Introduction to Layer 7-filter

Presenter:
Andrzej Bober

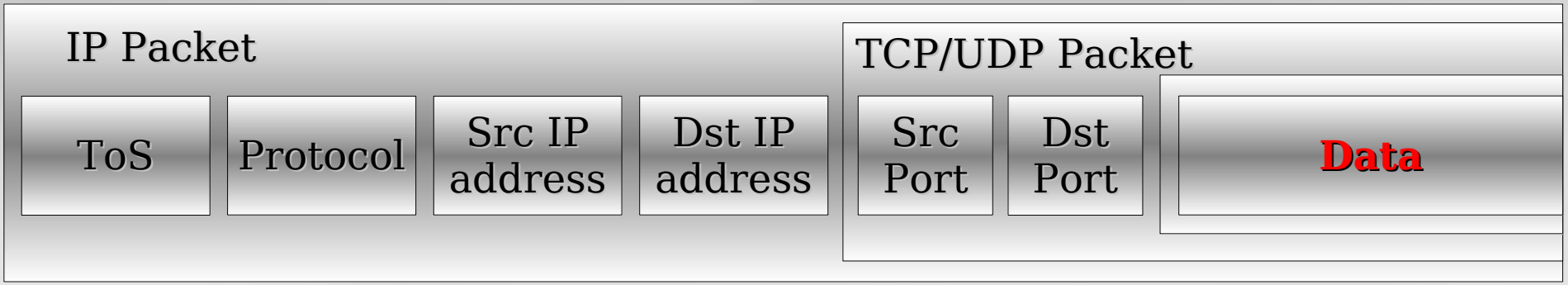
Questions

- What is and why we need L7 Filter
- How L7 works
- Regular expressions - example
- How to apply L7 on Mikrotik router
- Advantages and disadvantages

Traffic marking

Whatever we try to achieve, implement some security rules, bandwidth control or any accounting, first of all we need to define criteria on which we will classify our interesting traffic, from this first step depends the whole value of our configuration.

Traffic classification field

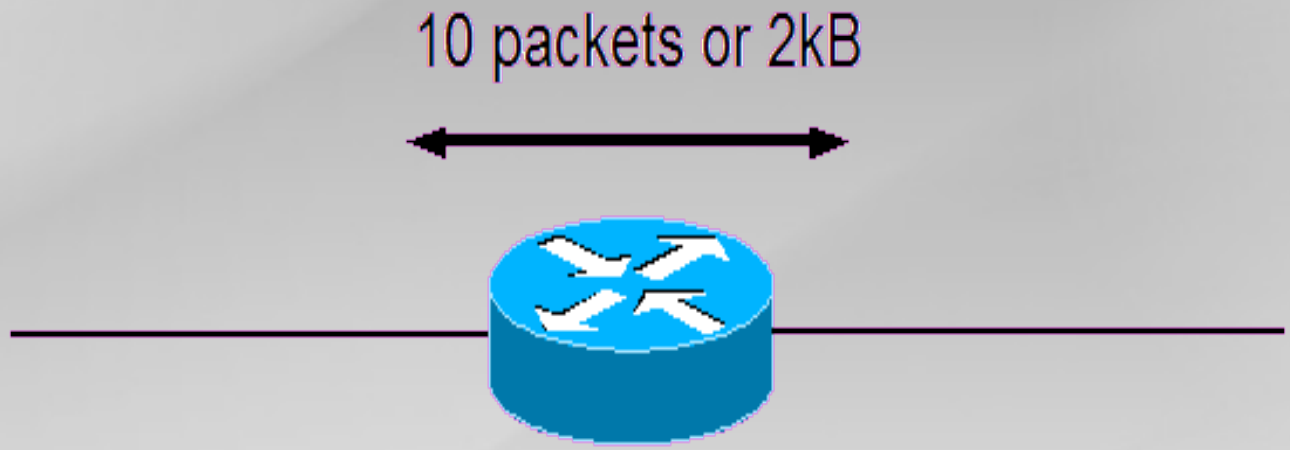


Analyse packet flow content

Recognise any traffic
Protocols
File types
Malware

Almost 150 pattern ready

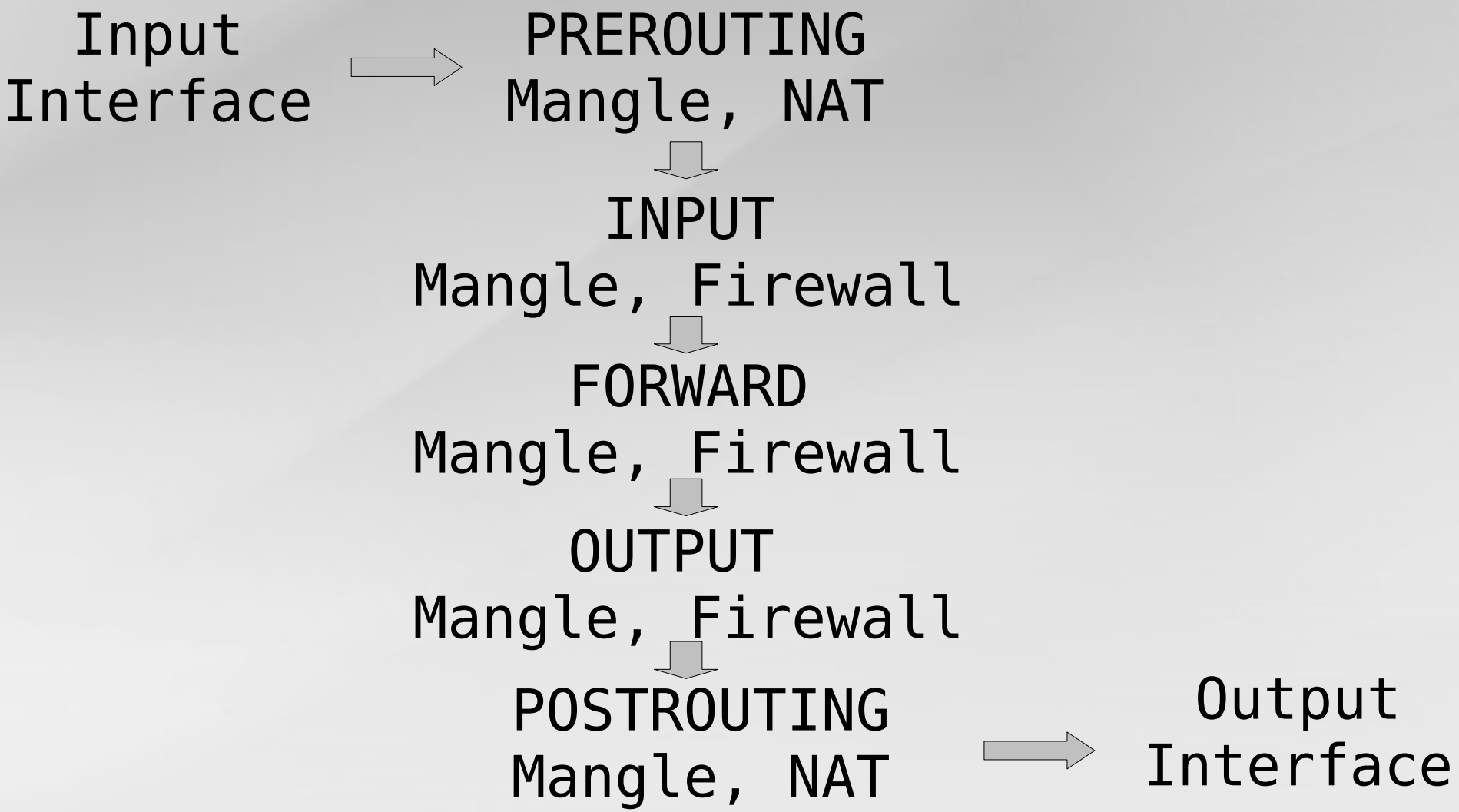
Analyse connections



L7 matcher, by default searching for pattern at the first 10 packets or 2kB, whichever is smaller (this value can not be changed). Any match made within this time is applied to the rest of the connection as well.

Traffic flow

simplified diagram



Best place to apply

Most of patterns to correct work need to see both sides of connection, that is why the best place to apply is on forwarding chain.

Regular Expressions

L7 uses regular expressions to investigate the content within an individual connection.

Regular expression is text string for describing a search pattern.

Searching examples:
"hello" messages such as "220 ftp server ready", "* ok", or "HTTP/1.1 200 ok".

Regular Expressions
quick reference chart

„^” (caret) Matches the begining of input
„$” Matches the end of input
„.” Matches any single character
„?” 0 or 1 occurrences of proceeding string
„*” (star) 0 or more occurrences of preceding string
„[...]” Matches any on the enclosed characters e.g. ca[tr] matches cat and car
„|” (pipe) Logical „or”, match either the part on the left side, or the part on the right side

Regular Expression

Useful things

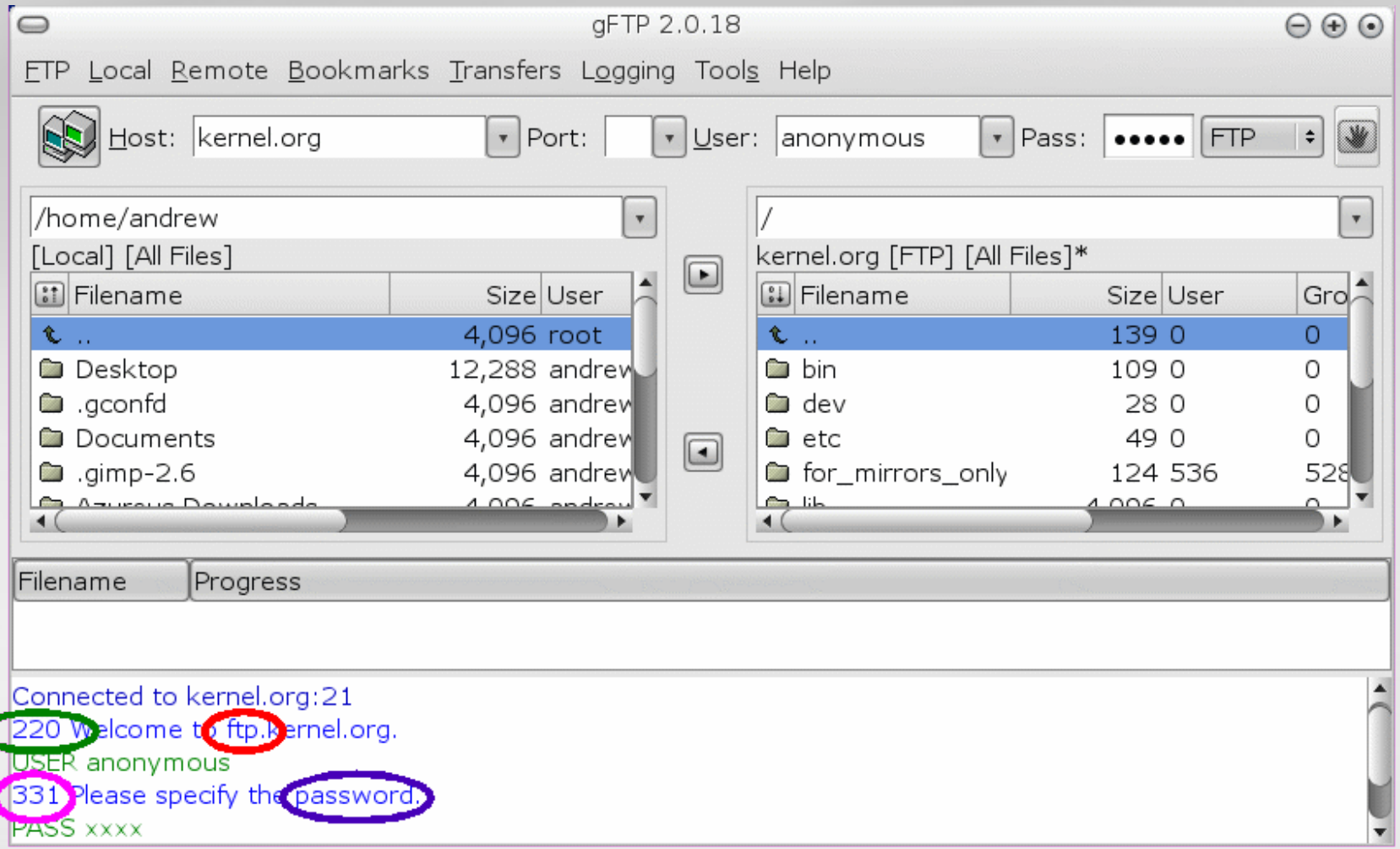
```
[\x09-\x0d -~] printable characters,
               including whitespace
[\x09-\x0d ] any whitespace
[!-~] non-whitespace printable characters
```

How to write own pattern

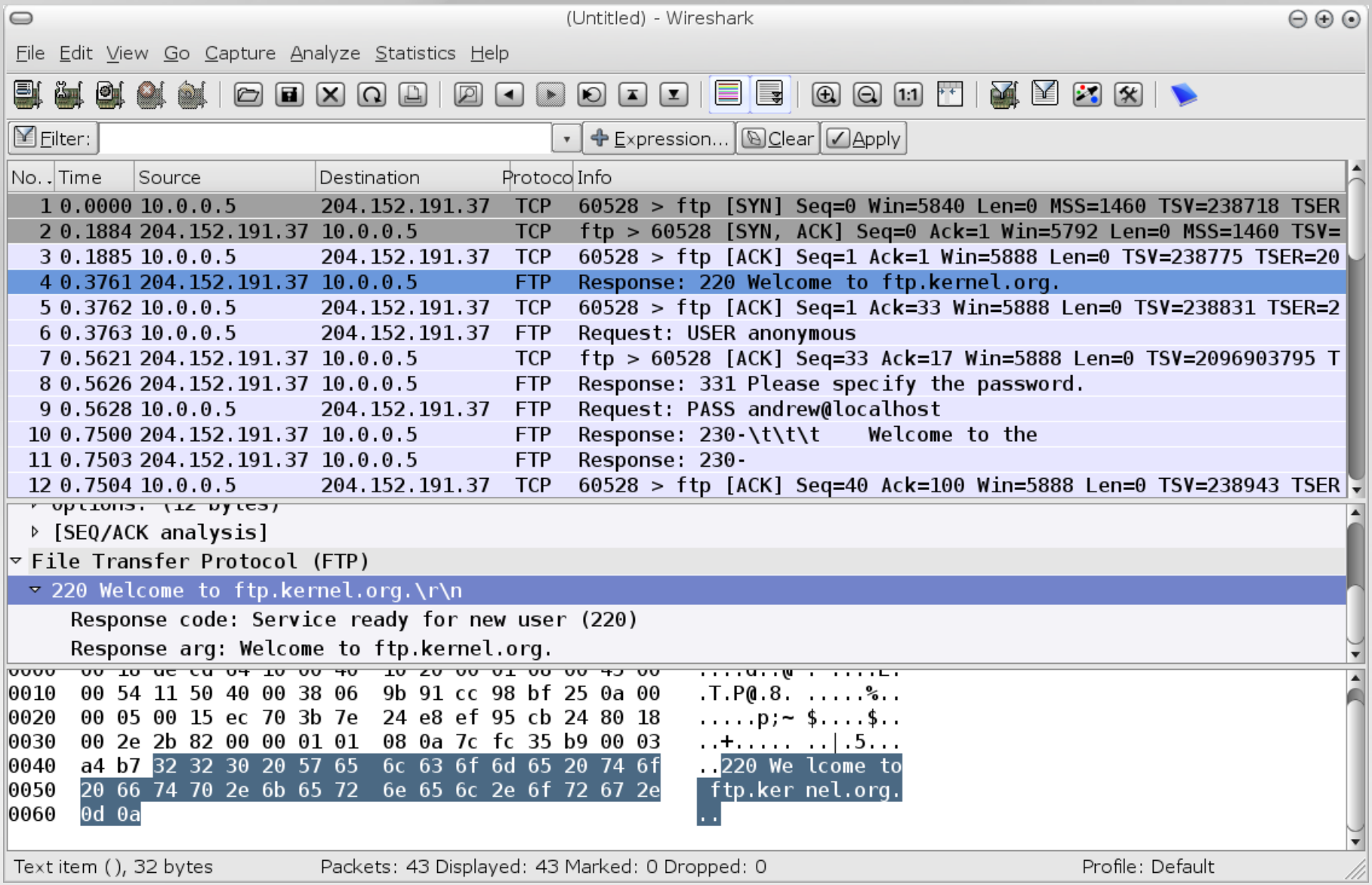
- Find and read specifications for the protocol you wish to match. For internet standard check RFCs, if it is proprietary protocol make general web searching for reverse-engineering specification.
- Use any network sniffer (e.g. Wireshark), to capture and watch packets of this protocol go by in a typical session of its use.
- Write a pattern that will reliably match one of the first few packets that are sent in your protocol. Test it.

FTP pattern

```
^220[\x09-\x0d -~]*ftp|331[\x09-\x0d -~]*password
```



FTP connection



Looking for pattern?

Pattern libraries can be found on:
http://protocolinfo.org/wiki/Main_Page
http://l7-filter.sourceforge.net/protocols

Script for Mikrotik with common programs list:
www.mikrotik.com/download/l7-protos.rsc

Layer 7 – CLI configuration

To define strings you will be looking for, add Regexp strings to the protocols menu.

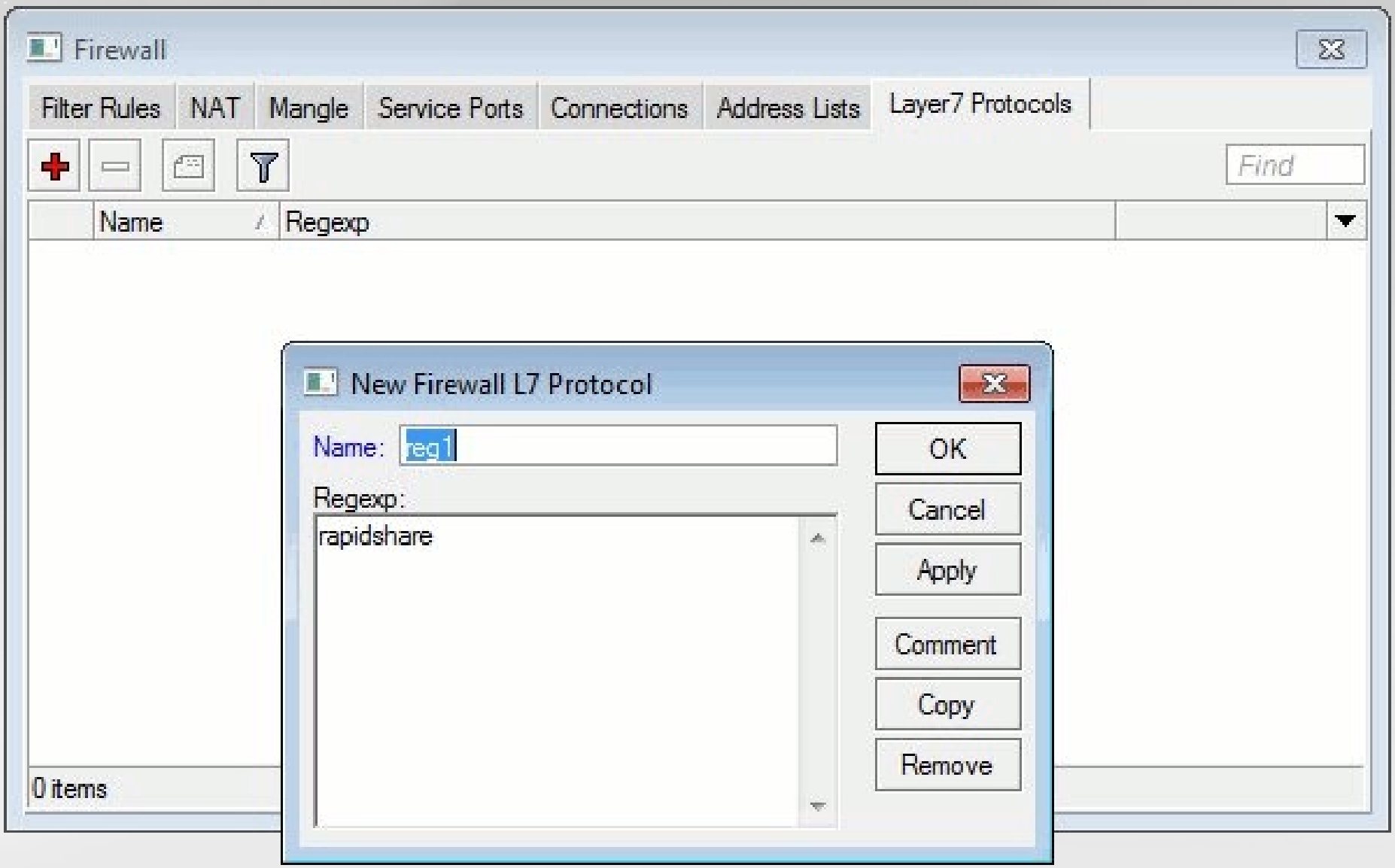
/ip firewall layer7-protocol add=

Then, apply defined protocols in firewall:

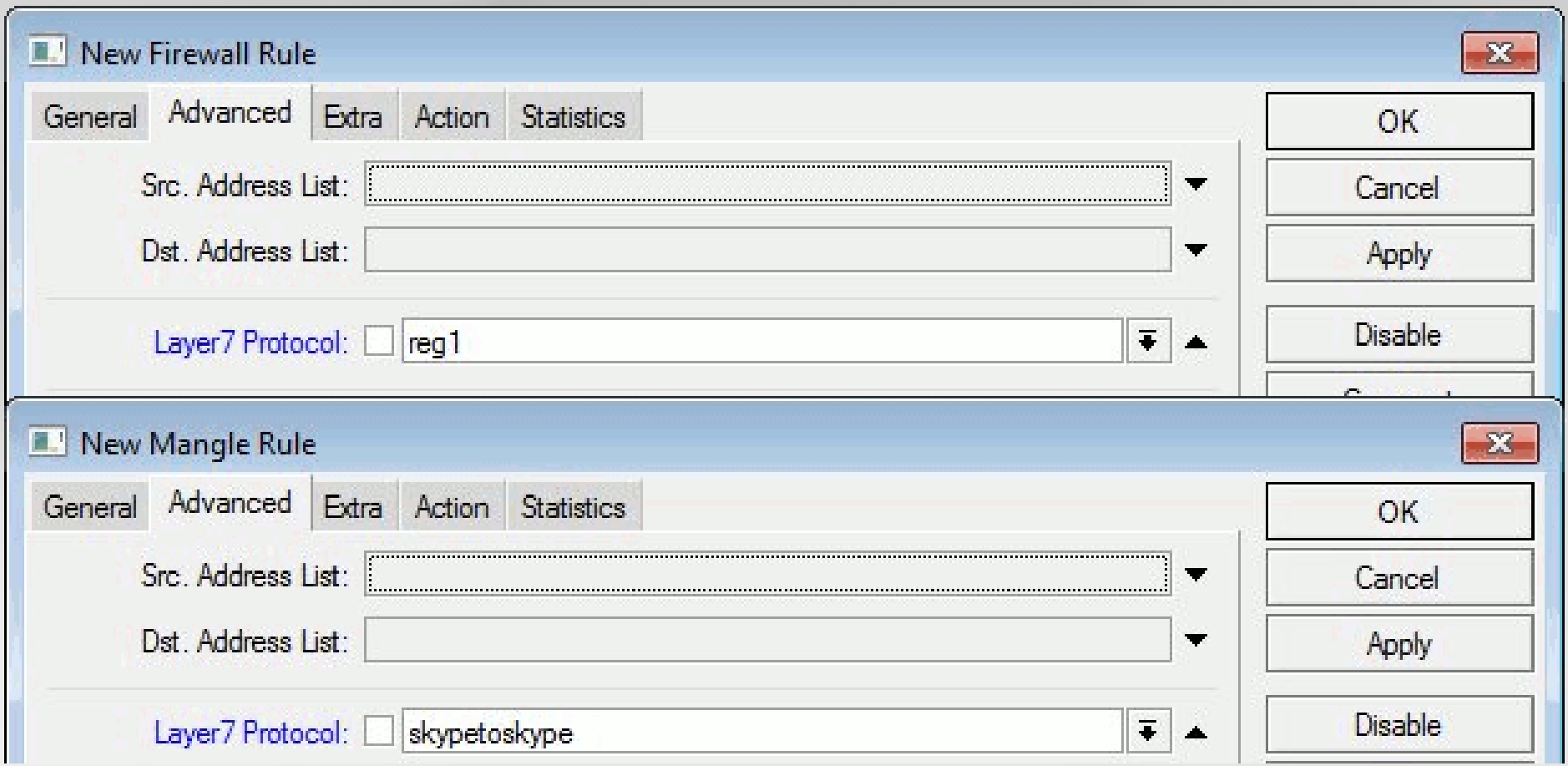
/ip firewall filter add layer7-protocol=

For traffic marking:
/ip firewall mangle add layer7-protocol=

Winbox configuration



Firewall and Mangle



Encrypted traffic

L7 do not work on SSL tunnel, this is because the only clear text packet following the TCP/IP handshake is the SSL server certificate.

One thing you might try is to look for criteria in the certificate, that is, you might decide not to trust individual certification authorities.

Summary

Advantages

Any traffic

High accuracy

Distinguish packets working on the same port

Disadvantages

CPU consumption

Can not recognize encrypted traffic

References

L7-filter project website:
http://l7-filter.sourceforge.net/

Blocking protocols at Layer 7 with the L7 patch by Jörg Harmuth