

Security on routers

Course code: S1

The course is best suited for network administrators and network security engineers. The participants will learn the basic principles of network security and its implementation of Cisco routers.

| Affiliate | Duration | Course price | ITB |
|------------|----------|--------------|-----|
| Praha | 3 | 23 100 Kč | 0 |
| Bratislava | 3 | 960 € | 0 |

The prices are without VAT.

Course terms

| Date | Duration | Course price | Type | Course language | Location |
|------|----------|--------------|------|-----------------|----------|
|------|----------|--------------|------|-----------------|----------|

The prices are without VAT.

Who is the course for

The course is best suited for network administrators and network security engineers.

What we teach you

- Security threats and policy (packet sniffers, password attacks, DoS, Man-in-the-middle attacks, application layer attacks, trust abuse, trojan horses, security policy definition)
- Basic security of Cisco routers (passwords, stopping unnecessary services, traffic filtering routing protocol authentication)
- Packet filtering, IOS Firewall (Standard ACL, Extended ACL, Reflexive ACL, IOS Firewall)
- Network Address Translation (NAT - terminology, Static NAT, Dynamic NAT, PAT, Load balancing)
- IOS Intrusion Detection System (Types of samples, Reaction to attacks)
- AAA (Authentication, Authorization, Accounting, TACACS+, Radius)
- Encryption, IPSec (Encryption on different layers, types of encryption, Certificates, Digital signature, IPSec VPN)

Required skills

Knowledge of internetworking, TCP/IP and basic Cisco router configuration as presented in the A0/INTRO and A1/ICND courses.

Teaching methods

Professional explanation with practical samples and examples.

Teaching materials

Participants will receive a copy of the presentation.