

目录

1. 文件说明.....	2
2. 考试项目说明.....	2
2.1 考试介绍.....	2
2.2 参加考试.....	2
考试知识点分布	4
网络安全概述	4
防火墙基础技术	4
防火墙用户管理	4
防火墙安全策略	4
网络地址转换技术	5
VPN 原理及配置	5
DPI 技术.....	5
应用控制技术	6

1. 文件说明

本文件是《构建 H3C 中小企业安全网络》的考试大纲，主要介绍《构建 H3C 中小企业安全网络》的考试内容。本文件由新华三编写，主要用于指导参加 H3CNE-Security 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《构建 H3C 中小企业安全网络》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

GB0-510

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

H3C 认证考试笔试由 H3CHOPE、ATAC 和 Prometric 考试平台代理。

A、 点击如下链接：<https://www.h3chope.com/EC/SearchEC.aspx?type=1>，查询 H3CHOPE、ATAC 考点并联系报名。

B、 登录 Prometric 官网 <http://www.prometric.com.cn> 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 GB0-510 考试中的考试知识点分布。

网络安全概述

- **TCP/IP 协议基础：**OSI 模型、TCP/IP 模型的层次结构、TCP 三次握手、传输层协议等。
- **TCP/IP 协议安全：**IPV4 安全隐患、TCP/IP 协议栈常见安全风险、线路侦听、MAC 欺骗、IP 欺骗攻击、Smurf 攻击、IP 地址扫描攻击、端口扫描攻击、TCP 拒绝服务、WEB 攻击等。
- **网络安全威胁方式：**主动攻击、被动攻击等。

防火墙基础技术

- **防火墙的发展背景及技术演进：**包括什么是防火墙、防火墙的分类、防火墙技术演进等。
- **防火墙应具备的基本功能：**路由交换功能、NAT、为什么需要攻击防范，各种攻击的原理和表现方式、在设备上如何配置防攻击、双机热备的原理和工作方式、日志审计等。
- **防火墙性能衡量指标：**吞吐量、时延、新建连接数、并发连接数等。
- **防火墙的组网方式：**二层模式的原理、三层模式的原理、防火墙的管理、配置防火墙的管理、文件管理、升级、License 管理、防火墙基本配置流程等。

防火墙用户管理

- **AAA 技术原理：**什么是 AAA、AAA 认证方式、RADIUS 认证、RADIUS 报文结构、RADIUS 属性、RADIUS 配置、HWTACACS 认证、HWTACACS 配置、LDAP 认证、LDAP 配置等。
- **防火墙用户分类：**设备管理类用户、网络接入类用户。
- **防火墙用户管理及应用：**基于域的用户管理、基于 ISP 域的 AAA 实现、本地用户配置、本地用户组配置、管理类用户的本地认证和授权配置、接入类用户的 RADIUS 认证和授权配置、上网类用户的认证和授权配置等。

防火墙安全策略

- **包过滤技术：**什么是包过滤、ACL 分类、ACL 规则的匹配顺序、包过滤配置任务、配置基本 ACL、配置高级 ACL、配置二层 ACL、接口上应用 ACL 包过滤等。
- **安全域：**什么是安全域、安全域与接口关系、安全域配置注意事项、安全域配置任务、安全域的显示等。
- **防火墙转发原理：**流与会话、会话的创建、会话表项与长连接、配置会话管理、报文转发流程等。

- **防火墙安全策略：**什么是安全策略、安全策略发展历程、安全策略优势与规则、规则的过滤条件与匹配顺序、安全策略流程、安全策略配置任务、配置地址对象组、配置服务对象组、配置安全策略等。

网络地址转换技术

- **NAT 概述：**NAT 的技术背景、公有地址和私有地址、NAT 技术原理、NAT 术语、NAT 分类、NAT 技术的优缺点等。
- **动态 NAT：**动态 NAT（NO-PAT 模式）原理与实现、动态 NAT（NO-PAT 模式）的配置、动态 NAT（PAT 模式）原理与实现、动态 NAT（PAT 模式）的配置、动态 NAT（Easy IP 模式）原理与实现、动态 NAT（Easy IP 模式）的配置等。
- **内部服务器：**内部服务器的原理、内部服务器的实现、内部服务器的配置等。
- **静态 NAT：**静态 NAT 原理、静态 NAT 的实现、配置静态 NAT 等。
- **NAT ALG 功能：**NAT ALG 原理、NAT ALG 实现。

VPN 原理及配置

- **VPN 概述：**包括 VPN 的关键概念术语、VPN 的分类、主要 VPN 技术概述等。
- **GRE VPN：**GRE 封装格式、GRE VPN 工作原理、GRE 如何穿越 NAT，在命令行方式下配置 GRE VPN、在 WEB 方式下配置 GRE VPN 等。
- **L2TP VPN：**L2TP 概念和术语、L2TP 拓扑结构、L2TP 协议封装、L2TP 协议操作与多实例、在命令行下配置 L2TP、在 WEB 方式下配置 L2TP 等。
- **IPSec VPN：**IPSec VPN 的概念和术语、IPSec VPN 的体系结构、AH 协议、ESP 协议、IKE 与 IPSec 的关系、IPSec VPN 穿越 NAT、在命令行下配置 IPSec VPN、在 WEB 方式下配置 IPSec VPN、IPSec 的故障排除。
- **SSL VPN：**SSL 协议的发展过程、SSL 的工作模型与体系结构、SSL 协议中的记录层、SSL 握手协议、SSL VPN 的功能与实现、SSL VPN 的配置等。

DPI 技术

- **DPI 技术背景：**安全威胁、什么是 DPI、DPI 特征库、DPI 业务、DPI 基本工作原理等。
- **DPI 技术原理：**IPS 技术、IPS 特征、IPS 动作、防病毒技术、病毒特征与动作、URL 过滤、过滤规则、规则匹配方式、文件过滤技术、数据过滤特性等。
- **DPI 技术配置：**DPI 基础配置、License 申请、特征库升级、IPS 配置、防病毒配置、URL 过滤配置等。

应用控制技术

- **应用控制技术概述：**应用识别面临的挑战。
- **应用过滤：**应用精准识别、精细应用授权、ACG 网关应用识别和审计原理、应用审计配置等。
- **带宽管理：**带宽管理的概念、全局流量管控、带宽利用率、带宽管理匹配原理、带宽管理配置等。
- **日志报表：**应用流量分析、日志的类型、日志信息的输出、网站访问日志、应用审计日志、日志分析与管理平台、深度数据挖掘等。
- **用户和认证：**用户身份发现、匿名用户、本地用户、微信认证、认证策略等。

新华三人才研学中心

2021 年 10 月