Lesson 5: Network perimeter security

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

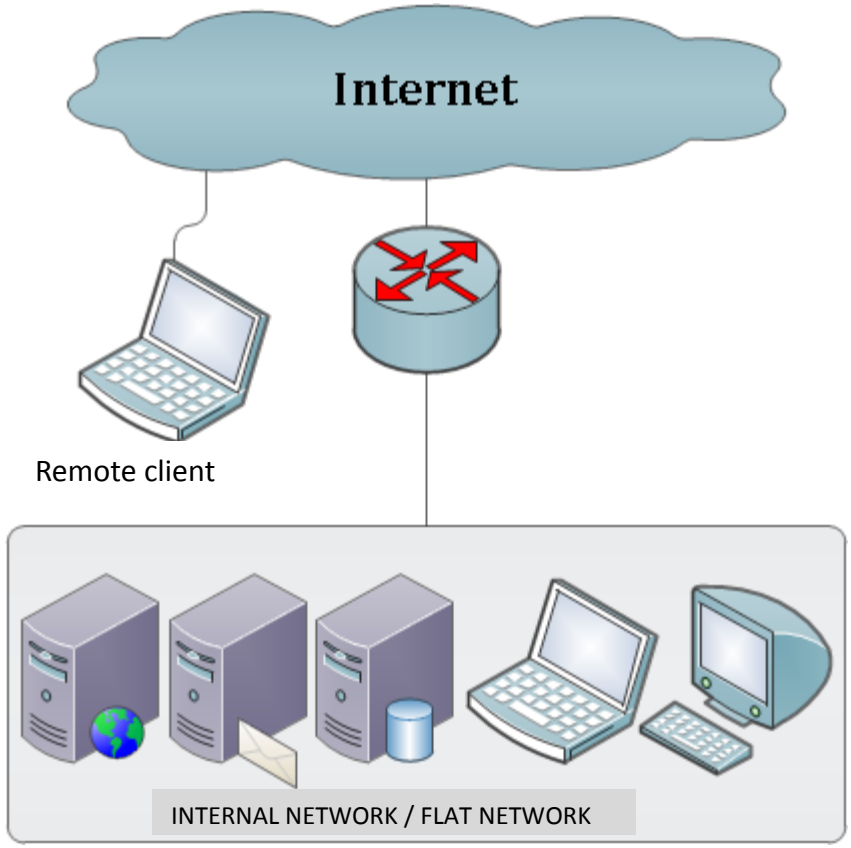
Alejandro Ramos Fraile
aramosf@sia.es
Tiger Team Manager (SIA company)
Security Consulting (CISSP, CISA)

Perimeter Security

- The architecture and elements that provide security to the perimeter of an internal network from other networks like the Internet:
  - Firewalls
  - Intrusion Detection and Prevention Systems
  - Antivirus and anti-spam gateways
  - Honeypots

Example of a network architecture without perimeter security

- Flat network without segmentation
- Internal services publishing: data base
- No monitoring elements
- No inbound or outbound traffic filtering
- No malware or spam e-mail verification
- The remote client has direct access to the services



Firewalls

- Network elements that define access policies to allow or deny traffic based on certain rules
- Two philosophies of use:
  - √ **Restrictive policy** (white list): denies all traffic except that which is specifically accepted
  - x **Permissive policy** (black list): accepts all traffic except that which is specifically denied

Types of Firewalls

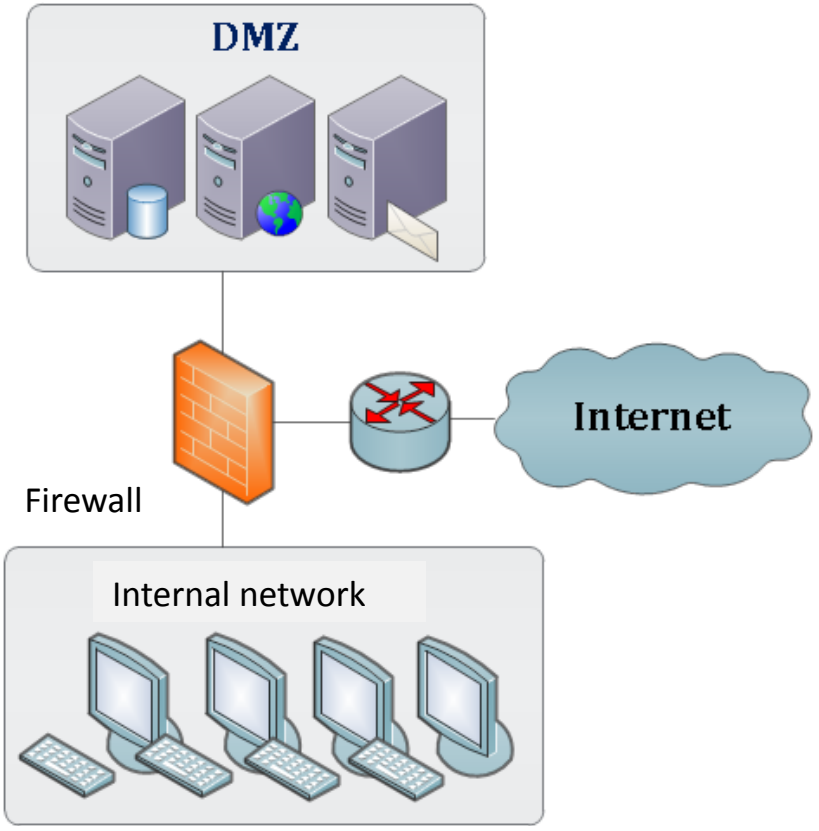
- Circuit level gateways
  - Work for specific applications
- Network layer firewalls
  - Filter on the network layer (source/destination IP) or the transport layer (source/destination port)
- Application layer firewalls
  - Filter based on the required protocol, like HTTP or SQL
- Personal firewalls
  - Software for personal devices such as PCs or mobile phones

Example of Firewall Rules

Rule	Action	Source IP	Destination IP	Protocol	Source Port	Destination Port
1	Accept	172.16.0.0/16	192.168.0.4	TCP	Any	25
2	Accept	Any	192.168.10.8	TCP	Any	80
3	Accept	172.16.0.0/16	192.168.0.2	TCP	Any	80
4	Deny	Any	Any	Any	Any	Any

Demilitarized Zone (DMZ)

- A local network placed between the intranet and an external network (like the Internet)
- Used for public services like DNS, e-mail, Web and ftp that are exposed to security risks
- Created with one or two firewalls that restrict traffic between the three networks
- Connections from the DMZ towards the internal network are not allowed

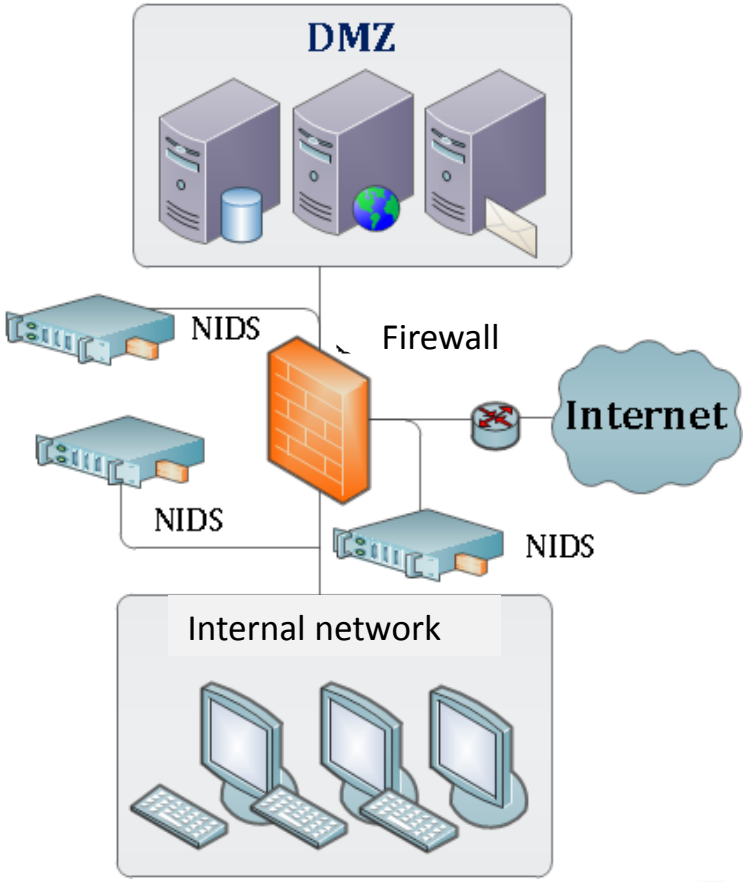


Intrusion Detection and Prevention Systems (IDS/IDPS)

- Devices that monitor and generate alarms when security alerts are triggered
- IDPS (Intrusion Detection and Prevention Systems) block attacks to avoid their effects
- Main functions:

Intrusion Detection and Prevention Systems (IDS/IDPS)

- Two types of IDS:
  - **HIDS**: Host IDS, monitor changes in the operating system and software
  - **NIDS**: Network IDS, monitor network traffic
- Two detection methods:
  - Signatures
  - Behaviour patterns



Example of an IDS signature: snort

alert tcp

$EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS

(**msg**:"WEB-IIS ISAPI .printer access";

flow:to_server,established;

uricontent:".printer"; nocase;

reference:arachnids,533; **reference**:bugtraq,2674; **reference**:cve,2001-0241; **reference**:nessus,10661; **classtype**:web-application-activity;

sid:971;

rev:9;)

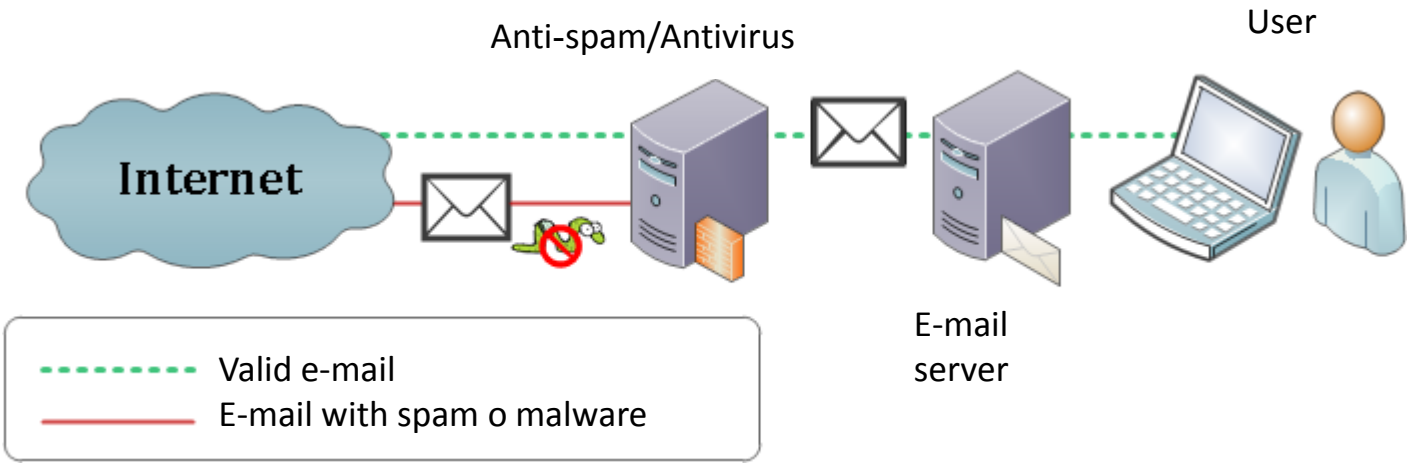
Honeypots

- Systems configured with vulnerabilities so they can receive attacks and be used to study new techniques
- Two main types of honeypots:
  - **Low-interaction**: simulate the operating system and applications
  - **High-interaction**: the operating system isn't simulated

- They are also used to gather examples of virus and spam
- They should be under close control and disconnected from all networks

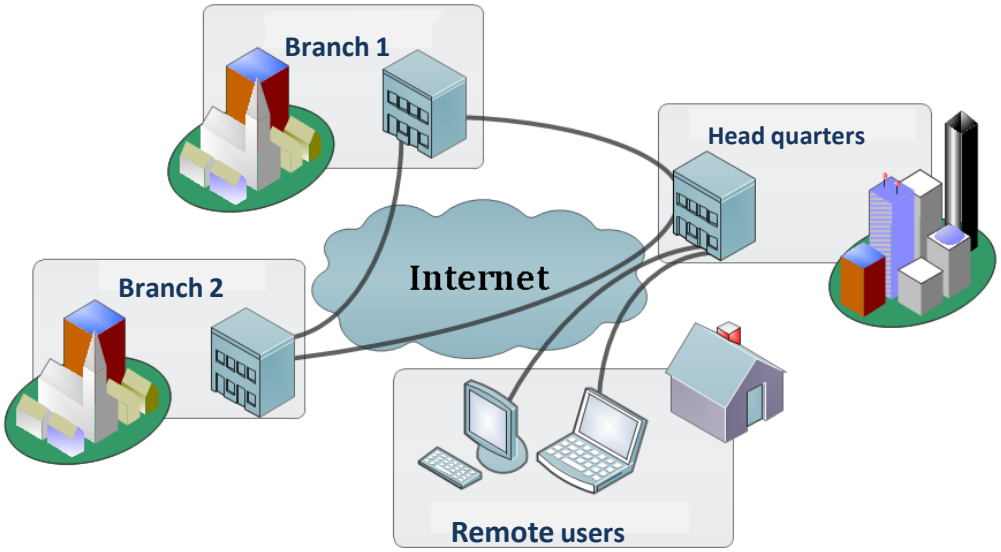
Antivirus and Anti-spam Gateways

- Intermediate services that filter malicious content from the network's input channels
- Malware detection in Web gateways and mail servers



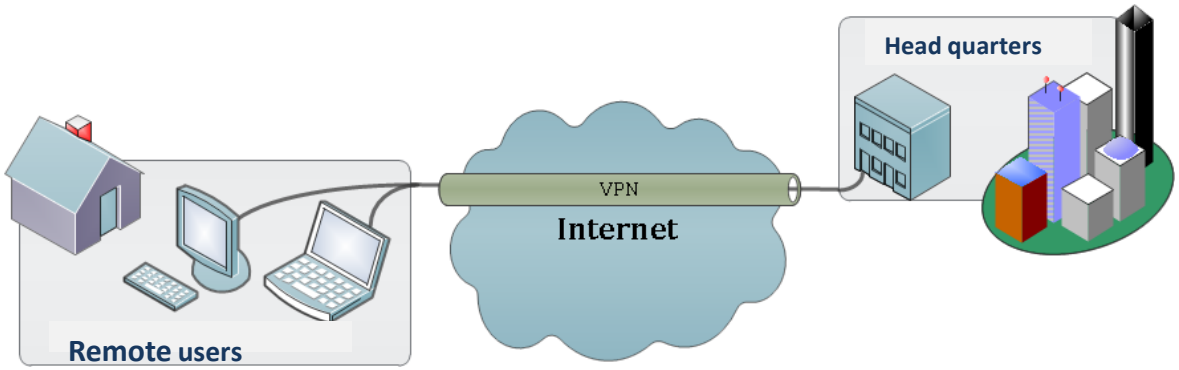
Virtual Private Networks (VPN)

- Networks that use a public infrastructure (non-secure) to access a private network in a reliable way
- Usually used to connect remote users, branches and offices with the internal network (point-to-point)



Virtual Private Networks: Characteristics

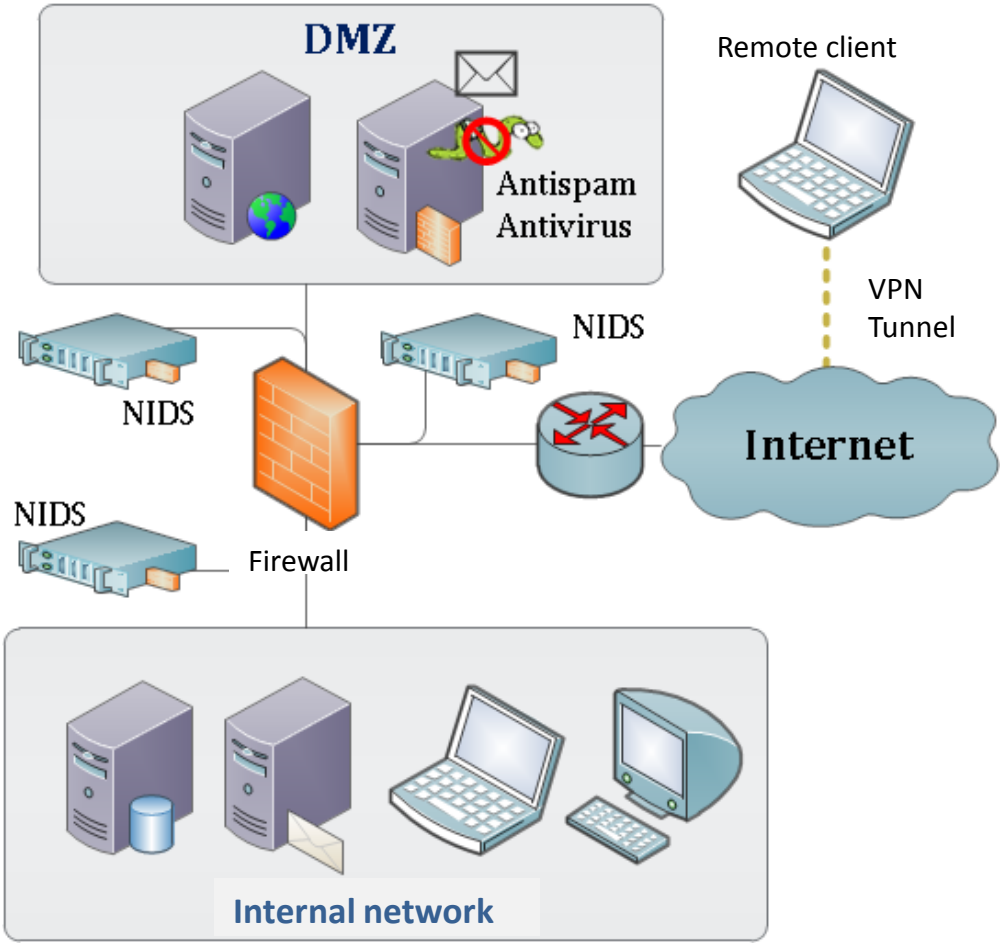
- **Authentication and authorization**: managing users, roles and permissions
- **Integrity**: with the use of *hash functions*
- **Confidentiality**: the information is encrypted with DES, 3DES, AES, etc.
- **Non-repudiation**: the transmitted data is signed



Unified Threat Management (UTM)

- Systems that integrate in one device a set of perimeter security solutions:
  - Firewalls
  - Intrusion Detection and Prevention Systems
  - Antivirus and anti-spam gateways
  - Virtual Private Networks

Example of a network architecture with perimeter security



- ✓ Firewall installed
  - ✓ DMZ and internal network
  - ✓ Restrictive policy
- ✓ Anti-spam and antivirus installed
- ✓ NIDS installed in the three interfaces
- ✓ Segmentation of public services: Web and antivirus/anti-spam gateway
- ✓ Internal services relocated: data base and mail
- ✓ Remote clients use VPN

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contact: info@intypedia.com