Who Moved My Firewall

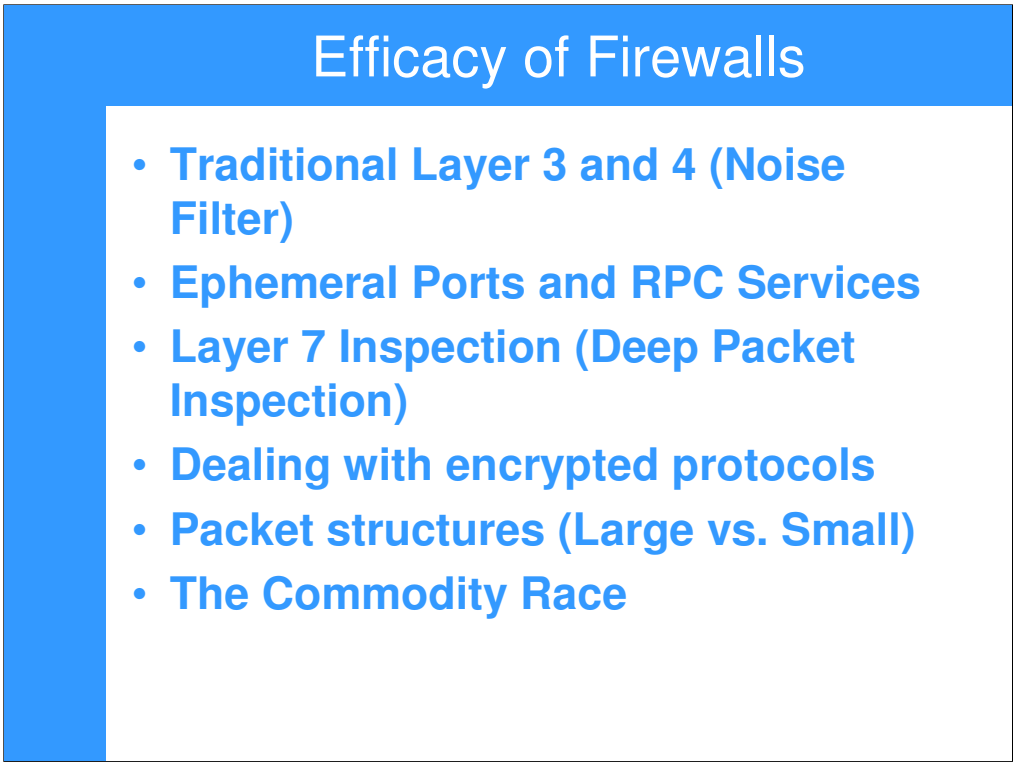
Clinton Thomson
Derivco (PTY) Ltd

Agenda

- Introduction to Derivco (Pty) Ltd
- Efficacy of Firewalls
- Firewall Roles
- Threat Landscape
- De-perimeterisation
- Q & A

Derivco as a company

- **Leading developer of online gaming software**
- **ICT Company of the year 2007 (KZN)**
- **Management of IT Services in online gaming**



One of the few things from the 80's that may not make us blush!

L3\4 Effective for publishing services to restricted locations – Stateful packet inspection the defacto standard today. Primarily noise filter. Limited value in logging unless you have the resources to manage and report. Nice for mngmt stats.

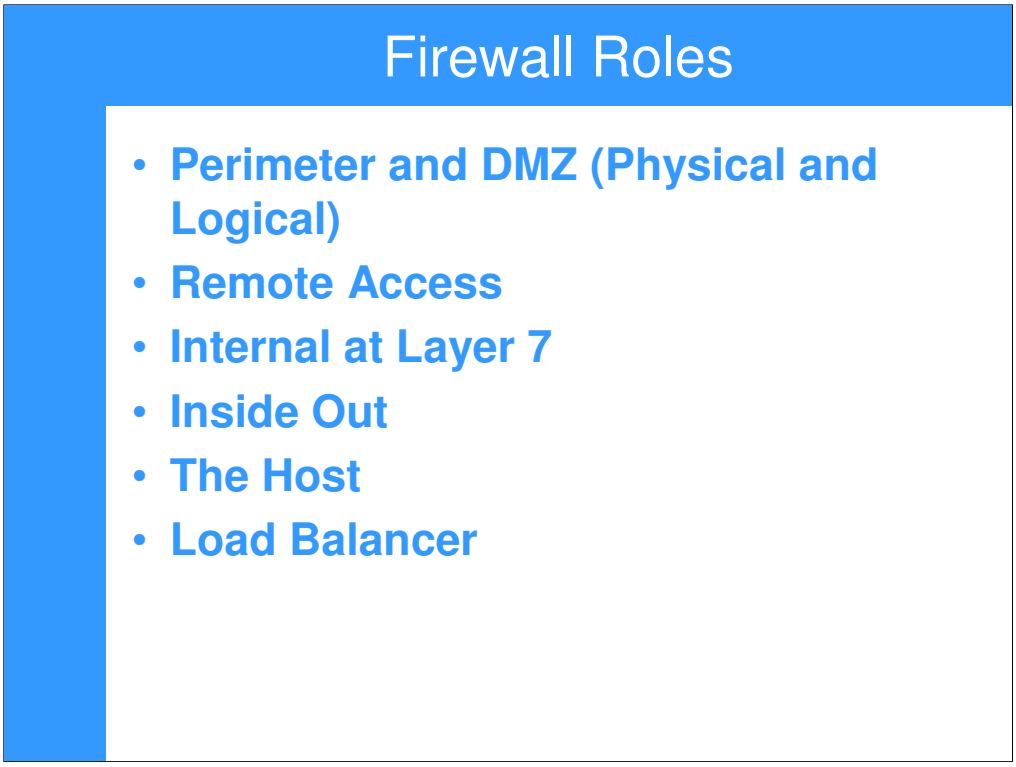
Still not entirely effective for ephemeral ports such and RPC\DCOM based services. Ability to use GUIDs with packet inspection helps but not everything is fully documented and supported. Results in hack jobs and registry settings to limit ports or alternatively some IPSec…

L7 nice for packet sanity. Good for clear text protocols such as FTP, HTTP, Telnet, SQL. More control at application level, limit commands that pose risk. Big perf penalties.

Encrypted protocols – no L7 insp which makes most FWs a L4 device. This makes attacks private too. Anything worthwhile on the web today needs protection, SSL and TLS more and more pervasive. Even SMTP will negotiate TLS. Can use SSL termination at firewall or edge device, results in performance hit.

Pckt structures Large vs. Small – NAT big penalties. Relationship between CPU and throughput not linear. DDoS mitigation not effective on large capacity networks, works in SA market. This is specific noted in a routed FW environment. Eg MPP packets and large number of players.

Commodity Race, stateful pckt insp, everyone's doing it. QOS, IPS, IPsec and SSL VPN. FW vendors adding as much as possible to offering to be competitive, enter UTM. Is this sustainable and is it exclusive to firewalls?



Perimeter and DMZ, typical model and not much has changed or is it changing? MS example of Server Isolation and will talk on this further under load balancer.

Remote Access for SSL VPN, Extranets etc Move load away from business as usual firewalls. Provides for different function vies a vie encryption and user based access.

L7 FW becomes more interesting internally, possibly less encryption. Monitor traffic to\from hosts, possible location for virtual patching, post SSL decryption (clear), isolation servers in the traditional sense and include application level checks.

Too externally focused, require firewall for all outbound pckts including L7 filtering on clear text protocols. Most web filtering vendors will provide SSL proxy and strip SSL, filter and establish SSL session. Required due to possible payload delivery and covert channels. Trusting servers over desktops not wise, server exploit exacerbated by allowing ANY outbound access incl DNS, NTP etc. Explain concept of tunneling data over DNS.

Host FW becoming increasingly important and essential even internally for all hosts. XP and 2003 FW, to include outbound as well as inbound. Last line of FW defense for host, reduces reliance on the absolute perimeter firewall, may be effective mitigation against non patched systems and systems running unapproved services.. Effective when used with GPO.

Load Balancers now provide Stateful Inspection, means to publish L4 to L7 services with inspection\action, Log and NAT connections, SSL offload etc. Relook at throughput issues of firewalls this becomes an interesting contender to remove traffic from FW. These devices can sit alongside a firewall and provide the very same services at a potentially better price\performance ratio.

Zero day attacks and variants are overwhelming today, compared to recent past there was much less activity in this space. Threats and attacks less visible, targeted, do more damage over time and are much more difficult to detect and remove. Behaviour based IPS and AV requirement. Patching needs to happen immediately and companies need to have the agility to do so.

Web applications feature rich with more functionality for the user. Risks now almost exclusively around applications. Systems are not developed with security in mind, junior developers do not possess knowledge and skill to develop secure solutions. Focus is on delivery to market and is time sensitive.

GUIs becoming richer for FW, Router and SYSAdmin while skills are spread wide from low to high with many in low area. Companies forced to take lower skills and assume the risks of human error and lack of experience. GUIs are great and believe they provide great value, dependant on the skill using the product.

Attacks on web systems reduced through effective patching and vendor practices. Attacks now more prevalent on user based services such as IM, VOIP and office arena.

Laptops and tapes seem to be the emerging way to lose lost of data in a very short space of time. More and more data loses now being attributed to loss of laptops and tapes. Good top see technology such as LTO 4 adding encryption, laptops need to be encrypted. These nullify protection mechanisms from firewall to host, but possibly not data…will talk more on this shortly.

De-perimeterisation

- Perimeters are bonnox fences at best
- Tunneling Applications
- Security at the host and data
- Pervasive
- Unobtrusive
- Defense in depth