IN2120 Information Security

Lecture 4: Network Security

Nils Gruschka

University of Oslo

Autumn 2019

Outline

- Network security concepts
- Transport Layer Security (TLS)
- VPN – Virtual Private Network
- Firewalls
- Intrusion Detection Systems

Network Security Concepts

Assumes that each organisation owns a network

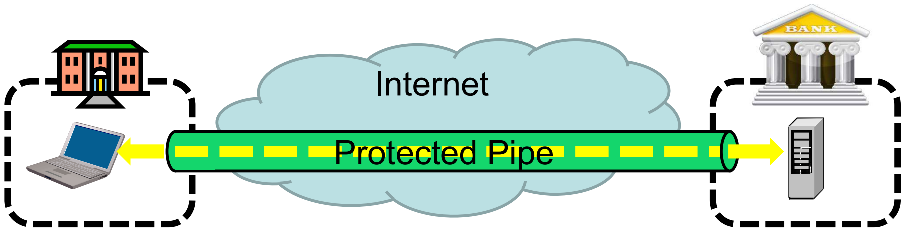
- – Wants to protect own local network
- – Wants to protect communication with other networks

Network Security: two main areas

- **Communication Security:** Protection of data transmitted across networks between organisations and end users
  - – Topic for this lecture
- **Perimeter Security:** Protection of an organization’s network from unauthorized access
  - – Topic for next lecture

Communication Security Analogy

Physical transport security



Digital communication security

Security Protocols

- Many different security protocols have been specified and implemented for different purposes
  - Authentication, integrity, confidentiality
  - Key establishment/exchange
  - E-Voting
  - Secret sharing
  - etc.
- Protocols are surprisingly difficult to get right!
  - Many vulnerabilities are discovered years later (e.g. for TLS: DROWN, POODLE, ROBOT, Logjam, FREAK, BEAST, …)
  - … some are never discovered (or maybe only by the attackers)

Transport Layer Security

TLS/SSL

SSL/TLS: History

- 1994: Netscape Communications developed the network authentication protocol Secure Sockets Layer, SSLv2.
  - Badly broken, officially deprecated 2011
- 1995: Netscape release their own improvements SSLv3.
  - Broken, officially deprecated 2015
- In January 1999, RFC 2246 was issued by the IETF, Transport Layer Security Protocol: TLS 1.0
  - Similar to, but incompatible with SSLv3
  - Followed by TLS 1.1 (2006) and TLS 1.2 (2008)
  - Current version: TLS 1.3 (2018), removes all old/insecure features/algorithms

TLS: Overview

- TLS is a cryptographic services protocol based on the Browser PKI and is commonly used on the Internet.
  - Each server has a server certificate and private key installed
  - Allows browsers to establish secure sessions with web servers.
- Port 443 is reserved for HTTP over TLS/SSL and the protocol https is used with this port.
  - http://www.xxx.com implies using standard HTTP using port 80.
  - https://www.xxx.com implies HTTP over TLS/SSL with port 443.
- Other applications:
  - IMAP over TLS: port 993
  - POP3 over TLS: port 995

TLS: Protocol Stack

TLS Handshake Protocol	TLS Change Cipher Suite Protocol	TLS Alert Protocol	Application Protocol (e.g. HTTP)
TLS Record Protocol			
TCP			
IP			

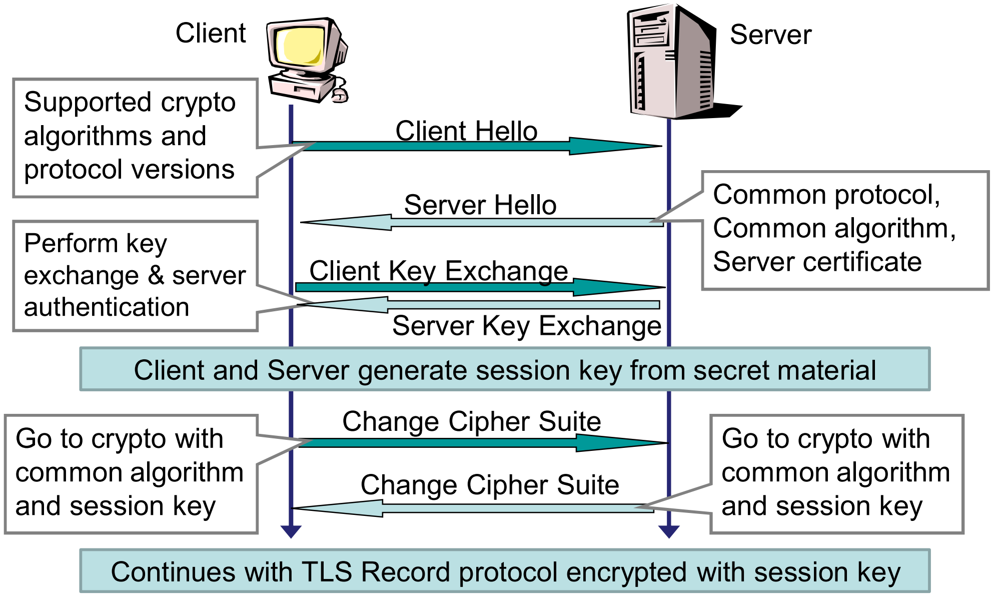
TLS: Architecture Overview

- Designed to provide secure reliable end-to-end services over TCP.
  - Confidentiality
  - Integrity
  - Authenticity
- Consists of 3 higher level protocols:
  - TLS Handshake Protocol
  - TLS Alert Protocol
  - TLS Change Cipher Spec Protocol
- The TLS Record Protocol provides the practical encryption and integrity services to various application protocols.

TLS: Handshake Protocol

- The handshake protocol
  - Negotiates the encryption to be used
  - Establishes a shared session key
  - Authenticates the server
  - Authenticates the client (optional)
- After the handshake, application data is transmitted securely (encrypted + integrity protected)

TLS: Simplified Handshake



Client

Server

Supported crypto algorithms and protocol versions

Client Hello

Server Hello

Common protocol, Common algorithm, Server certificate

Perform key exchange & server authentication

Client Key Exchange

Server Key Exchange

Client and Server generate session key from secret material

Go to crypto with common algorithm and session key

Change Cipher Suite

Change Cipher Suite

Go to crypto with common algorithm and session key

Continues with TLS Record protocol encrypted with session key

TLS: Elements of Handshake

- Client hello
  - Advertises available algorithms (e.g. RSA, AES, SHA256)
  - Different types of algorithms bundled into "Cipher Suites"
  - Format:
    TLS_*key-exchange-algorithm*_WITH_*data-protection-algorithm*
  - Example (TLS 1.2): TLS_RSA_WITH_AES_256_CBC_SHA256
    - RSA for key exchange
    - AES (128 bit key) with CBC mode for encryption
    - SHA256 as hash function for authentication and integrity protection
  - Example (TLS 1.3): TLS_AES_256_GCM_SHA384
    - DH for key exchange (implicit)
    - AES with GCM for encryption + integrity protection
    - SHA384 as hash function for authentication

Details for the interested

TLS: Elements of Handshake

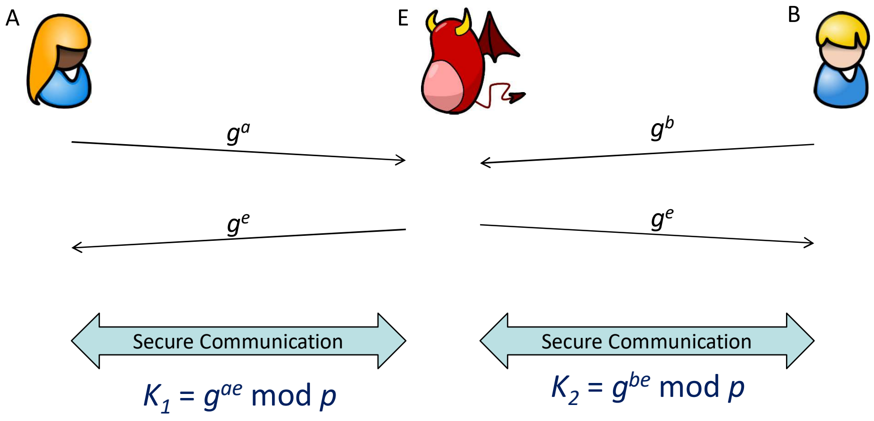
- Server hello
  - Returns the selected cipher suite
  - Server adapts to client capabilities
- Server Certificate
  - X.509 digital certificate sent to client
  - Client verifies the certificate including that the certificate signer is in its acceptable Certificate Authority (CA) list. Now the client has the server's certified public key.
- Client Certificate
  - Optionally, the client can send its X.509 certificate to server, in order to provide mutual authentication
- Server/Client Key Exchange
  - The client and server can a establish session key using asymmetric encryption or DH key exchange (details below)

Details for the interested

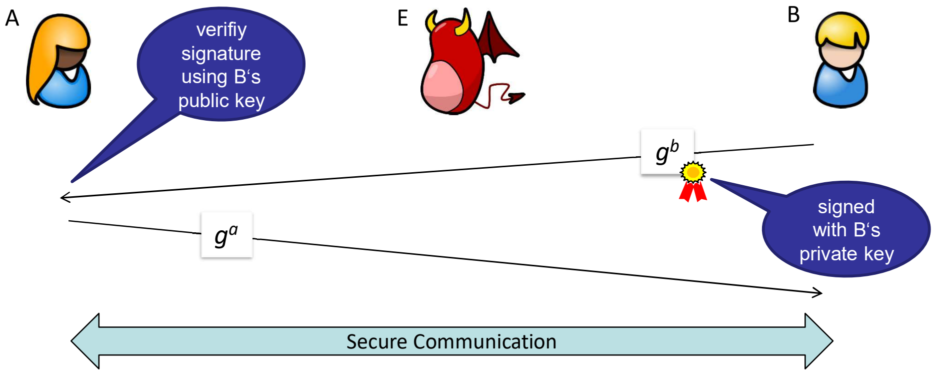
TLS: Record Protocol Overview

- Provides two services for TLS connections.
  - Message Confidentiality:
    - Encrypt the payload using symmetric encryption (e.g. AES)
  - Message Integrity/Authenticity:
    - Calculate a MAC to ensure the message was not modified in transmission
- For both operations the session key exchanged during the handshake is used

Weakness of DH Key Exchange



Countermeasure

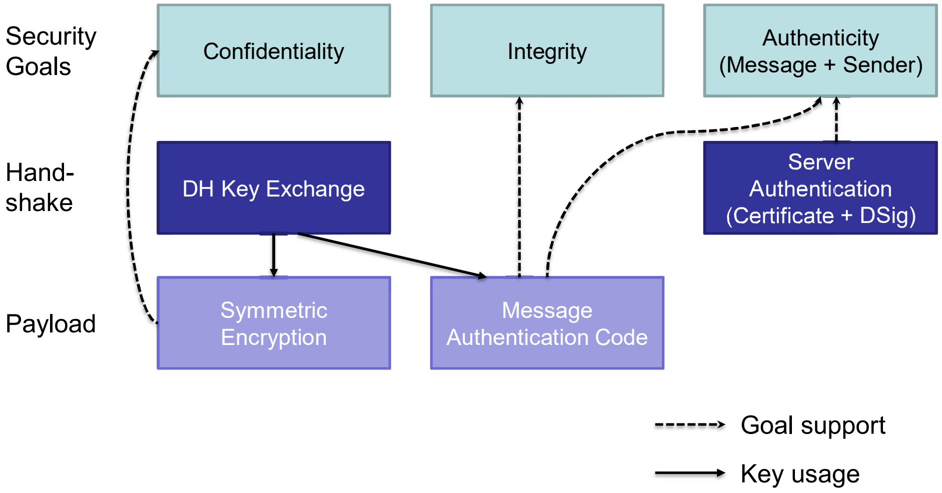

A
verifiy signature using B's public key
E
B
g^b
signed with B's private key
g^a
Secure Communication

$K = g^{ab} \bmod p$

TLS: Key Exchange

- DH exchange:
  - Client and server perform Diffie-Hellman-Exchange (DH)
  - Server signs his DH value with server private key (RSA)
  - Client validates signature with server public key (RSA)
- ~~RSA exchange:~~
  - ~~Asymmetric encryption of symmetric key~~
  - ~~Was in the past the preferred method (simpler)~~
  - ~~Some security issues (no "forward secrecy")~~
    ~~→ not recommended any more~~

TLS in a nutshell



Security Goals

Confidentiality

Integrity

Authenticity (Message + Sender)

Hand-shake

DH Key Exchange

Server Authentication (Certificate + DSig)

Payload

Symmetric Encryption

Message Authentication Code

Goal support

Key usage

TLS Challenges

- Many vulnerabilities exist for TLS
  → keep client and server software up-to-date
- Also vulnerabilities in cryptographic algorithms
  → configure server to exclude weak algorithms
- TLS provides security just for a single TCP connection
  - Browser can establish HTTP and HTTPS connections; even to the same server (e.g. HTML via HTTPS, images via HTTP)
- Relies on browser PKI which has many security issues
- No trust indicator
  - Owner of "mafia.com" can get a legitimate certificate
  - Phishing and TLS can be easily combined
  - "Secure Connection" indicator can be misleading

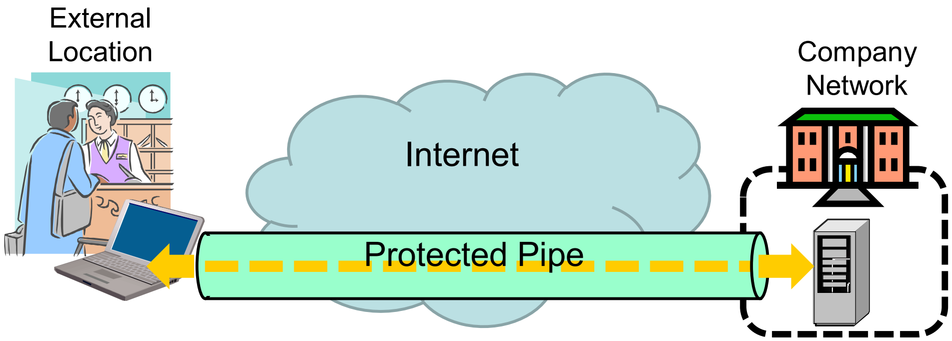
VPN

Virtual Private Networks

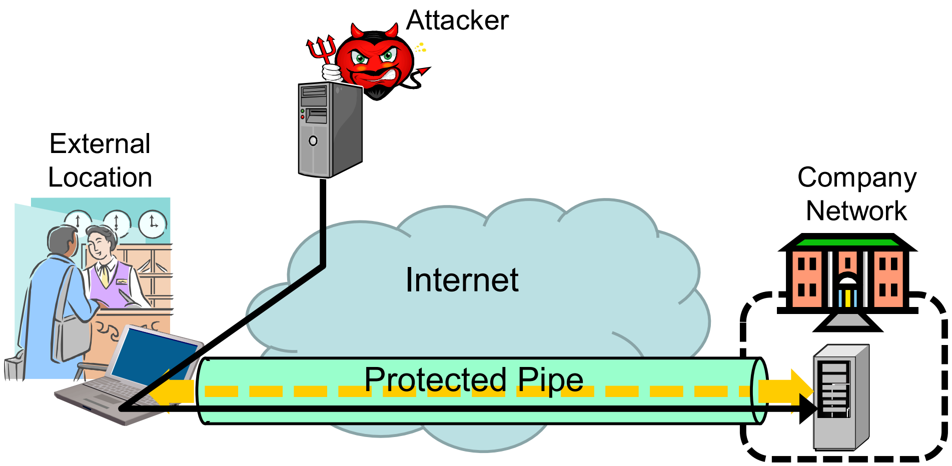
VPN

- TLS secures only a single TCP connection
- Sometimes:
  - **all** communication from a computer shall be secured
  - also non-TCP communication shall be secured
- Typical application:
  - VPN tunnel into a company network
  - Tunnel can only be established after authentication
  - All communication is routed (and secured) through the tunnel
  - Client is virtually part of the local company network
  - Client gets access to internal services

Typical usage of VPN



Risk of using VPN

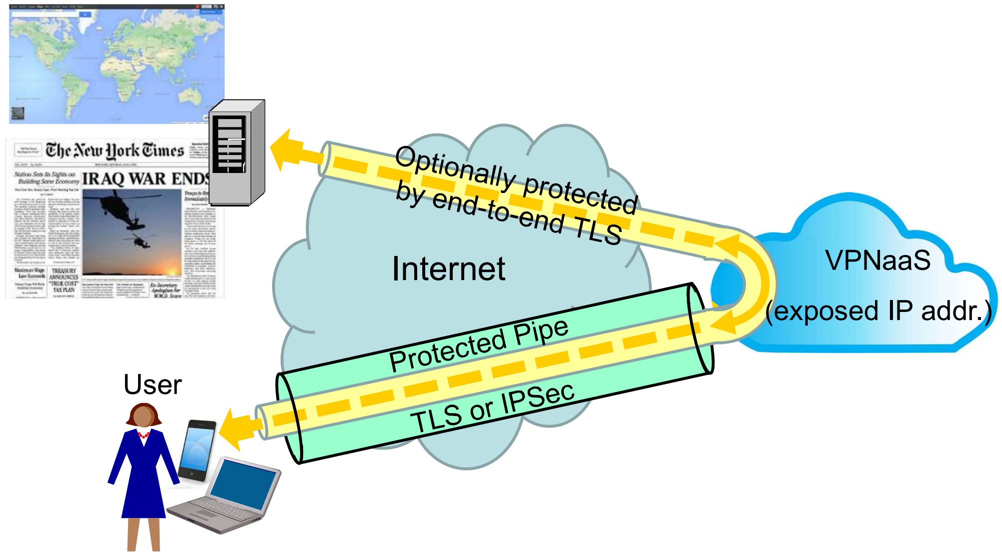


Secure pipe can be attack channel to company network !

VPN

- Another application: VPN Browsing Proxy
- Usage Examples:
  - Access to services subscribed by own organization
  - Hide user’s true location (circumvent geo-blocking or censorship)

VPN Browsing – via VPN Proxy



Tor – The Onion Router

Image courtesy indymedia.de

- An anonymizing routing protocol
- Originally sponsored by the US Naval Research Laboratory
- From 2004 to 2006 was supported by EFF
- Since 2006 independent nonprofit organisation

- Creates a multi-hop proxy circuit through the Internet from client to destination.
- Each hop “wraps” another encryption layer thereby hiding the next destination.
- No cleartext-gap, except at the exit-node.
- No node knows end-to-end client-server association

„Onion“ Message

Destination: Jane
Payload

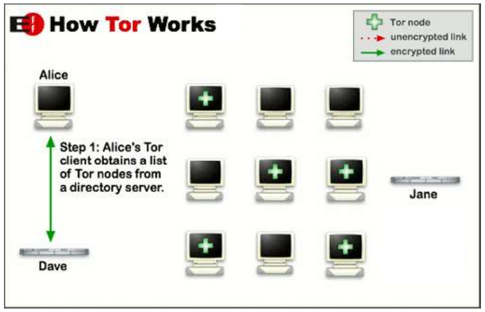
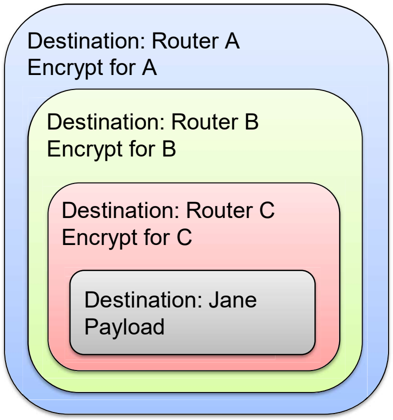

How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave

Image courtesy https://www.torproject.org

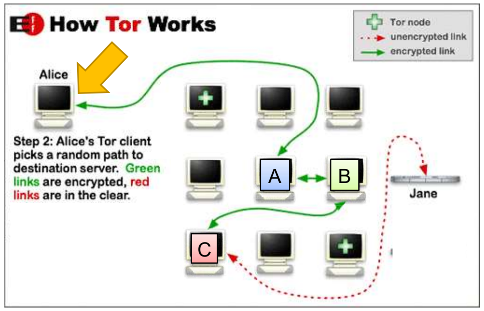
„Onion“ Message


Destination: Router A
Encrypt for A

Destination: Router B
Encrypt for B

Destination: Router C
Encrypt for C

Destination: Jane
Payload

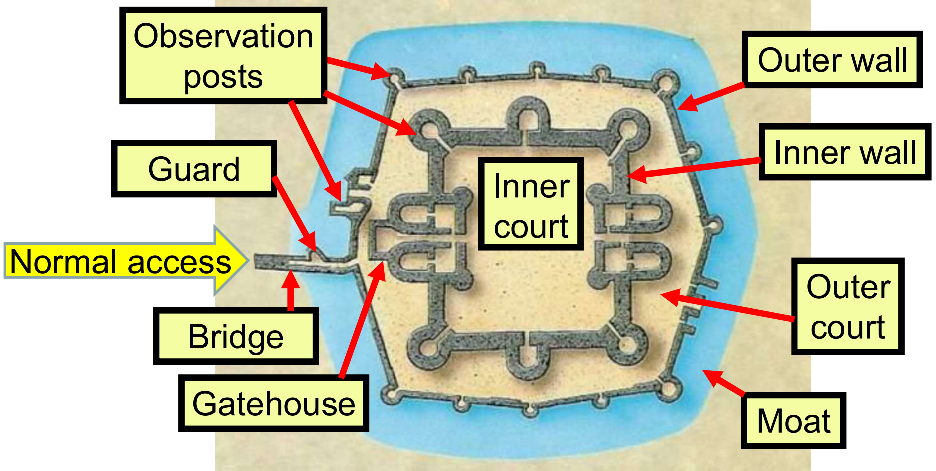


Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

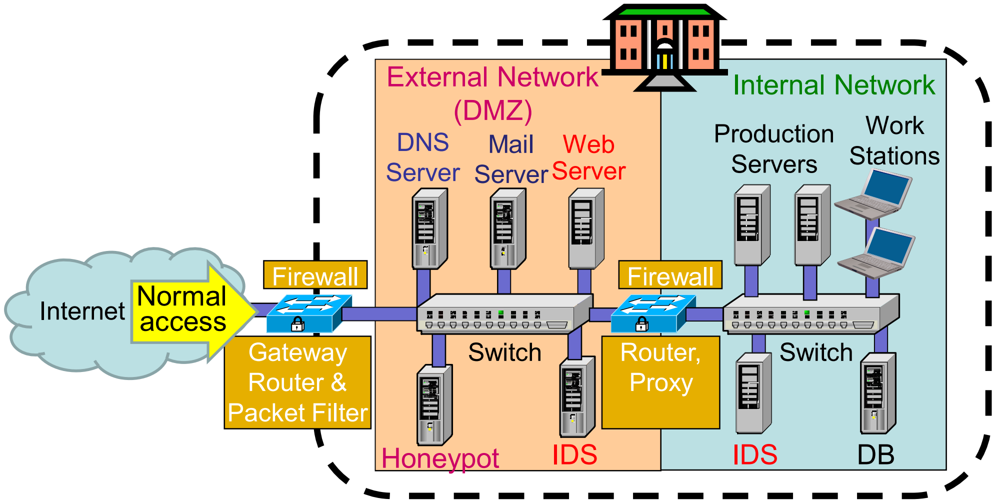
Image courtesy https://www.torproject.org

Firewalls

Perimeter security analogy
Medieval Castle Defences

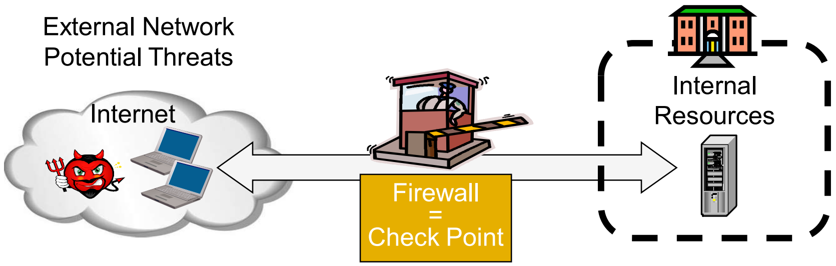


Defending local networks
Network Perimeter Security



Firewalls

- A firewall is a check point that protects the internal networks against attack from outside networks
- The check point decides which traffic can pass in & out based on rules



External Network
Potential Threats

Internet

Firewall
=
Check Point

Internal
Resources

Firewalls: Overview 1

- If the risk of having a connection to the Internet is unacceptable, the most effective way of treating the risk is to avoid the risk altogether and disconnect completely.
- If disconnection from the Internet is not practical, then firewalls may provide an effective level of protection that can reduce the risk to an acceptable level.
- Firewalls are often the first line of defence against external attacks but should not be the only defence.
- A firewall's purpose is to prevent unauthorized access to or from a private network.

Firewalls: Overview 2

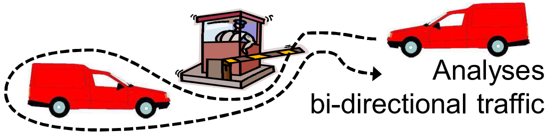
- All traffic entering or leaving must pass through firewall
- The network owner must define criteria for what is (un)authorized
- The effectiveness of firewalls depends on specifying authorized traffic in terms of rules
  - The rules defines what to let pass through;
  - The rules defines what to block.
- Firewalls must be effectively administered, updated with the latest patches and monitored.
- Firewalls can be implemented in both hardware and software, or a combination of both.

Types of Firewall Technology (vehicle analogy)

- Packet Filters

Inspects packet headers only

- Stateful Packet Filters

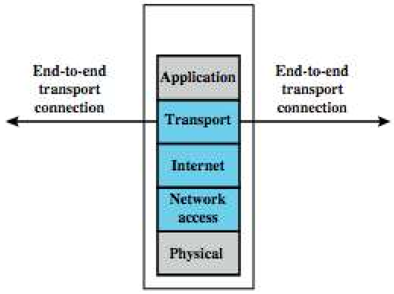


Analyses bi-directional traffic

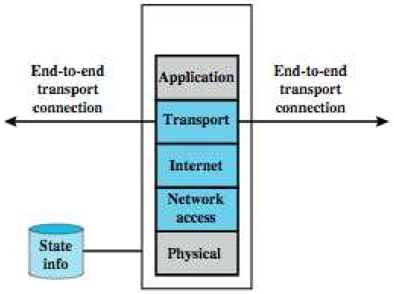
- Application Level Gateway/ Next Generation Firewall

End-to-end connection inspects payload, and analyses traffic

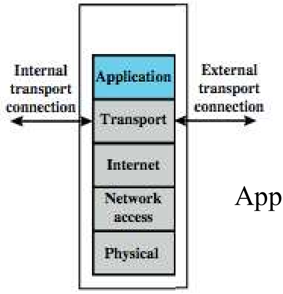
Types of firewalls


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

Simple Packet Filter


End-to-end transport connection
Application
Transport
Internet
Network access
State info
Physical
End-to-end transport connection

Stateful Packet Filter



Application Level Gateway

(Stateless) Packet Filter

- A packet filter is a network router that can accept/reject packets based on headers
- Packet filters examine each packet's headers and make decisions based on attributes such as:
  - Source or Destination IP Addresses
  - Source or Destination Port Numbers
  - Protocol (UDP, TCP or ICMP)
  - ICMP message type
  - And which interface the packet arrived on
  - Unaware of session states at internal or external hosts
  - High speed, but primitive filter

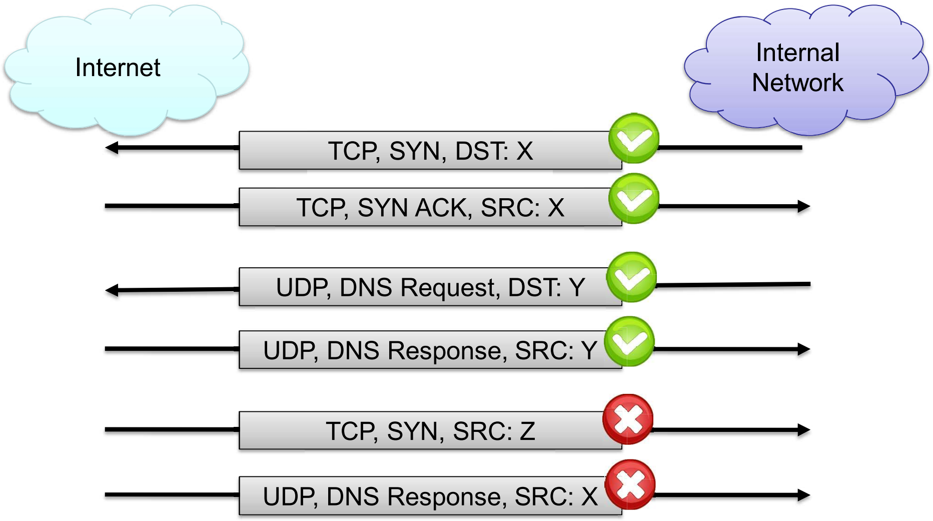
(Stateless) Packet Filters

- Widespread packet filter software (Linux):
  - iptables / netfilter
  - nft / nttables
- Examples (iptables)
- `iptables -A FORWARD -s 131.234.142.33 -j ACCEPT`
  - All packets from source IP Address 131.234.142.33 are accepted
- `iptables -A FORWARD -p tcp -d 10.0.0.56 --dport 22 -j ACCEPT`
  - All packets using transport protocol and destination address 10.0.0.56 and destination port 22 are accepted

Problems with Stateless Filtering

- Assume a typical "security policy":
  - Access from internal to external allowed
  - Access from external to internal prohibited
  - Example application: home network
- Naive packet filter configuration:
  - outgoing packet → forward
  - incoming packet → reject
- Problem?
- Most internet applications would not work!

Stateful Filtering



Internet

Internal Network

TCP, SYN, DST: X ✓

TCP, SYN ACK, SRC: X ✓

UDP, DNS Request, DST: Y ✓

UDP, DNS Response, SRC: Y ✓

TCP, SYN, SRC: Z ✗

UDP, DNS Response, SRC: X ✗

Stateful Packet Filters

- Stateful packet filters track current state of a connection
  - More ‘intelligent’ than simple packet filters.
- Stateful packet filters keep track of sessions
  - Recognise if a particular packet is part of an established connection by ‘remembering’ recent traffic history.
  - Will add a temporary rule to allow the reply traffic back through the firewall.
  - When “session” is finished, the temporary rule is deleted.
- This makes the definition of filtering rules easier to accomplish and therefore potentially more secure.
- High speed, can use relatively advanced filter rules
- Requires memory
  - So can be subject to DOS (Denial of Service) attacks

Stateful Packet Filters

- Examples (iptables)
- `iptables -A FORWARD -m state --state NEW -i eth0 -j ACCEPT`
- Accept new connections (i.e. TCP SYN) from network interface eth0 („from inside“)
- `iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT`
- Accept ALL packets which belong to an established TCP connection or are related to an existing UDP communication

(Stateful) Packet Filter: Evaluation

- Strengths:
  - Low overhead and high throughput
  - Supports almost any application
- Weaknesses:
  - Unable to interpret application layer data/commands
    - may allow insecure operations to occur
  - Allows direct connection between hosts inside & outside firewall

Application Level Gateway

- Inspects payload in end-to-end or proxy application connection
- Support specific application protocols
  - e.g. http, telnet, ftp, smtp etc.
  - each protocol supported by a specific proxy HW/SW module
- Can be configured to filter specific user applications
  - E.g. Facebook, Youtube, LinkedIn
  - Can filter detailed elements in each specific user application
- Can provide intrusion detection and intrusion prevention
- Very high processing load in firewall
  - High volume needs high performance hardware, or else will be slow

Next Generation Firewalls

paloalto NETWORKS

High range model: *PA-7050*

Up to 120 Gbps throughput

Prices starting from: US$ 150,000

Check Point SOFTWARE TECHNOLOGIES LTD.

High range models: 44000 / 64000

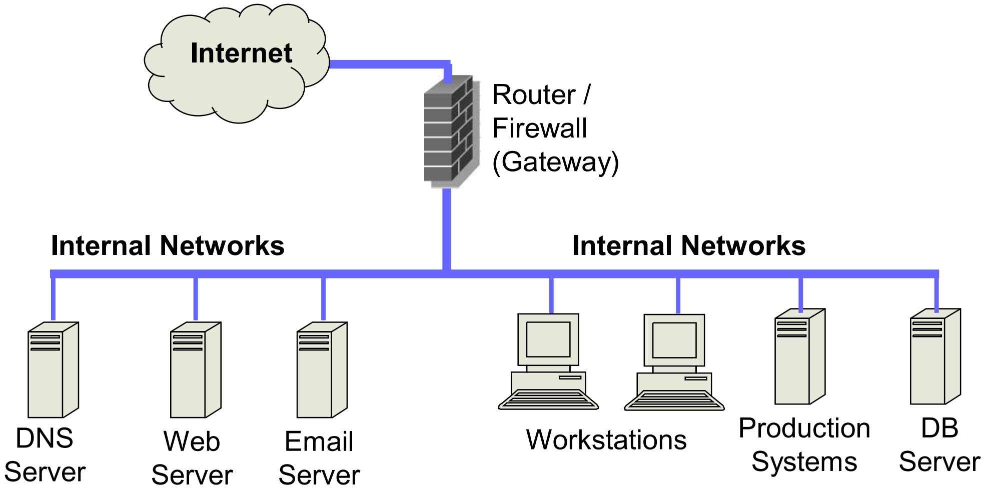
Up to 200 / 400 Gbps throughput

Prices starting from: US$ 200,000

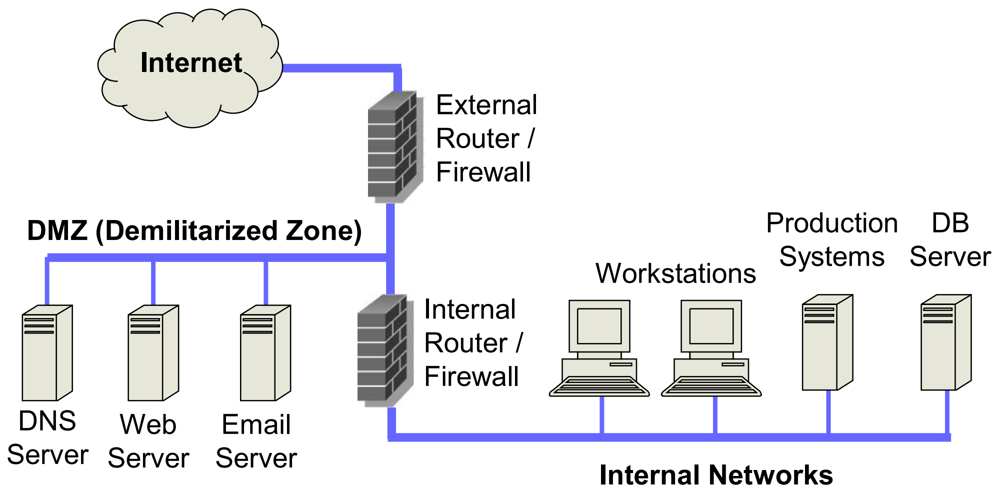
Application Level Gateway – Pros & Cons

- Strengths:
  - Easy logging and audit of all incoming traffic
  - Provides potential for best security through control of application layer data/commands
- Weaknesses:
  - May require some time for adapting to new applications
  - Much slower than packet filters
  - Much more expensive than packet filters

Firewalls: Simple Firewall Architecture



Firewalls:
DMZ Firewall Architecture



Intrusion Detection Systems

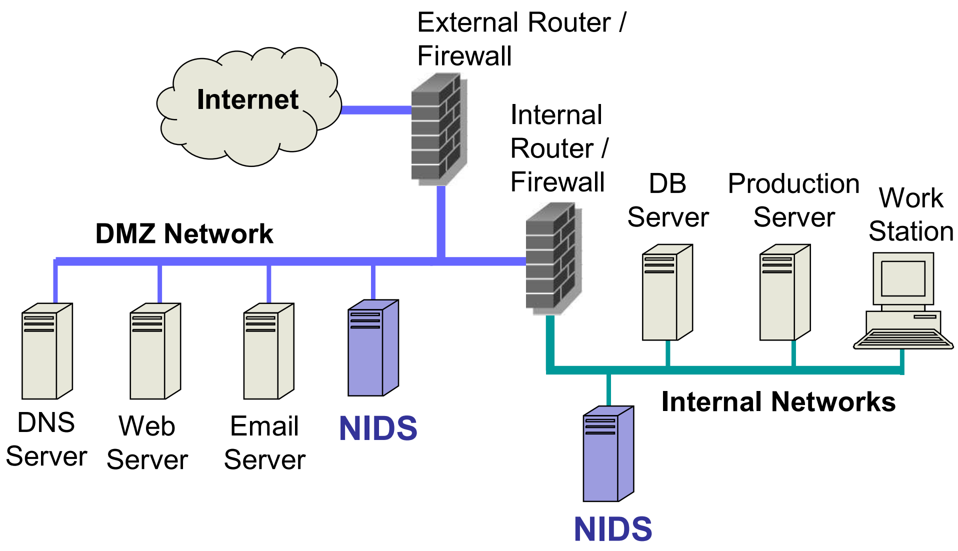
Intrusion Detection and Prevention

- **Intrusion**
  - Actions aimed at compromising the security of a target network (confidentiality, integrity, availability of resources)
- **Intrusion detection**
  - The identification of possible intrusion through intrusion signatures and network activity analysis
  - IDS: Intrusion Detection Systems
- **Intrusion prevention**
  - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network
  - IPS: Intrusion Prevention Systems
  - IDPS: Intrusion Detection and Prevention Systems

Intrusion Detection Systems:

- IDS are automated systems that detect suspicious activity
- IDS can be either host-based or network-based.
- A host-based IDS is designed to detect intrusions only on the host it is installed on
  - monitor events, changes to host’s OS files and traffic sent to the host
- Network based IDS (NIDS) detect intrusions on one or more network segments, to protect multiple hosts
  - monitor networks looking for suspicious traffic
- What can be detected:
  - Attempted and successful misuse, both external and internal agents
  - Malware: Trojan programs, viruses and worms
  - DoS (Denial of Service) attacks

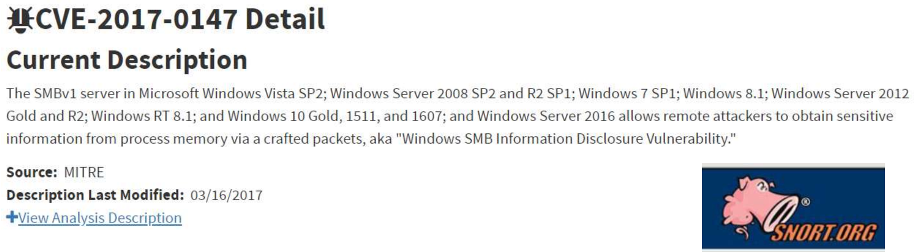
Network IDS Deployment



Intrusion Detection Techniques

- **Misuse** detection
  - Use attack “signatures” (need a model of the attack)
    - Sequences of system calls, patterns of network traffic, etc.
  - Must know in advance what attacker can do, based on known attack patterns
  - Can only detect known attacks
  - Relatively few false positives
- **Anomaly** detection
  - Using a model of normal system behavior, try to detect deviations and abnormalities
    - e.g., raise an alarm when a statistically rare event(s) occurs
  - Can potentially detect unknown attacks
  - Many false positives

Example: Vulnerability + Snort Rule



CVE-2017-0147 Detail

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

Source: MITRE

Description Last Modified: 03/16/2017

+View Analysis Description

```
alert tcp $HOME_NET 445 -> any any ( msg:"OS-WINDOWS Microsoft Windows SMB
possible leak of kernel heap memory"; flow:to_client,established;
content:"Frag",fast_pattern; content:"Free"; content:"|FA FF FF|";
content:"|F8 FF FF|",within 3,distance 5; content:"|F8 FF FF|",within
3,distance 5; metadata:policy balanced-ips alert,policy security-ips
drop,ruleset community; service:netbios-ssn; reference:cve,2017-0147;
reference:url,technet.microsoft.com/en-us/security/bulletin/MS17-010;
classtype:attempted-recon; sid:42339; rev:2; )
```

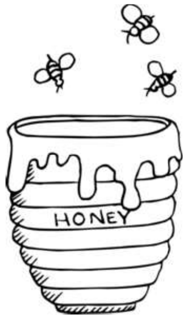
Intrusion Detection Errors

- **False negatives**: attack is not detected
  - Big problem in signature-based misuse detection
- **False positives**: harmless behavior is classified as attack
  - Big problem in statistical anomaly detection
- Both types of IDS suffer from both error types
- Both false positives and false negatives are problematic

Remarks on Intrusion Detection

- Most alarms are false positives
  - Requires automated screening and filtering of alarms
- Most true positives are trivial incidents
  - can be ignored,
  - the attacks will never be able to penetrate any system
- Serious incidents need human attention
  - Can be dealt with locally
  - May require external expertise
- Potential for improvement through more intelligent IDS
  - Less false positives
  - Better detection of advanced attacks (APT)

Honeypots



- A honeypot:
  - is a computer configured to detect network attacks or malicious behavior,
  - appears to be part of a network, and seems to contain information or a resource of value to attackers.
- But honeypots are isolated, are never advertised and are continuously monitored
- All connections to honeypots are per definition malicious
- Can be used to extract attack signatures
- Honeynet is an international security club, see next slide

End of lecture