深信服智安全技术认证
SCSA 讲师笔试大纲

2018年4月

深信服智安全
SANGFOR SECURITY

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

深信服智安全技术认证介绍

深信服智安全技术认证是面向网络运维、安全解决方案、安全架构设计类人员的专业技术认证，主要涉及网络基础、安全基础、渗透测试、应急响应、安全解决方案类的，是对企业网络安全知识和技能的考察和认证。

深信服智安全技术认证强调新的网络安全理念："可视是安全的基础"、"安全技术应当转向持续检测和快速响应"、"安全交付应该简单易用"，在新的理念指导企业建设"安全可视、安全感知、全网互联的企业网络安全架构"，并结合一些典型的场景及案例，帮助工程师理解企业网络安全场景和需求，了解如何全面防御新型攻击手段和如何规避企业安全风险。

深信服智安全技术认证包括安全工程师认证（SCSA），安全资深工程师认证（SCSP）和安全专家认证（SCSE），覆盖企业网安全基础解决方案到企业网安全架构设计 3 个等级的技术认证。

通过 SCSA 级别的认证（Sangfor Certified Security Associate）可以有效证明该认证人员具备以下能力：

- 具备网络运维、网络安全、应用层协议相关的基础知识
- 能够根据企业的业务需求，基于业界主流的安全产品和技术手段有效的制定安全解决方案和企业最佳实践
- 能够熟练的使用和操作上网行为管理、下一代防火墙、SSL VPN等主流安全产品
- 能够诊断企业网络中常见网络和安全问题并找到相应的解决方案

认证考试形式和结构

一、试卷满分及时间

试卷满分为 120 分，考试时间为 90 分钟，80分通过

二、考试形式

在线考试

三、答题方式

闭卷

四、试卷内容

知识结构	试题比例
网络基础	15%
信息安全基础	5%
数据传输安全	15%
上网行为安全	30%
边界安全	20%
移动接入安全	15%

五、试卷题型

题目类型	题目数量	分值
单选题	60 题	每题 2分

六、试卷内容范围

- **网络基础考试内容：**
  - ✓ TCP/IP基础知识
  - ✓ 以太网帧结构/IP编址/ICMP协议/ARP协议/传输层协议/数据转发过程
  - ✓ Wirshark数据包捕获和分析
  - ✓ 交换网络基础
  - ✓ IP路由基础/静态路由基础/距离矢量路由协议-RIP/链路状态路由协议-OSPF
  - ✓ VLAN技术原理
  - ✓ 基于源IP地址NAT技术/基于目的IP地址NAT技术/双向NAT技术/NAT应用场景
  - ✓ DNS协议/DHCP协议/HTTP协议/SNMP协议
  - ✓ 掌握数据包在传输过程中五元组的变化情况
  - ✓ 掌握网口混杂模式的作用
  - ✓ 掌握TCP协议SYN/FIN/RST数据包的作用
  - ✓ 掌握常见协议基础知识，如DNS/HTTP/SNMP/LDAP
  - ✓ 掌握HTTP头部字段和响应字段的作用
  - ✓ 了解HTTPS协议的关键字段的作用
  - ✓ 掌握访问网站的全过程以及过程中涉及的网络技术
  - ✓ 掌握常见应用使用的端口，如SSH/远程桌面/MYSQL等

- **信息安全基础考试内容：**
  - ✓ 了解企业安全建设的需求变化
  - ✓ 掌握企业安全建设的基本要素
  - ✓ 了解网络通信中面临的四种网络威胁
  - ✓ 掌握对称加密、非对称加密、数字证书的基础技术原理

- **数据传输安全考试内容：**
  - ✓ 掌握标准IPSEC VPN基本技术原理
  - ✓ 掌握AH/ESP协议的区别
  - ✓ 掌握传输模式和隧道模式的封装格式

- ✓ 了解主模式和被动模式的区别
- ✓ 掌握NAT环境与IPSEC VPN同时存在的冲突的解决方案
- ✓ 掌握SANGFOR VPN基本技术原理及优势
- ✓ 掌握SANGFOR VPN建立连接过程、
- ✓ 掌握隧道内NAT、隧道间路由、本地子网的作用
- ✓ 掌握移动PDLAN的通信原理

- **上网行为安全考试内容：**
  - ✓ 掌握上网行为管理设备的登录方式
  - ✓ 掌握上网行为管理恢复密码和恢复出厂设置的方法
  - ✓ 掌握升级客户端的使用方法
  - ✓ 了解上网行为管理设备的登录、升级、认证、数据中心的端口
  - ✓ 掌握上网行为管理的各种部署模式的适用场景和特点
  - ✓ 掌握上网行为管理的端口映射和发布服务器的作用
  - ✓ 掌握上网行为管理防火墙规则使用方法
  - ✓ 掌握上网行为管理不需要认证、密码认证的配置
  - ✓ 掌握上网行为管理跨三层识别的配置及注意事项
  - ✓ 了解识别https网站的工作原理
  - ✓ 掌握上网策略策略不生效的排查步骤（包括准入策略 上网权限策略）
  - ✓ 掌握共享接入管理和终端接入管理的应用场景及功能
  - ✓ 掌握共享接入管理识别终端的方法
  - ✓ 了解上网行为管理流控的和传统流控的的区别
  - ✓ 掌握惩罚通道的使用方法
  - ✓ 掌握日志中心的常见功能
  - ✓ 掌握网页版邮箱和客户端邮箱审计的配置方法
  - ✓ 掌握上网行为管理邮件过滤、关键字过滤、SSL内容识别配置的常见问题解决办法
  - ✓ 了解行为感知系统的常见app和部署条件
  - ✓ 掌握日志中心和行为感知系统的联动方式
  - ✓ 掌握外置日志中心的登录和通信方式

- **边界安全考试内容：**
  - ✓ 了解防火墙的发展过程
  - ✓ 掌握区域和接口定义
  - ✓ 掌握下一代防火墙部署方案
  - ✓ 掌握下一代防火墙基本功能
  - ✓ 掌握DOS攻击的原理
  - ✓ 了解IPS和IDS的作用
  - ✓ 了解SQL注入的原理和危害
  - ✓ 了解病毒的传播方式和生命周期
  - ✓ 了解僵尸网络的原理和危害
  - ✓ 了解信息泄露攻击的原理和危害
  - ✓ 了解风险发现和分析功能
  - ✓ 掌握实时漏洞分析原理
  - ✓ 了解威胁情报预警与处置功能

- **移动接入安全考试内容：**
  - ✓ 掌握SSL协议相关的基础技术原理
  - ✓ 掌握SSL VPN的技术原理及应用场景
  - ✓ 掌握SSL VPN中三种常规资源（WEB、TCP、L3VPN）的技术原理及特点、应用特点
  - ✓ 了解SSL VPN中远程应用发布（应用虚拟化技术）技术原理
  - ✓ 掌握SSL VPN中用户、资源、角色之间的关系及作用
  - ✓ 掌握SSL VPN设备/系统的基本部署及网络配置(网关模式、单臂模式）
  - ✓ 掌握SSL VPN多种用户身份认证的基础技术原理及区别（本地认证、硬件特征码、短信认证、外部认证、数字证书）