

目录

1 概述	1
1.1 文件说明	1
1.2 H3CSE SECURITY 认证简介	1
2 考试项目说明	2
2.1 ISF 考试说明	2
2.2 ISF 考试试题分配比例	3
3 考试知识点分布	4
3.1 防火墙技术介绍	4
3.2 SECPATH 防火墙体系结构	4
3.3 SECPATH 防火墙图形化管理平台和日志系统	4
3.4 安全区域	4
3.5 访问控制列表（ACL）	4
3.6 包过滤技术	5
3.7 NAT	5
3.8 报文统计与攻击防范	5
3.9 网页过滤和邮件过滤	5
3.10 用户认证原理与配置	6
3.11 运行模式和双机备份	6
3.12 防火墙典型组网及常见故障诊断	6

1 概述

1.1 文件说明

本文件是 H3C 培训中心发布的 ISF (Implementing Secure Firewalls, 布署安全防火墙系统) 课程的考试大纲。本文件由 H3C 培训中心编写, 主要用于指导考生复习 ISF 课程内容和参加 ISF 中文考试。

1.2 H3CSE Security 认证简介

【H3C 认证安全技术高级工程师】(H3CSE Security) 主要定位于主要定位在从事信息安全产品安装、调试、运行、维护人员。涵盖当今网络安全领域三大热门技术, 共包含 ISF (Implementing Secure Firewalls, 布署安全防火墙系统)、BSVPN (Building Secure Virtual Private Networks, 构建安全 VPN 网络)、AIPSC (Advanced Intrusion Prevention System Configuration, 高级 IPS 系统配置) 三门课程。内容涉及 VPN 网关产品介绍与基本配置、各种 VPN 业务技术原理与配置、加密算法、VPN 常见故障及处理、防火墙体系结构、访问控制列表、包过滤、网页过滤和邮件过滤、防火墙典型组网及常见故障诊断等技术。通过相应的认证考试即可获得由 H3C 公司统一签发的“H3C 认证安全技术高级工程师”(H3CSE Security) 证书。

2 考试项目说明

2.1 ISF 考试说明

ISF (Implementing Secure Firewalls, 布署安全防火墙系统) 考试项目代码为 GB0-500, 对应于 H3CSE Security 培训教材《布署安全防火墙系统》V1.0 及更高版本。

考试要求

H3CSE Security 考试对考生没有特殊要求, 可以直接参加考试。

考试内容

包含但不限于 H3CSE Security 培训教材《布署安全防火墙系统》涵盖的所有内容。考试试题绝大多数来源于教材, 但个别题目可能会超出教材所包含的内容。

考试代码

GB0-500

考试时长

60 分钟

试题数量

50 道单/多项选择题和判断题

通过分数线

你至少须获得 600 分。

请注意: H3C 公司保留在任何时间变更分数线的权利, 并不负有将此变更通知应考者的义务。

参加考试

您可以选择最近的 Prometric 授权考试中心 APTC 报名并参加 GB0-500 的考试。如欲查询最近的考试中心 请访问 Prometric 官方网站: <http://www.prometric.com.cn> 或者向 Prometric 授权考试中心咨询。

2.2 ISF 考试试题分配比例

下面是 ISF 课程各章节相应试题的大致数量：

序号	课程章节名称	出题数量	备注
1	防火墙技术介绍	3	
2	SecPath 防火墙体系结构	3	
3	SecPath 防火墙图形化管理平台和日志系统	3	
4	安全区域	3	
5	ACL	6	
6	包过滤技术	5	
7	NAT	3	
8	报文统计和攻击防范	11	
9	网页过滤和邮件过滤	5	
10	用户认证原理与配置	3	
11	运行模式和双机备份	3	
12	防火墙典型组网及常见故障诊断	2	
总计题数		50	

注意：上表所示之题目数量和比例仅供参考，而不是严格数值。同时，H3C 公司保留在任何时间调整上述题目数量和比例的权利，并不负有将此变更通知应考者的义务。

3 考试知识点分布

下面是 ISF 课程主要的考试知识点分布：

3.1 防火墙技术介绍

- **网络安全基本概念：**要求对网络有一个基本的概念，了解常见的安全威胁、网络安全关注的范围、网络安全设备的分类等
- **防火墙必备的技术范围：**要求掌握防火墙的必备安全特性，包括网络隔离及访问控制、攻击防范、NAT、应用层状态检测、身份认证、内容过滤、安全管理等

3.2 SecPath 防火墙体系结构

- **SecPath 防火墙产品：**SecPath 系列防火墙各产品的性能、基本结构、功能和业务特性、管理方法、适用场合
- **SecPath 防火墙的业务特性：**防火墙的多种攻击防范手段（如 TCP Proxy、内网安全、流量监控、网址过滤、网页过滤、邮件过滤等），ASPF 状态检测技术、多种智能分析和管理工作手段、AAA、NAT、防火墙支持的多种 VPN 业务（如 L2TP VPN、IPSec VPN、SSL VPN、GRE VPN、DVPN 等）、路由能力、QoS 特性、SecPath 防火墙的配置和管理手段等
- **SecPath 防火墙典型应用**

3.3 SecPath 防火墙图形化管理平台和日志系统

- **Web 管理：**Web 管理的特点和功能，配置和执行基本 Web 管理等
- **BIMS 管理：**BIMS 工作原理，BIMS 管理的特点和功能，配置和执行基本 BIMS 管理等
- **VPN Manager 管理：**VPN Manager 管理框架，VPN Manager 管理的特点和功能，配置和执行 VPN Manager 管理等

3.4 安全区域

- **安全区域的概念**
- **安全区域的划分：**接口、网络与安全区域的关系，入方向和出方向，安全区域的优先级等
- **安全区域的配置：**安全区域的创建、修改、优先级设置等

3.5 访问控制列表（ACL）

- **ACL 原理：**ACL 的定义，ACL 的功能和用途，ACL 的分类，基本访问控制列表、高级访问控制列表、基于接口的访问控制列表和基于 MAC 的访问控制列表的工作原理等
- **ACL 配置：**基本访问控制列表、高级访问控制列表、基于接口的访问控制列表、基于 MAC 的访问控制列表的配置，时间段的配置，访问控制列表的信息显示和调试等

3.6 包过滤技术

- **包过滤介绍：**包过滤技术的作用和实现方法等
- **包过滤基本配置：**缺省过滤方式、分片检测及其上下限域值，在接口上应用访问控制列表，包过滤信息的显示与调试等
- **ASPF 原理：**包过滤防火墙的不足，ASPF 的相关概念，ASPF 检测应用层协议的工作原理等
- **ASPF 基本配置：**ASPF 策略的配置及其相关参数的调节等
- **黑名单原理：**定义、功能及相关概念，黑名单列表及其表项的来源，黑名单能过滤的报文类型等
- **黑名单基本配置：**黑名单的使能和禁止，黑名单表项的配置，黑名单信息的显示和调试等

3.7 NAT

- **NAT 的产生背景及其基本概念**
- **NAT 工作原理：**多对多地址转换、NAPT、内部服务器、Easy IP、ALG 等
- **NAT 的配置：**一对一、多对多、NAPT、Easy IP、内部服务器等的配置及其信息显示和调试

3.8 报文统计与攻击防范

- **报文统计的概念和作用**
- **报文统计基本配置：**报文统计的启用和关闭，系统连接数量监控、系统报文比率异常告警检测等、域统计功能、IP 统计功能等的配置，报文统计的信息显示与调试
- **典型网络攻击：**IP 地址欺骗（IP Spoofing）攻、Land 攻击、Smurf 攻击、WinNuke 攻击、SYN Flood 攻击、ICMP Flood 攻击、UDP Flood 攻击、地址扫描与端口扫描攻击、Ping of Death 攻击等的攻击原理及其防范措施
- **攻击防范基本配置：**主要攻击防范功能的配置及其参数调节，攻击防范功能的信息显示和调试

3.9 网页过滤和邮件过滤

- **网页过滤和邮件过滤的用途和功能**
- **网页过滤配置：**使能和关闭网页过滤，配置默认过滤行为，配置过滤地址，保存和装载网页地址过滤文件，网页地址过滤显示与调试；使能或关闭网页内容过滤功能，配置网页内容过滤关键字，保存或装载网页内容过滤文件，网页内容过滤显示与调试
- **邮件过滤配置：**使能或关闭邮件地址过滤功能，配置默认过滤行为，配置邮件过滤地址，

保存或装载邮件地址过滤文件；使能或关闭邮件主题过滤功能，配置邮件主题过滤关键字，保存或装载邮件主题过滤文件；使能或关闭邮件内容过滤功能，配置邮件内容过滤关键字，保存或装载邮件内容过滤文件，使能或关闭邮件附件过滤功能，配置过滤邮件附件名，保存或装载邮件附件过滤文件，邮件过滤显示与调试等

3.10 用户认证原理与配置

- **AAA:** AAA 的定义，认证、授权和计费功能，AAA 基本配置、信息显示和调试等
- **RADIUS:** RADIUS 的概念和功能，协议部件，工作原理，报文结构，组网应用，用 RADIUS 实现 AAA，RADIUS 基本配置、信息显示和调试等
- **HWTACACS:** HWTACACS 的概念和功能，协议部件，工作原理，报文结构，组网应用，用 HWTACACS 实现 AAA，HWTACACS 基本配置、信息显示和调试等

3.11 运行模式和双机备份

- **SecPath 系列防火墙的工作模式:** 路由模式、透明模式、混杂模式，以及它们的工作原理
- 透明模式的基本配置及信息显示和调试
- 双机热备与负荷分担的工作原理与配置

3.12 防火墙典型组网及常见故障诊断

- 防火墙常见应用和组网
- 防火墙常见故障诊断：熟悉常见故障现象，了解常规故障诊断流程

H3C 培训中心

2007 年 4 月