Security on routers

Course code: S1

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

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, Autorization, 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.

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk