CSNE COURSE OUTLINE

Certified Stormshield Network Expert

Introduction

The aim of this training course is to present the advanced features of the Next Generation Firewall / Stormshield Network Security UTM product.

Target audience

IT managers, network administrators and IT technicians who have obtained CSNA certification.

Learning objectives

At the end of the course, and after revising basic principles, trainees will be able to:

- Use the advanced features of the GUI,
- Accurately configure the intrusion prevention engine,
- Set up a PKI and transparent authentication,
- Set up a certificate-based IPSec VPN,
- Create a high availability cluster.

Venue, duration and registration

Stormshield offers training programs at its offices in Paris, Lille and Lyon.

Our instructors may also travel to conduct on-site training sessions if there are at least 5 trainees.

Stormshield also relies on its distribution network and training partners to conduct courses.

The Expert training course takes place over three consecutive days over 21 hours. Trainees are expected to turn up at 9.30 a.m. on the first day of the course and at 9 a.m. on the following days (unless otherwise indicated by the instructor or Stormshield). All registration requests have to be sent to your Stormshield Network-certified training center (SNTC) or to Stormshield's training department (training@stormshield.eu). The maximum class size is 8 trainees per session. Training material will be provided for each trainee.

Requirements and hardware

The trainee must have passed the CSNA exam within the 3 years prior to the CSNE course.

Good TCP/IP knowledge (routing, phases in the establishment of a TCP connection, structure of an IP packet, etc.).

This course is reserved for those who have already obtained Administrator certification (CSNA).

Before conducting the exercises suggested in the course, trainees should be equipped with a laptop on which a Windows operating system (physical or virtual with bridge access) with administrator privileges has been installed in order to do the exercises, as well as the following programs: Firefox, PuTTY (or any other SSH client), WinSCP (or an equivalent SCP client), Wireshark, VirtualBox or Vmware equivalent (Vmware player or Vmware workstation).

Detailed description

Day 1

- Detailed presentation of the Stormshield Network intrusion prevention engine
  o Differences between intrusion prevention and detection
  o Intrusion prevention engine
  o The various types of scans
  o Application and protocol profiles
- Public Key Infrastructure
  o What is cryptography?
  o Types of encryption
  o PKI Stormshield Network
  o Creating a certificate authority, user certificate and server certificate

Day 2

- SSL Proxy
  o Operating principle
  o SSL proxy settings
- Advanced IPSec VPN
  o The NAT traversal mechanism and detailed operation
  o Dead Peer Detection (DPD) support
  o Star / spoke to spoke VPN
  o NAT in IPSec
  o IPSec VPN architecture with a backup tunnel
  o Configuring a site-to-site VPN with certificates
  o VPN for Mobile

Day 3

- GRE and GRETAP
  o Operating principle
  o Configuration and setup
- Transparent authentication
  o Operating principle
  o SPNEGO authentication method
  o SSL certificate authentication method
- High Availability
  o Operating principle
  o Wizard for creating and configuring HA clusters
  o Configuring network interfaces
  o Advanced properties

Certification exam

Certification consists of an exam carried out online (2 hours 10 minutes, 90 questions).

The minimum score required in order to obtain the certification is 70%.

Access to the exam automatically opens the day after the end of the course on the https://institute.stormshield.eu platform and will remain open for three weeks. In the event of a failure or inability to sit for the exam within this time frame, a second and last attempt will automatically open with immediate effect for an additional week.