Advanced Juniper Security (AJSEC)

ID AJSEC **Preis** CHF 5'250.– (exkl. MwSt.) **Dauer** 4 Tage

Zielgruppe

This course benefits individuals responsible for implementing, monitoring, and troubleshooting Juniper security components.

Empfohlenes Training für die Zertifizierung zum

Juniper Networks Certified Internet Professional Junos Security (JNCIP-SEC)

Voraussetzungen

Students should have a strong level of TCP/IP networking and security knowledge. Students should also attend the Juniper Security (JSEC) course prior to attending this class.

Kursziele

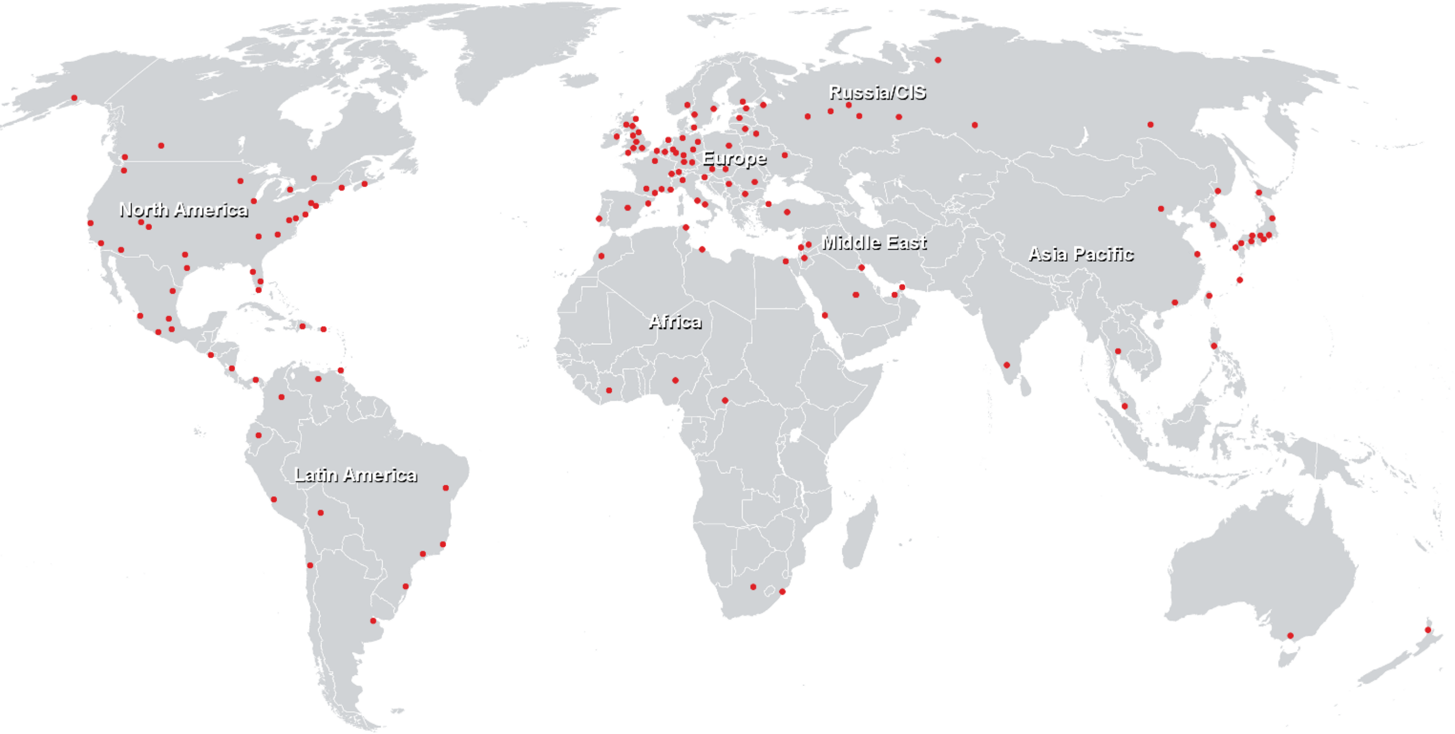
After successfully completing this course, you should be able to:

- Demonstrate understanding of concepts covered in the prerequisite Juniper Security courses.
- Describe the various forms of security supported by the Junos OS.
- Describe the Juniper Connected Security model.
- Describe Junos security handling at Layer 2 versus Layer 3.
- Implement next generation Layer 2 security features.
- Demonstrate understanding of Logical Systems (LSYS).
- Demonstrate understanding of Tenant Systems (TSYS).
- Implement virtual routing instances in a security setting.
- Describe and configure route sharing between routing instances using logical tunnel interfaces.
- Describe and discuss Juniper ATP and its function in the network.
- Describe and implement Juniper Connected Security with Policy Enforcer in a network.
- Describe firewall filters use on a security device.
- Implement firewall filters to route traffic.
- Explain how to troubleshoot zone problems.
- Describe the tools available to troubleshoot SRX Series devices.
- Describe and implement IPsec VPN in a hub-and-spoke model.
- Describe the PKI infrastructure.
- Implement certificates to build an ADVPN network.
- Describe using NAT, CoS and routing protocols over IPsec VPNs.
- Implement NAT and routing protocols over an IPsec VPN.
- Describe the logs and troubleshooting methodologies to fix IPsec VPNs.
- Implement working IPsec VPNs when given configuration that are broken.
- Describe Incident Reporting with Juniper ATP On-Prem device.
- Configure mitigation response to prevent spread of malware.
- Explain Sectel uses and when to use them.
- Describe the systems that work with Sectel.
- Describe and implement advanced NAT options on the SRX Series devices.
- Explain DNS doctoring and when to use it.
- Describe NAT troubleshooting logs and techniques.

Kursinhalt

- Course Introduction
- Junos Layer 2 Packet Handling and Security Features
- Firewall Filters
- Troubleshooting Zones and Policies
- Hub-and-Spoke VPN
- Advanced NAT
- Logical and Tenant Systems
- PKI and ADVPNs
- Advanced IPsec
- Troubleshooting IPsec
- Juniper Connected Security
- Sectel
- Advanced Juniper ATP On-Prem
- Automated Threat Mitigation

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch