Tűzfal és Behatolás felismerés

Architekturális védelem

- Hálózatok, eszközök védelme
  - Hozzáférés védelem
    - Tűzfalak
      - Network Address Translation (NAT)
  - Behatolás felismerés
    - Intrusion Detection Systems (IDS)

Tűzfalak

Tűzfalak

- What is the firewall?
  - Coming from architecture: Wall, that prevents fire to go from one house to the other
  - Computer networks
    - A system (software, hardware, both, or neither) that enforces an access-control policy between two networks. (Intranet Firewalls; Fuller, Pagen; 1997)
    - At the perimeter of the network it enforces a security policy
- What is it good for?
  - Stop attacks coming from other networks
  - Security policy: Only the allowed services can be used
    - Dangerous services
    - Risk of the open Internet access

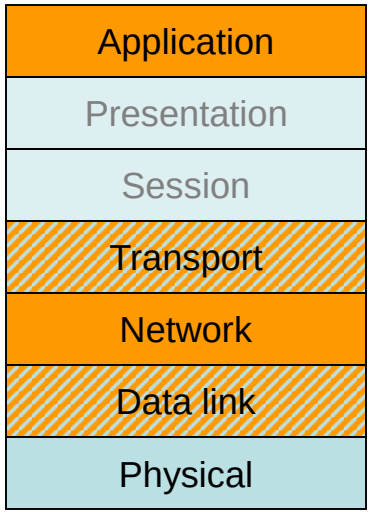
Tűzfal feladatok

- A hálózatok határán!
  - Intranet és Internet – Belső és külső hálózat
  - Lokális hálózat szegmentációja
- Védelem
  - Forgalomfigyelés
  - Kívülről jövő támadások megállítása
    - Hosztok egyéni védelme nem szükséges (mert drága is)
  - A tűzfal elrejti a belső hálózatot
    - Sérülékenységek elrejtése
    - Topológia elrejtése

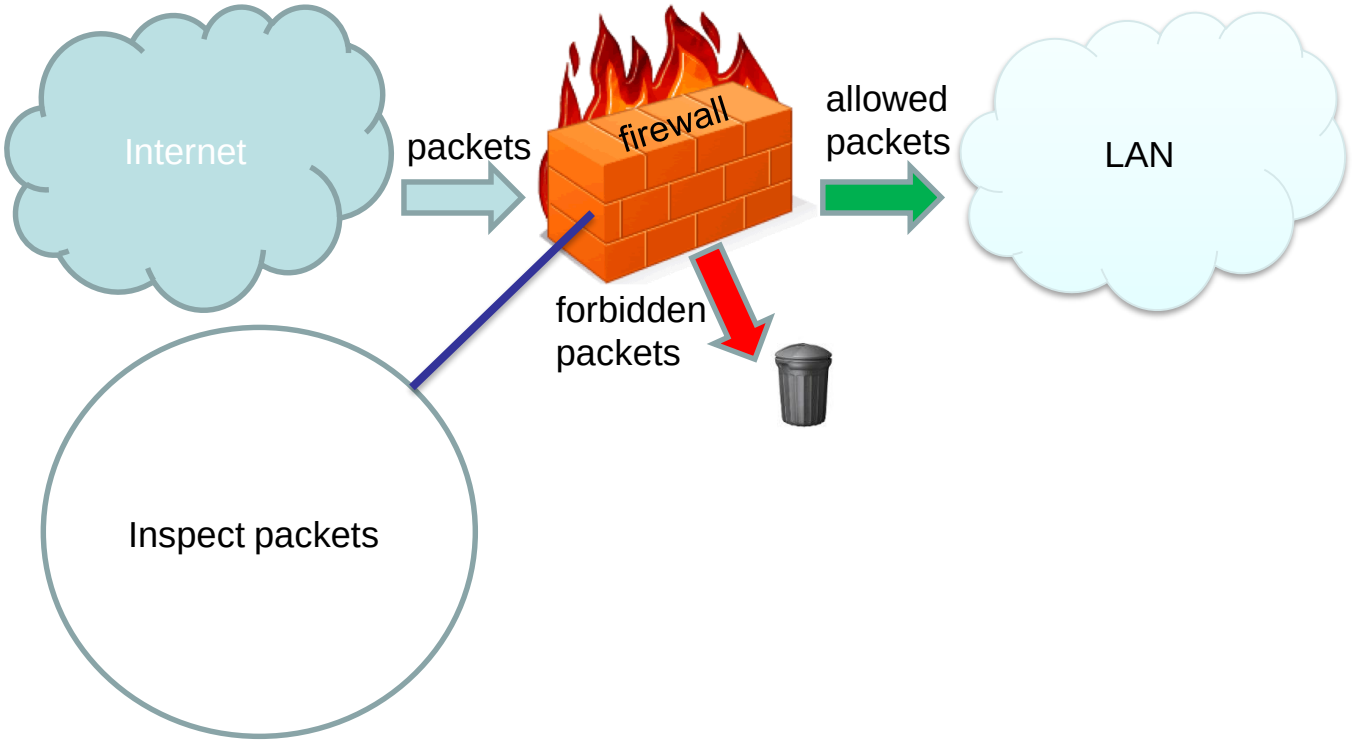
Tűzfal típusok

- Alkalmazás réteg
  - Application gateway
  - Proxy firewall

- Hálózati réteg (IP)
  - *Packet Filter*
  - *Screening Router*
    - Stateless – Állapot nélküli
    - Stateful - Állapottároló



Packet filters



Packet filters

- Available information in a router
  - Source and destination port of the router
- Inspected header fields
  - IP addresses: source and destination
  - Protocol type (IPv4, ICMP, IP/TCP, IP/UDP)
  - TCP, UDP source and destination port
    - Identify services. Example: port 80 -> web service
  - TCP flags
    - SYN, ACK bit (TCP connection initiation, packet acknowledgement)
      - Theoretically easy to decide, whether a packet is a new connection or already part of an ongoing session, as SYN and SYN-ACK is for a specific direction.
  - Size of the packet
  - Fragmentation
    - The correct assembly of the fragments can be a problem

Packet filtering control

- ACL - Access Control List
  - Block by default (whitelist)
    - If there is no rule for a packet then block it
    - Allowed services are listed

or

  - Allow by default (blacklist)
    - If there is no rule for a packet then allow it
    - Blocked services are listed

The action after the packet filter

- Possible actions
  - ACCEPT - Send packet to the destination
  - BLOCK - Drop packet without notification
  - Drop packet with notification
    (ICMP): host/network <administratively> unreachable
  - Log the packet
  - Generating alert
  - Modify packet
  - Send packet to an other destination
  - Modify the filtering rules

Packet filter configuration

- Configuration example

Source IP	Source port	Dest. IP	Dest. port	Action
Any	Any	Web server	80 (Web)	Accept
Outside	Any	Inside	139 (Netbios)	Block
Outside	Any	Inside	110 (POP3)	Block

Dynamic packet filtering

- Inspecting whole sessions
  - TCP connection tracking
  - Necessary for UDP traffic
    - There are no connections here
- Advantages
  - More advanced filtering
  - Handling UDP traffic
- Disadvantages
  - More load on the firewall
  - DoS against firewall states
  - Sometimes it is unnecessary to store states

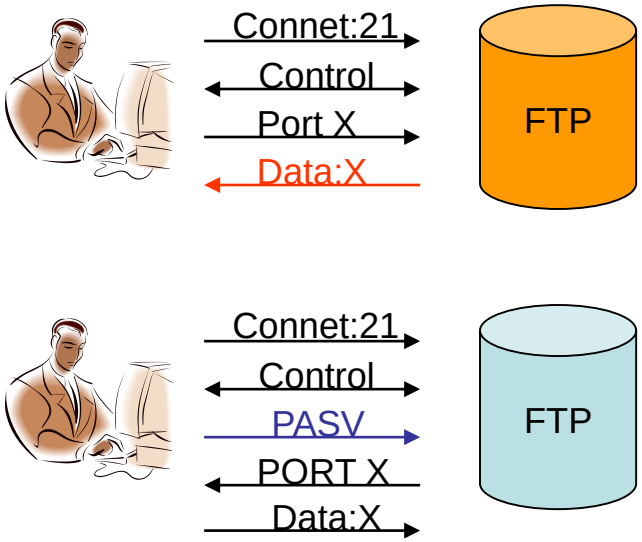
Packet filtering firewalls

- Benefits of packet filtering firewalls?
  - A single packet filter can protect the whole network
  - Inspecting headers does not require extra load:
    Fast even in the case of high traffic volume
  - Lots of products, cheap to expensive

- Problems with packet filtering
  - Defining rules is not easy after a certain complexity
    - Conflicts between the rules
  - No filtering support for users and applications
  - Hiding services: anything over HTTP
  - Problematic application
    - Opening separate connections from outside: FTP, VoIP, …
    - Using non defined ports

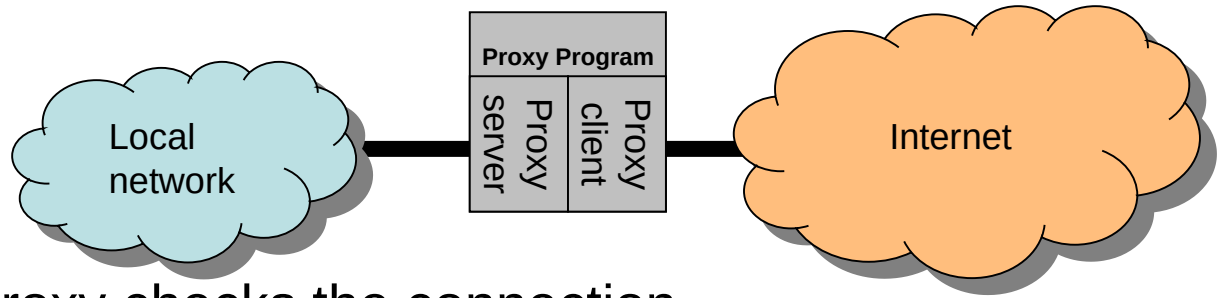
Problematic service: FTP

- File Transfer Protocol (FTP)
  - Command channel (TCP 21)
  - Data channel (TCP 20)
  - Active mode:
    - PORT command
    - Tells where to send the data
    - The server initiates the data connection
  - Passive mode:
    - PASV command
    - The server creates a port and it is the one who sends the PORT command
    - The client initiates the data connection
- The firewall can monitor FTP connections
  - More than inspecting IP headers
  - Allow connection open based on the PORT command



Application firewall

- There is no direct connection between client and server



- The proxy checks the connection
  - Knows the protocol
- Other traffic is blocked
  - Ca not be avoided

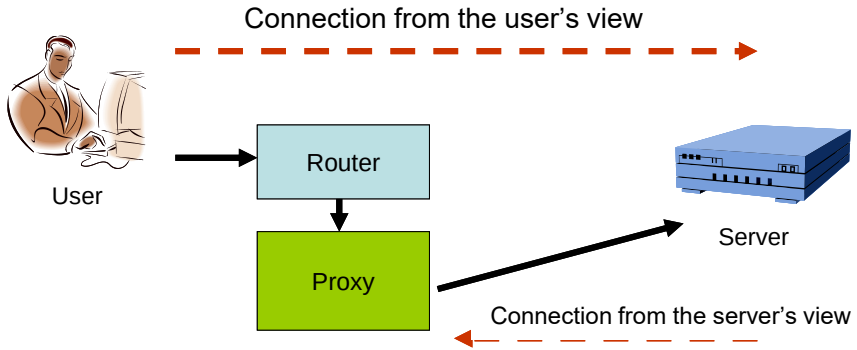
Proxy function

- Client and server in one hand
  - Classical Proxy (Pl. HTTP, FTP)
    - The goal is to speed up the browsing
  - Firewall Proxy
    - Access control

- Connection setup
  1. The proxy receives the connection
  2. Connects to the desired server
  3. Investigate the traffic while forwarding the protocol

Transparent proxy

- Traditional proxy
  - Disadvantage that clients have to be configured manually
- Transparent proxy
  - Hacking source/destination address at the firewall



Application proxy attributes

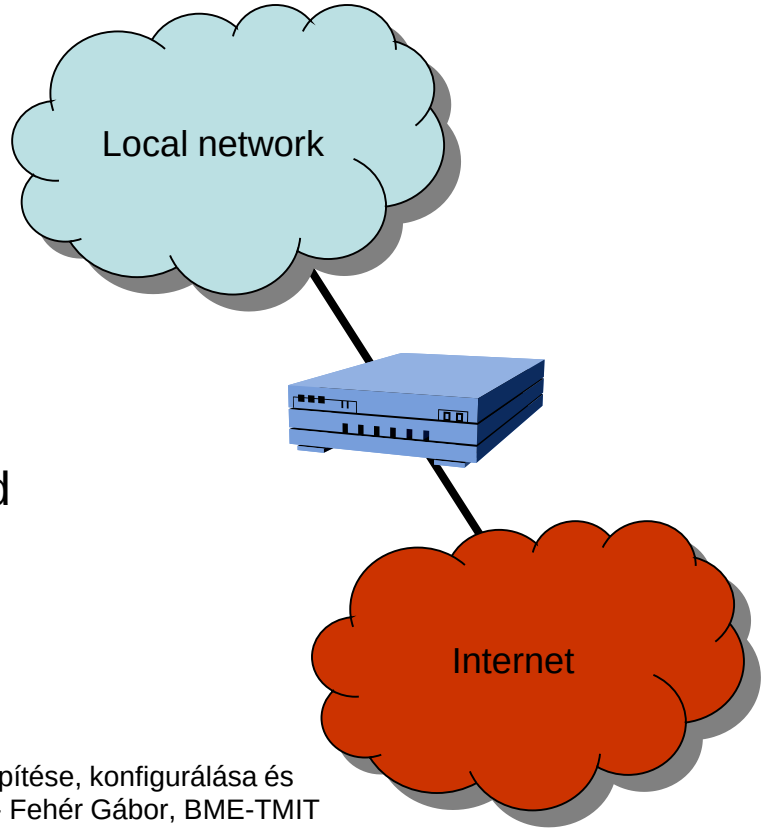
- Why it is good?
  - Looks inside the traffic
    - More powerful filtering (intelligent)
    - Content filtering
    - Powerful logging
  - User and application filtering is possible
  - Additional device between client and server
    - Fix broken protocol implementations

Application proxy attributes 2.

- Disadvantages
  - Continuous development
    - Changing protocols
    - New releases – even non public?
    - New attacks
  - Each service is a separate proxy
  - Performance problems
    - Server and client in one piece
    - Looks inside the packet payload
    - Two connections instead of one
  - Handling secret communication?
    - HTTPS

Firewall architectures 1.

- Screening Router architecture
  - Signe packet filter between Internet and local network

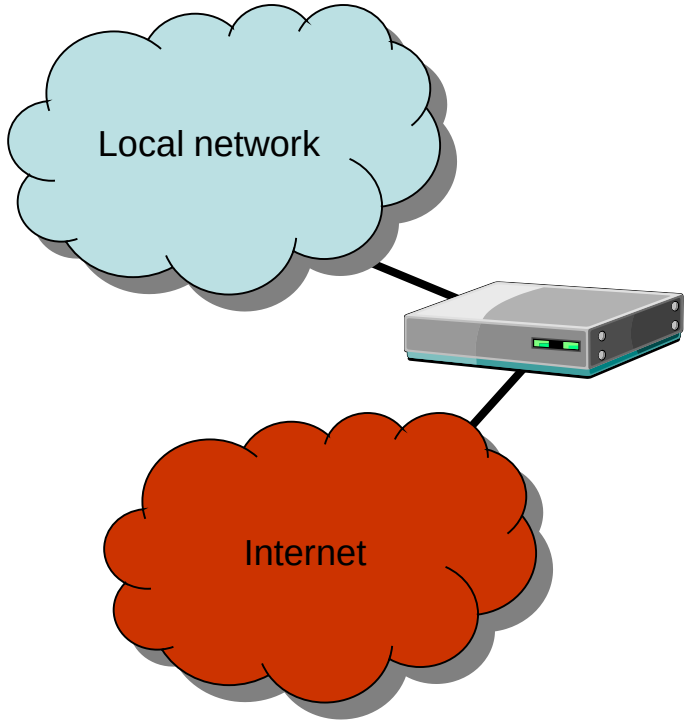


Using screening router

- Where to deploy?
  - String host security in the network
  - Small number of simple services
  - Performance counts
- Advantages
  - Simple
- Disadvantages
  - Same as the disadvantages of packet filters
    - Network can be discovered, complex configuration, application problems, …
  - If the packet filter is down the there is no more security

Firewall architectures 2.

- Dual-Homed Host architecture
  - Separate interface for the local network and the Internet. No traffic forwarding!
  - Application gateway or login to the dual-homed host
- Often there are two different protocols on the ports of the dual-homed host
  - Example: NetBEUI (not exists today) and IP
- Internet packet in the local network: surely a security problem

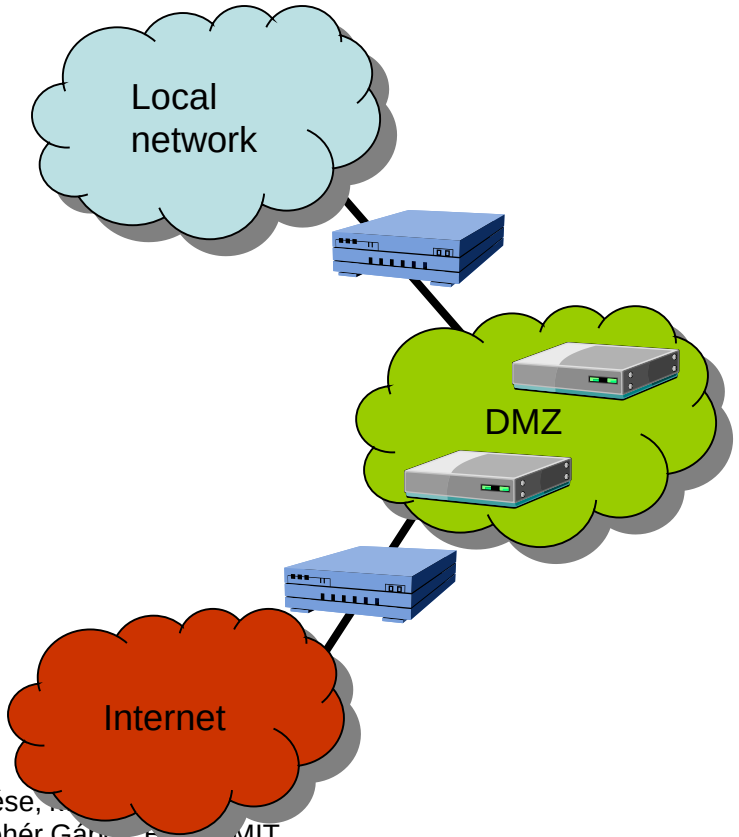


Use of Dual-homed host

- Where to deploy?
  - Small amount of Internet traffic (due to the performance)
  - The traffic is not so critical in business view (for the case when the firewall is hacked)
  - No service for the Internet
- Advantages
  - Internet only sees the firewall, no more
- Disadvantages
  - Disadvantages of application firewalls
  - Not really comfortable without the proxy (but X windows)
  - If the firewall is down the there is no more security

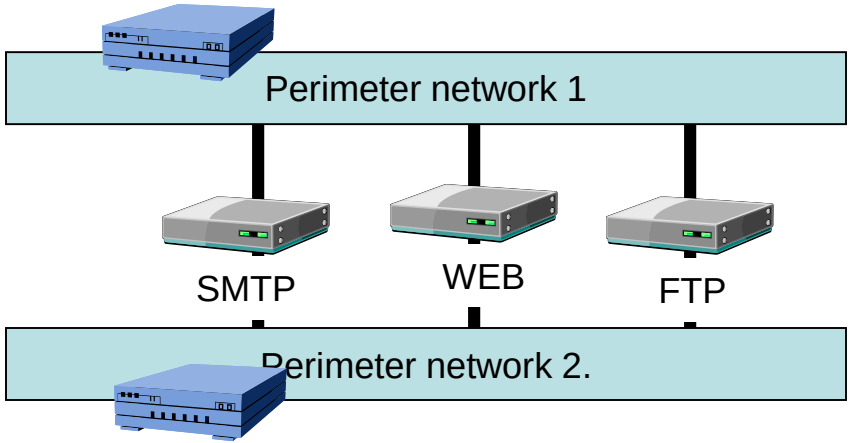
Firewall architectures 3.

- Screened Subnet architecture
  - Separate network with an inside and outside packet filter (DMZ)
  - Using application proxy within the DMZ
  - The packet filter protects the local network if DMZ would be hacked
  - Separating users and services



DMZ

- Demilitarized zone
  - Place for the servers
    - Servers are separated
    - DNS: Hiding names in the local network
  - There can be multiple DMZs



Use of screened subnet

- Where to deploy?
  - Everywhere ☺
  - Services for Internet users as well
    - Web and ftp server of the company in the DMZ
- Advantages
  - Very powerful
  - Separate service, separate zone
- Disadvantages
  - Usual firewall disadvantages

Firewall protection

- Protects against attacks, coming from outside using a know or unknown exploit

- No protection against worms or Trojans
  - We use other protections for them
- No protection against DoS
  - Moreover, firewalls are frequent victims

Firewall attacks

- Attacks from outside
  - IP source routing
    - Protection: disable source routing
  - ICMP Redirect, redirect the routing
    - Protection: ICMP traffic monitoring
  - Software errors in firewalls, OSs
    - Protection: frequent update, purchase a better product

Firewall tendencies

- More advanced packet filers (looks inside more and more)
  - Virus filtering
  - Content filtering
- More application proxies
  - Identifying the user
- Personal firewalls
  - Filtering between the local network and the host
- Managed firewalls
  - The security service provider manages the firewall
- Handling secure connections
  - The firewall terminates the secure connection and initiates a new one
  - User trusts the firewall

Intrusion detection

Intrusion detection and prevention

- Intrusion
  - Sequence of events that leads to a malicious operation
- Intrusion Detection System - IDS
  - Facilities and methods that helps to identify and report unacceptable activities
  - Passive
- Intrusion Prevention System - IPS
  - IDS + action to prevent damages
  - Reactive

IDS types

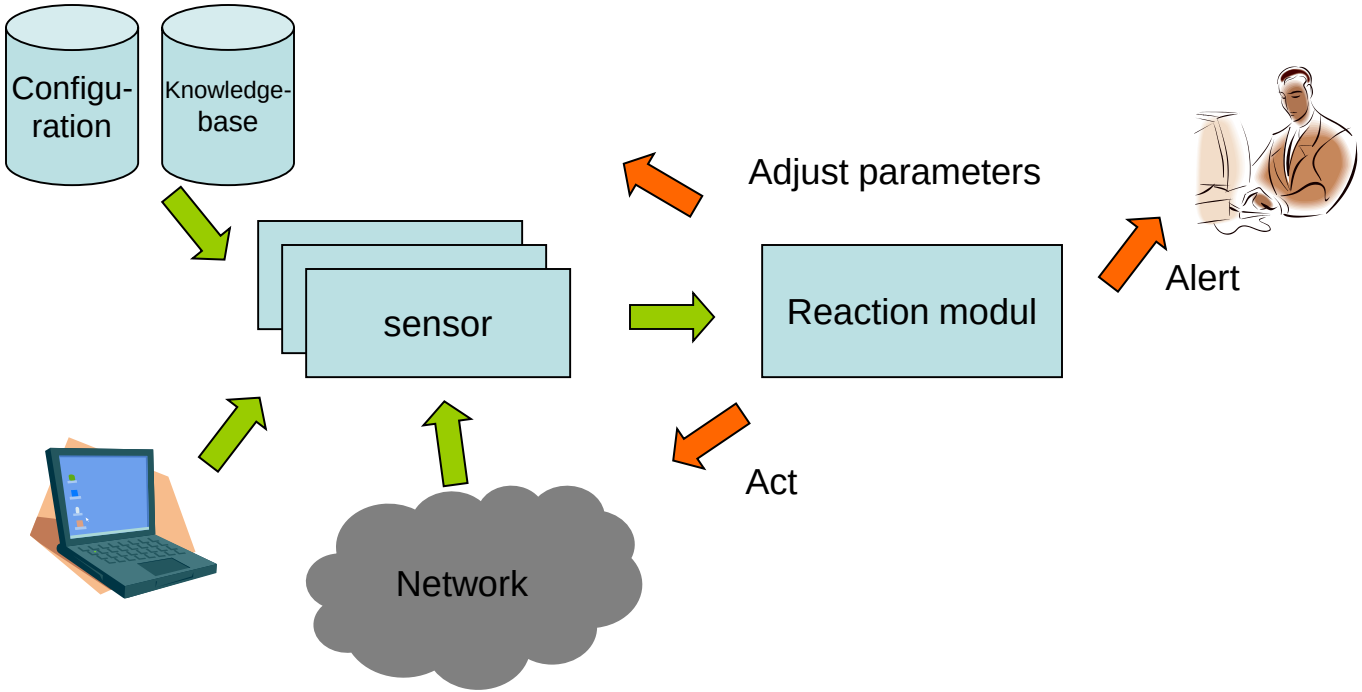
- Network IDS (NIDS)
  - IDS in the network
  - Detecting attacks by monitoring the network traffic
    - Headers of the packets
    - Content of the packets
  - Protecting many resources at once
    - Resources connected to the network
- Host IDS (HIDS)
  - IDS on the host machine
  - Analyses log information produced by the host
    - Multihost IDS: Log from many host
  - Protects the host(s)

IDS types (cont.)

- File system IDS
  - IDS on the host machine
  - File and registry entry integrity
    - Using hash codes
  - Protects the host

- None of a single IDS type substitute the others
  - Hybrid IDS
    - Together IDSs are stronger

IDS architecture



Intrusion analysis

- Analysis phases
  - Preprocessing – Processing the information gathered from sensors
  - Analysis – Compare results to the knowledge base. Recognizing an attack or drop the information
  - Response – Alert or modification
  - Fine tuning – Adjusting the system based on previous intrusion alerts

Rule based detection

- Storing a rule set
  - Fitting rules to the information from sensors
  - Rules are maintained and continuously upgraded based on experiences (E.g.: CERT)
  - The rule set are periodically refreshed in IDSs
    - There are general rules that are need not be refreshed

- Two categories
  - Signature based detection: Signatures of known attacks
  - Specification based detection: Definition of the good behavior

Anomaly detection

- Intrusion means abnormal behavior
- Using statistical metrics to describe the behavior
  - Users, groups, files, resources, …
  - Profiles:
    - Information from past activities
    - Explicit values
  - Using a model (E.g.: Markov model)
- Examples for the abnormal behavior
  - Use resource out of the working time
  - Abnormal frequency of file access
  - Downloading extreme amount of data

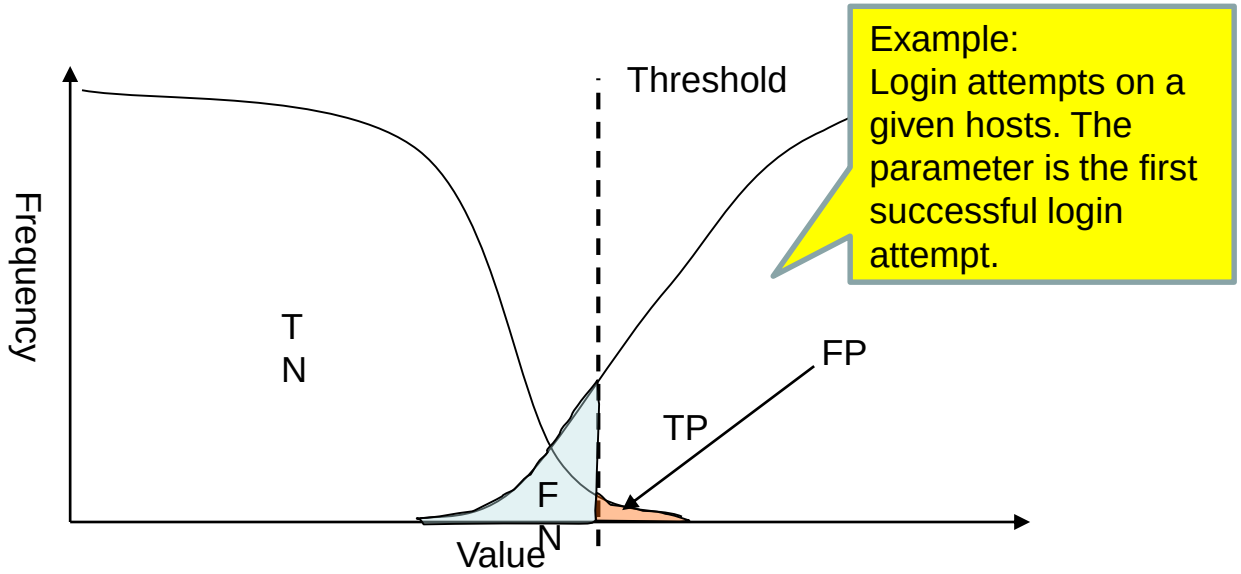
IDS performance

- Attack and alert
  - Real attack and alert: true positive
  - No attack and no alert: true negative
  - Real attack, but no alert: false negative
  - No atatck, but alert: false positive

- Danger of false positives
  - Causing additional workload for the administrator
  - Flooding the network or other resources
    - No resource for the real attack
  - Decoy a real attack

IDS performance (cont.)

- For a given analyzed parameter
  - Attack or not: based on a threshold



Real time and batch operation

- Batch operation
  - Run periodically (no real time working)
  - It can be too late
- Real time operation
  - Run always, sense the attack in real time
  - Performance problems might arise
    - Adaptive operation: Monitoring only a few event and if they are suspicious then extend the monitoring to other fields
- Both operation mode can be useful
  - Certain attacks can be recognized in real-time other in bach operation mode

NIDS sensors

- Sensors
  - Listening on the network capturing all the packets: promiscuous mode
  - Placing is important
    - Where can we see all the packets?
      - Switched network
      - SPAN port
    - First device after the router or firewall
    - Between two subnets (gateway)
  - Performance problem: heavy load

NIDS detection work

- The information is inside the packet
- Attacks that can be detected
  - Protocol errors
    - Examples: Ping of Death, SYN Flood
  - Implementation errors (bug)
    - Examples: Sendmail bug, CGI bugs, Buffer overflows
  - Confidential information stealing
    - Examples: „confidential” word, credit card number
  - Attacks in longer period
    - Example: Port scanning
    - However slow port scanning remains hidden!

NIDS attack blocking

- Reaction
  - Combined with a firewall
    - If the attack is detected then stop that connection
  - Possible attack back
    - Not legal!
    - What about false alarms?
  - Problem with spoofed IP addresses

NIDS limits

- NIDS can not capture all the packets
  - Less accuracy
  - Surviving attacks
- Secret connections
  - No confidentiality after the VPN gateway
  - Secure connection can be checked by Host IDS only

NIDS limits (cont.)

- Different IP stack implementations
  - IDS can not know if the host accepts the packet or not
    - Fragments, bad checksum, fake SYN packets
- DoS attack against the NIDS
  - Memory depletion

HIDS

- Host based detection - HIDS
  - Run on the protected machine
  - Protects the system integrity
    - Creates hash values
    - System files, registry protection
  - Log analysis
    - Make deductions from log files
    - More and more important to protect application than OS
    - Check firewall logs (Firewall + HIDS)
  - Usually HIDS only listens, however it can also block attacks. Example: deny file access