

XSec Training

Ausbildung durch Xperten – im Xantaro Schulungszentrum oder bei Ihnen vor Ort, als Training-on-the-Job innerhalb eines Projektes oder „customized“ entsprechend Ihrer Anforderungen: Wir finden die Lösung.

Kursbeschreibung:

Das XJSec Training behandelt den Betrieb, die Konfiguration und die Entstörung von Juniper Firewalls der SRX-Serie. Es werden grundlegende Kenntnisse in der Konfiguration von JUNOS Enhanced Services™ vermittelt sowie die Funktionsweise und Implementierung von Security Mechanismen auf Juniper SRX Firewalls behandelt.

Der 5-tägige Kurs beinhaltet Laborübungen, die das Erlernete in praktischen Übungen vertiefen. Jedem Teilnehmer steht für die Übungen eine eigene Firewall zur Verfügung. Eine Vielzahl von Konfigurationsschritten beginnend von der Grundkonfiguration bis hin zu komplexen Netztopologien mit umfangreichen Sicherheitsfunktionen werden während des Trainings im XT³Lab abgebildet.

Als Voraussetzung zur Teilnahme am XJSec Training sollte der Teilnehmer mit der TCP/IP Protokollfamilie vertraut sein und Grundkenntnisse in der Funktionsweise von Routing-Protokollen besitzen. Erste Erfahrungen mit der Konfiguration von Firewalls anderer Hersteller sind hilfreich aber nicht erforderlich. Es besteht je nach Vorkenntnissen der Trainingsteilnehmern die Möglichkeit, den Verlauf des Trainings anzupassen.

Kursinhalte im Detail:

Junos Software CLI

- Access to the JUNOS CLI
- CLI Operational Mode and Configuration Mode
- JUNOS Software Overview
- Software Installation and Upgrade Procedures
- Initial System Configuration

Interface Configuration and Troubleshooting

- Interface Configuration Overview

Routing Protocol Usage

- JUNOS Software Routing Tables and Route Selection Process
- Static Routes
- OSPF

Juniper SRX Hardware Overview

- Branch SRX Serie
- Enterprise SRX Serie
- High-End ISP SRX Serie
- Network Security Manager
- Security Threat and Response Manager

Juniper SRX System Architecture

- Platform Architecture and Components
- Packet Flow and CPU Functionality
- Flow Session Processing
- Software Architecture

Basic Configuration

- Initial Configuration Steps
- CLI Security Configuration Hierarchy

High Availability

- HA Cluster Terminology
- Redundancy Groups and Interfaces
- Failover Scenarios
- Configuration
- Operation and Troubleshooting

Security Zones

- Zone-based Network Segmentation
- Zone Definition
- Configuration and Interface Assignment
- Monitoring of Security Zones

Screening Functionality

- Types of Attacks
- Attack Handling (Reconnaissance, DoS, Suspicious Packets)
- Applying Screens
- Monitoring and Troubleshooting

Security Policies

- Functionality and Default Behavior
- Policy Match Conditions and Actions
- Verifying Policy Operation

Address Translation

- NAT Overview
- Next Generation NAT
- Policy NAT Interaction
- Flavours of NAT
- NAT Rulesets and Rules
- Operation and Troubleshooting

Virtual Private Networks

- Site-to-Site IPsec VPNs
- Remote Access VPNs
- Dynamic VPN Functionality
- Operation and Troubleshooting