

StoneGate Training Program

Course Outline

StoneGate SSL VPN Course v.1.2

StoneGate SSL VPN Fundamentals and Implementation

In this course, **StoneGate SSL VPN**, the student will learn the basics of SSL VPN, including where and when SSL VPN communication should be used. **StoneGate SSL VPN** course is a two-day introduction to the world of SSL VPN and it will give the students an overview of all the major features of StoneGate SSL VPN.

The course will be divided into units each containing a presentation on a specific topic and a classroom exercise, which will exemplify the theoretical part of the unit.

Course Goals

Upon completion **StoneGate SSL VPN** course, student should know the basic StoneGate SSL VPN and be able to configure and implement secure resource access via StoneGate SSL VPN access point using user authentication.

Student should understand the principles of dialoguing with the GUI and know how to configure and create the elements (users, user storages, web- and tunnel resources, tunnel sets, access rules etc.) necessary for setting the SSL VPN to function according to the access policy to be applied.

Student should also understand the role of SSL VPN product and be able to explain different deployment options for SSL VPN installations.

Student should know the different ways to enable user authentication using proprietary StoneGate Authentication methods or external authentication services. Student should also understand the difference between user storage location and user directory service.

Finally student should be able to locate and read SSL VPN logs and alerts. Student should also be able to monitor the StoneGate SSL VPN system status, manage logs and run basic reports on SSL VPN activity using Administration Console.

Course Objectives

Upon completing **StoneGate SSL VPN** course, student is able to:

- Explain basics of SSL VPN technology
- Explain three different SSL VPN deployment scenarios
- Understand the role of an SSL VPN in the overall security framework
- Install and configure a StoneGate SSL VPN system
- Explain the functioning of the SSL VPN system
- Create web and tunnel resources
- Create new access rules
- Create user accounts in internal user storage
- Configure client firewall
- Use assessment tools
- Configure abolishment
- Examine and manage logs and alerts
- Generate statistical reports from the log data

Course Program for Two-Day Training

Day 1

- Introduction to SSL VPN
- StoneGate SSL VPN Architecture
- **LAB 1:** StoneGate SSL VPN initial configuration
- Web Console Overview
- **LAB 2:** Remote upgrade and license installation
- User Account Management
- **LAB 3:** Defining User Accounts and Storage
- StoneGate SSL VPN Authentication
- **LAB 4:** Managing User Authentication
- Web and Tunnel Resources
- **LAB 5:** Configuring Web Resource Access
- **LAB 6:** Configuring Tunnel Resources
- **LAB 7:** Configuring All Network Access

Day 2

- Logs and Alerting
- **LAB 8:** Logs and Alerting
- Access Client Security (ACS)
- **LAB 9:** Client Firewall
- End-Point Security (EPS)
- **LAB 10:** Assessment
- **LAB 11:** Abolishment
- Monitoring and reporting
- **LAB 12:** Monitoring and reporting

Certification Exam: ***StoneGate SSL VPN Architect (SGSSLA)***

Disclaimer

This document and the contents herein are provided as a convenience to you. The contents of the Course Outline document are provided on "as is" and "as available" basis without any warranties. Stonesoft Corporation does not warrant that this document will be without inaccuracies or contextual or typographical errors. Stonesoft Corporation reserves the right to revise this document or withdraw access to it at any time without prior notification.

Stonesoft Corporation

Itälahdenkatu 22 A
FIN 00210 Helsinki, Finland
tel. +358 9 476 711
fax +358 9 4767 1234
www.stonesoft.com

Stonesoft Inc.

1050 Crown Pointe Parkway,
Suite 900, Atlanta, GA 30338, USA
tel. +1 866 869 4075
fax +1 770 668 1131
info.americas@stonesoft.com