Les 4 Firewalls

PfSense

2019.10.03

M. DIMA

katholieke hogeschool
associatie KU Leuven
vives

Overzicht

- Introduction to Firewalls
- Firewall Taxonomy
- Firewall Architectures
- Firewall Planning & Implementation
- Firewall Limitations

Introduction

- *Firewalls* are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures.

Introduction

- What can firewalls do?
  - Manage and control network traffic
  - Authenticate access
  - Act as an intermediary
  - Protect resources
  - Record and report on events (IDS, NIDS, IPS)

- Firewalls operate at Layers 2, 3, 4, and 7 of the OSI model

Firewall - A device or application that analyzes packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port. Packets that do not match policy are rejected.

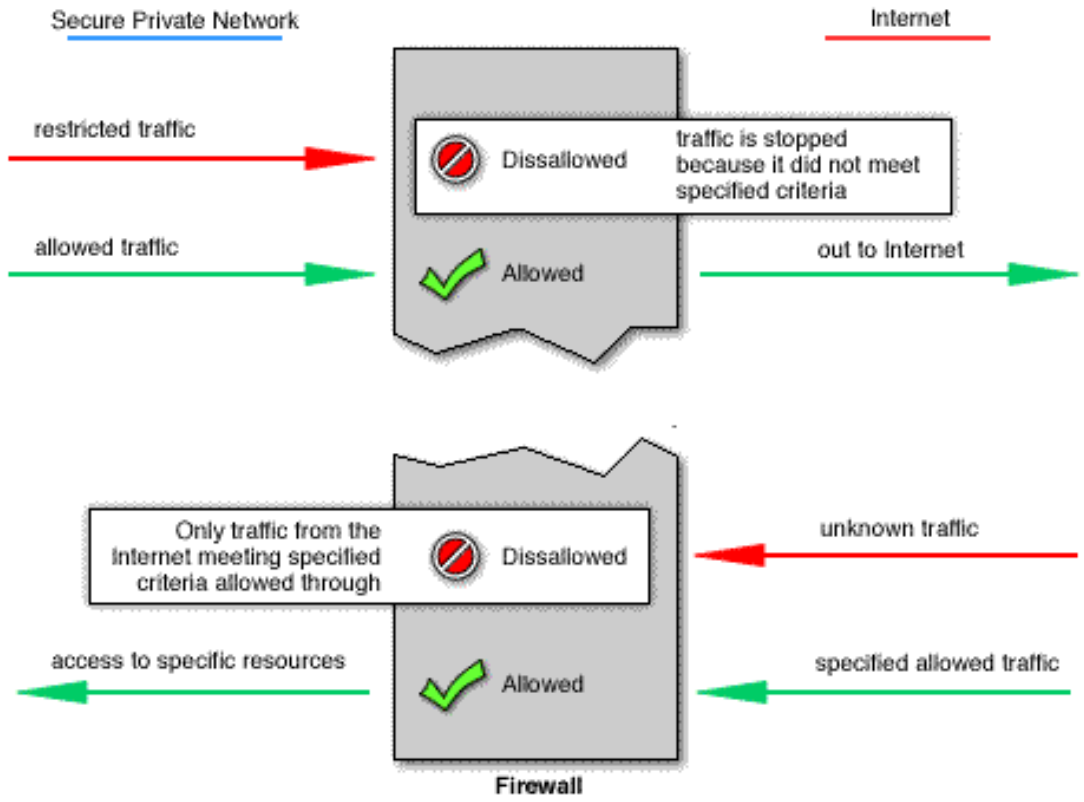
Intrusion Detection System - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event.

Intrusion Prevention System - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected.

Introduction

How does a firewall work?

deny/grant access based on the rules pre-defined by admin



Taxonomy

- FW Products
  - **Software**

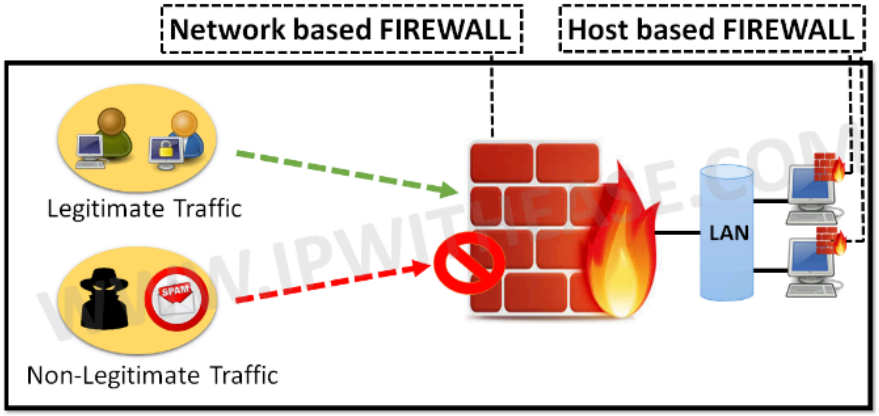
    ISA Server, Iptables, Comodo, ZoneAlarm,…
  - **Appliance**

    Cisco PIX, Checkpoint, SonicWall, WatchGuard,…
  - **Integrated**

    Multiple security functions in one single appliance: *FW, IPS, VPN, Gateway Anti-virus/spam, data leak prevention…*
- Open vs. Closed Source FWs

  ipfw, ModSecurity, pfSense,…

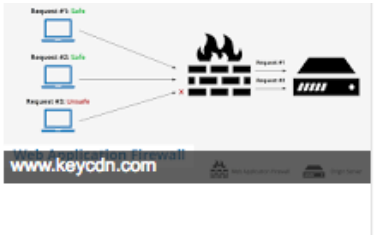
Taxonomy (classificatie)



FW Technologies

- **Host-based** (or **Personal) FW**
  Windows FW, Firestarter,…
- **Network FW**
  - ✓ (Simple) Packet Filtering monitor in/out packets ip addresses (headers)
  - ✓ Stateful Inspection app layer. dynamic
  - ✓ Application FWs
  - ✓ Application-Proxy Gateways
  - ✓ Dedicated Proxy Servers NAT, cache, block sites, ..
  - ✓ Transparent (Layer-2) FWs https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book/zbfw-l2-transp-fw.pdf

An **application firewall** is a form of **firewall** that controls input, output, and/or access from, to, or by an **application** or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the **firewall**.



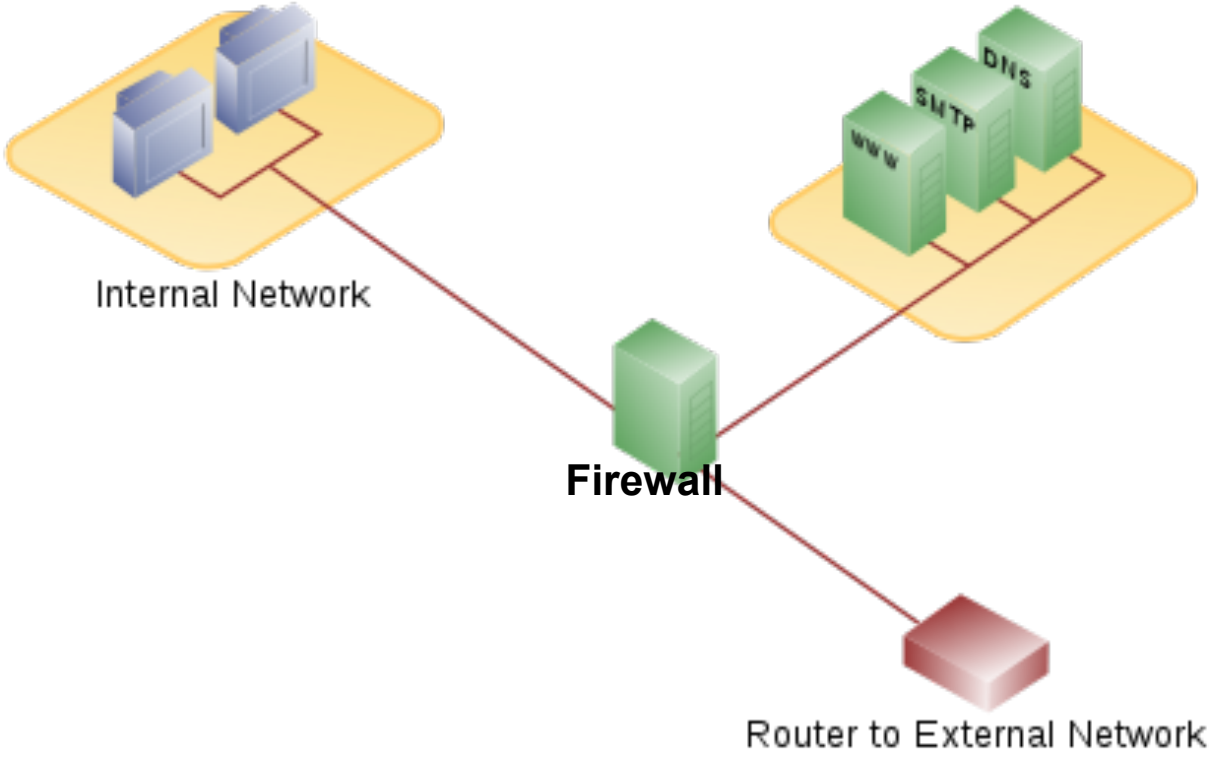
Taxonomy

- FW Technologies
  - **Others** (Network FW)
    - ✓NAT (*it is actually a routing technology*)
    - ✓VPN
    - ✓Network Access Control/Protection (NAC/NAP)
    - ✓Web Application FW
    - ✓Firewalls for Virtual Infrastructures
    - ✓Unified Threat Management (UTM)

katholieke hogeschool associatie KU Leuven vives

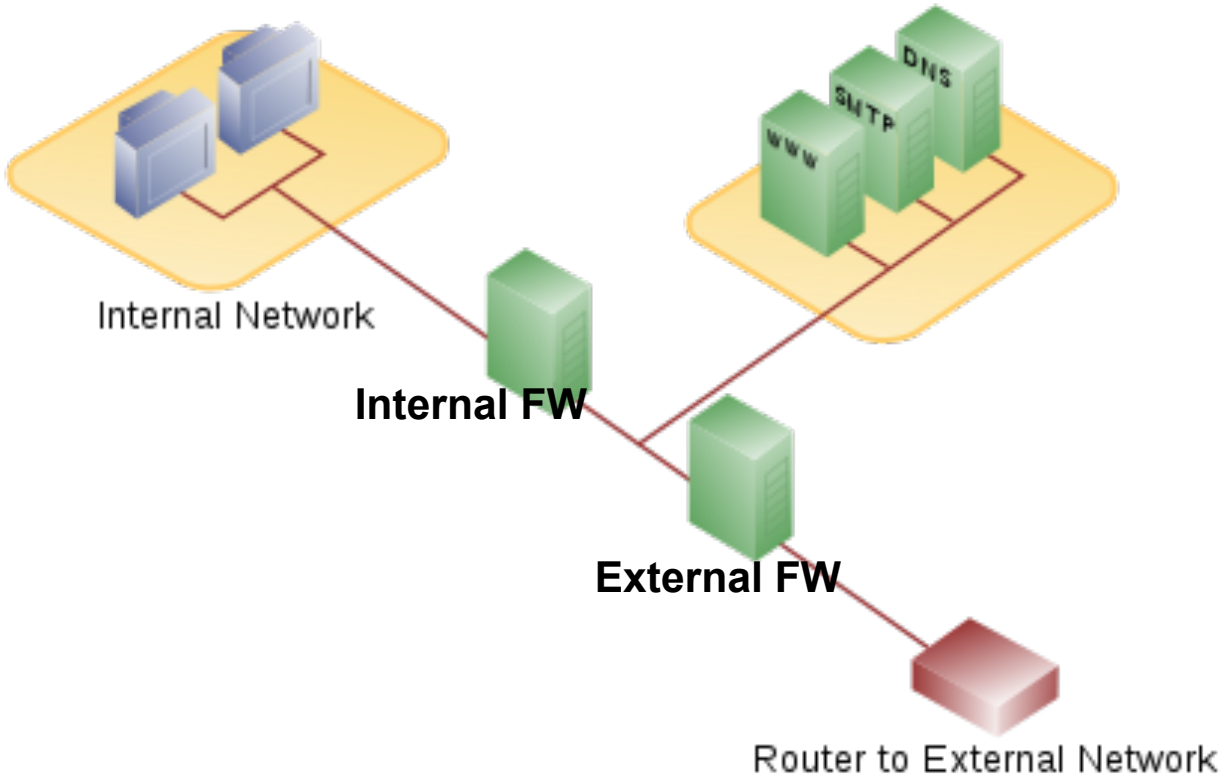
Architectures

- DMZ
  - Single (Three legged) firewall

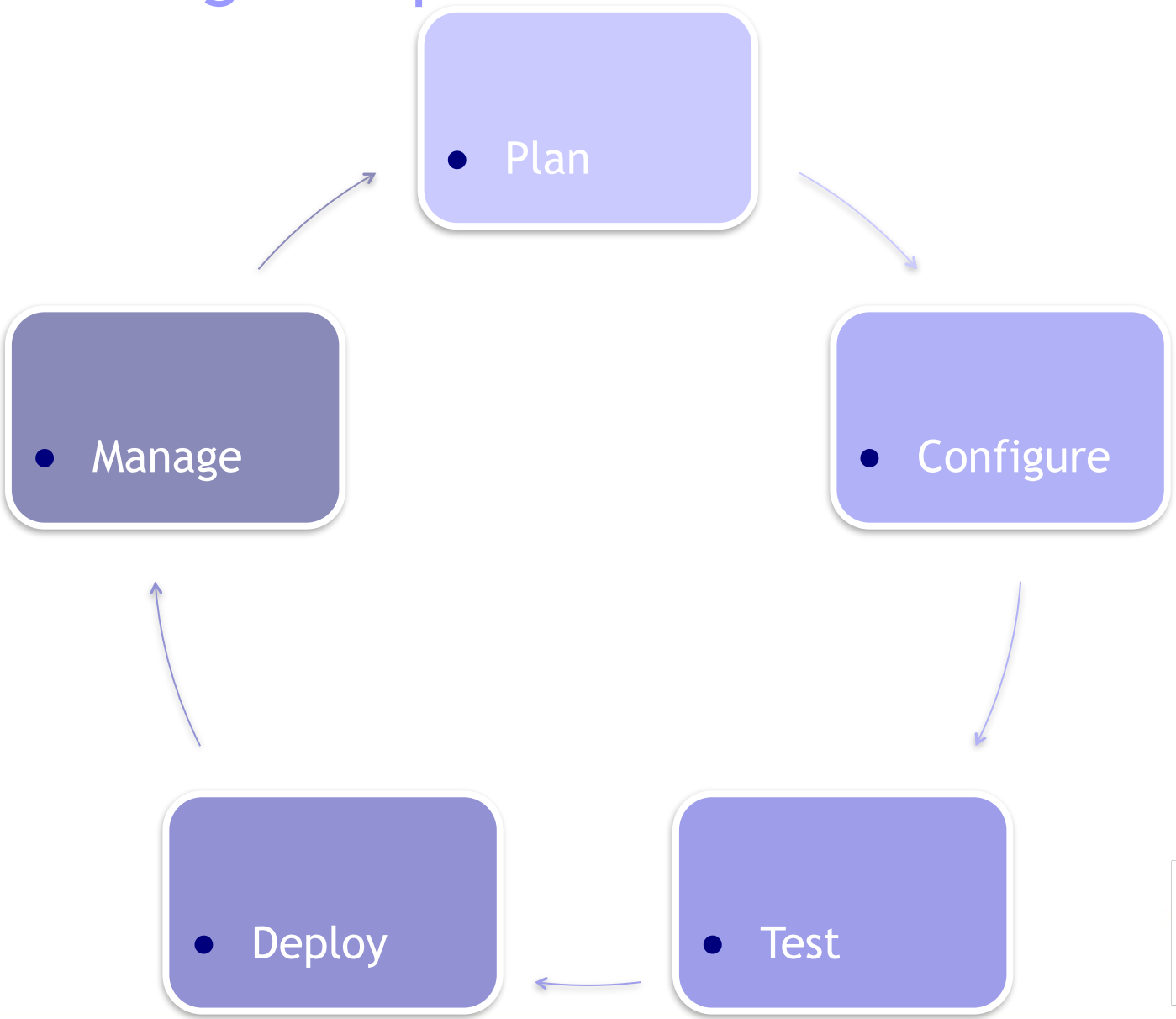


Architectures

- DMZ
  - Dual firewall



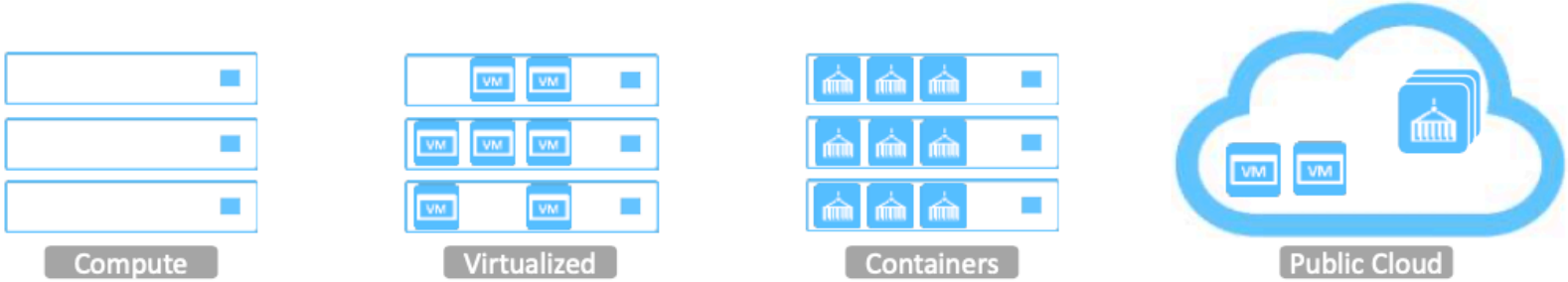
Planning & Implementation



Limitations

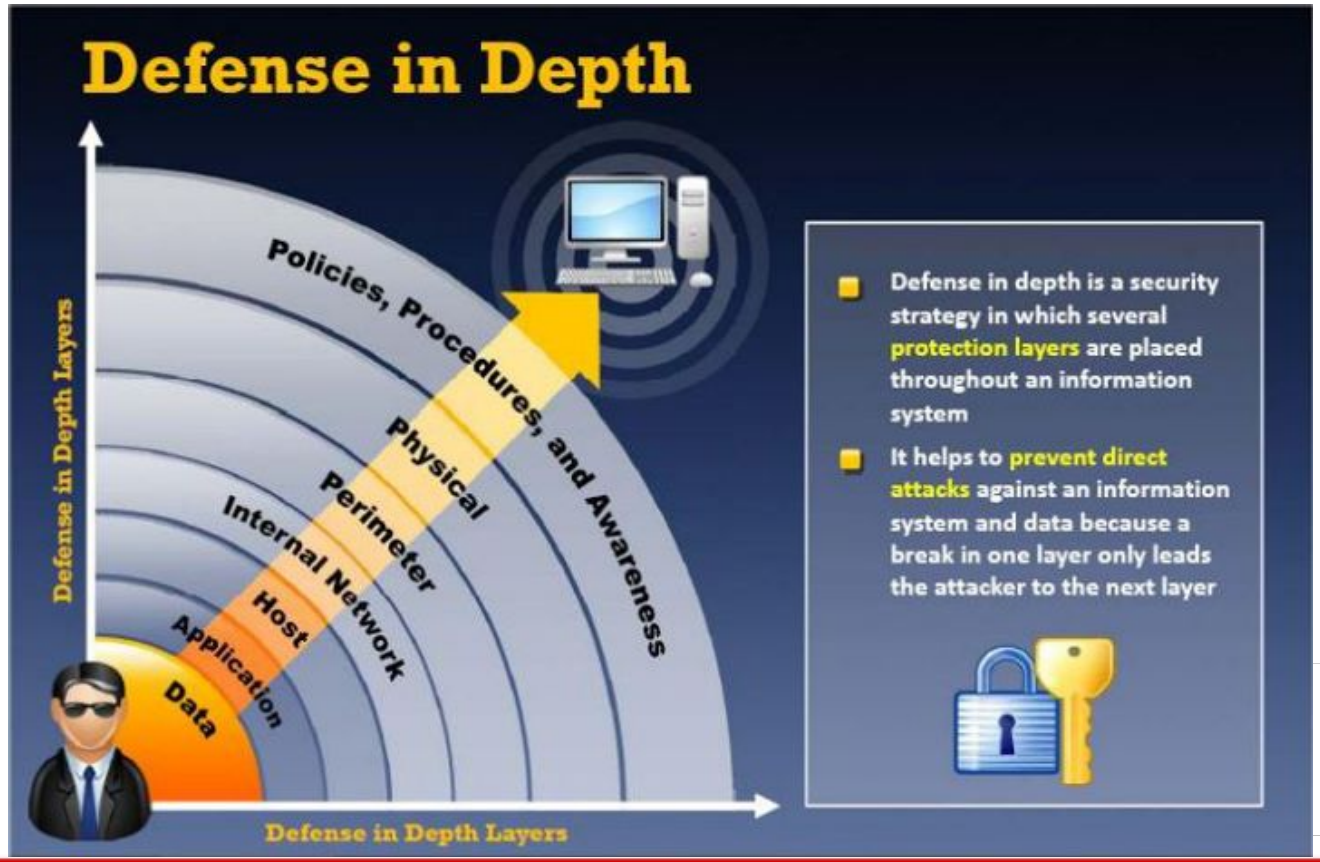
- What a firewall CAN'T protect against:
  - viruses/malwares
  - internal threats (*disgruntled workers, poor security policy*…)
  - attacks that do not traverse the firewall (*social engineering, personal modems or unauthorized wireless connections*…)
  - attacks on services that are allowed through the firewall (*HTTP, SMTP, FTP*…)

VIRTUALIZATION TECHNOLOGY



Conclusion

- Firewalls are an integral **part** of any Defense in Depth strategy



References

[1] *Firewall Fundamentals*, Cisco Press (2006)

[2] *Tactical Perimeter Defense*, Element K (2007)

[3] *Module 16 of CEH v7*, EC-Council (2010)

[4] *Building Internet Firewalls 2nd Edition*, O'Reilly (2000)

[5] *Guidelines on Firewalls and Firewall Policy*, NIST (2009)

- 1. Theorie FW: Firewall PfSense
- 2. PF Sense Installeren : https://www.pfsense.org/download/
- 3. Oefenen op rules Pf sense : http://resources.intenseschool.com/pfsense-series-firewall-rules/
- 4. Opdracht Toledo (op punten) : TaakPfSense.docx