

## Advanced network traffic and content filtering (code: LX-NETFILTERING)

### Overview

The course discusses network traffic filtering tools on Linux, including application layer filtering and specifically web content filtering using transparent proxies. Participants learn how to use filters for virus protection and how to establish safe Internet access policies for companies and organizations.

### Ask for details

Phone +44 203 608 6289

info@alx.training

### Duration

1 day

### Agenda

1. Firewalls on Linux
2. The iptables command
  - blocking or allowing access to services from internal and external networks
  - rules, criteria, targets, user chains, policies
  - testing the setup, nmap scanner
3. Network topology
4. Proxy servers, Squid
  - configuration: squid.conf
5. Access control
  - creating ACLs
6. Transparent proxy, forcing the user to go through our server
7. Content analysis
  - DansGuardian scanner, definitions, keyword filtering
  - ClamAV anti-virus scanner
8. Configuring user workstations
9. Deploying a company-wide Internet access policy

### Target audience and prerequisites

This course targets at least intermediate-level Linux administrators.

Participants are expected to have good knowledge of general system administration and TCP/IP networks and protocols.

### Certificates

Course participants receive completion certificates signed by ALX.

### Locations

- Warsaw (English) – Jasna 14/16A
- Online (English) – your home, office or wherever you want
- any other location (London, UK, EU) on request

### Price

490 EUR

The price includes:

- course materials,

- snacks, coffee, tea and soft drinks,
- course completion certificate,
- one-time consultation with the instructor after course completion.

**Ask for details**

Phone +44 203 608 6289  
info@alx.training