Topic 4 - Firewalls and network security

Eric Casanovas

Universitat d'Andorra

20th April, 2022

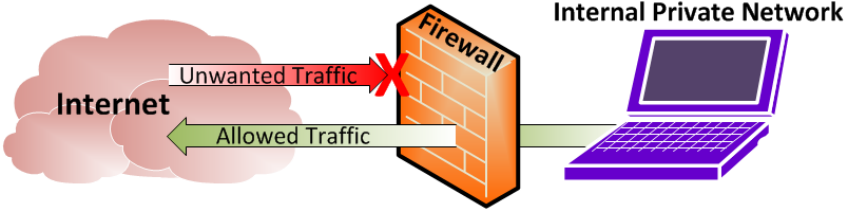
Introduction

- Network security is really important to protect against attackers
- It provides an "external security" to our machines
- Network security goes from WANs to LANs
- We will focus on LANs
- We will consider 5 main securizations:
  - Firewalls
  - Network Access Control
  - Network Segmentation
  - VPNs
  - IDS/IPS
- But we will cover more topics during this topic

What are firewalls I

- Is a system or group of systems used to control the access between two networks using pre-configured rules and filters
- Used to implement and enforce a security policy between networks
- Examines all packets and decides what to do with the given rules
- So, it provides perimetral security to our network

What are firewalls II



Why are firewalls necessary

- To protect information from those who don't have access to
- Protect network from malicious users
- Protect from attacks as DDoS

Types of firewall I

- We can divide it in physical or software firewalls:
  - Hardware firewalls
  - Software firewalls
- But we can also divide it depending the layer:
  - Packet filtering (Netwrok Layer)
  - Stateful Inspection (Transport Layer)
  - Application Based Firewall (Application Layer)

Types of firewall II

Hardware Firewalls:

- Physical device
- Usually placed between router and computer
- Protects the entire network
  But...
- Hard to configure and expensive
- CISCO, Fortinet, Netgear...

Types of firewall III

Software Firewalls:

- Software application
- Installed in the device that you wish to protect
- Protects a single computer
- Easier to configure and cheaper
- PfSense, OPNsense, Untangle firewall...

Types of firewall IV

Parameters	Software Firewall	Hardware Firewall
Broad vs. Granular Protection	Provides granular protection for all individual devices within the network	Protects the network as a whole.
Complex vs. Simplicity	Simpler to set up, change, and maintain	Requires skilled staff, and physical proximity to the data center.
High Cost vs. Low Cost	Cost little to deploy and maintain	High initial investment in hardware, and a continued investment in skilled staff.
Inconvenient vs. Convenience	Software firewall is difficult to bypass, and has very little effect on user experience.	Hardware firewall is often bypassed by employees seeking faster, more reliable connection or access to certain restricted sites.
Expertise vs. Usability	Software firewall is easy to use and designed to be easily managed by anyone.	Hardware firewall require advanced IT knowledge to install and manage

Types of firewall V

Packet filtering:

- Simplest firewall (inbound and outbound rules)
- Filters packets based on specific criteria (IP addresses, subnets, ports...)
- Does not read the packet payload, just the header (reduces overhead)
- Vulnerable to IP spoofing (modification of IP header packets)
- Works at network layer
- Advantages:
  - Simple
- Disadvantages:
  - Can be compromised by many attacks as source spoofing

Types of firewall VI

Stateful Inspection:

- Addition to packet inspection
- Validates packets for multi-packet flows
- Keeps track of connection state (TCP streams, active connections...)
- Advantages:
  - Adds state to packet filter and keeps track of ongoing connection
- Disadvantages:
  - Slower (increases overhead)

Types of firewall VII

Application based firewall:

- Allows data into/out of a process based on that process' type
- Can act on single computer or at network layer
- Examines incoming app data and verifies that data is safe before passing it to the system.
- Advantages:
  - Filter bad data (malware)
  - Complete view of packet
- Disadvantages:
  - Slower as it inspects the whole packet payload

Firewall Components

- DMZs
- Bastion Host
- IDS/IPS

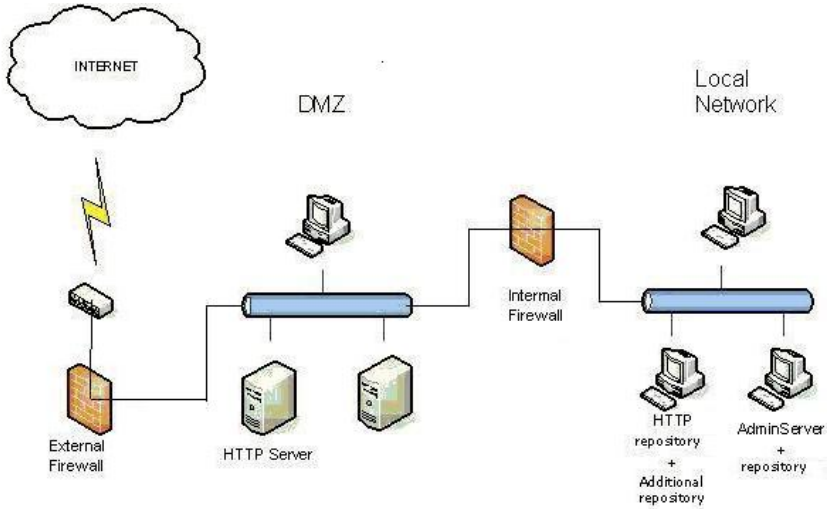
DMZ I

- Subnetwork that exposes an organization's external-facing services to a larger and untrusted network
- The term refers to an area between nation states in which military operation is not permitted (e.g. The good and the bad Korea)
- Adds an additional layer of security

DMZ II


NORTH
KOREA
Military
Demarcation
Line
Demilitarized Zone (DMZ)
2nd Tunnel
4th Tunnel
38th Parallel
1st Tunnel
3rd Tunnel
SOUTH
KOREA
Seoul

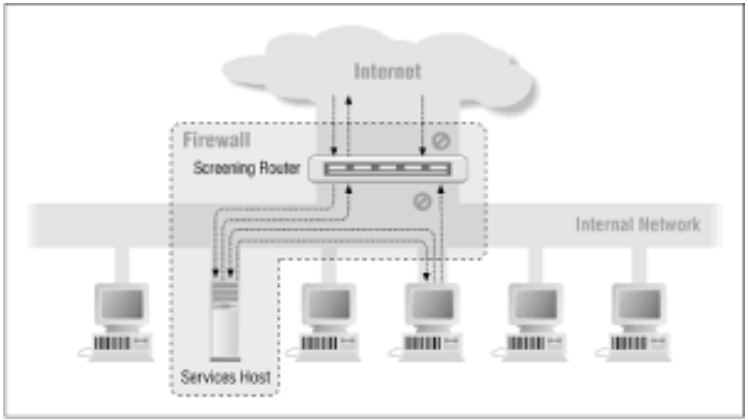
DMZ III


INTERNET
DMZ
Local
Network
Internal
Firewall
External
Firewall
HTTP Server
HTTP
repository
+
Additional
repository
AdminServer
+
repository

Bastion Host I

- A bastion host is a specialized computer that is deliberately exposed on a public network
- Typically placed in the DMZ
- Very prone to attack
- It is like the hall of a building, Outsiders may not be able to go upstairs but they can walk freely there
- Usually it is a proxy server or load balancer

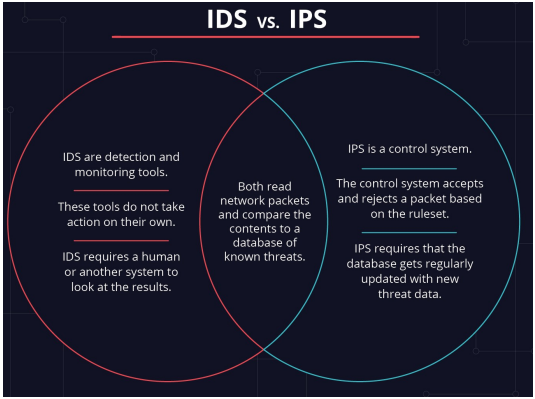
Bastion Host II



IDS/IPS I

- IDS: Intrusion Detection System
  - Analyze and monitor network traffic for signs that indicate attackers are using a known cyberthreat to infiltrate or steal data from your network
- IPS: Intrusion Protection System
  - IPS proactively deny network traffic based on a security profile if that packet represents a known security threat.
- Both are highly related with firewalls as they also inspect packets
- Interesting Machine learning techniques

IDS/IPS II


IDS vs. IPS
IDS are detection and monitoring tools.
These tools do not take action on their own.
IDS requires a human or another system to look at the results.
Both read network packets and compare the contents to a database of known threats.
IPS is a control system.
The control system accepts and rejects a packet based on the ruleset.
IPS requires that the database gets regularly updated with new threat data.

IDS/IPS III

Advantages/Disadvanatges

- Response: An IDS is passive (you must take action after the alert), while an IPS is an active control system.
- Protection: IDS offers less help when under threat. An IPS tries to protect you actively.
- False positives: If an IDS gives you an alert about something that isn't troublesome -> no problem. However IPS shuts down traffic and many people could be impacted.

IDS/IPS IV

Examples:

- **Snort**
  - Free open source network intrusion detection system created in 1998 and today owned by CISCO
- **Suricata**
  - open source-based intrusion detection system and intrusion prevention system. It was developed by the Open Information Security Foundation in 2010

Advantages

- Increases security of the network (anti malware, attackers...)
- Isolation
- Traffic monitoring

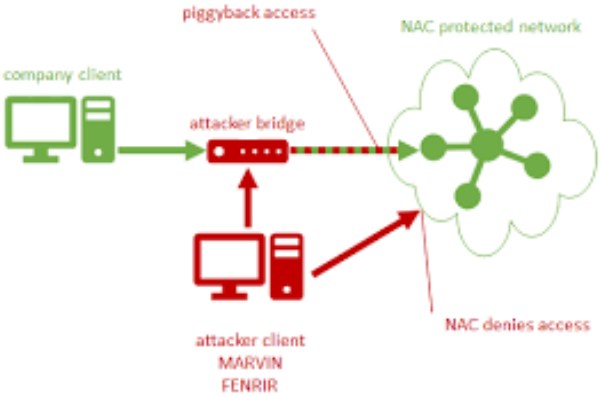
Downsides

- They should be properly configured to avoid being bypassed by users or malicious actors
- Increses overhead of network

Network Access Control I

- Is the act of keeping unauthorized users and devices out of a private network
- Requires users to meet some requirements, for example:
  - Minimum security requirements (i. e. antivirus)
  - Authentication
  - System updates
  - Configurations

Network Access Control II



Advantages

- Mitigation of zero-day attacks
- Identity and access management
- Authorization and Authentication of network connections

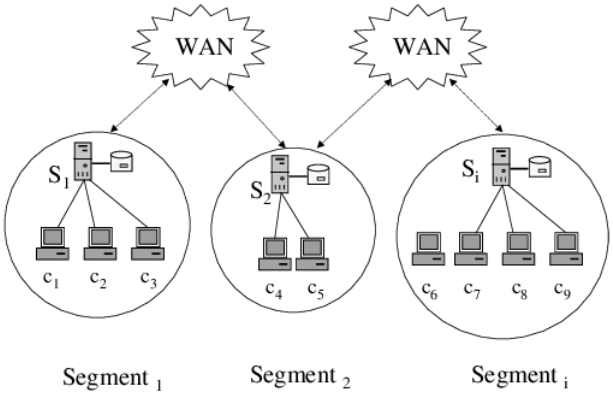
Downsides

- Unauthorizxed accesses
- An attacker can have access to the network if he is able to get credentials
- Difficult to detect this attacks

Network Segmentation I

- Is a technique that divides a network into smaller, distinct sub-networks
- Each sub-networks has its own security controls and services
- Isolates each sub-network from the others
- VLANs

Network Segmentation II



Advantages

- Reduced congestion
- Improved security
- Isolation of active attacks before they spread across the network

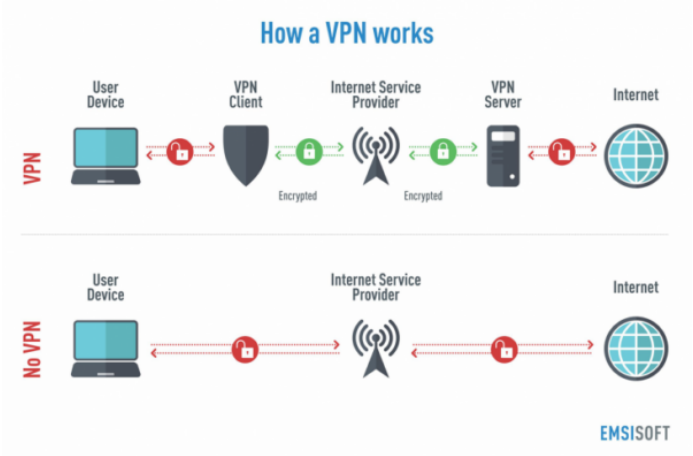
Downsides

- Bottleneck between segments of network
- Reduces productivity

VPN I

- Extends a private network across a public network
- Enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network
- Usually communications are encrypted, but it is not necessary
- The connections are established point-to-point
- Extremely useful in non-trusted networks to encrypt communications

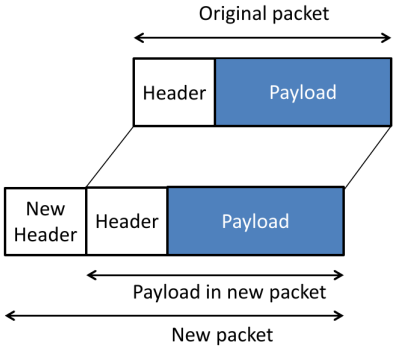
VPN II


How a VPN works
VPN
User Device
VPN Client
Internet Service Provider
VPN Server
Internet
Encrypted
Encrypted
No VPN
User Device
Internet Service Provider
Internet
EMSISOFT

VPN III

- VPNs are build using tunnels and cryptography
  - Cryptography: for encryption and authentication
  - Tunneling:
    - The tunneling protocol encapsulates the data
    - Encapsulated packets are routed between tunnel endpoints

VPN IV


Original packet
Header
Payload
New Header
Header
Payload
Payload in new packet
New packet

Use Cases

- Encrypt communications
- Security on public wi-Fi
- Access to any content in any place
- Security when working remotely

Advantages

- Improve security and privacy
- Connect to private networks from public networks
- Flexibility and scalability

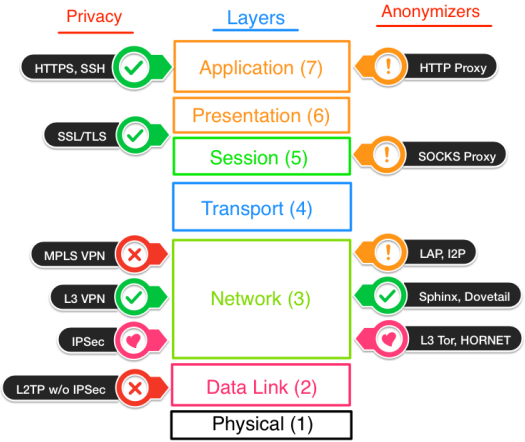
Downsides

- VPNs don't provide anonimity*
- Lower bandwidth

VPN Protocols

- There are many VPN protocols today:
  - **IPSec**
  - **IKEv2/IPSec**
  - OpenVPN
  - Wireward
  - PPTP

IPSec I


Privacy
Layers
Anonymizers
HTTPS, SSH
Application (7)
HTTP Proxy
Presentation (6)
SSL/TLS
Session (5)
SOCKS Proxy
Transport (4)
MPLS VPN
LAP, I2P
L3 VPN
Network (3)
Sphinx, Dovetail
IPSec
L3 Tor, HORNET
L2TP w/o IPSec
Data Link (2)
Physical (1)

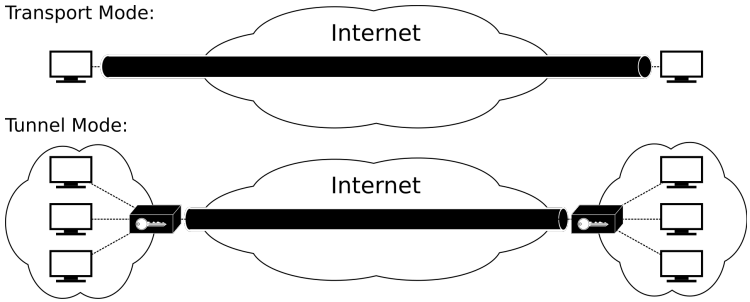
IPSec II

- According to wikipedia: Is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network
- IPsec uses the following protocols to perform various functions:
  - IKE (Internet Key Exchange): IP peer authentication and negotiation of security parameters (generation of Security Associations)
  - AH (Authentication Header Protocol): Data authentication
  - ESP (Encapsulation Security Protocol): Authentication and confidenciality

IPSec III

- Two modes of operation:
  - Tunnel mode:
    - Typically for site-to-site VPNs
    - The entire IP packet is encrypted and authenticated
    - It is then encapsulated into a new IP packet with a new IP header
  - Transport mode
    - Typically for remote access
    - Only the payload of the IP packet is usually encrypted or authenticated
    - IP header is neither modified nor encrypted

IPSec IV



IPSec V

- Further read here

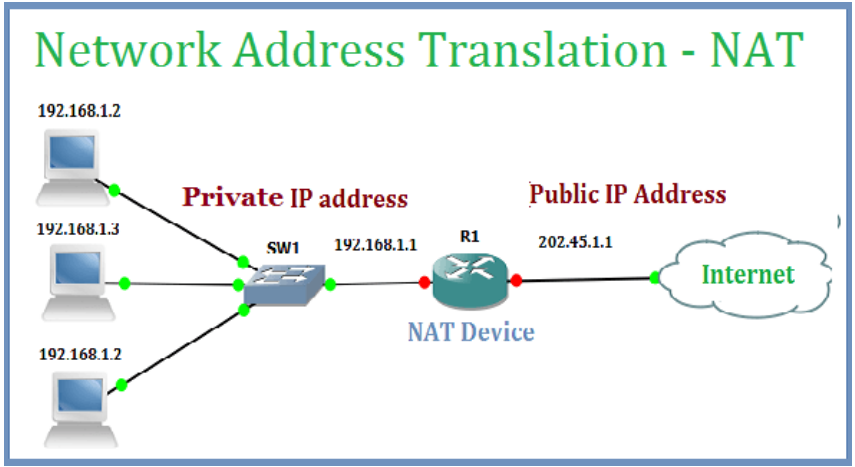
NAT I

- Problem: Not enough IPv4 addresses 4,294,967,296 (2^{32})
- Solution: Private IPs -> Available adress blocks:
  - A class: 10.0.0.0/8
  - B class range: 172.16.0.0/16-172.31.0.0/16
  - C class range: 192.168.0.0/16
- Problem2: private IPs cannot be used in internet

NAT II

- Mechanism that translates IP addresses
- Allows to connect public and private networks and to save public IP addressing
- When using NAT, two address translations are performed:
  - One translation when the packet departs the NAT router
  - The reverse translation when the packet returns to the NAT router

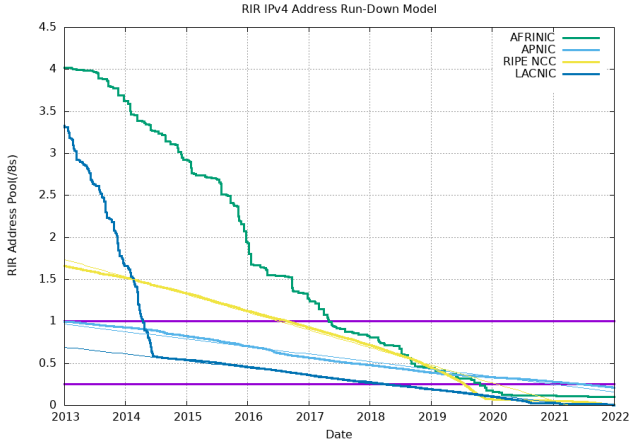
NAT III


Network Address Translation - NAT
192.168.1.2
Private IP address
Public IP Address
192.168.1.3
SW1
192.168.1.1
R1
202.45.1.1
Internet
NAT Device
192.168.1.2

NAT IV

- However the limitation is the bottleneck in the NAT router
- Also there is a limitation in the number of public IPv4
- Switch to IPv6 :)

NAT V


RIR IPv4 Address Run-Down Model
AFRINIC
APNIC
RIPE NCC
LACNIC
RIR Address Pool(/8s)
Date
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022

The END!