

## 课程 201——FortiGate 安全产品系列 I——管理和内容检测

### 概述:

该课程是两天的课堂式培训，详细地讲述配置基础和故障定位的知识，对于每天的 FortiGate 维护来说是非常有价值的。

学生通过课程中的实验可以学到真实环境中的配置，能够将 FortiGate 最常用的功能应用到各种规模的企业。

学生同时还强化了如何将 FortiGate 产品集成到现有环境，以及如何操作以提高和优化性能来保护企业的资产。

**认证:** 该课程帮助学生通过如下认证考试:

**Fortinet Certified Network and Security Associate (FCNSA)**

**Fortinet Certified Network and Security Professional (FCNSP)**

该课程的目标:

- 通过图形界面和命令行可以完成系统设置和网络配置，管理账户的创建，系统的备份，报警的监控，设备性能和工作状态，FortiGuard 服务和升级，系统软件的管理等等 FortiGate 的维护和管理工作。
- 使用 FortiAnalyzer 对 FortiGate 设备进行日志和监控状态。
- 根据内容检测、时间计划，源和服务类型，记录非授权的服务等配置防火墙策略
- 配置防火墙策略中的认证、虚拟 IP、IP 地址池和流量整形
- 创建保护内容表来实现 FortiGate 的防病毒服务的功能，比如文件类型阻断、灰色软件扫描、文件隔离和病毒扫描。
- 采用 FortiGuard 的反垃圾邮件服务和禁忌词汇来创建邮件过滤策略
- 使用 URL 过滤、内容过滤和 FortiGuard 的 Web 分类服务来创建 Web 过滤策略。
- 配置即时通讯和 P2P 流量的内容归档和过滤
- 理解 NAT/路由模式和透明模式之间的区别

参与人员的要求:

- 中级的网络安全经验
- 对核心网络的安全和防火墙概念有充分地了解

适用的人群:

每天负责维护和管理 FortiGate 产品的工程师

课程章节：

第一天的课程：

第一章：概述和系统设置

- FortiGate 产品概述
- 管理
- 系统的仪表盘
- 网络拓扑
- 接口 IP 地址的设置
- DHCP 的中继和服务器
- 静态路由
- 命令行

第二章：日志和报警

- 系统日志设置
- 日志信息的优先级
- 事件日志
- 内容检测的日志
- 流量日志
- 查看日志文件
- 内容归档
- 报警邮件
- FortiAnalyzer 设置
- SNMP

第三章：维护

- 配置备份
- Fortinet 的服务注册
- FortiGuard 升级网络
- 防病毒和 IPS 特征库的升级
- 系统软件的维护、升级和支持双系统文件
- FortiGuard 中心
- 系统状态的监控
- 防火墙会话表

第四章：防火墙策略——基础

- 防火墙策略概况
- 状态检测
- 防火墙地址——IP 和 FQDN
- 防火墙服务的概述

- 防火墙服务的定义
- 防火墙的时间表
- IPV6 和支持多播

## 第五章：防火墙策略——认证

- 认证
- 用户的类型
  - 本地
  - Radius
  - LDAP
  - FSAE
  - X.509 认证
- 认证的应用
  - 防火墙策略
  - SSL VPN
  - IPSec VPN
  - PPTP 和 L2TP
  - 管理员的登录
  - FortiGuard 的 Web 过滤的跳过

## 第六章：防火墙策略——选项

- 防火墙策略：标准的，IP 地址池和固定端口
- 虚拟 IP：静态 NAT 和负载均衡
- 差分服务
- 流量整形和优先级
- 保护内容表

## 第二天课程

## 第七章：防病毒

- 防病毒概述
- 引擎和特征值的升级
- 防病毒扫描
- 防病毒引擎
- 扫描非标准端口
- 触发的命令
- 启发式扫描
- 替代信息
- 灰色软件、间谍软件
- 文件类型阻断和允许通过
- 客户端的舒适
- 超大文件

- 病毒扫描的归档
- 解压缩的限制
- 隔离

## 第八章：反垃圾邮件过滤

- 邮件基础
- 反垃圾邮件的过滤概述
- FortiGuard 反垃圾邮件服务
- 禁忌词汇检测
- 黑白名单
- HELO DNS 查询
- 返回邮件 DNS 查询
- DNSBL

## 第九章：Web 过滤

- Web 过滤概述
- URL 过滤
- 内容阻断
- 内容免屏蔽
- FortiGuard Web 过滤服务
  - 配置
  - 本地分类
  - 本地类别
  - 跳过
  - 过程
  - 图片分类

## 第十章：IM 和 P2P 过滤

- IM 配置
- IM 内容归档
- P2P 特征
- IM 防病毒

## 第十一章：SSL VPN

- FortiGate SSL VPN 网关
- SSL VPN 的类型
- SSL VPN 的配置
- Web 门户的特性
- Web 门户的配置
- Web 门户的界面
- 通道模式的特性

- 客户端检测
- 通道模式的配置
- 通道模式的用户体验
- IPSEC