

课程 221——FortiMail 邮件过滤

概述:

该课程是两天的课堂式培训，详细地讲述如何配置、管理和维护 FortiMail。

该课程首先会介绍很多企业所面临的邮件安全问题。学生将亲自动手学习如何配置 FortiMail 的功能，比如说防病毒、反垃圾邮件、内容检测和邮件归档等功能。

同时，对 SMTP 协议给予一个大致描述，也讲述 FortiMail 邮件流的具体情况。学生通过熟悉策略和保护内容表的使用来优化对邮件攻击的防御体系。还将讲述如何进行日常的维护和实时的网络解决方案，最后介绍如何配置主动被动模式的高可用性。

学生将深入地了解如何将 FortiMail 邮件平台整合到现有邮件架构里来实现阻断不需要的垃圾邮件，最大程度地防御混合式的邮件攻击和符合国家法律的要求。

该课程的目标:

- 通过图形界面和命令行可以完成 FortiMail 的管理和维护工作，比如系统的备份，路由和域的配置，高可用性的配置，垃圾邮件的隔离，产生报表。
- 通过验证接收者和阻挡发送给不合法用户的邮件来保护珍贵的企业 MTA 资源。
- 配置策略来应用检测和防护的保护内容表到发送的邮件安全以及强制部署邮件管理策略。
- 了解 FortiMail 的系统架构，邮件如何流过，如何部署路由和策略来管理邮件流。
- 配置保护内容表来实现防病毒，反垃圾邮件，和反间谍软件。
- 配置归档功能，实现对邮件归档的要求。
- 部署反垃圾邮件过滤功能，比如深度头检测、启发式扫描、图片扫描、禁忌词汇检测、第三方的 DNSBL 和 SURBL 服务器以及 FortiGuard 反垃圾邮件服务。
- 配置防病毒过滤保护内容表以实现病毒扫描和删除邮件中的病毒和间谍软件。

参与人员的要求:

- 邮件和 SMTP 的基础知识

适用的人群:

负责部署、维护和管理 FortiMail 产品的工程师

课程章节：

第一天的课程：

第一章：概述

- 产品概述
- 邮件基础
- FortiMail 的工作模式
 - 透明模式
 - 网关模式
 - 服务器模式

第二章：系统和邮件设置

- 管理访问
- 网络设置
- 日志和报表
- 邮件设置
- 访问列表
- 接收者地址验证
- 推迟传送和传送状态
- 定义消息
- 地图或邮件地址的别名
- 域管理

第三章：策略和保护内容表

- 定义的策略和保护内容表
- 策略和保护内容表的优点
- 基于接收者的策略
- 什么时候使用基于 IP 的策略
- 策略检测——如何工作的
- 策略规则
- 认证选项

第四章：反垃圾邮件的保护内容表

- FortiMail 的邮件流分析
- 垃圾邮件检测
- 基于会话的反垃圾邮件技术
 - 会话速度的限制
 - 发送者检验
 - 协议检测
 - 非认证的会话

- SMTP 错误
- 接受者地址检测
- 灰名单和 IP 黑名单检测
- 应用层的反垃圾邮件
 - FortiGuard 反垃圾邮件服务(DNSBL, SURBL, SHASH)
 - 伪造 IP 检测
 - 深度信头检测
 - 灰色列表过滤
 - 图片分析过滤
 - 本地信誉过滤
 - 启发式扫描
 - 基于用户和域的贝叶斯算法
 - 黑白名单
 - 禁忌词汇和辞典扫描

第五章：防病毒和保护内容表

- 病毒检测
- 内容过滤
- 附件过滤
- 词典内容表设置

第六章：邮件归档

- 邮件归档
- 归档策略和免屏蔽的策略
- 访问归档的邮件

第七章：管理

- 维护
 - 系统软件升级
 - FortiGuard 升级服务
 - 系统设置备份
- 故障分析
 - 网络连接状况测试
 - 邮件队列
 - 邮件历史信息

第八章：高可用性

- FortiMail 高可用性
- HA 主动被动模式
- 邮件数据的同步
 - 系统邮件目录

- 用户本地目录
- MTA 的露露
- HA 服务监控
- HA 只读配置
- HA 网络接口配置
- HA 说明