IC3: Network Security

Firewals

Antony Stone
Rockstone Ltd

Firewals

- What is a Firewall ?
- What types of Firewall are there ?
- What use are Firewalls ?
- How are Firewalls configured ?
- What problems do Firewalls introduce ?
- What don't Firewalls do ?
- How do you get round Firewalls ?
- Firewalls in context.

What is a Firewall ?

- A Firewall is a network security device designed to restrict access to resources (information or services) according to a security policy.
- Firewalls are not a “magic solution” to network security problems, nor are they a complete solution for remote attacks or unauthorised access to data

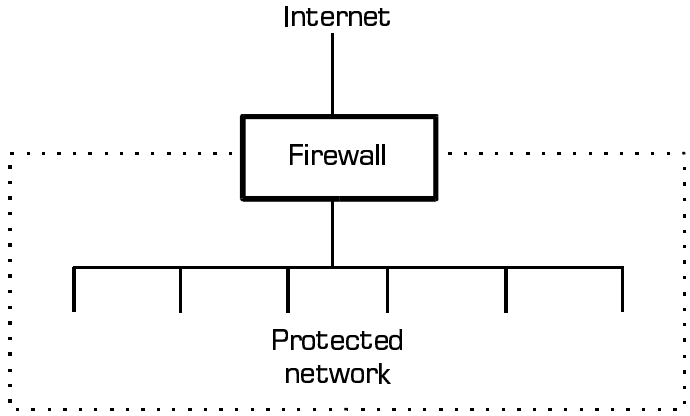
What is a Firewall ?

- A Firewall is a network security device
- It serves to connect two parts of a network a control the traffic (data) which is allowed to flow between them
- Often installed between an entire organisation's network and the Internet
- Can also protect smaller departments

Where does a Firewall go ?

- A Firewall must be the single path of communication between protected and unprotected networks
  - (Special case of multiple Firewalls, redundant connections, fault-tolerant failover etc)
- A Firewall can only filter traffic which passes through it
- If traffic can get to a network by other means, the Firewall cannot block it

Where does a Firewall go ?



What different types of Firewall are there ?

Four basic types:

1. Packet filter
2. Circuit-level proxy
3. Stateful packet filter
4. Application-level proxy

OSI Networking model

A brief reminder:

7	Application	SMTP, HTTP, SSH, FTP
6	Presentation	
5	Session	
4	Transport	TCP / UDP packets (ports)
3	Network	IP packets (addresses)
2	Data link	Ethernet frames, 802.11
1	Physical	

OSI Networking model

- Layer 3 – Network
  - Source & destination IP addresses
    - Source address
    - Destination address
      - Both are numerical – it is not easy for a Firewall to deal with machine or domain names
      - eg ww.hotmail.com
    - Request: client = source, server = destination
    - Response: server = source, client = destination

OSI Networking model

- Layer 4 – Transport
  - This is where TCP & UDP port numbers exist
    - eg: 25 SMTP – sending email
    - 110 POP3 – collecting email
    - 143 IMAP – collecting email
  - 80 HTTP – web pages
  - 443 HTTPS – secure web pages
  - 53 DNS – name lookups
- Most Firewalls assume _____ that the port number defines the service – <u>not necessarily !</u>

OSI Networking model

- Layer 7 – Application
  - There is where all the 'interesting' stuff is:
    - Web requests
    - Images
    - Executable files
    - Viruses
    - Email addresses
    - Email contents
    - Usernames
    - Passwords

Packet filter

- TCP/IP packet filtering router
  - A router which can throw packets away
- Examines TCP/IP headers of <u>every</u> packet going through the Firewall, in <u>either</u> direction
- Choice of whether to allow or block packet based on:
  - IP source & destination addresses
  - TCP / UDP source & destination ports

Circuit-level proxy

- TCP / IP proxy server
- Packets are received and go no further
- Proxy software generates new packets
- New packets go to destination

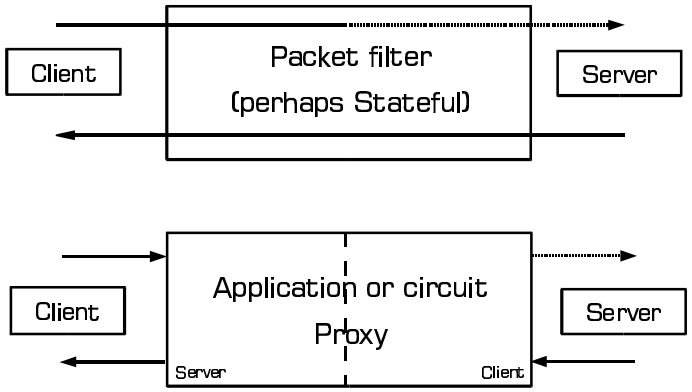
Stateful packet filter

- TCP / IP packet filtering router
- Same as a packet filter, except initial packets in one direction are remembered, and replies are automatically allowed for
- Simpler rules than packet filter
- Support more layer-7 protocols than a simple packet filter can

Application-level proxy

- Layer-7 proxy server
- Client and server in a single machine
  - For every supported application protocol
    - SMTP, POP3, HTTP, SSH, FTP, NNTP…
- Packets are received and processed by 'server'
- New packets generated by 'client'

Firewall types



Packet filter

- Rules specify which packets are allowed through the Firewall, and which are dropped
- Rules must allow for packets in both directions
- Rules may specify source / destination IP addresses and source / destination TCP / UDP port numbers
- Certain (common) protocols are very difficult to support securely (eg FTP)
- Low level of security

Circuit-level proxy

- Similar to a packet filter, except that packets are not routed
- Incoming TCP/IP packets accepted by proxy
- Rules determine which connections will be allowed and which blocked
- Allowed connections generate new connection from Firewall to server
- Similar specification of rules as packet filter
- Low-medium level of security

Stateful packet filter

- Packet filter which understands requests and replies (eg: for TCP: SYN, SYN-ACK, ACK)
- Rules need only specify packets in one direction (from client to server – the direction of the first packet in a connection)
- Replies and further packets in the communication are automatically processed
- Supports wider range of protocols than simple packet filter (eg: FTP, IRC, H323)
- Medium-high level of security

Application-level proxy

- Complete server & client implementation in one box for every protocol which can be expected through it
- Client connects to Firewall
- Firewall validates request
- Firewall connects to server
- Response comes back through Firewall and is also processed through client/server
- Large amount of processing per connection
- High level of security

Firewall types

- Packet filters, circuit-level proxies and stateful packet filters are like telephone call-barring by number
  - block or allow mobile calls
  - block or allow international calls
  - block or allow premium rate calls
  - from different internal extensions
- Application level proxy is like telephone call monitoring by listening to the conversations
  - conversations may still be encoded, or in a foreign language...

Firewall terminology

- "Personal Firewalls"
- Applications which run on Windows machines
  - commonest home PCs
  - often insecure
  - increasingly connected using ADSL etc
- Packet filter (sometimes stateful)
- Learn which applications are permitted to make what type of connections outbound
- Block inbound access except replies

Firewall terminology

- "Deep Packet Inspection"
- Packet Filtering firewall (usually stateful)
- Understands structure and syntax of layer 7 protocols: HTTP, FTP, IRC etc
- Compromise solution between packet filter and application proxy
- Speed and flexibility of packet filter
- Greater content control, like application proxy
- Greater security – harder to bypass

What use are Firewalls ?

- Firewalls control network traffic to and from the protected network
- Can allow / block access to services (both internal and external)
- Can enforce authentication before allowing access to services
- Can monitor traffic in/out of network

What use are Firewalls ?

- Firewalls typically defend a protected network against an attacker, who tries to access vulnerable services which should not be available from outside the network
- eg: Microsoft Exchange server running SMTP
  - can it be accessed using HTTP, FTP, SMB ?
- eg: Unix mail server or web server
  - can it be accessed using Telnet or rlogin ?

What use are Firewalls ?

- Firewalls are also used to restrict internal access to external services for many different reasons:
  - security (don't want people downloading and installing unknown applications)
  - productivity (don't want people wasting time on non-work related websites etc)
  - cost (many Internet connections, eg: JANet are charged by data transferred – ensure this is all necessary)

What use are Firewalls ?

- Legal compliance
- eg: UK Data Protection Act 1998
- 7th Principle:
  - "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"
    - Note that "processing" explicitly includes "accessing"

How are Firewalls configured ?

- Two basic approaches:

1. Allow all traffic, but block...
   - irc
   - telnet
   - snmp etc.
2. Block all traffic, but allow...
   - http
   - pop3
   - smtp
   - ssh etc.

How are Firewals configured ?

- Allow by default, block some
  - Easy to make mistakes
  - If you forget something you should block, it's allowed, and you might not realise for a while
  - If somebody finds find a protocol is allowed, they might not tell you.....
- Block by default, allow some
  - Much more secure
  - If you forget something, someone will complain and you can allow the protocol

How are Firewalls configured ?

- Typical Firewall ruleset:
- Allow from internal network to Internet:
  - HTTP
  - FTP
  - SSH
  - DNS
- Allow reply packets
- Allow from anywhere to Mail server:
  - TCP port 25 (SMTP) only

How are Firewals configured ?

- Allow from anywhere to Mail server:
  - TCP port 25 (SMTP) only
- Allow from Mail server to Internet:
  - SMTP
  - DNS
- Allow from inside to Mail server:
  - SMTP
  - POP3
- Block everything else

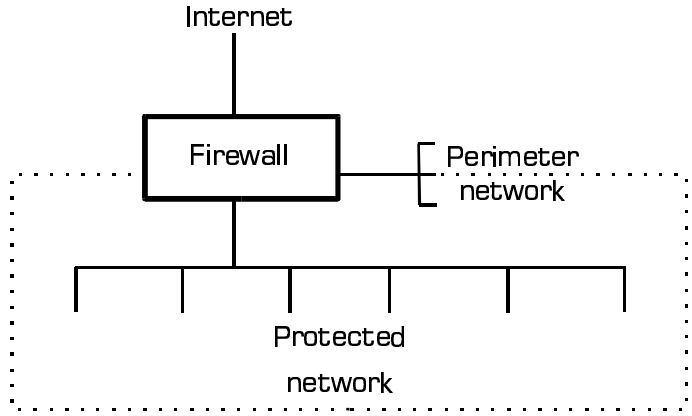
How are Firewalls configured ?

- As well as filtering out some packets, Firewalls are common locations for:
  - Virtual Private Networking
    - all traffic passes through the Firewall
    - convenient location to route some traffic via VPN
  - Network Address Translation
    - internal machines with private addresses can be hidden behind public IP address
    - public addresses can be translated to private addresses for internal servers
    - source address is always changed by proxies

Common Firewall networking

- A Firewall can only filter traffic which goes through it
- Where to put, for example, a mail server ?
- Requires external access to receive mail from the Internet
  - should be on the inside of the Firewall
- Requires internal access to receive mail from the internal network
  - should be on the outside of the Firewall
- Solution: use a "perimeter network" (aka DMZ)

Common Firewall networking



Common Firewall networking

- Perimeter network
  - used to locate servers which require (selective) access from both inside and outside of Firewall
    - eg: mail server
    - web server
    - name server (DNS)
- Firewalls can have many interfaces
  - multiple internal departments
  - multiple client networks eg: for ISP

What problems do Firewals introduce ?

- Some services don't work, because they're blocked
  - People complain
- Network diagnostics may be harder
- Network Address Translation can cause confusion
- Some protocols are hard to support
  - FTP
  - IRC
  - H.323

What don't Firewals do ?

- Packet filtering Firewalls do not provide any content-based filtering
  - if email is allowed through, then emails containing viruses are allowed through
  - if web access is permitted, then pornographic websites can be accessed
  - if web access is enabled for a browser, then it is also enabled for Nimda
- Encrypted traffic cannot be examined / filtered
  - https
  - ssh

What don't Firewals do ?

- Packet filters do not check content
- Even application-proxy Firewalls may not perform thorough checks on content
  - An increasing number of services are being offered across the Internet using TCP port 80 (HTTP) – no longer just web page access
  - This makes it increasingly difficult for Firewalls to allow or block access to different services
- Well-established dilemma:
  - Security versus convenience

What don't Firewals do ?

- Encrypted data is a problem for Firewalls
- Encryption is becoming more widespread
  - Privacy
  - E-commerce
- SSH, TLS etc are end-to-end, client to server
- Any system in between cannot decode data
- Users can visit unknown websites
  - non-productive business time
- Downloads cannot be anti-virus checked

How do you get round Firewals ?

- Modem or other external link
  - if traffic does not go through the Firewall, the Firewall cannot block it
- Poor configuration
  - eg: allow access to any machine, inside or outside, on TCP / UDP ports 53
- Inbound / outbound filtering
  - inbound traffic may be blocked, but an outbound initiated link works both ways (eg: SIP phones)
- Protocol tunnelling

Protocol tunnelling

- Suppose you want to send smtp traffic through a firewall which blocks smtp
  - find a port number which is allowed, and run the external smtp server to listen on that port
  - create a DIY VPN
    - eg IPsec – FreeS/WAN using Linux
  - tunnel through SSH
    - many firewalls allow SSH
    - SSH supports port forwarding
  - PPP over SSH – ugly but effective

Firewals in context

- Firewalls protect against network threats
- No understanding of Operating System or Application vulnerabilities
- Application proxy Firewalls provide close control over content of both requests and responses
  - Complex processing – poor performance, high cost, complicated to configure
  - Good security, provided configuration is appropriate

Firewals in context

- Packet filters and circuit-level proxies
  - High performance, lower cost
  - Coarser control over filtering
  - Simpler to specify acceptable traffic
- Firewalls must be between the good guy and the bad guy if they are to be any help
  - The Insider Threat

Real-world Firewals

- Market leader – Check Point Firewall-1
  - Stateful Packet Filter
  - Some proxy capabilities
  - Some authentication capabilities
  - Very expensive: £10,000s
- Symantec Raptor
  - Application Proxy
  - Also very expensive
- Cisco PIX
  - High performance

Real-world Firewalls

- SOCKS server
  - Circuit-level proxy
  - Not very commonly encountered
  - Difficult to establish a purpose
    - eg instead of packet filter
  - Very general security
  - No clear reason for proxy service
  - Difficulties with some protocols eg: SSH

Real-world Firewals

- Linux
  - Contains stateful packet filter
  - Called netfilter / iptables
  - Freely available (in both senses)
  - Commercial systems with GUI interface
  - High performance networking
  - Good protocol support (eg: FTP, IRC, H.323)
  - No authentication
  - No load-balancing / high-availability

Firewals in context

- A good Firewall is good for network security
- Much better is a Firewall with:
  - Network Intrusion Detection Systems
    - Internal and external detectors
  - Host Intrusion Detection Systems on internal machines
  - Secure Applications on internal clients and servers
  - Strong passwords on user accounts !

Firewals in context

- Balanced security
- An attacker will always try to find and attack the weakest element in a security system
- A weak Firewall is poor security
- A strong Firewall needs to be supported by strong security elsewhere