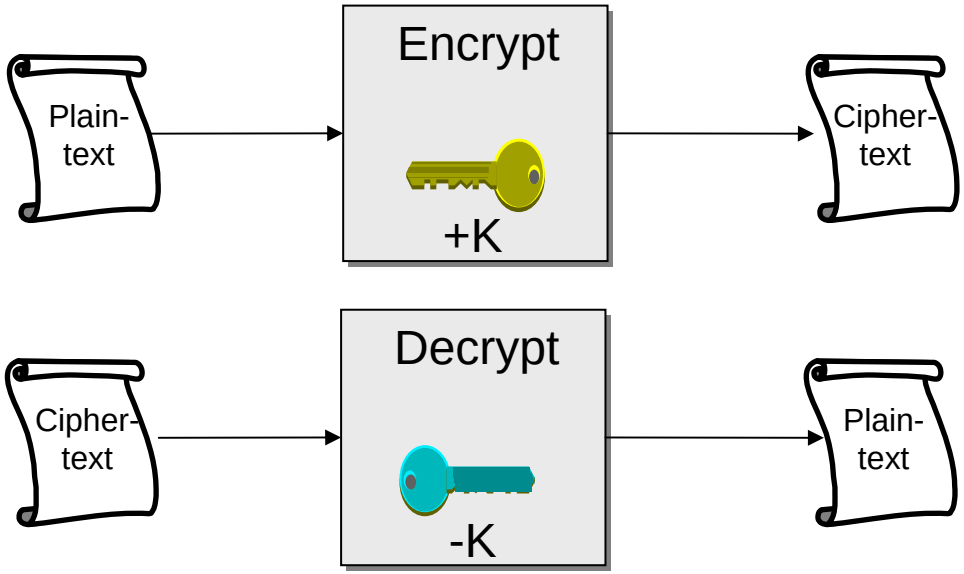
- General description
  - The same key $K_{A,B}$ is used for enciphering and deciphering of messages



- Notation
  - If *P* denotes the plaintext message $E(K_{A,B}, P)$ denotes the ciphertext and it holds $D(K_{A,B}, E(K_{A,B}, P)) = P$
- Examples: DES, 3DES, IDEA, AES ...

Asymmetric cryptography (1)

- General idea:
  - Use two different keys +K and -K for encryption and decryption
  - Given a random ciphertext c = E(+K, m) and +K, it should be infeasible to compute m = D(-K, c) = D(-K, E(+K, m))
    - This implies that it should be infeasible to compute -K when given +K
  - The key -K is only known to one entity A and is called A's private key $-K_A$
  - The key +K can be publicly announced and is called A's public key $+K_A$

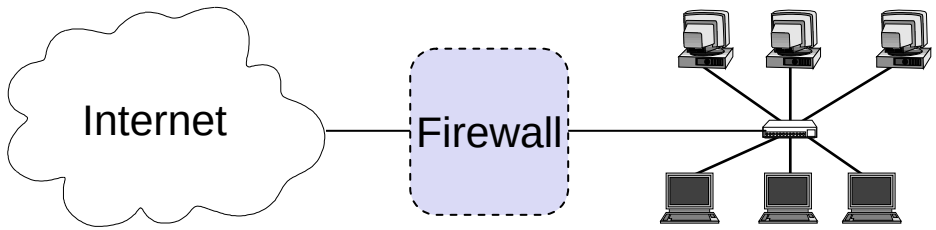


Asymmetric cryptography (2)

- Applications
  - Encryption
    - If B encrypts a message with A's public key $+K_A$, he can be sure that only A can decrypt it using $-K_A$
  - Signing
    - If A encrypts a message with his own private key $-K_A$, everyone can verify this signature by decrypting it with A's public key $+K_A$
  - Attention
    - It is crucial that everyone can verify that he really knows A's public key and not the key of an adversary!
- Practical considerations
  - Asymmetric cryptographic operations are about magnitudes slower than symmetric ones
  - Therefore, they are often not used for encrypting / signing bulk data
  - Symmetric techniques are used to encrypt / compute a cryptographic hash value and asymmetric cryptography is just used to encrypt a key / hash value
  - Public Key Infrastructure (PKI) needed

Example: Internet firewalls

- A network firewall can be compared to a castle moat
  - It restricts people to entering at one carefully controlled point
  - It prevents attackers from getting close to other defenses
  - It restricts people to leaving at one carefully controlled point
- Usually, a network firewall is installed at a point where the protected subnetwork is connected to a less trusted network
  - Example: Connection of a corporate local area network to the Internet



  - Firewalls often realize access control on the subnetwork level

Firewalls: Terminology (1)

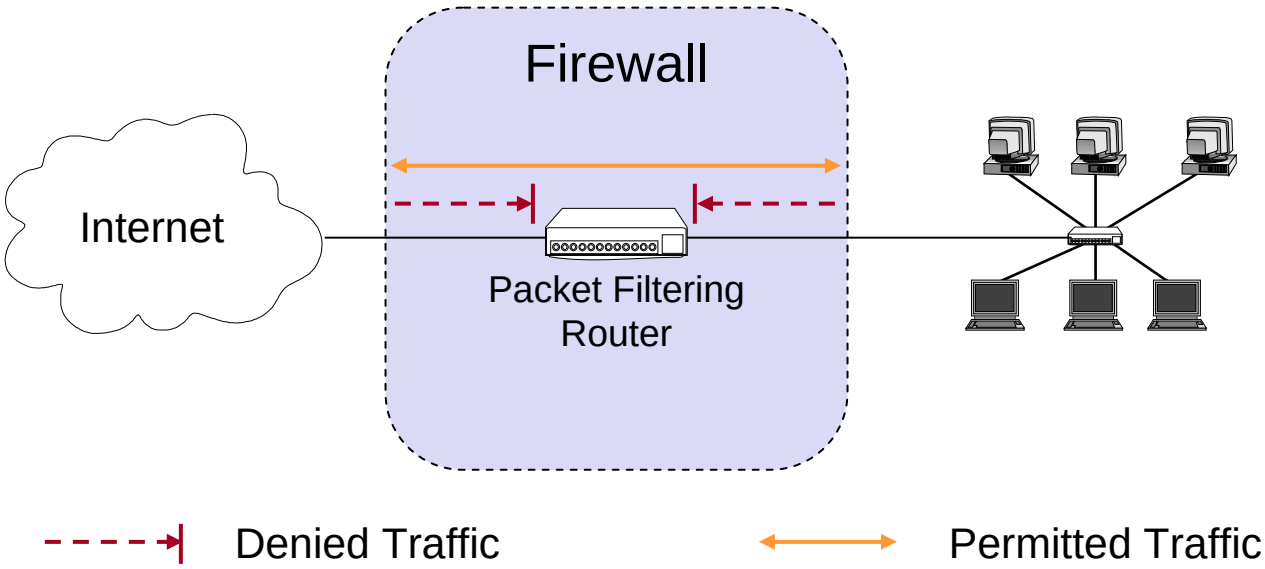
- Firewall
  - A component or a set of components that restricts access between a protected network and the Internet or between other sets of networks
- Packet Filtering
  - The action a device takes to selectively control the flow of data to and from a network
  - Packet filtering is an important technique to implement access control on the subnetwork-level for packet oriented networks, e.g. the Internet
  - A synonym for packet filtering is screening
- Bastion Host
  - A computer that must be highly secured because it is more vulnerable to attacks than other hosts on a subnetwork
  - A bastion host in a firewall is usually the main point of contact for user processes of hosts of internal networks with processes of external hosts
- Dual-homed host
  - A general purpose computer with at least two network interfaces

Firewalls: Terminology (2)

- Proxy
  - A program that deals with external servers on behalf of internal clients
  - Proxies relay approved client requests to real servers and also relay the servers' answers back to the clients
- Network Address Translation (NAT):
  - A procedure by which a router changes data in packets to modify the network addresses
  - This allows to conceal the internal network addresses (even though NAT is not actually a security technique)
- Perimeter Network
  - A subnetwork added between an external and an internal network, in order to provide an additional layer of security
  - A synonym for perimeter network is de-militarized zone (DMZ)

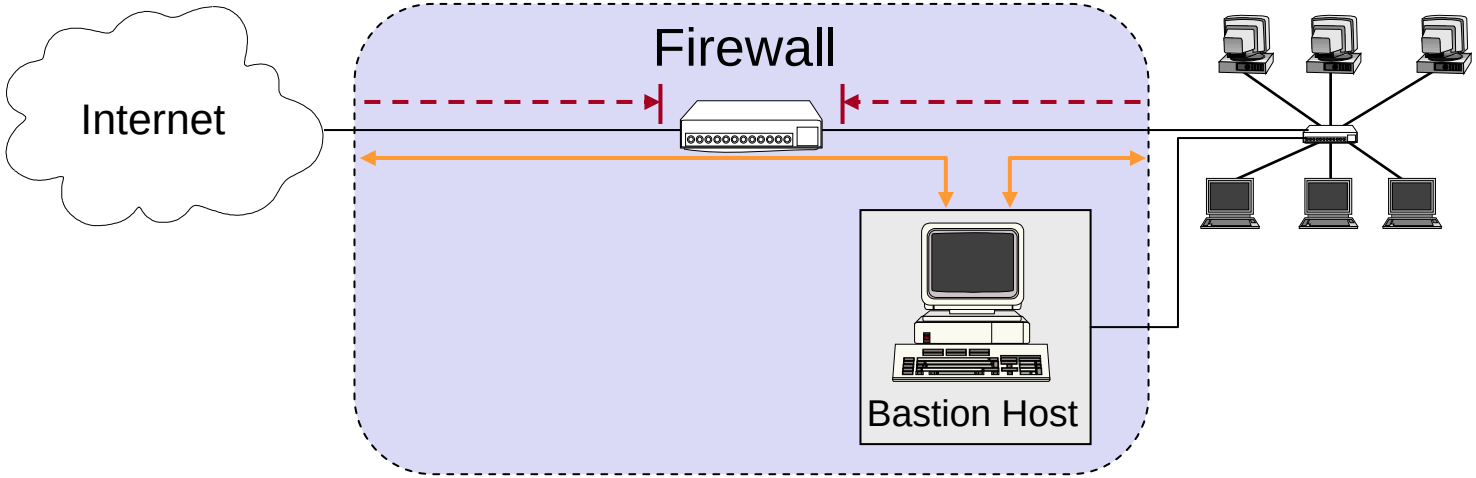
Firewalls architecture: Simple packet filter

- The most simple architecture just consists of a packet filtering router
- It can be either realized with
  - A standard workstation (e.g. Linux PC) with at least two network interfaces plus routing and filtering software
  - A dedicated router device, which usually also offers filtering capabilities



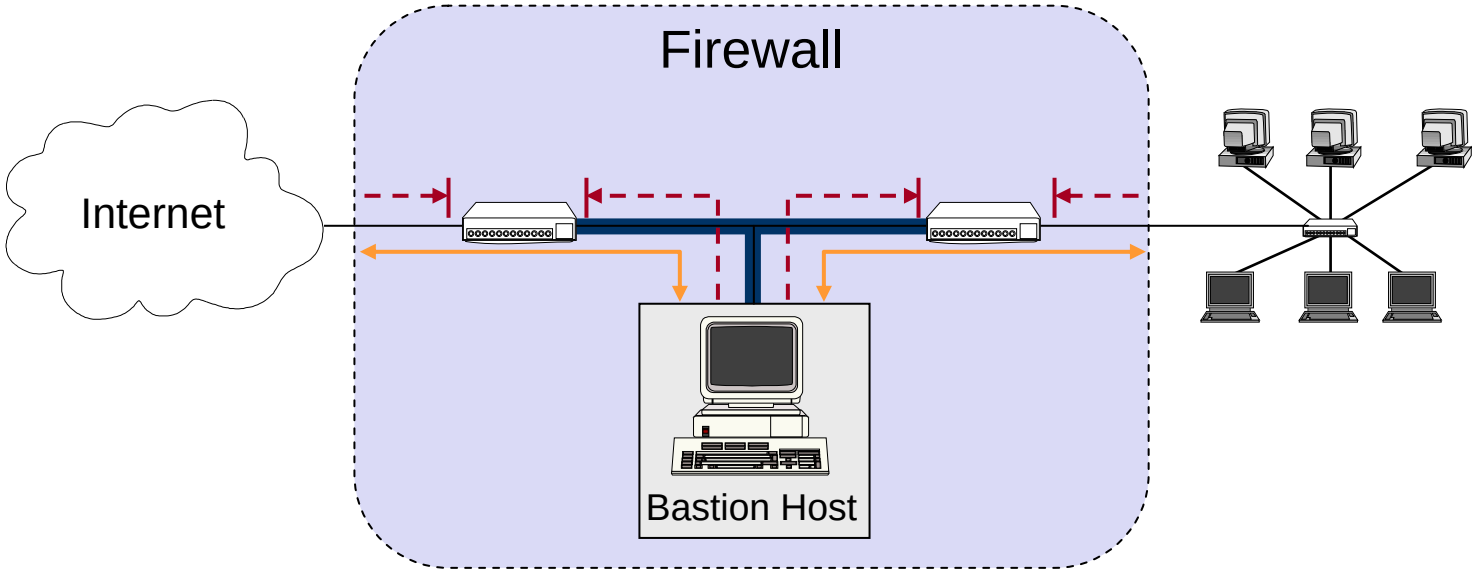
Firewall architecture: Screened host

- The packet filter
  - Allows permitted IP traffic between the screened host and the Internet
  - Blocks all direct traffic between other internal hosts and the Internet
- The screened host provides proxy services:
  - Despite partial protection by the packet filter the screened host acts as a bastion host



Firewall architecture: Screened subnet

- A DMZ is created between two packet filters
- The inner packet filter serves as additional protection in case the bastion host is ever compromised
  - For example, this avoids a compromised bastion host to sniff on internal traffic
- The perimeter network is also a good place to host a publicly accessible information server, e.g. a WWW server



Firewalls: Packet filtering

- What can be done with packet filtering?
  - Theoretically speaking everything, as all information exchanged in a communication relation is transported via packets
  - In practice, efficiency tradeoffs against proxy approaches have to be considered
- Basic packet filtering enables to control data transfer based on:
  - Source IP Address
  - Destination IP Address
  - Transport protocol
  - Source and destination application port
  - Potentially, specific protocol flags (e.g. TCP's ACK- and SYN-flag)
  - The network interface a packet has been received on

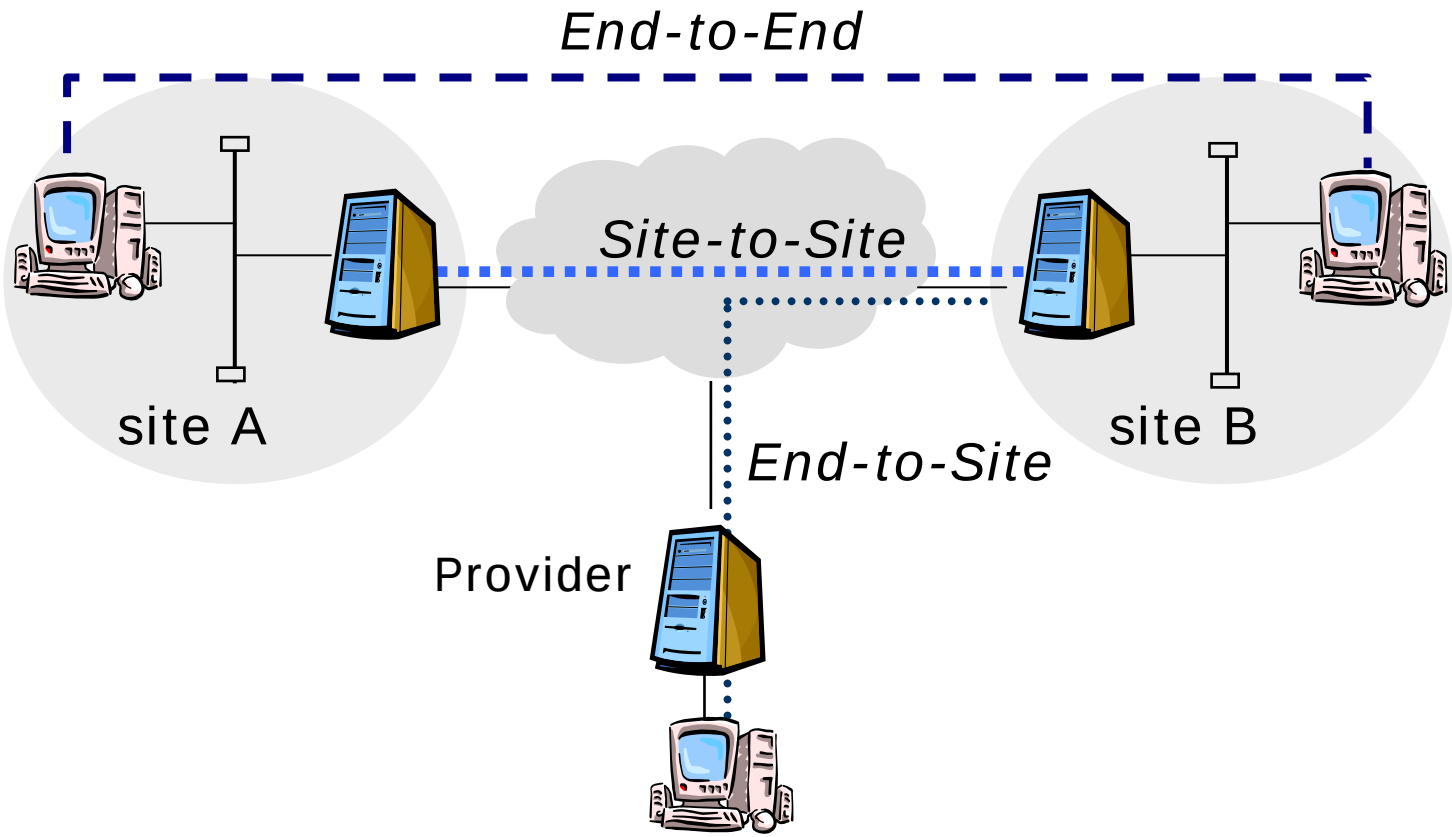
Firewalls: An example packet filtering rule set

- This rule set specifies that incoming and outgoing email is the only allowed traffic into and out of a protected network
  - Email is relayed between two servers by transferring it to an SMTP daemon on the target server (server port 25, client port > 1023)
  - Rule A allows incoming email to flow to the bastion host and rule B allows the bastion host's acknowledgements to exit the network
  - Rules C and D are analogous for outgoing email
  - Rule E denies all other traffic

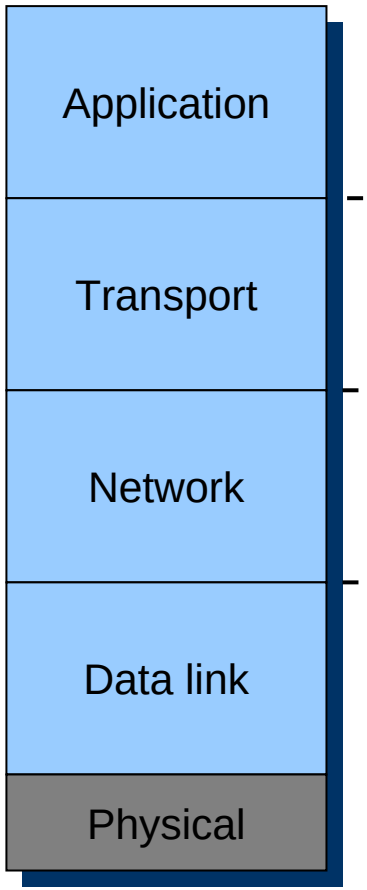
Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Bastion	TCP	>1023	25	Any	Permit
B	Outbound	Bastion	External	TCP	25	>1023	Yes	Permit
C	Outbound	Bastion	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Bastion	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

Example: Virtual private networks (VPNs)

- **Goal:** Offer a secure data exchange between remote communication partners via potentially insecure transit networks (e.g. the Internet) with the help of authentication and encryption.



VPNs in the Internet



Protection of single application layer protocols (e.g. Pretty Good Privacy (PGP), Secure Sockets Layer (SSL)).

Protection of TCP and UDP by modification of layer 4 in the end systems (proprietary).

Protection of IP packets by modification of the IP stack (e.g. IPSec).

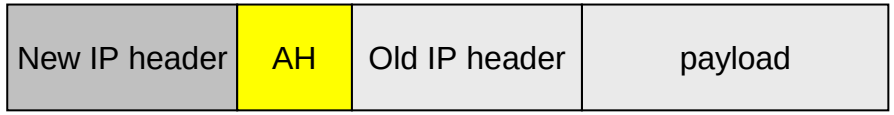
Protection of user data on link layer (e.g. Point-to-Point-Tunneling-Protocol (PPTP), Layer-2-Tunneling-Protocol (L2TP)).

Example: IP Security (IPSec)

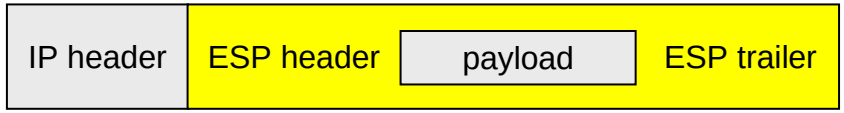
- Authentication Header
  - Authentication, data integrity
- Transport mode
  - No change in addresses (direct communication)
- Tunnel mode
  - New IP addresses between arbitrary partners
- Encapsulating Security Payload
  - Authentication, data integrity, confidentiality

Transport mode

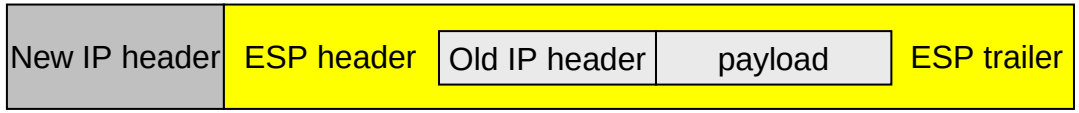
Tunnel mode



Transport mode

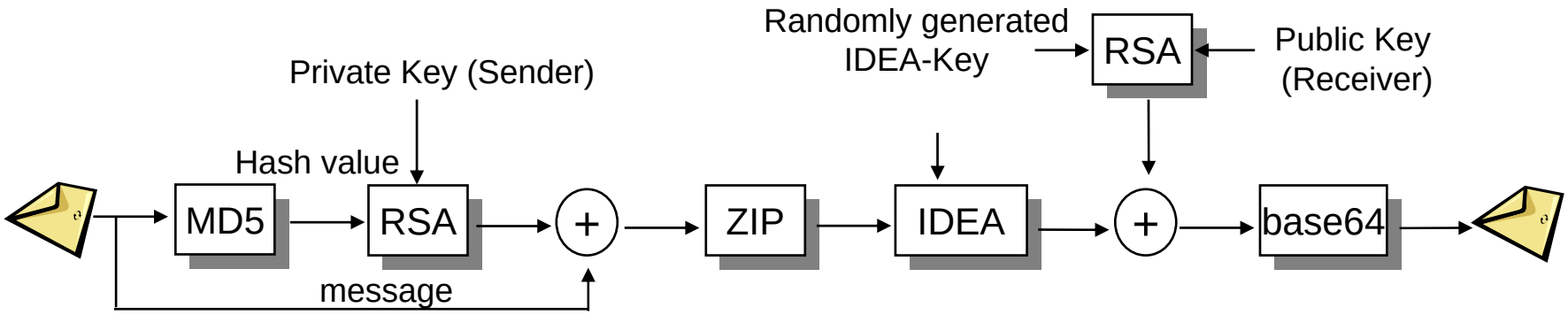


Tunnel mode



Example: E-Mail protection via PGP (Pretty Good Privacy)

- Encryption, authentication and compression of emails
  - MD5 (Message Digest 5) calculates hash value based on the message
    - No message resulting in the same hash value should be constructible within reasonable time
  - RSA (Rivest, Shamir, Adelman) algorithm
    - Each use has a public and a private key
    - The sender uses its private key to encrypt the MD5 hash value (thus authentication of sender possible)
    - The public key of the receiver is used to encrypt the idea key (thus authentication of receiver)
  - IDEA (International Data Encryption Standard) encrypts the message
    - Much faster than RSA



Conclusion

- Network security is an important, but extremely complicated and complex topic
  - We have not even scratched the surface, we just know that there is an iceberg out there…