Network Firewalls

Josef Pojsl, jp@tns.cz
Trusted Network Solutions, a.s.

March 14, 2011

Kernun

Agenda

1) What is a firewall?

2) A word about topology

3) On the origin of firewalls

4) Statefulness, transparency, proxies

5) The evolution of UTM appliances

6) Real threats, future firewalls

The Definition of Firewall

- ✗ No personal firewalls
- ✗ No home firewalls
- ✗ No small office firewalls
- There are many definitions of firewall

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 them.

Topology

- Hosts with different trust levels must be separated into different networks
- Connections should only be initiated from a more trusted (e.g. internal) network to a less trusted network zone whenever possible

Firewalls provide network security,
not host security

Firewall 1.0

- Late 1980s / early 1990s
- Packet filtering routers (DEC, AT&T)
- Circuit level gateways (AT&T)
- Bastion hosts / proxies (DEC SEAL)

FW 1.0: Packet Filtering

- **Selective blocking of individual packets based on IP addresses & TCP/UDP ports**
- **Default-allow policy**
- **Evolved from routers as their add-on feature**
- **Typically combined with Network Address Translation (NAT)**

Basic filtering on routers is still being used together with modern firewalls

FW 1.0: Circuit Level GWs

- Stand between packet filters and application proxies
- Work on session layer
- Terminate client TCP/UDP sessions and replicate them to servers
- Do not operate on application layer

Some proxy firewalls still use them for unknown application protocols

FW 1.0: Proxies

- Evolved from so-called „Bastion hosts“
- Application layer commands
- Users must have known about them
- Default-deny policy

Most modern firewalls still use proxies even if the vendors do not admit it

Firewall 2.0

- Mid 1990s
- Stateful filtering (Check Point)
- Transparent proxies (Gauntlet)

Stateful filters and transparent proxies are still at the heart of most modern firewalls

FW 2.0: Stateful Filtering

- PF: One rule out, another rule in
- Stateful Packet Inspection (SPI) takes care about who initiates the communication
- Handles TCP / UDP / ICMP traffic (?FTP, SIP)
- Default-deny or default-allow policy
- Still often combined with NAT

The most important firewall feature up to these days

FW 2.0: Transparent Proxies

- Proxies placed at the border of perimeter
- Transparency = no visibility for users
- Inherently translates addresses (NAT)
- Provides application layer control
  - *Authentication*
  - *Content checking (antispam, antivirus,...)*
  - *Needs specific code for each app. layer protocol*

Firewall 3.0

- Early 2000s
- Unified Threat Management (UTM)
- Firewall / UTM appliances (NetScreen - now Juniper, FortiGate, Symantec)
- European projects (Phion - now Barracuda, NetASQ, Astaro, Kernun)

FW 3.0: UTM

- Integration of additional features:
- → Intrusion detection / prevention (IDS / IPS)
- → Antivirus / antispam / anti-anything
- → Content filtering / blocking
- → Network Access Control (NAC)
- → Anomaly detection

FW 3.0: Appliances

- Earlier, firewalls came as software
- Now, they were sold as hardware
- Rack form factor
- Pre-packaged appliances equiped with hardened OS and the software
- Multi-gigabit throughput

Threats and challenges today

- Forget about ports and IP addresses
- Phishing / Pharming
- Botnets / DDoS
- Cyber War
- Viruses / worms attacking PDF
- XSS, CSRF, ClickJacking etc.

Phishing / Pharming

- A large attack against Česká Spořitelna in March 2007
- Forged bank site (very authentic)
- Fraudulent e-mails (several versions received by thousands of users)
- Accompanied with a Trojan capturing authentication from keyboard

DDoS on Estonia

- In spring 2007, Russian-Estonian conflict was accompanied with a large-scale cyber attack against Estonian government, newspaper and technology sites
- Russian riots in Tallin and cyber attacks were coordinated and both came in three ways
- Estonia, one of the Europe's most wired countries, showed very vulnerable
- Russia was blamed to orchestrate the attacks, officially denied
- NATO's investigation

Great Firewall of China

- Internally called „The Golden Shield Project“, Chinese government launched the biggest firewall in the world in 2003
- Many sites are completely unreachable from the whole of China (BBC)
- Even encrypted HTTP traffic is being scanned
- During Olympic Games in Beijing in 2008, the firewall rules were relaxed after protests from journalists

MS SQL Slammer Worm

- Exploit of a buffer overflow bug in MS SQL Server
- SQL Slammer worm hit the Internet on Jan 25, 2003
- A patch had been released 6 months earlier
- 90% of its 75,000 victims were infected within 10 minutes, some of the infected systems belonged to MS
- Its spread followed an exponential curve with doubling time of 8.5 seconds in the early phases of the attack
- The entire worm (376 bytes) fit into a single UDP packet
- In Aug 2002, D. Litchfiled made available his proof of concept code which the worm was probably based on

Botnets

- Groups of computers controlled by attackers
- Real computer owners are unaware of the botnet
- Botnets spread via unpatched vulnerabilities
- Used for Distributed Denial of Service attacks, sending SPAM, adware/spyware distribution etc.
- Botnets may typically be leased for a fee

Botnet Examples

BredoLab

- 30M computers
- Originated in Russia or Kazakhstan
- Dismantled in Nov 2010

Mariposa

- 12M computers
- Spanish hackers
- Slovenian authors
- All arrested in July 2010

Stuxnet

- 2009: Special purpose worm, attacking industrial SCADA systems
- Large piece of code, written in several programming languages; rootkit
- Takes advantage of several Windows vulnerabilities; centrally controlled
- Used to attack nuclear facilities in Iran, possibly originated in Israel/USA

PDF attacks

- Adobe Acrobat runs scripts within PDF documents
- Many people are unaware of the risks
- In 2009, Acrobat PDF attacks (48%) finally outnumbered attacks on MS Word (39%)

Challenges

- Securing network perimeter, access control
- Recognizing applications
- Performing identity management
- Providing accurate statistics and forensics data
- IPv6

Applications & Users

Applications are not ports

Users are not IP addresses

IPv6 and Firewalls

- IPv4 exhaustion → transition to IPv6
- New shape of security
  - Multicast
  - Avoidance of NAT?
  - Network Discovery Protocol (NDP)

Specific problems of dual-stack

Firewall 4.0?

- Early 2010s (Palo Alto, Kernun)
- Combination of many technologies
  - Stateful Filtering
  - Transparent Proxies
  - Intrusion Detection Systems
  - Anomaly Detections Systems
  - Heuristic Analysis

Access control for users
to real applications

Recommended Reading

- **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**

Useful Links

- SecurityFocus - Vulnerabilities
  http://www.securityfocus.com/
- Open Web Application Security Project
  http://www.owasp.org/
- Marcus J. Ranum Site
  http://www.ranum.com/

Network Firewalls

Josef Pojsl, jp@tns.cz

Trusted Network Solutions, a.s.

March 14, 2011

Kernun