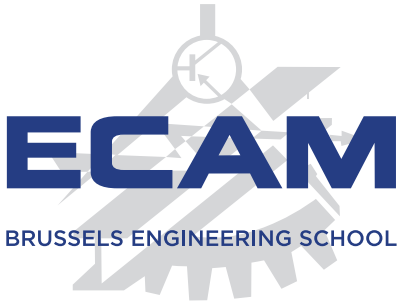


I5020 Computer Security

Session 6

Network Protections: DoS, Firewall and IDS

Sébastien Combéfis

Fall 2019

Objectives

- Discovering global network attacks

  Denial-of-Service and intrusion of a computer system

- Network Denial-of-Service attacks mechanisms
  - SYN spoofing and packet flooding attacks
  - Distributed DoS, reflection and amplification

- Two protection mechanisms for a network

  Intrusion detection system and firewall to block traffic

Denial-of-Service Attack

Denial-of-Service (1)

- Denial-of-Service (DoS) attack hampers availability

  Obstruction or total block of services provision

- Process by depletion of critical resources used

  Flood a web server with fake and unnecessary requests

- One of the most difficult to detect attack

  The attacker often uses legitimate requests...

Denial-of-Service (2)

- DoS attacks amplified due to throughput increase

  400 MB/s in 2002 → 100 GB/s in 2010 → 300 GB/s in 2013

- Damage to internet core servers and DNS servers

  Eased with distributed DoS starting with 50 GB/s

"A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing unit (CPU), memory, bandwidth, and disk space."

DoS Attack Target

- Bandwidth of network links connecting servers to the internet

  Generate legitimate traffic that will decrease the quality of service

- System resources used by the software managing the network

  Saturate buffer/RAM (SYN spoofing), exploit bug (poison packet)

- Application resources implementing provided services

  Consume maximum of resources or exploit software bug

Classic DoS Attack (1)

- Using a system with a high capacity network

  To be able to attack a weaker system

- At the simplest, massively sending PING request to a server
  - Very easy to do massively with large network capacity
  - Saturated attacked server starts throwing packets
  - Decrease in the availability of services provided by the server

- Two weaknesses to this type of attacks
  - The source of the attacker is in the *ICMP echo request*
  - Mirror attack on the attacker with the *ICMP echo response*

Source Address Spoofing

- Spoofing the source address to hide identity

  Attacker must falsify source address in issued packets

- Using a raw socket interface on its system

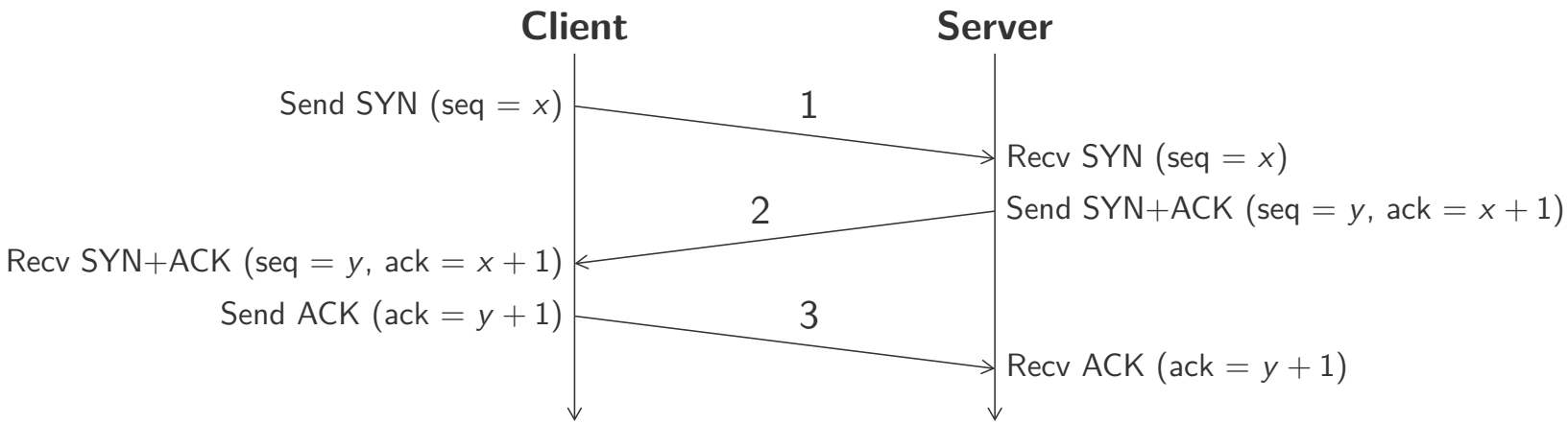
  Most OSes offer this kind of access (for test/research)

- Attack amplification and overloading the abused server
  - *ICMP echo response* packets sent everywhere on the internet
  - Error response of true systems and ICMP dest. unreachable

Classic DoS Attack (2)

- SYN spoofing attack exploits a weakness of TCP protocol
  - Saturation of tables that handle TCP connections
  - Legitimate clients will be rejected
- Opening a TCP connection with a three-way handshake

  Connection marked established by server after three exchanges



SYN Spoofing

- TCP on IP protocol that is not reliable, even if best-effort

  Client and server keep packets for retransmission in case of loss

- Attacker sends SYN packets with spoofed source addresses
  - Server stores connection information and answer SYN+ACK
  - Existing machine should send a RST packet
  - Server will make several retransmissions before aborting

- Saturation TCP ongoing connections table of the server

  New legitimate requests will be rejected...

Flooding Attack

- Overload network capacity by flooding attacks on a server

  Several possible attacks depending on the used network protocol

- Three main attack types: ICMP, UDP, TCP SYN
  - Ping often blocked, but TCP/IP control packet are not
  - Sending to an UDP port, as *diagnostic echo service*
  - Sending TCP packets just to flood

- Main goal is to produce a large volume of traffic

  Indirect attacks: DDoS, reflector/amplifier attacks

Distributed DoS

- Great improvement of DoS attacks with several systems

  Typically workstations and compromised computers

- Installing an attacker-controlled agent through a malware
  - Such a compromised machine is called a zombie
  - A network of zombies is called a botnet, allowing DDoS
  - New infected machine contacts a handler to signal its presence
- Zombie individually commanded or hierarchically

  Attacker $\rightarrow$ *Zombies handler* $\rightarrow$ *Zombie agent* $\rightarrow$ *Target*

SIP Flood (1)

- Attacking the Session Initiation Protocol (SIP) used with VoIP

  Text protocol in the same style as HTTP

- SIP INVITE to initiate communication between Alice and Bob

  It triggers a considerable resource consumption

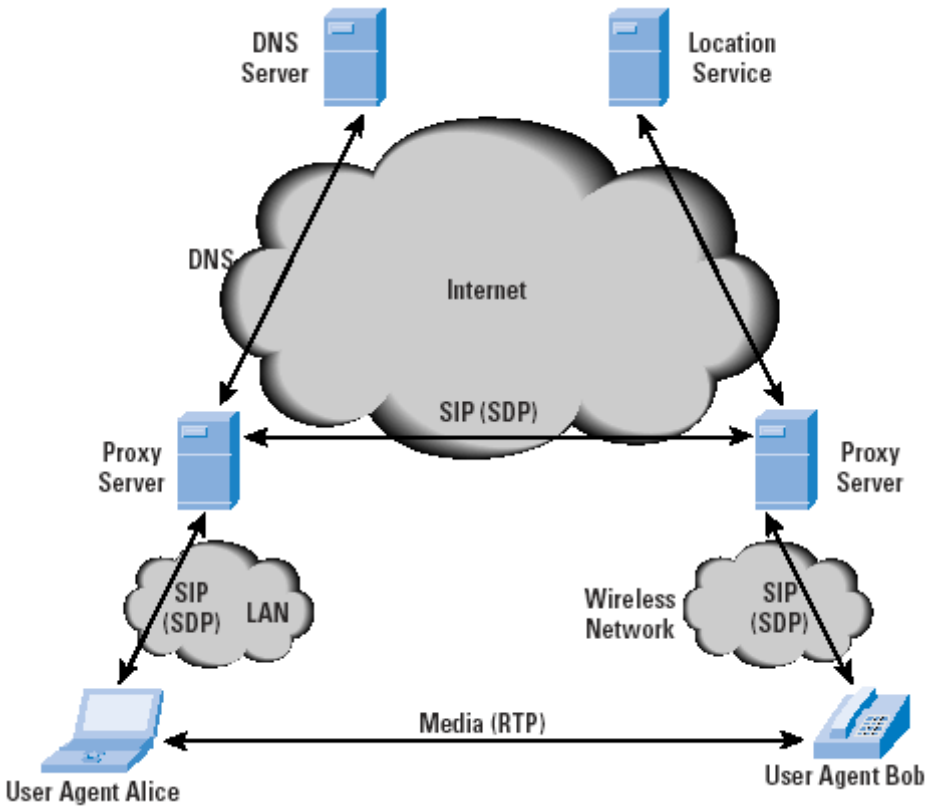
- Two kinds of victims can be targeted by attacks

  Proxy servers and machines receiving unsolicited calls

SIP Flood (2)

- Proxy server hurts in two different ways

  Depletion of resources and consumption of network capacities



HTTP Flood

- Bombarding an HTTP server with requests from bots

  Targeting requests that consume maximum server resources

- Attack asks for large file download, for example
  - Reading file from the disk, storing it in memory
  - Transformation into packet streams and transmissions
- Another variant of HTTP flooding is the spidering

  Follow recursively all the links of a page

Slowloris

- Exploits server multi-threading to manage requests

  Requests directed towards the same application server

- Resource monopolisation by unfinished HTTP requests
  - Depending on HTTP protocol, request finished by empty line
  - Regular sending of HTTP headers to maintain the connection
  - The server cannot launch new threads

- Very difficult to discover since legitimate requests

  Timeout varying with load, limiting requests from one source...

Reflection (1)

- Attacking an intermediary targeting a known service

  Attacker used a spoofed IP source address

- Intermediary answer is sent to spoofed address

  It is the real target of the attacker

- Properties to satisfy for a successful attack
  - Responses must be larger than the original query
  - Often target UDP services (DNS, SNMP, ISAKMP...)
  - Intermediate must have high-capacity network

Reflection (2)

- Example of reflection attacks on the DNS
  - Falsified request on port 7 (*echo service*)
  - Creating a loop between the target and the DNS server

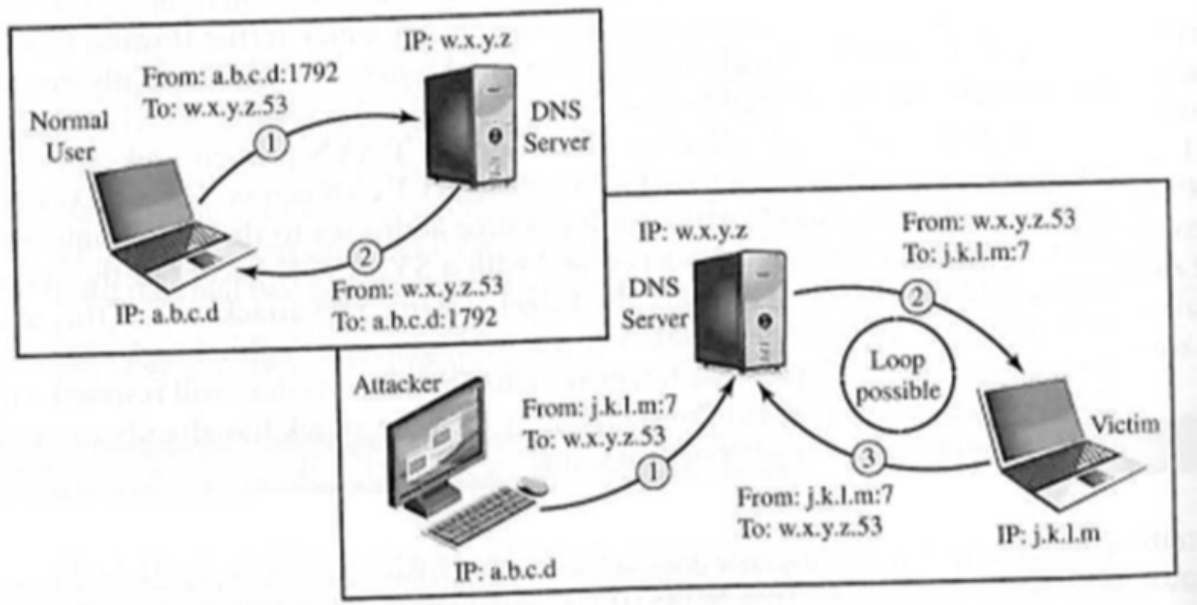


Figure 7.6 **DNS Reflection Attack**

Amplification

- Generation of several packets for each request

  By directing a request to a broadcast address, for example

- Requires a service heavily used on the attacked network
  - For example, the ICMP echo request
  - Only targets UDP because broadcast not available on TCP

- Important to filter external broadcast requests

  List of weak networks can be bought on the black market!

Defence Against DoS (1)

- Impossible to protect 100% from DoS attacks

  A large legitimate traffic is enough to be harmful...

- Slashdot effet not avoidable, possible "legitimate" DoS attacks
  - Popular website shares a link to a smaller website (*Slashdot*)
  - Specific event (Olympic Games, Soccer World Cup...)

- Anticipation of network load and high traffic is necessary

  Increasing bandwidth, distribution and replication

Defence Against DoS (2)

- Four courses of action to minimise DoS attacks
  - Prevention by resource consumption policy (before)
  - Detection and attack filtering (during)
  - Retracing and identification of attacker (during/after)
  - Reaction to eliminate effects of the attack (after)
- Avoiding spoofing of packets source addresses

  Near emitters, by router/gateway/ISP, depending on context

DoS Response

- Importance of a good incident response plan

  In particular contacts with the ISP technician

- Only possibility is a filtre upstream of the network connection

  In addition to all the precautions to be taken internally

- Identify the vulnerability that made the attack possible

  Wrong configuration, hardware or software fault...

Intrusion Detection

Intruder

- Several types of external intruders do exist

  Cyber-criminal, activist, state-sponsored organisation...

- Three skill levels exist amongst hackers

  Apprentice, journeyman, master

- Attacks can range from benign to most serious one
  - Compromise a mail server, disfigure website...
  - Guess/crack password, copy credit card numbers DB...
  - Execute packet sniffer, hack FTP to send fake files...
  - ...

Intruder Behaviour

- Behaviour patterns common to many intruders

  Enriched or modified due to new vulnerabilities

- Using six common steps

  1. Acquiring the target and collecting information
  2. Initial access to the system (often through remote access)
  3. Privileges escalation (through vulnerabilities)
  4. Information harvest and system exploit
  5. Maintaining access to the attacked target system
  6. Cover traces (delete log files, for example)

Intrusion Detection (1)

- Intrusion detection (not authorised) on a system

  Monitoring system events

- Three logic components to an IDS
  - **Sensor**: network packet, log file, system call trace...
  - **Analyser**: combines sensor information and check for intrusion
  - **User interface**: control, manager, console, etc.

"A security service that monitors and analyses system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorised manner."

Intrusion Detection (2)

- An IDS can use a single server and analyser

  In particular the case for those installed on a machine

- Three types of IDS according to source and analysed data type
  - **HIDS**: monitors characteristics of a single host
  - **NIDS**: monitors network traffic of a segment
  - **D/H-IDS**: combines information from several sensors

Interest of IDS

- Three main motivations to use an IDS
  - Identification and kick out of intruders before damage
  - Can be deterrent to intrusions
  - Information harvesting to learn intrusion techniques
- Intruders behaviour should be $\neq$ from legitimate behaviour
  - The difference should at least be quantifiable
  - Possibility to have false positive and false negative
  - Maximise detection rate and minimise false alarm rate

Analysis Technique

- Two approaches to use data from the sensors
  - **Anomaly detection** based on normal behaviours

    Require prior collection of legitimate data
  - **Signature detection/heuristic** analyses behaviour

    Data pattern (signature) or attack rules (heuristic)
- Malicious behaviour should be expected

  Less with the first approach than with the second one

Anomaly Detection

- Need for a legitimate behaviour model

  On the basis of data collected during normal operation

- Three main ways to classify data
  - Statistical analysis (univariate, multivariate, time-series)
  - Based on knowledge with an expert system
  - Machine learning to train a model by data mining

- Pay attention to detection performance (efficiency and cost)

  Important to think about training on abnormal data

Signature Detection

- Analyse of a flow of events on the system
  - Applying a set of signature patterns
  - Data characterisation by a set of rules
- Requires a large collection of signatures

  Used in anti-virus, network scan proxy, NIDS
- Need to design rules (machine and OS specific)

  For example, SNORT system (NIDS)

Host-Based IDS

- Adding a security software layer to a vulnerable system

  Monitor system activity and detect internal/external attacker

- Several data sources and classical sensors
  - System calls trace is the best data source
  - Audit like records (often log files)
  - Cryptographic checksums for integrity of critical files
  - Access to the registry on Windows

- Possible to have distributed HIDS on a network

  Coordination and cooperation of several local HIDS

Network-Based IDS (1)

- Traffic monitoring at certain precise points in a network

  Traffic analysis, packet by packet in real-time

- Act on network, transport and application layers
  - Potential targets are any machine of the network
  - Embedded or in relation with the firewall
  - Monitor intrusion attempts from the outside

- Must be able to understand protocols and read packets

  Operation undermined by using data encryption

Network-Based IDS (2)

- Two kinds of sensors for NIDS
  - **Inline** segment embedded and see all (through firewall, switch)

    Embedded or standalone software sensor (detection + prevention)
  - **Passif** monitors a copy of the traffic

    More efficient since it does not slow down packet throughput
- Possible to have WIDS (Wireless IDS)

  Only them will have access to wireless traffic

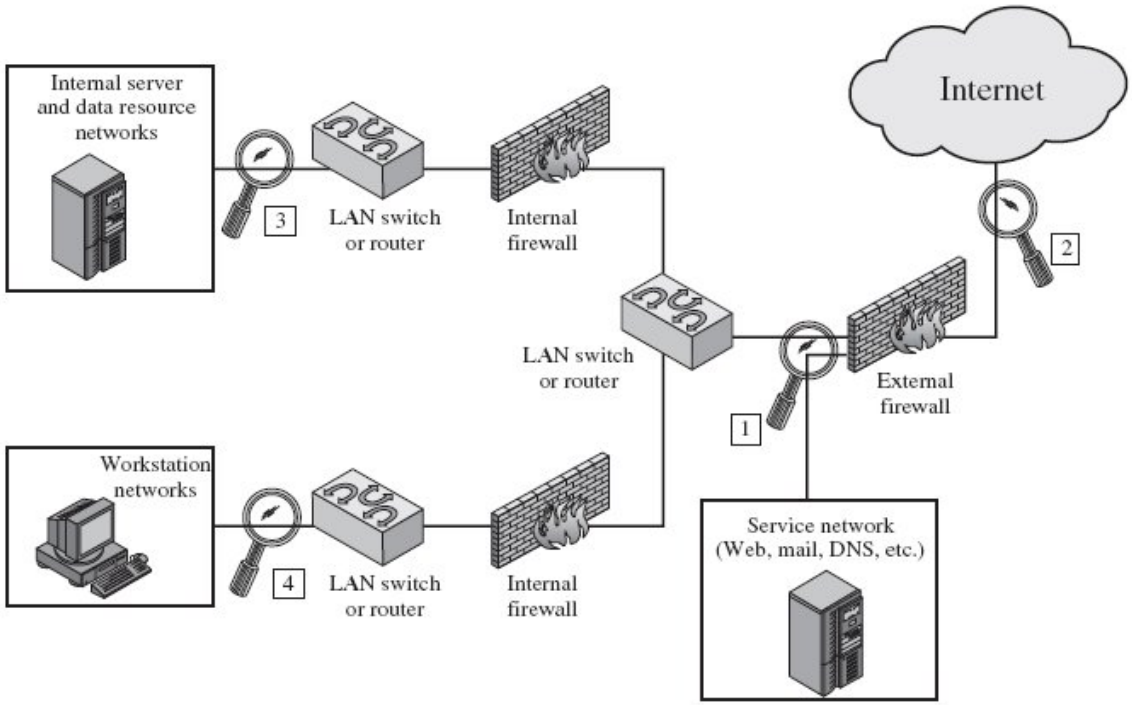
NIDS Placement

- In front of or behind the main firewall

  Control work of firewall, detect attack coming from internet

- internal placement behind firewall to protect subnetwork

  Control of authorised users traffic




Traber
MX
SELFKANT
Rantapohja
ORI JALONEN
Firewall

Firewall

- System protection from threats coming from the network

  Using firewalls that can block the traffic

- Three design rules to get a good firewall
  - All the incoming and outgoing traffic pass through the firewall
  - Only authorised traffic can pass through the firewall
  - Firewall is hardened against penetration

- Protection quality strongly depends on access policy

  Types of authorised traffic (address, port, protocol, etc.)

Action Point

- Firewall can act at several levels on network layers

  From network to application layer, through transport

- Access to several characteristics to establish its policy
  - IP addresses and values related to the protocol (port, etc.)
  - Application protocol (SMTP, HTTP, etc.)
  - User identity, in particular using IPSec
  - Network activity such as hour, queries rate, etc.

Ability

- Single bottleneck reject unwanted users

  Vulnerable services cannot come in, nor go out

- Place allowing the monitoring of events related with security

  Makes it possible to implement audits and alarms

- Ideal place to add services not related to security

  NAT, network management function (audit, internet usage, etc.)

- Can be used as a platform for IPSec

  Implementing VPN thanks to the tunnel mode

Limitation

- No protection against systems bypassing the firewall

  Systems with dial-out or connection through data mobile

- No protection against internal attacks

- A poorly secured wireless network can be an entry point

  Wireless connection from both side of an internal firewall

- A portable, PDA, external disk can go out then come back

  Internal network infection risk by device that went outside

Firewall Type

- Firewall can monitor the traffic at different levels
  - Low level network packets, individually or by stream
  - All the traffic in a transport level connection
  - Detailed inspection of application level protocol
- Operating mode as a positive or negative filter

  Let the traffic pass/reject it, depending on criteria
- Examining one or several headers in each packet

  Can look at packet payload, or sequence of packets

Packet Filtering

- Apply rules for each incoming or outgoing packet

  Then decide to forward or delete the packet

- Rule based on several information contained in the packet
  - Source/destination addresses of the packet (IP/transport)
  - IP protocol field that defines the transport
  - Interface through which the packet entered the firewall
- Très grande simplicité et aussi transparence pour l'utilisateur
  - Pas de protection sur vulnérabilité couche applicative
  - Pas de support de l'authentification des utilisateurs

Attack Prevention

- IP addresses spoofing

  Throw packet with internal source from external interfaces

- Source routing attacks (force packets journey)

  Throw packet if final destination inside protected network

- Small fragments attacks (to avoid header everywhere)

  First packet should contain minimum set of headers

Stateful Inspection

- Taking into account connection context

  TCP protocol choose port between 1024 and 65535 dynamically

- Memorising a list of outgoing connections that are legitimate
  - Authorising incoming traffic only for established connections
  - Possibility to monitor TCP sequence numbers

- Some advanced firewalls analyse protocol information

  Filtering FTP, IM, SIPS, etc. commands depending on the state

Application-Level Gateway

- Application proxy relay application level traffic

  Transfer of TCP packets once user authenticated to proxy

- Several possible actions for the gateway
  - Limit services that are supported by the gateway
  - Only supports some functions of a service
- Much better than a packet filtering analysis
  - Only analyse authorised services
  - Easy to audit and log all the incoming traffic
  - Additional cost is the decrease of performance

Circuit-Level Gateway

- Standalone system that splits into two TCP connections

  Simple relay of TCP segments once connection accepted

- If internal users can be trusted
  - Application-Level Gateway for incoming connections
  - Circuit-Level Gateway for outgoing connections

Firewall Base

- Typically placed on a dedicated machine under UNIX/Linux

  Or software module on routers or LAN switch

- Placed on a bastion host identified by the administrator
  - Very strong machine placed on critical point of the system
  - Hardened OS, minimal services installed, etc.
- Host-Based Firewall protecting a particular host

  Typically present on servers, directly through the OS

- Protecting personal machine with a personal firewall

  Software on personal machine or on the modem-router

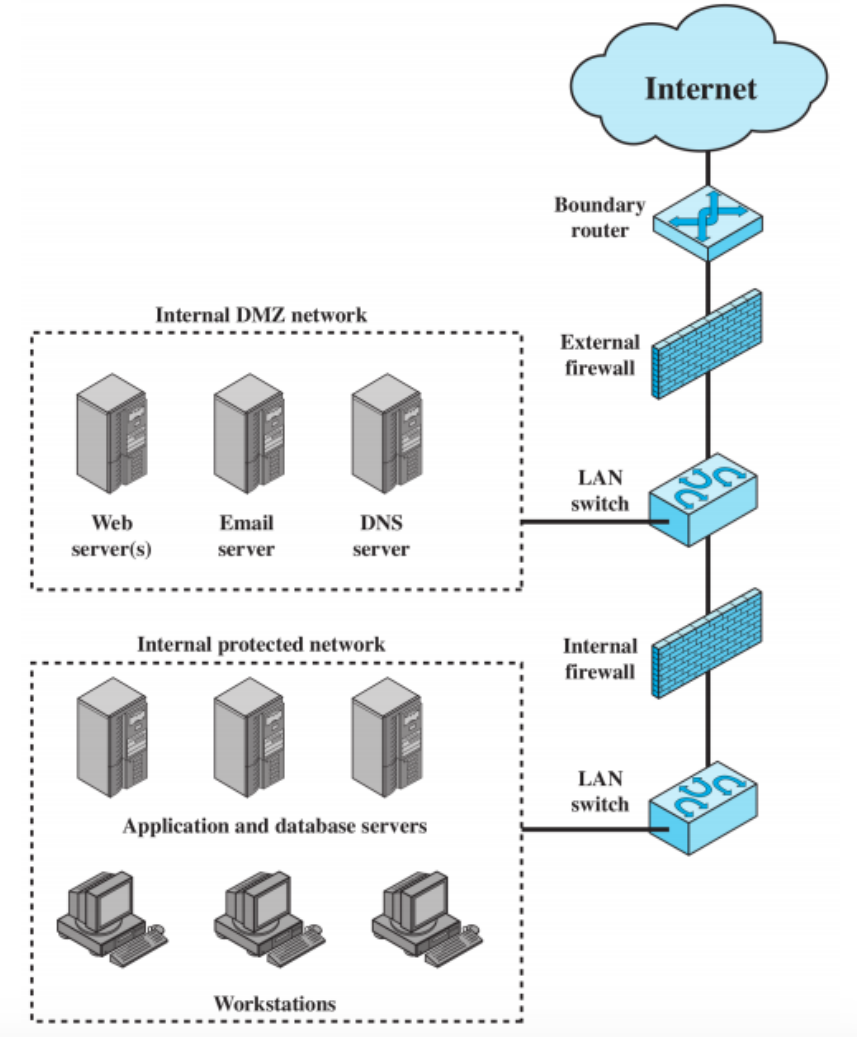
DMZ Network

- Possibility to define a demilitarised zone (DMZ)

  Additional network segment between external and internal firewall

- Systems to protect but accessible from the outside

  Server with company website, e-mail, DNS, etc.



Virtual Private Network (1)

- VPN protects machines on an unsecured network

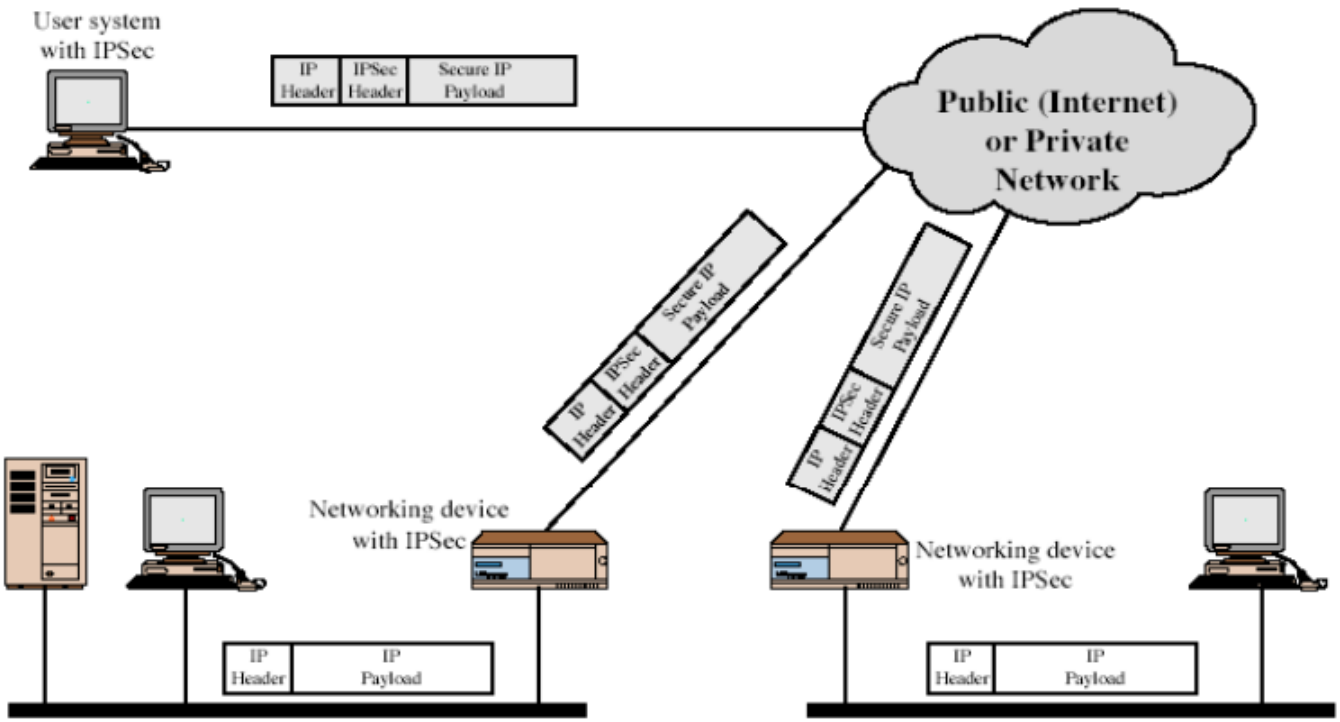
  Special protocols and encryption to provide security

- Creation of a LAN network with machines on several sites
  - Encryption and authentification done in lower layers
  - Cheaper than having private lines between sites
  - Require same encryption level on both sides

Virtual Private Network (2)

- Typically based on IPSec protocol

  Totally transparent for users



Intrusion Prevention System

- Extending IDS to block malicious activity

  Can block or modify packets, system calls, etc.

- Several types of IPS exist, as for IDS

  HIPS, NIPS and distributed or hybrid versions

Credits

- William John Gauthier, 2011, https://www.flickr.com/photos/wgauthier/5571099814.
- https://www.cisco.com/c/dam/en_us/about/ac123/ac147/images/ipj/ipj_6-1/session_initiation_1.gif.
- https://pt.slideshare.net/pfloeschel/denial-of-service-attacks/11.
- Richard C, November 26, 2017, https://www.flickr.com/photos/155733895@N04/37769444605.
- http://ptgmedia.pearsoncmg.com/images/ch06_9780136004240/elementLinks/fig05.jpg.
- Mikko Nyman, May 9, 2011, https://www.flickr.com/photos/mikko_nyman/5704624456.
- http://hw.siit.net/files/001408.pdf.
- https://arxiv.org/pdf/1001.4200.pdf.