CSNTS COURSE OUTLINE

Certified Stormshield Network Troubleshooting & Support

Introduction

The aim of this course is to explain the use of the tools and methods to gather the necessary information for examining and correcting issues using the command line interface (CLI) on Stormshield Network UTM products.

It targets employees from organizations that are seeking to attain the highest Stormshield partnership level as well as candidates aiming to become support engineers or expert trainers on our UTM products.

Target audience

IT managers, network administrators and IT technicians.

Learning objectives

Trainees attend a classroom training session that incorporates both theory and practice.

Trainees are given a printed training book, composed of the theoretical course and the labs.

In order to practice, they benefit from a complete technical environment.

Trainees will have access to all the training book's updates for 3 years on https://institute.stormshield.eu, as well as to a virtual environment which will enable them to do the labs again on their own.

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

- understand the organization of the file system as well as the daemons and processes on a Stormshield Network appliance
- explore the configuration and diagnose anomalies based on appliance logs
- analyze and diagnose network configuration and routing
- capture and examine network traffic
- analyze and diagnose network traffic that has been processed by a security policy
- identify processes that have been applied to current connections
- produce summaries of adapted, comprehensive and usable information
- configure and diagnose IPSec VPN policies
- analyze and diagnose high availability configurations
- analyze and diagnose configurations with authentication
- analyze and diagnose configurations with proxies (explicit and implicit)

Venue, duration and registration

Stormshield offers training programs in France, Germany, Italy, Spain, Poland, Hungary, Norway, UK, UAE, APAC, Africa… Our instructors may also travel on-site to conduct training sessions if there are at least 4 trainees.

The Troubleshooting & Support course takes place over four consecutive days over 28 hours. Trainees are expected to turn up at 9.30 a.m. on the first day of training 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 Stormshield's training department (training@stormshield.eu). The maximum class size is 6 trainees per session. Training material will be provided for each trainee.

Requirements and hardware

Trainees must hold a valid CSNE certification.

In-depth knowledge of TCP/IP and UNIX shell.

Before conducting the exercises suggested in the training 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, 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

- Introduction
- Operating system and related UNIX commands
  - Methods of accessing the shell and settings
  - SSH: features
  - File system and associated commands
  - Folders and associated commands
  - System and user environment
  - Files and associated commands
- Logs
  - Local logs: location, characteristics, syntax and categories
  - Associated commands
  - Configuration files
  - Logd, logctl, logging of kernel messages
- Configuration files
  - Folders, structure and general syntax
  - Backups (*.na), deckbackup, tar
  - Default configuration
- Network and routing
  - Network interface settings
  - Bridges and associated commands

- Routing: routing functions and their priorities
- Default routes and static routes
- Gatemon and router objects
- Dynamic routing
- Related commands, route display
- Verbose mode

- Traffic capture and analysis
  - Introduction and tips
  - General syntax and arguments
  - Common filters
  - Examples with explanations and preparations for making good captures
  - Traffic analysis using tcpdump (TCP, UDP/icmp traffic)

Day 2

- Daemons and processes
  - List and role
  - Monitoring daemon
  - Related commands
- Objects
  - Object syntax
  - Dynamic objects
- ASQ: stages in the analysis
  - Step- by-step analysis of network layers
  - Associated commands
  - Global parameters
  - Profiles and special settings
  - Asynchronous ASQ: various cases and watermarking
  - ASQ verbose mode
- ASQ: security policy
  - Configuration files and folders, rule syntax
  - Filter: associated commands
  - Filter: examples of loaded rules (action, inspection level, plugins, PBR, QoS, interfaces, proxy)
  - Filter: translation of groups and lists
  - NAT: recaps (dynamic NAT, port-based static NAT, static/bimap NAT, no NAT)
  - NAT: associated commands
  - NAT: syntax of loaded rules
- ASQ: Stateful and state tables
  - Table of protected addresses
  - Host table
  - Connection table: examples of connection states (NAT, vconn, FTP plugin, async, lite...)

- FTP: synthetic case study
    - Passive and active mode mechanisms
    - Necessary filter rules

Day 3

- Eventd: event manager
- IPSec VPN
    - IKE/IPSec Stormshield Network implementation
    - Configuration files
    - Security policy (SPD, SA)
    - IKE negotiations
    - Negotiations: Main and aggressive mode
    - ISAKMP and IPsec SA
    - IKE proposals
    - Particularities: NAT-T, DPD, Keepalive, SharedSA, None policy, SPD Cache
    - Associated commands
    - Analysis of an IPSec-SA
    - Logs
    - "Delete SA" notifications
    - ISAKMP traffic capture and analysis
    - Particularities of dynamic peers
    - Verbose mode and common errors

Day 4

- PKI & Certificates
    - Recaps and global directives
    - CA directory
    - Configuration tips
    - Certificate verification
- High Availability
    - General points
    - Configuration files
    - Related commands
    - Activation phases, management of network interfaces
    - Processes and traffic involved
    - Replications/synchronization
    - Events and HA logs
- Authentication and users:
    - User databases
    - Internal LDAP base structure
    - User base configuration files
    - Mapped attributes
    - Importing/exporting the internal LDAP base in LDIF
    - Internal LDAP base's verbose mode
    - Authentication methods: LDAP/AD, Kerberos, Radius, SSL, SPENEGO, SSO
    - Multi-user mode

- Configuration files in the authentication module
  - Associated commands
  - Verbose mode on the authentication module and the SSO agent
  - Configuration of the captive portal in HTTP
- Proxies
  - General points
  - Explicit HTTP proxy
  - Implicit / transparent HTTP proxy
  - Implicit / transparent SMTP, POP3 and FTP proxy
  - Implicit SSL proxy

Certification exam

Certification consists of an exam carried out online (3 hours 30 minutes, 60 questions).

The exam contains MCQs and open questions on features, settings and advanced troubleshooting methods to be implemented in order to exhaustively respond to clients' incident reports.

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 six months. In the event of a failure or inability to sit for the exam within this timeframe, a second and last attempt will automatically open with immediate effect for an additional week.