Network Firewalls

Josef Pojsl

jp@tns.cz

Trusted Network Solutions, a.s.

April 26, 2006

Agenda

1. The term “firewall”
2. Network topology
3. Firewall technology
4. Integration of additional functions
5. 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.

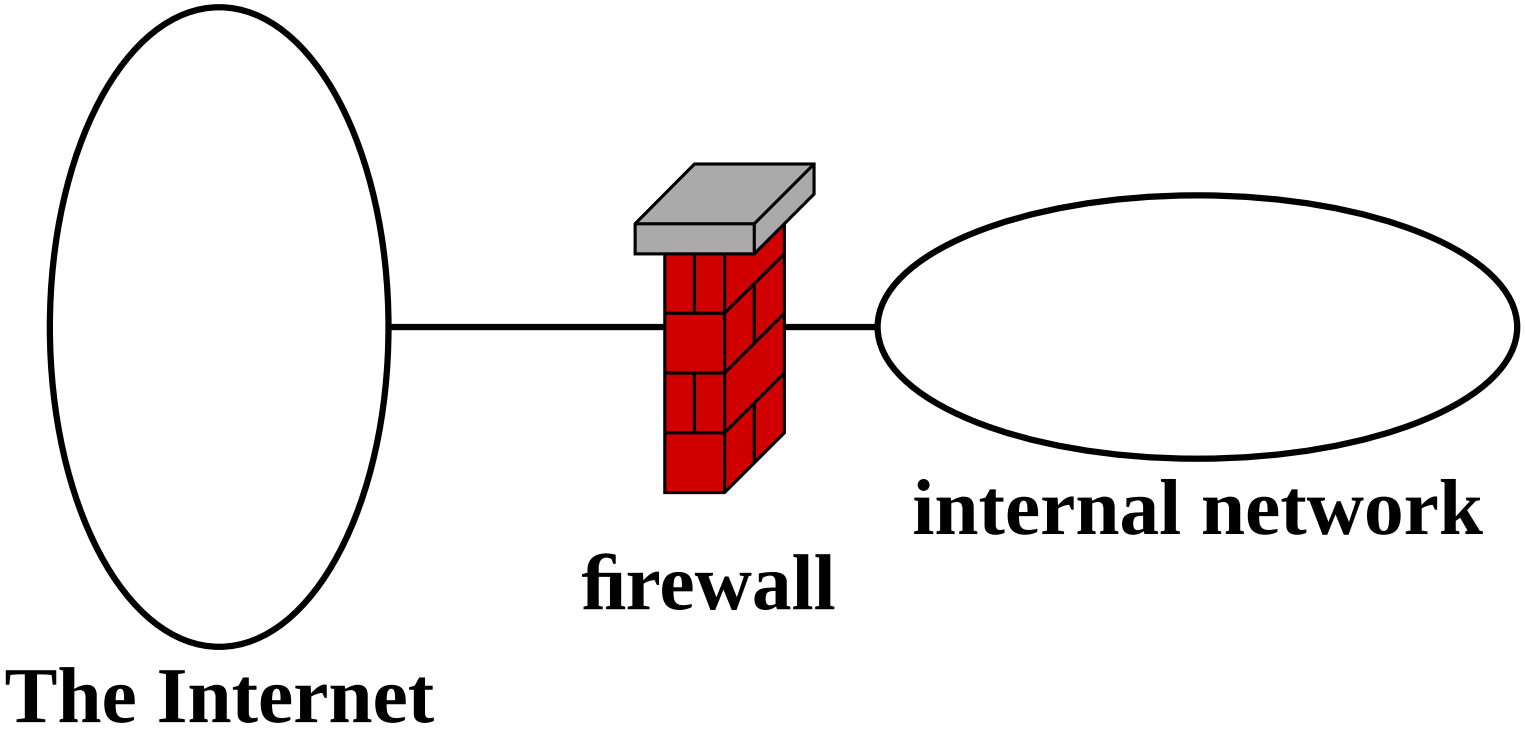
The term “Firewall” (2)

- *Personal firewalls:* secure against insiders’ attacks, supplement network perimeter firewalls, centralized management
- *Firewalls for small networks:* WinRoute & company

A properly working firewall must be formed as a balanced combination of quality hardware, software and staff.

Risks can only be diminished, never completely eliminated.
Firewalls secure against a fixed set of risks (risk patterns).

Network topology (1)

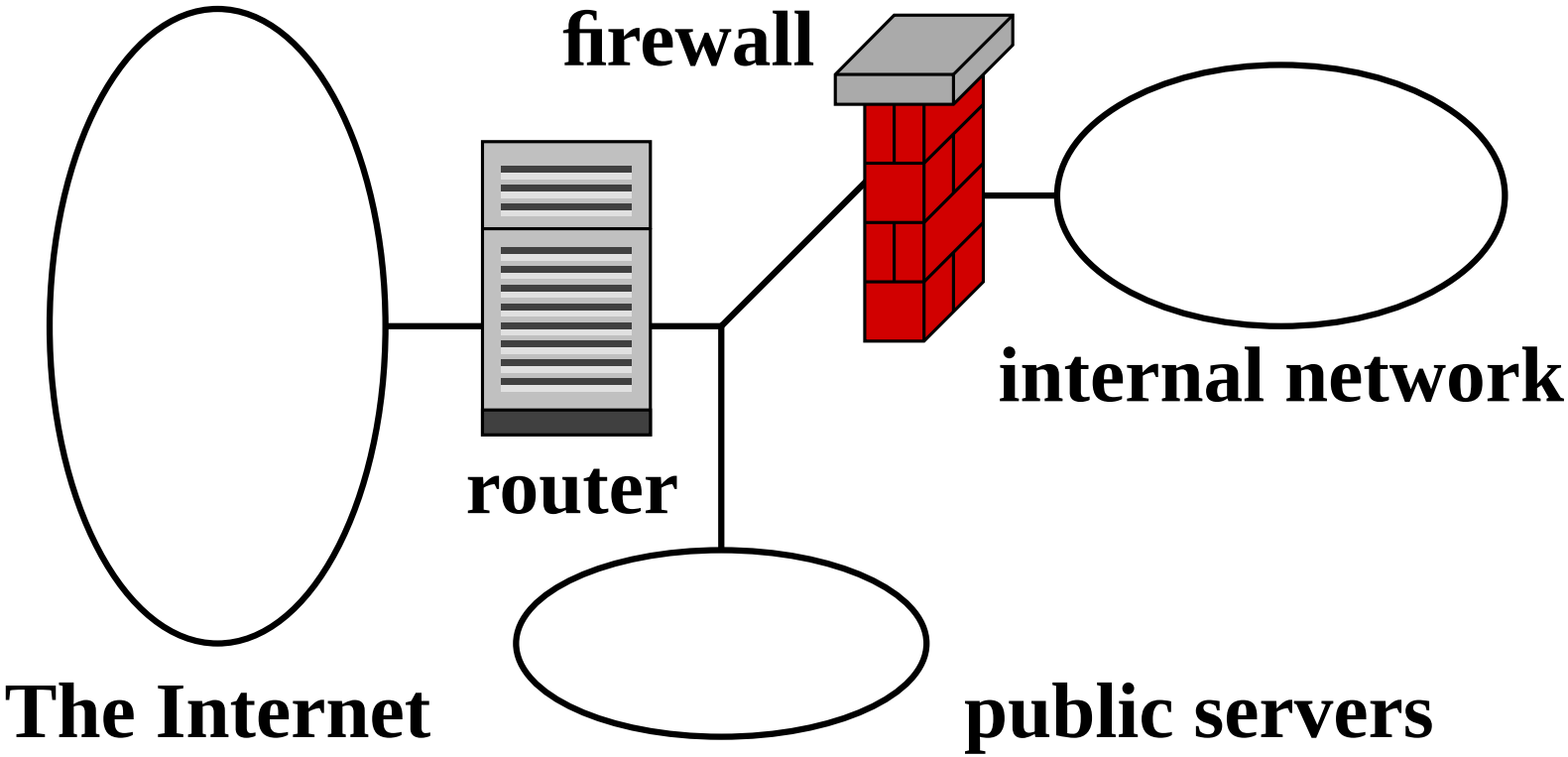


Network topology (1)

- 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)

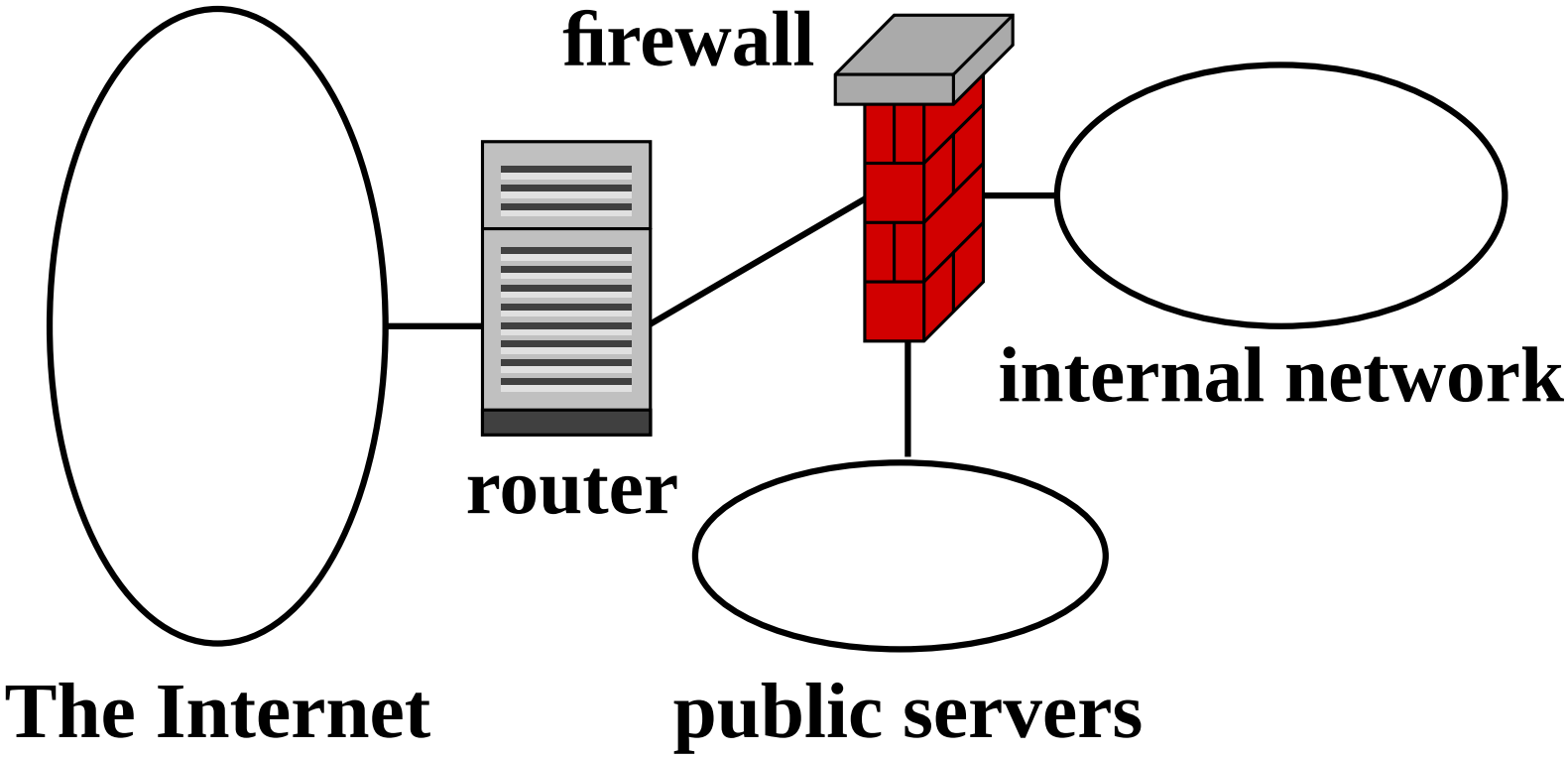


Network topology (2)

- 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)

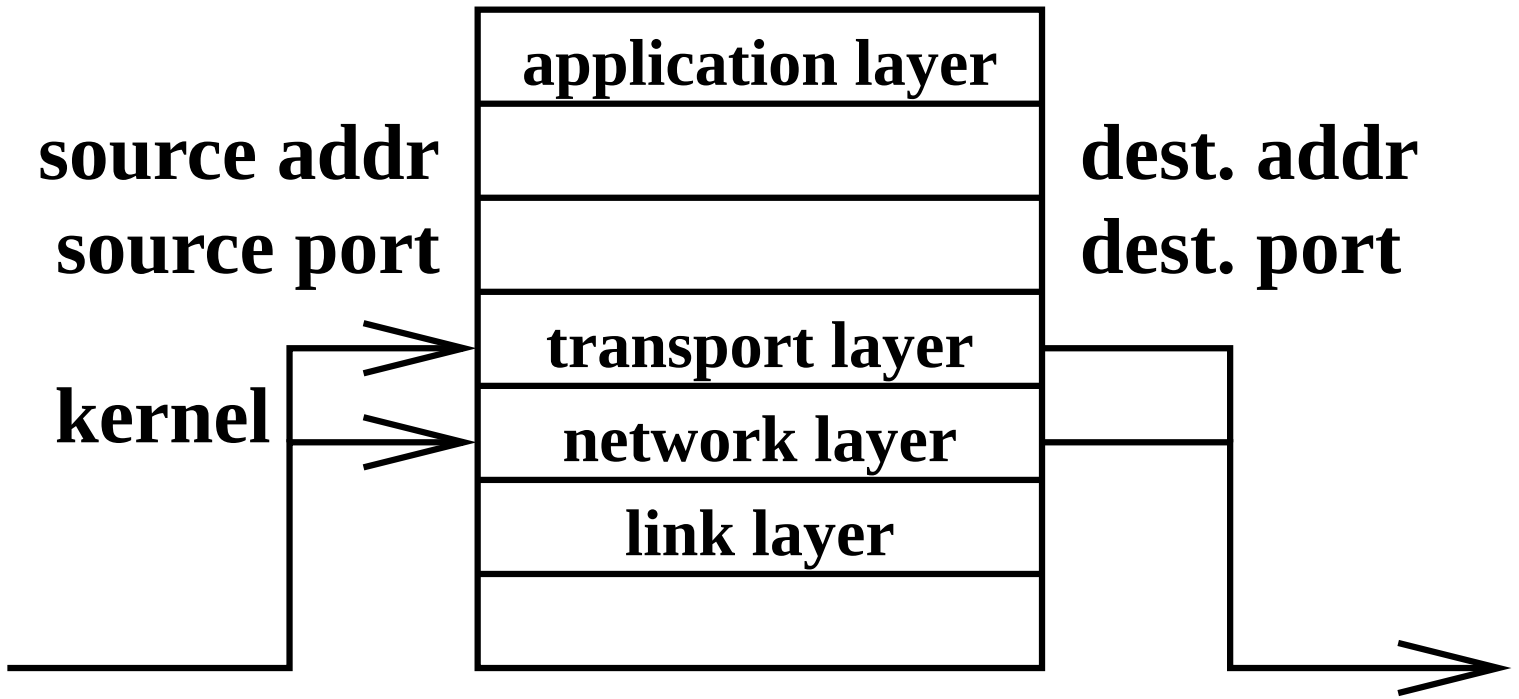


Network topology (3)

- 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)

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

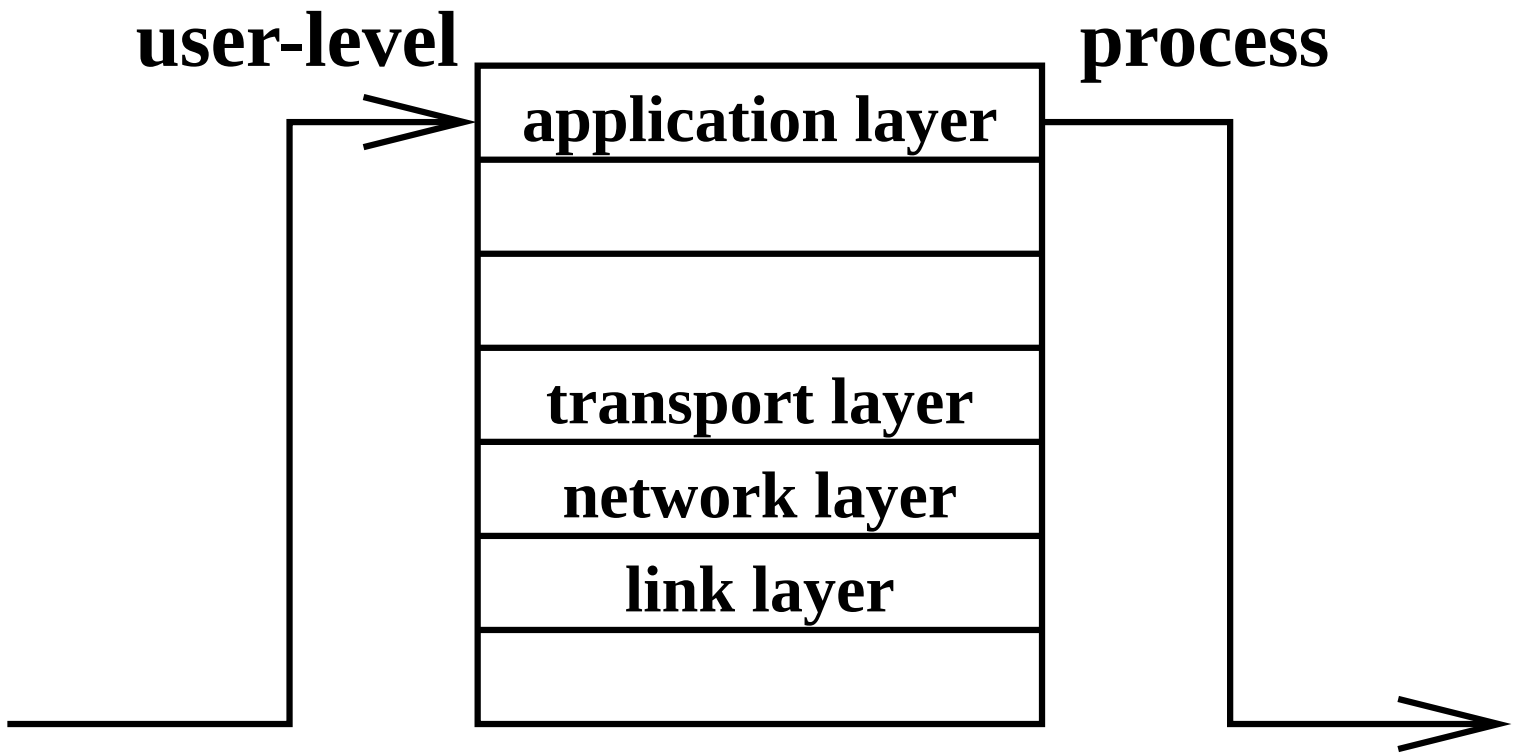
⟶ No content control, no authentication etc.

⟶ 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, H323, ICQ

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⟷proxy, proxy⟷server)

Technology – proxies (3)

- ⟶ 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

- Faster (Gbps)
- Easier adaptability to new protocols
- Lower level of security
- *No* content filtering, authentication

Proxies

- Slower (hundreds of Mbps)
- Need more work to adapt to new protocols
- Higher level of security
- Content filtering, 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.

Prevention vs. Detection vs. Reaction

Prevention: Firewalls work as a preventive measure,
but what about detection and reaction?

Successful attacks often remain undetected (ever)!!!

Detection: Comprehensive logging, integrated intrusion detection

Diverted attacks are not as important
as looking for anomalies in permitted communication

Reaction: May be counterproductive (easy DoS attacks)

- Automated shutdown
- Automated blocking of originator

Challenges

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

$\Rightarrow$. . . Additional functions integrated into firewalls.

$\Rightarrow$. . . Too much expectations linked to firewalls.

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

$\Rightarrow$. . . Integration cannot solve everything

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

Challenges (2) — Attacks

Most attacks: performed by an insider, or with collaboration by an insider

$\Rightarrow$. . . Firewalls can secure against known attacks

$\Rightarrow$. . . Human intervention is vital.

New threats can be eliminated by:

i) shuting down a service

ii) patch from vendor

iii) configuration (if the system is granular enough)

“Full disclosure” war

Challenges (3) — Risks

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

- Executable content
- Automated attack scripts
- Coordinated distributed attacks
- Encapsulation of protocols into HTTP
- Unsolicited commercial e-mails (SPAMs)

Solution: $\Rightarrow$. . . Integration of additional functions

Integration – Content filtering

- Virus/worm detection
  - On the firewall (not good from security point of view)
  - Content Vectoring Protocol (CVP)
  - External proxy or transparent gateway
- *Always catching up*

- Misuse detection/elimination
  - Internet blacklists
  - Integrated or external
  - False positives/negatives
- Executable content
  - Integrated
  - Sandbox approach

Integration – Spam detection

Methods:

- Blacklists
- Heuristics
- Balance between the number of *false negatives* (undetected spam)
  and *false positives* (non-spam detected as spam)

$\Rightarrow$ Spam detection is seldom used to kill e-mails

Integration – Virtual private networks

- IPsec—complicated but still the best (ESP, AH, IKE and X.509 authentication)
- PPTP, L2TP—included with MS Windows but is less secure
- OpenVPN—upcoming free software standard, very popular and easy to use

VPN clients often imply the use of *Personal firewalls* as VPNs bring risks to the internal network though the VPN clients.

Integration – High availability

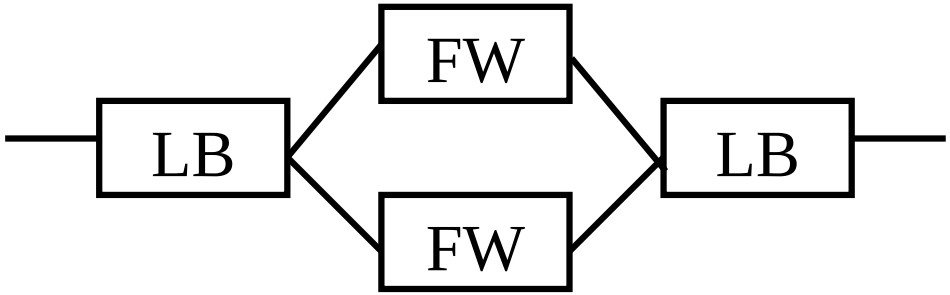
Exclusivity makes firewall the *single point of failure*.

⇒. . . Firewalls are often duplicated *(clusters)*

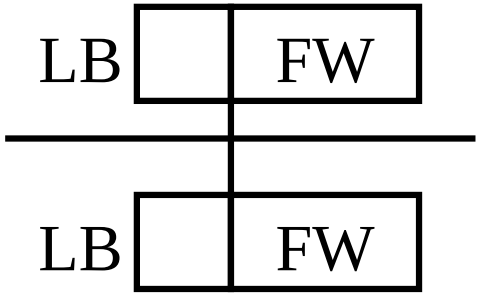
⇒. . . Automatic failure detection

⇒. . . Redundant firewall takes over

Redundant firewalls are used for *load balancing*.



network-based



host-based

Integration – Log processing

Firewall is primarily used for *prevention*

Its *detection* and *reaction* potential is disregarded

Log information processing:

- Alarms (false positives/negatives), usually approved by a human
- Automatic reaction (unreliable, potential DoS attacks)
- Statistics (and other lies ;-)

Future trends

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

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 the cost of risks against the cost of countermeasures.*
- At best, the 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 misvalued.

Recommended reading

- Ranum, M. J.: *Thinking About Firewalls V2.0: Beyond Perimeter Security*, `http://www.ranum.com/pubs/think/`, 1997.
- 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