

设置 FortiMail 服务器模式

说明：

本文档针对 FortiMail 服务器模式配置进行说明。服务器模式指 FortiMail 本身就是邮件服务器，它负责邮件的收发和过滤功能。

环境介绍：

本文使用 FortiMail100 做演示。本文使用的系统版本为 3.00,build527。

步骤一：网络环境

本文档以域名 test15.com 为例做说明。服务器模式需要防火墙配合完成地址影射配置。在服务器模式下，FortiMail 的接口 IP 地址就是邮件服务器的 IP 地址。本例是 10.1.1.11

MX 记录：test15.com---->mail.test15.com

A 记录： mail.test15.com----> 208.1.1.1

在防火墙上的地址映射：

进入方向：

mail.test15.com----> 208.1.1.1---->映射给 FortiMail（整个 IP）

步骤二：设置邮件服务器

在邮件服务器—设置—本地主机中输入主机名和本地域名

主机名：FortiMail 主机名，本例是 mail

本地域名：FortiMail 域名，本例是 test15.com

FortiMail 的完全有效域名（FQDN）格式是：主机名.本地域名，本例是 mail.test15.com。

基于 SSL/TLS 的 SMTP：勾选则接收 SMTPS 连接。除非用户说明要 FortiMail 接收 SMTPS 发来的邮件，一般不需要勾选此项。

The screenshot shows the 'Local Host' configuration section in the FortiMail web interface. It includes the following fields and values:

本地主机	
主机名：	mail
本地域名：	test15.com
SMTP服务器端口号：	25
基于SSL/TLS的SMTP：	<input type="checkbox"/>
SMTPS服务器端口号：	465
POP3服务器端口号：	110

在邮件服务器—设置—表现中设置 Webmail 语言

The screenshot shows the 'Webmail 语言' (Webmail Language) dropdown menu in the FortiMail web interface. The selected language is '简体中文' (Simplified Chinese).

Webmail语言：	简体中文
------------	------

在邮件服务器—域中点击新建

域：输入保护的域名，本例为 test15.com

如果有多个域则点击新建，再输入一个域名。

在邮件服务器—访问中配置收发邮件规则

Receive(收)：对于 FortiMail 设备，SMTP 连接是从外部设备发送给 FortiMail 的。

收方向规则检查信封中的发信人地址 (MAIL FROM)，收信人地址 (RCPT TO)，认证 (AUTH) 和加密 (TLS)。规则是按从上到下逐条匹配的，一封邮件只能匹配一条规则。

双向（收、发）过滤则必须要写规则，本例的写法是：

#	发送者样式	接收者样式	发送者IP/掩码	动作
1	/*	/*@test15.com	0.0.0.0/0	RELAY
2	/*@test15.com	/*	0.0.0.0/0	RELAY
3	/*	/*@test16.com	0.0.0.0/0	RELAY
4	/*@test16.com	/*	0.0.0.0/0	RELAY
5	/*	/*	0.0.0.0/0	DISCARD

第一条：所有接收者的域是 test15.com 的邮件全部转发

第二条：所有发送者的域是 test15.com 的邮件全部转发

第五条：不符合上面条件的邮件全部丢弃

如果有多个域，上图的第三和第四条规则就是对第二个保护域 test16.com 的写法，其他域以次类推。

写法：在接收者或发送者中写 *@test15.com 就表示所有 test15.com 上的邮件。

写*表示所有邮件，一般不需要勾选正则表达式。

反向 DNS 样式：写*

Authentication Status: 选择 any 默认

TLS Profile: 选择 none 默认

动作：Relay, 转发邮件，做垃圾邮件、杀毒和内容过滤

Bypass, 转发邮件，做杀毒和内容过滤

Reject, 丢弃邮件，通知发信的服务器

Discard, 丢弃邮件，不做任何通知

New Rule

发送者样式: *

正则表达式

接收者样式: *@test15.com

正则表达式

发送者IP/掩码: 0.0.0.0 / 0

反向DNS样式: *

正则表达式

Authentication Status: any authenticated

TLS Profile: < none >

动作: RELAY

Delivery(发): 对于 FortiMail 设备, SMTP 连接是从 FortiMail 发送给外部设备的。

对于发方向一般没有具体配置要求, 建议使用下面的配置。该配置的作用是 FortiMail 在向外发送邮件时不使用 SMTPS 协议, 使用标准的 SMTP 来发送。因为一些邮件服务器对 SMTPS 支持不标准, 会导致邮件发送失败。使用 SMTP 发送邮件是比较稳妥的做法。

在内容表—TLS 中点击新建

New TLS Profile

Profile Name: notls

TLS level: None

Action on failure: Temporarily Fail

是 取消

在邮件服务器—Delivery 中点击新建

Message Delivery Rule

Destination Domain Pattern: *

Destination IP/Netmask: 0.0.0.0 / 0

TLS Profile: notls

步骤三: 设置用户

在设置用户—用户—对应的域名中点击新建

输入用户名和口令, 在用户登录到 WebMail 时需要输入完整的用户名, 即 pc15@test15.com。

显示名: 输入该用户好记的名称

步骤四：设置内容表

防垃圾邮件：在内容表—防垃圾邮件中设置，一般可以采用 FortiMail 自带的内
容表，做一些修改即可。

点击 antispam_basic_predefined_medium 后面的复制图标  输入表名，编辑新复制的表

不勾选 DNSBL 和 SURBL，FortiGuard-Antispam 已经有这两项功能，这样可以
减少误报率。

DNSBL 扫描 [\[配置\]](#)

SURBL 扫描 [\[配置\]](#)

展开深度邮件头扫描，勾选邮件头分析

深度邮件头扫描 动作
 Black IP scan
 邮件头分析

展开动作—隔离，将删除邮件该为 30 天，即 FortiMail 会自动删除 30 天以前的
垃圾邮件，输入 0 天则不删除。

在释放条件中不勾选用邮件释放，因为用 Web 释放更方便。

勾选允许用户从发送的邮件自动更新“非垃圾邮件”。

隔离
 发送垃圾邮件报表
 删除邮件 天以前 (0指关闭)
 释放邮件
 用邮件方式释放
 用Web方式释放
 把释放邮件的发送者加到白名单
 允许用户从发送的邮件自动更新“非垃圾邮件”

点击最下面的是完成编辑。

防病毒：建议使用 antivirus_def

内容：建议使用 content_def

其他：建议使用 misc_def

会话：建议使用 session_strict，需要作适当修改。

编辑 session_strict 内容表，展开连接设置，限制每个客户连接数为 200 每 5 分钟；每个用户只能连接 5 次并发。



展开发件人信誉，取消允许发件人信誉检查



步骤五：设置策略

基于 IP：使用 IP 策略的目的是对进方向邮件作会话限制，对出方向邮件不做限制。

策略匹配顺序：策略按从上到下的顺序匹配。

先匹配基于 IP 策略再匹配下面的基于接收者策略。

本例的配置为：从 FortiMail (10.1.1.11) 发出的邮件不做会话限制；其他设备发送的邮件做会话限制。

#	匹配	会话	防垃圾邮件	防病毒	内容	IP地址池	认证
1	10.1.1.11/32	none	none	none	none	none	none
2	0.0.0.0/0	session_strict	none	none	none	none	none

策略：策略可以对垃圾邮件、杀毒、内容表和认证做设置

进入邮件策略：对收信人地址在保护域上的邮件做过滤

如果有多个域，要先选择域名



用户名：收信人地址，*表示所有用户

Profile：选择步骤三中定义好的过滤内容表

用户/组名称

用户名

本地组名称

LDAP组名称 LDAP 内容表

Profile

防垃圾邮件内容表

防病毒内容表

内容内容表

其他内容表

发出邮件策略：对收信人地址不在保护域上的邮件做过滤
用户名：收信人地址，*表示所有用户

New/Edit Policy User

用户名

Profile

防垃圾邮件内容表

防病毒内容表

内容内容表

步骤六：隔离邮件设置

在电子邮件过滤—隔离—垃圾邮件报表中展开 **webmail** 访问选项

勾选没有认证情况下受限的访问；过期时间设置为 720 小时（30 天）

Web 释放主机名/IP：输入映射给 FortiMail 的公网 IP 地址或对应的域名

此项的作用：FortiMail 会每天给用户发送垃圾邮件隔离报告，如果隔离的邮件是正常邮件用户点击报告中的链接即可释放邮件。该链接的地址用户必须可以访问，一般使用公网 IP 地址。

Webmail访问设置

没有认证情况下受限的访问

过期期间: Hours (1 - 720)

使用HTTPS

Web释放主机名/IP: