

## RCNA-security 课程大纲

<b>参培前提条件</b>	RCNA-R&S基础	
<b>课程目标</b>	1、具备安全的基本意识 2、能够承接小型网络中的安全产品的交付，小型网络中的安全产品主要为单台防火墙产品	
<b>课程时长</b>	5天	
<b>课程模块</b>	<b>课程名称</b>	<b>课程内容</b>
<b>信息安全与安全概述</b>	1.1 信息安全概述	信息安全的要素，信息安全部署不到位的威胁与应对 等级保护建设基础知识，等级保护解决方案与建设过程 安全产品部署时的规范性配置要求
	1.2 网络协议概述	TCP/IP、路由交换基础
	1.3 信息安全威胁与防范	安全威胁分类介绍；网络层、应用层、终端安全威胁介绍；DDoS、漏洞、钓鱼、社工、中间人等威胁原理、流程、防御方式介绍；
	1.4 信息安全发展趋势	安全防范基本要素；安全意识；安全发展趋势；
<b>操作系统与主机安全</b>	2.1 操作系统简介	操作系统基础、主机防火墙介绍
	2.2 常见服务器种类与威胁	服务器介绍、分类、服务器安全威胁、防御方法
	2.3 主机防火墙和杀毒软件	杀毒软件介绍、安全补丁等
<b>网络安全基础</b>	3.1 安全产品概述	简述锐捷网络安全产品组成，以及对应分类
	3.2 防火墙产品发展史	发展历史、原理、包过滤、状态检测、会话表等
	3.3 防火墙基础安全功能	安全策略原理、配置；源NAT、目的NAT、一对一、一对多和多对多等形式的NAT；NAT源端口复用
	3.4 应用层安全技术基础	IPS、病毒防护、应用控制
	3.5 防火墙双机热备基础	HA功能简介，工作模式与区别，HA切换条件及逻辑，HA应用场景
<b>加解密与应用</b>	4.1 加解密技术原理	加密概念；对称非对称原理、应用；
	4.2 公钥基础设施	证书、PKI原理与应用
	4.3 加密技术应用	VPN概念介绍；L2TP、GRE、IPSec、SSL VPN基本原理、配置；IPSec、SSL VPN实验
<b>基础安全运维</b>	5.1 安全运营简介	安全运营概念介绍；安全运营具体内容、案例、工具介绍；
	5.2 数据取证与分析技术	数据取证概念、流程、工具； 数据分析概念、流程、方法；
	5.3 网络安全应急响应	信息安全应急响应技术概述、理念演变、技术体系介绍；安全加固概念、流程介绍；安全评估、方案、实施介绍；
	5.4 案例分析	信息安全规范，安全威胁，安全运营案例实战训练