Network Firewalls

Josef Pojsl

jp@tns.cz

Trusted Network Solutions, a.s.

April 10, 2008

Agenda

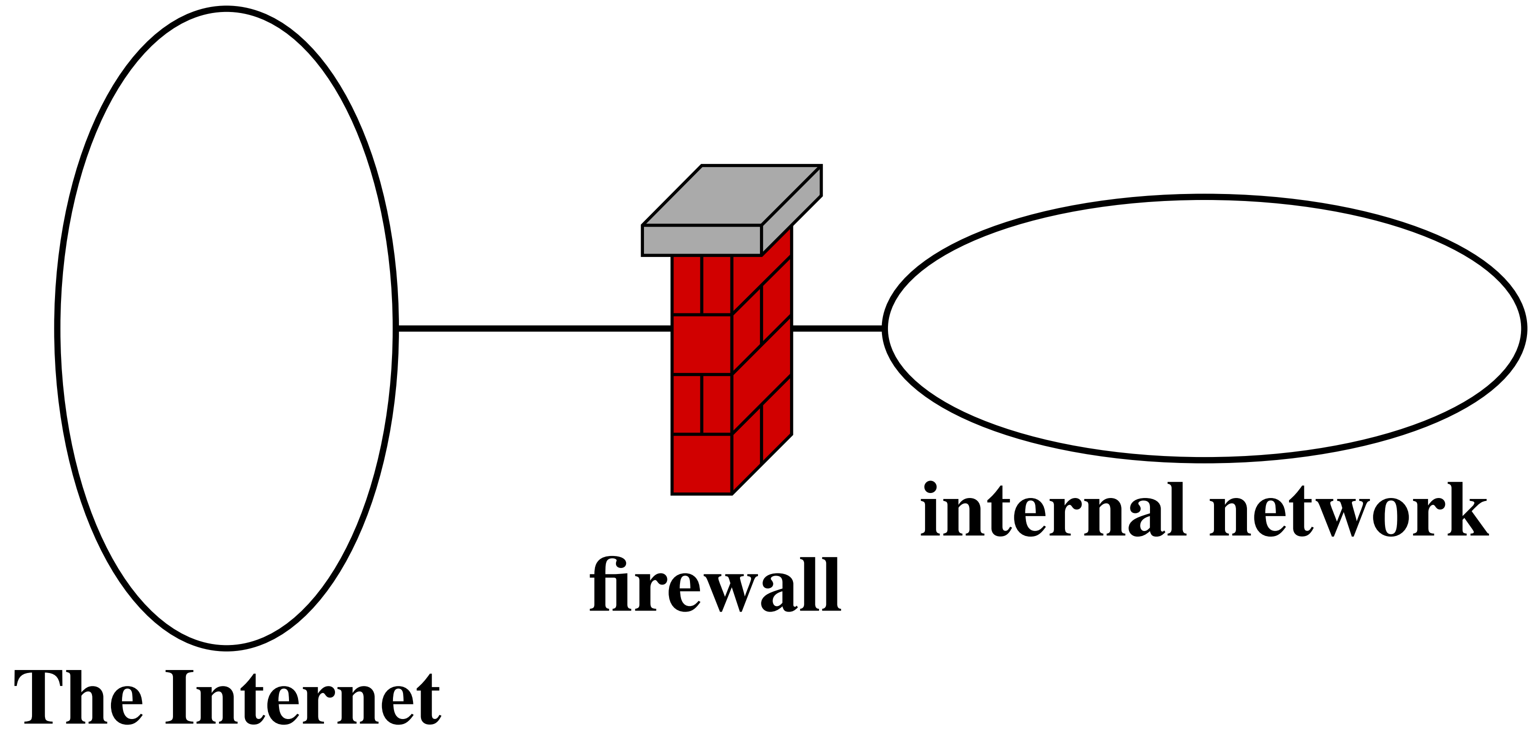
1. The term “firewall”
2. Network topology
3. Firewall technology
4. Integration of additional functions
5. Real threats today
6. The need for *security policy*

The term “Firewall”

- Personal firewalls—installed on desktops
- SOHO (Small-Office, Home-Office) firewalls
- *Large-scale network perimeter firewalls*

Network firewall is a set of measures (hardware, software, personell) whose primary goal is to separate two or more networks with different trust levels and mitigate threats implied by communication between those networks.

Network topology (1)

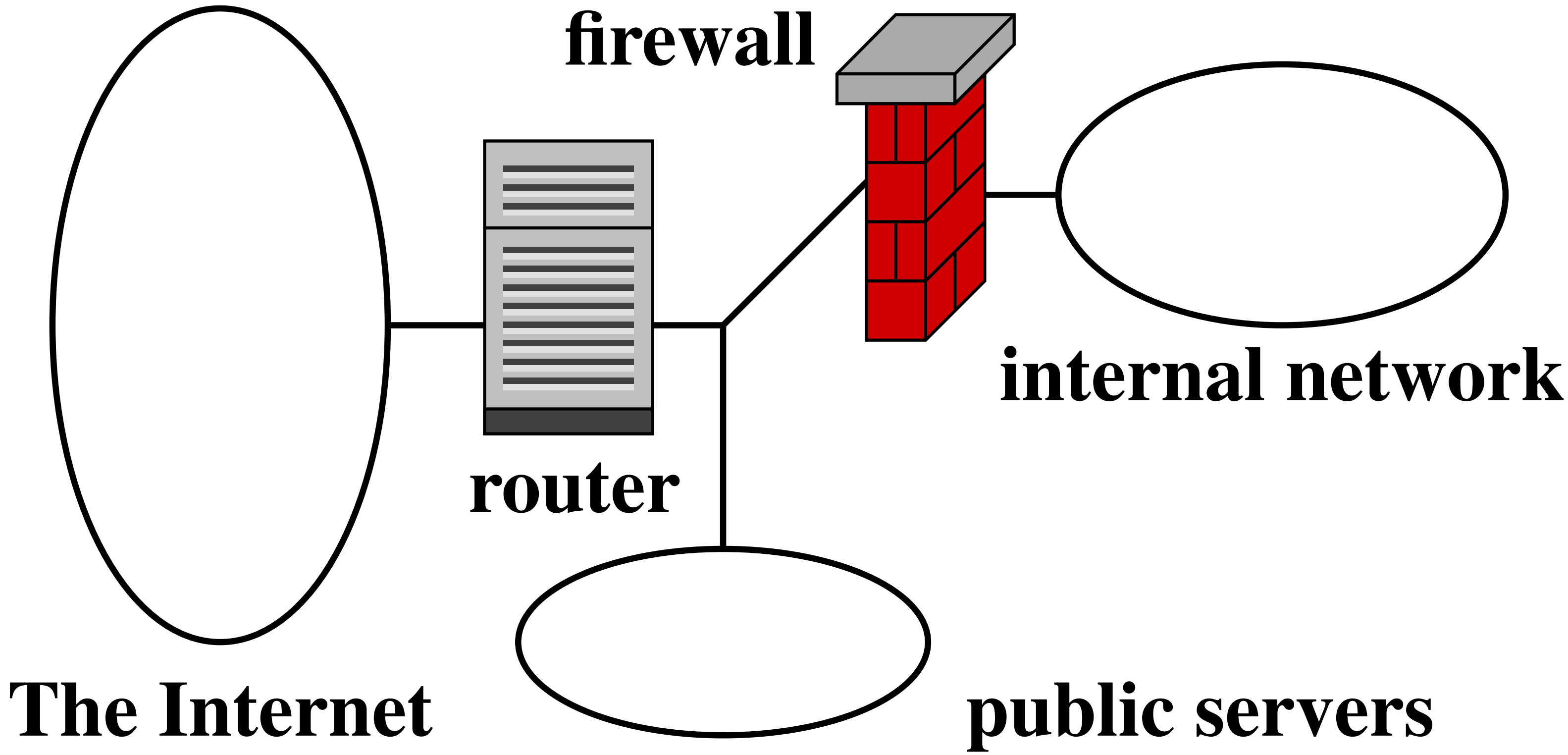


Network topology (1)

- Traditional, simple firewall model
- External and internal networks are separated with firewall
- *Firewall represents the only means of communication between those two networks*
- There could be more than two network zones (several internal networks, zones within an internal network, links to partners,. . .)

One of the most secure strategies: *Connections can only be initiated from a more trusted (e.g. internal) to a less trusted network zone.*

Network topology (2)

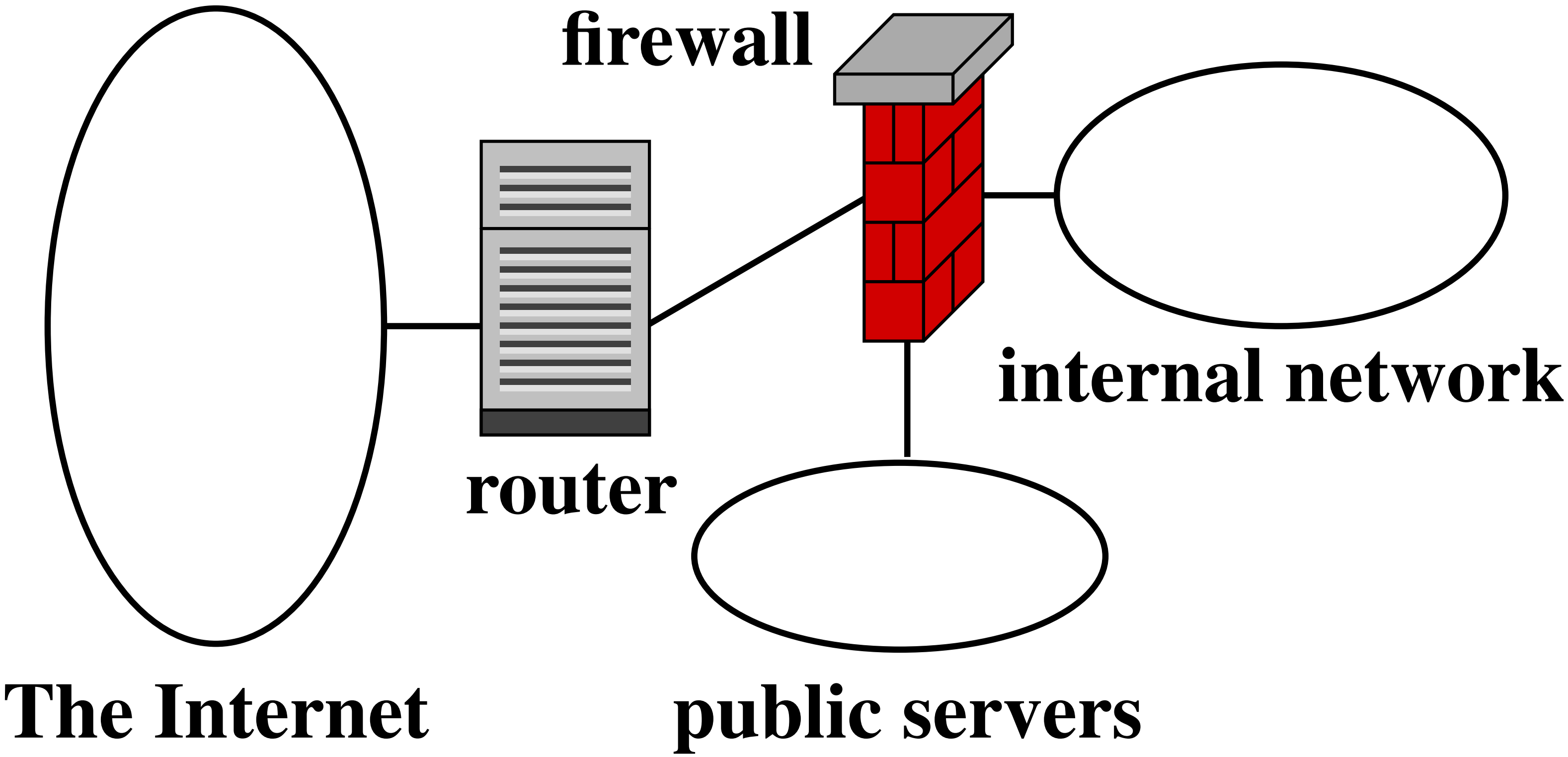


Network topology (2)

- Public servers network aka. Demilitarized Zone (DMZ) introduced
- Router could also work as a firewall (different technology)
- WWW, FTP, Application servers
- DataBase server:
  - Either in the internal network,
  - Or in DMZ (read-only copy of relevant data)

DataBase connections should always be initiated from the internal network to the DMZ (push method).

Network topology (3)

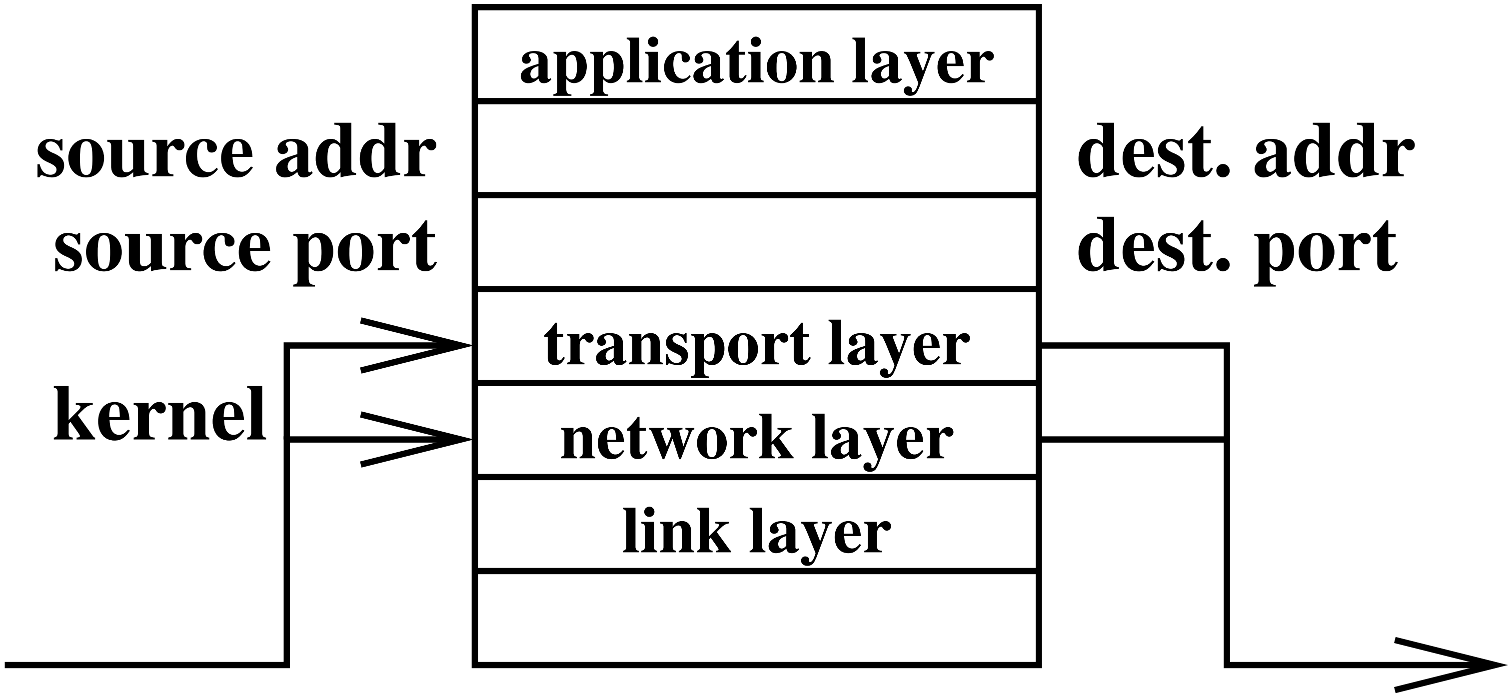


Network topology (3)

- Firewall completely controls the DMZ
- Allows for application specific settings for DMZ
- More complex topologies are possible
- Different number of separate zones of trust

The ultimate topology always depends on the security policy.

Technology – IP filters (1)



Problem of “complex” protocols (FTP)

Technology – IP filters (2)

- Originally gateways with add-on IP filtering
  - Communication permitted by default
  - No application layer control
  - Easy integration of new protocols
- Later specialized filtering gateways
- *Stateful packet filtering* (TCP, UDP, ICMP)
  - A state table (maintained in kernel)
  - Monitor traffic and adapt the state table to it
  - Permit traffic according to rules *and the state table*
  - Limited ability to control application layer

Technology – IP filters (3)

1. Client 192.168.1.10 initiates connection to web server 5.6.7.8. Initial SYN packet coming from 192.168.1.10 port 1234 destined for 5.6.7.8 port 80 arrives at firewall.

2. State table is checked, but no match is found. Then, rule table is checked, a rule permitting the connection is found, and a state is created. That state permits packets from 192.168.1.10:1234 to 5.6.7.8:80 and back from 5.6.7.8:80 to 192.168.1.10:1234. The initial SYN packet is sent to server.

3. Server receives SYN packet and responds with SYN+ACK answer.

Technology – IP filters (4)

4. The SYN+ACK packet going from 5.6.7.8:80 to 192.168.1.10:1234 arrives at firewall. State table is checked, and a match is found. The packet is sent to client.

5. Packets flow in both directions between client and server thanks to state table match.

6. Upon connection termination, firewall deletes the state. No further packets coming from 5.6.7.8:80 to 192.168.1.10:1234 get through.

Technology – IP filters (5)

→ The communication in terms of IP protocol between hosts is intact, but can be blocked.

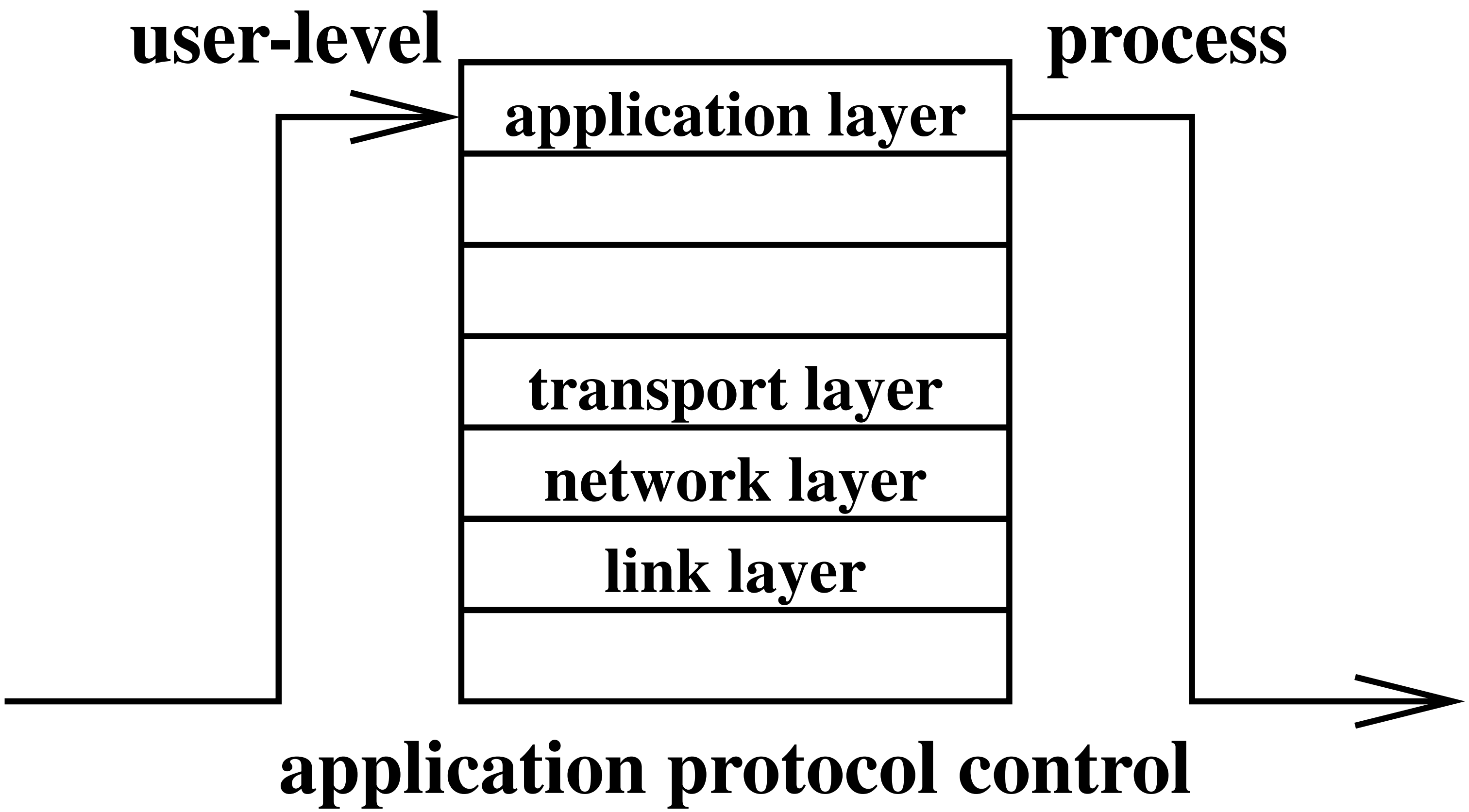
→ No content control, no authentication etc.

→ Typically implemented in OS kernels

Advanced stateful filters:

- Fully control the states of TCP connections and UDP streams
- Properly implement and distinguish TCP/IP diagnostics (ICMP)
- Must adapt to “complex” protocols like FTP, SIP, H.323

Technology – proxies (1)



Technology – proxies (2)

- Originally "bastion hosts" with a single NIC
  - Communication denied by default
  - Application layer control
  - A specific application proxy for each protocol (set)
- Later as gateways
- *Transparent proxy gateways* are designed so that users do not know about their existence

Two separate connections (client$\longleftrightarrow$proxy, proxy$\longleftrightarrow$server)

Technology – proxies (3)

1. Client 192.168.1.10 initiates connection to web server 5.6.7.8. Initial SYN packet coming from 192.168.1.10 port 1234 destined for 5.6.7.8 port 80 arrives at firewall.

2. Firewall transparently grabs that packet even when it is detined for another host. The proxy at port 80 (usually HTTP proxy) receives that connection.

3. Firewall sends back SYN+ACK packet, pretending the source address to be that of the real server 5.6.7.8 and port 80. TCP connection gets established, and the client sends its HTTP request data. No single packet is sent to the real server at 5.6.7.8 yet.

Technology – proxies (4)

4. The HTTP proxy checks the whole request and decides how it should be handled. If it is permitted, firewall establishes a second connection to the server at 5.6.7.8.

5. The HTTP proxy receives the response from server and checks it thoroughly. If it contains malicious data or non-permitted content, the proxy can replace the unwanted content with a policy violation message.

6. The client receives the response from proxy, and the connection is closed.

Technology – proxies (5)

- The communication in terms of IP protocol between original hosts is broken, instead, the proxy communicates with both end hosts
- Allow for content control, authentication etc.
- Typically implemented as user-level processes

Even a simple generic TCP proxy without specific application protocol controls is better than IP filters in terms of security because it isolates TCP/IP stacks of internal hosts.

Technology – comparison

IP filters	Proxies
• Faster	• Slower
• Easier adaptability to new protocols	• Need more work to adapt to new protocols
• Lower level of security	• Higher level of security
• *No* content filtering, *no* injected authentication	• Content filtering, injected authentication

Technology – comparison (2)

Consequence: Proxies are principially more secure than IP filters, at the cost of speed and adaptability.

Most comercial firewalls are primarily based on one of these technologies but combine both.
Firewall vendors often hide their usage of the other "non-marketed" technology.

Challenges

Original firewall model does not address all of network security. . .

Data equivalence problem: At the firewall, we can never be sure how both ends interpret the data we are seeing.

DoS attacks, distributed attacks, social attacks

$\Rightarrow$. . . Many security measures must stay at workstations and especially application servers.

$\Rightarrow$. . . Technical vs. organizational countermeasures

Challenges (2) – Risks

In the last few years, new risks appeared and extended:

- Social attacks
- Executable content
- Automated attack scripts
- Zero day/hour/minute attacks
- Coordinated distributed attacks
- Encapsulation of protocols into HTTP

(Partial) Solution: $\Rightarrow\ldots$ Integration of additional functionality

Attacks – Phishing, etc.

⇒A forged bank site, and a fraudulent e-mail including scrambled link to that site

⇒Trying to trick users into inserting their confidential authentication data into the attacker's system

- A large attack of that kind against Česká spořitelna in March 2007
- Several versions of fraudulent e-mails were received by thousands of users
- The forged web site copy was very authentic
- Accompanied with a Trojan horse, collecting authentication data from users upon typing them on the real web site (Pharming)

Attacks – Coordinated DDoS attack on Estonia

- Ethnical Russian-Estonian conflict accompanied with a large-scale cyber attack against Estonian government, newspaper, bank and ISP sites
- Russian riots in Tallin and cyber attacks against Estonia both came in three waves: Apr 27, May 3, May 9 2007
- Estonia, one of the Europe's most wired countries, was very vulnerable to that kind of attack
- Estonia accused Russia of direct involvment in the attacks, but Russia denied it

Great Firewall of China

- Internally called “The Golden Shield Project”, Chinese government launched probably the biggest firewall in the world in 2003
- Many sites are completely unrechable from the whole of China (e.g. BBC)
- Even encrypted HTTPS traffic is scanned (bank sites' certificates forgery)

http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China

Integration of Additional functionality

- Content filtering
  - Virus/worm/phishing detection
  - Misuse detection/elimination
  - SPAM/pharming detection
- Virtual private networks
- High availability (active/passive, active/active clusters)
- Log processing (Alarms, statistics)

Future trends

- Signature Recognition (Intrusion Detection, Virus Detection)
  - + Well established technology, little to no false positives
  - – Does not prevent against zero day attacks, resource exhaustive
- Intrusion Prevention (Intrusion Detection + automatically blocked traffic)
  - + Instant reaction
  - – False positives cause damage, false sense of security
- Anomaly detection (statistical analysis, expert systems)
  - + Instant reaction
  - – False positives cause damage, time and cost of learning

Security policy

Firewall is only a security tool

It is of no use without:

- Security policy
  - Assets: what to secure
  - Risks: what to secure against
- Proper deployment and configuration
- Quality staff

Security is not a state, it is a process

Security policy (2)

- *Security policy is a balance of the cost of risks against the cost of countermeasures.*
- At best, firewall is as effective as the security policy it implements.

— Some organizations invest in firewalls, hoping that they will ultimately secure their network.

— Information security management system is often underrated.

— Operational costs and training are often undervalued.

Recommended reading

- Schneier, B.: *Secrets and Lies: Digital Security in a Networked World,* John Wiley & Sons, Inc., ISBN 0-471-25311-1, 2000.
- Cheswick, W. R., Bellovin, S. M., Rubin, A. D.: *Firewalls and Internet Security: Repelling the Willy Hacker,* 2nd edition, Adison-Wesley, ISBN 0-201-63466-X, 2003
- Schneier, B.: *Beyond Fear,* Springer Verlag, ISBN 978-0387026206, 2006.
- Crypto-gram newsletter, http://www.schneier.com/crypto-gram.html

Useful links

- *SANS Internet Storm Center* `www.incidents.org`
- *US-CERT Vulnerability Notes DB* `www.kb.cert.org/vuls/`
- *SecurityFocus* `www.securityfocus.com`
- *Common Vulnerabilities and Exposures* `cve.mitre.org`
- *Netcraft* `www.netcraft.com`