building a

PERFECT FIREWALL

No time...

Not possible…

What we can do

- restrict access to the network services
- limit the number of active connections
- detect some port-scan atacks
- drop illegal traffic

What we can not do

- regain the channel already consumed
- detect 'smart' attacks
- look inside the application protocol

Components of the filter

- protocol classifier
- invalid packet filter
- port-scan detector
- policy classifier
- application protocol filter
- TCP-specific filters
- application protocol specific filters

Using marks

Mangle has four types of marks may be used for different applications:

- packet mark – queue policies
- connection mark – protocol policies
- routing mark – policy routing rules (not used in this setup)
- ToS – DiffServ service policy transfer (not used in this setup)

Protocol classifiers

- prerouting mangle
- packets opening new connections
- connection mark
- for TCP and UDP, check both, source port (usually, 1024-65535) and destination port.

Invalid packet filter

- forward filter
- invalid addresses (local, not registered with IANA, broadcast, multicast)
- invalid connection state
- NAT traversal

Port-scan detection

- PSD matcher
- TCP flags for Xmas and Null scans
- put violators in blocked IP address list

Policy classifier

- different customer profiles
- classify by addresses, then jump to separate policy enforcement chains
- ARP for binding IP with MAC

Application protocol filter

- choose the protocols allowed
- drop everything alse
- AUTH (TCP/113) should be rejected to avoid slowdown for some programs expecting it to be available

TCP-specific filters

- maybe drop TCP RST?

Application-specific filters

- AUTH – reject
- SMTP – drop the first connection, allow only second connection from a particular source address

More to do

- proxy everything: NTP, DNS, HTTP
- filter HTTP connections to some sites (porn site list was published somewhere on the forum)
- use a dedicated IDA
- use trusted software
- protect local traffic
- outsource

If you loose a connection

THANK YOU!

- Come to the Security Discussion Table, I will be waiting
- Have a nice trip back home!
- Get the firewall configuration script done with this scheme on monday evening at wiki.mikrotik.com