目录

1. 文件说明

本文件是《部署内容安全系统》的考试大纲，主要介绍《部署内容安全系统》的考试内容。本文件由新华三大学编写，主要用于指导参加 H3CSE-Security(新)认证考试的考生进行复习和考试准备。

2. 考试项目说明

2.1 考试介绍

考试对象

本考试对考生没有特殊要求，任何没有被新华三明确禁止的人均可以直接报名参加考试。

考试内容

包含但不限于《部署内容安全系统》课程涵盖的内容。考查知识点绝大多数来源于教材和培训，但个别题目可能会超出教材和培训所包含的内容。

考试代码

GB0-550

考试时长

60 分钟

试题数量

50 道单/多项选择题。

通过分数

总分 1000 分，至少应获得 600 分才能通过。

2.2 参加考试

本认证考试由 ATAC 考试平台代理。如果希望参加此认证考试，您可以通过登录 ATAC 官网 www.atacchina.com 查询并联系考点报名。

注意：本文档提供的信息仅供参考，H3C 保留在不通知考生的情况下调整考题、时间和分数线的权利。

考试知识点分布

下面是 GB0-550 考试中的考试知识点分布。

部署内容安全系统概述

- **部署内容安全系统概述：**内容安全概念，内容安全所面临的风险。
- **内容安全风险：**DDOS 攻击概念、原理、危害，WEB 应用所面临的风险，漏洞的概念以及安全危害。
- **内容安全需求：** 数据交换安全需求内容，运维安全现状、运维安全需求内容，数据库安全风险、数据库安全需求内容。

运维审计系统

- **运维审计系统的基本工作原理：**运维现状，设备基本实现原理。
- **运维审计系统的设备类型及部署方式：**单机部署、双机部署方式如何进行部署。
- **运维审计系统的用户验证方式：**用户的类型分类，认证方式分类。
- **运维审计系统的设备运维：**设备支持的运维协议，如何在设备上创建各类型运维的对象，访问权限、命令权限的创建，双人授权，命令复核配置。
- **运维审计系统的会话审计：**各种方式的运维审计记录如何查看，如字符会话、图形会话、文件传输。
- **运维审计系统的自动运维：**脚本配置，自动改密配置。
- **典型配置举例：**常见运维方式的审计配置，如 ssh 运维 linux 服务器。

WEB 应用防火墙

- **WAF 产品基础：**产品基本特点，设备优势，系统构架。
- **WAF 设备管理：**设备管理方式，登陆设备方式，特征库升级如何操作，许可证导入如何操作。
- **WAF 工作原理及部署模式：**透明模式、反向代理模式、旁路监听/阻断模式、混合模式如何部署，各个部署模式下设备的工作原理、各个部署模式下设备如何配置。
- **WAF 功能介绍及配置：**策略引用配置，WEB 安全策略配置，包括协议安全配置、内容安全配置、特征库配置、例外配置、webshell 侦听配置、入侵防护策略配置、防 DDOS/CC 攻击配置、黑白名单配置、网络功能配置和高可用性配置。

异常流量清洗系统

- **什么是 DDOS 攻击：**DOS、DDOS 攻击基础概念，DDOS 攻击的危害。

- **常见的 DDOS 攻击及攻击原理简介：**DDOS 攻击的分类，常见 DDOS 攻击的原理：ping of death、icmp flood、syn flood、ack flood、rst flood、fin flood、land flood、smurf、fraggle 等。
- **AFC 与 AFD 系统概述：**AFC、AFD 基本概念，有哪些主要的功能模块。
- **AFC 与 AFD 部署方案：**包含常见部署方案的组网、部署思路、实现原理，如：单机单通道串联、单机多通道串联、双机主备串联、多机集群串联、BGP/OSPF 三层回注等。
- **AFC 与 AFD 防御原理：**防御机制、规则顺序、针对各种攻击的防范原理。
- **AFC 与 AFD 配置：**AFC、AFD 常见功能模块配置，如各种部署方案在设备上如何配置。

数据库审计系统

- **概述：**为什么需要部署数据库审计系统，数据库有哪些安全需求，业务有哪些安全需求。
- **数据库审计原理：**数据库审计系统的实现原理，如何形成审计记录，数据库审计系统能够审计哪些数据库。
- **数据库审计系统部署：**如何部署数据库审计系统，包括网络配置、部署模式的选择、监听配置、业务系统配置、如何进行审计、数据归档和回档的配置、终端录像等。

漏洞扫描系统

- **概述：**漏洞存在什么样的安全风险，漏洞扫描系统支持对哪些模块的安全评估。
- **漏洞扫描原理介绍：**漏洞扫描的实现原理，包含主机在线监测、icmp echo 扫描、broadcast icmp 扫描、non-echo icmp 扫描、主机扫描技术、端口扫描技术、开放扫描、半开放扫描、隐藏扫描技术。
- **设备类型及功能配置：**基础网络配置、资产配置、主机扫描任务配置、主机弱口令扫描任务配置、数据库扫描任务配置、web 扫描任务配置、web cookie 录制扫描任务配置。
- **设备维护：**设备基本维护，如管理口 IP 忘记如何处理、扫描任务创建失败、目标主机不能被扫描等。

安全隔离与信息交换系统

- **网络隔离现状：**隔离技术的发展过程、安全隔离与防火墙的区别。
- **安全隔离与信息交换系统概述：**网闸隔离技术的技术原理，网闸所应具备的安全要点，适用组网和部署模式。
- **网闸的系统结构：**网闸的系统构架，包含数据迁移控制单元、私有协议、管理控制中心等。
- **网闸的主要功能：**包含受控通道、http 应用模块、邮件应用模块、文件访问模块、文件同步模块、数据库访问模块、数据库同步模块等。

- **网闸的功能配置：**基本功能的配置以及主要功能的配置，如设备管理、网络相关配置、HA 配置、负载均衡配置、通道配置、策略配置、文件同步配置等。
- **网闸的维护**：如忘记密码如何处理，忘记管理 IP 如何处理，以及常用注意事项。

新华三大学

2019 年 5 月