

设置 FortiMail 网关模式（双 A 记录）

说明：

本文档针对 FortiMail 网关模式（双 A 记录）配置进行说明。网关模式指 FortiMail 作为邮件服务器的邮件网关对进出方向邮件做转发和过滤。双 A 记录指邮件服务器和 FortiMail 分别有一个公网 IP 和 DNS A 记录。

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 test11.com 为例做说明。网关模式需要防火墙配合完成地址影射配置。

MX 记录：test11.com---->smtp.test11.com

A 记录：smtp.test11.com----> 208.1.1.1

mail.test11.com----> 208.1.1.2

在防火墙上的地址映射：

进入方向：

smtp.test11.com----> 208.1.1.1---->映射给 FortiMail（整个 IP 影射）

mail.test11.com----> 208.1.1.2---->映射给 FortiMail（tcp 25 端口）

mail.test11.com----> 208.1.1.2---->映射给邮件服务器（tcp 80、110、443 等端口）

出网方向：

FortiMail 使用 208.1.1.1 出网；邮件服务器使用 208.1.1.2 出网。

进方向邮件过滤：依靠防火墙的地址映射完成

外网的邮件服务器发信时先发送到 FortiMail（smtp.test11.com）然后转给内网邮件服务器。

使用客户端软件如 outlook 的用户接收和发送的地址都是 mail.test11.com；发送邮件时先发送到 FortiMail 然后转给内网邮件服务器。

出方向邮件过滤：需要邮件服务器将 FortiMail 设为中继服务器

邮件服务器先将邮件发送给 FortiMail，然后 FortiMail 将邮件转发出去。

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 smtp

本地域名：FortiMail 域名，本例是 test11.com

FortiMail 的完全有效域名 (FQDN) 格式是: 主机名.本地域名, 本例是 smtp.test11.com。该名称要与 DNS 的 A 记录一致。

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。

邮件服务器设置

本地主机

主机名:

本地域名:

SMTP服务器端口号:

基于SSL/TLS的SMTP:

SMTPS服务器端口号:

在邮件服务器—设置—表现中设置 Webmail 语言

Web邮件接口

Webmail语言:

在邮件服务器—域中点击新建

域: 输入保护的域名, 本例为 test11.com

SMTP Server: 保护邮件服务器的 IP 地址。如果需要也可以使用 MX 记录。此项如果没有特殊需求建议直接写 IP。

域名

域FQDN:

Use MX Record:

SMTP Server: Port: 使用SMTPS:

Fallback MX Host: Port: 使用SMTPS:

验证接收者地址: 选择 Use SMTP Server, 可以减轻邮件服务器负担。FortiMail 先检查接收者地址是否有效再做转发, 可以提高垃圾邮件过滤效果 (标准的 SMTP 都支持该功能)。如果用户的邮件服务器扩展性一般, 不支持该功能可以选择 Disable。

验证接收者地址

Disable

Use SMTP Server

Use LDAP Server

高级设置: 下面的两个功能对出方向过滤有效, 如果只要求做进方向过滤不用配置。

SMTP 问候:

使用这个域名: 向外发邮件时使用域名 ehlo, 本例为 test11.com

使用这个系统主机名：向外发邮件时使用主机名 ehlo, 本例为 smtp.test11.com
 当用户为 DNS 的 A 记录做了 PTR（反向 DNS 解析）时，要使用系统主机名
 Remove Received Header of Outgoing Email：勾选该项后 FortiMail 去掉邮件头中保护邮件服务器的 Received 部分，起到对外隐藏邮件服务器的作用。



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。

如果只有收方向过滤，可以不写规则。FortiMail 将采用默认的规则转发邮件。
 默认的规则是：收信人地址属于保护域的邮件全部转发
 收信人地址不是保护域的邮件全部丢弃

如果做了双向（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	/*	/*@test11.com	0.0.0.0/0	RELAY
2	/*@test11.com	/*	0.0.0.0/0	RELAY
3	/*	/*@test12.com	0.0.0.0/0	RELAY
4	/*@test12.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 test11.com 的邮件全部转发

第二条：所有发送者的域是 test11.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 test12.com 的写法，其他域以次类推。

写法：在接收者或发送者中写 *@test11.com 就表示所有 test11.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

Modify Rule	
发送者样式:	* <input type="checkbox"/> 正则表达式
接收者样式:	*@test11.com <input type="checkbox"/> 正则表达式
发送者IP/掩码:	0.0.0.0 / 0
反向DNS样式:	* <input type="checkbox"/> 正则表达式
Authentication Status:	<input checked="" type="radio"/> any <input type="radio"/> 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 ▼
<input type="button" value="是"/> <input type="button" value="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。



展开深度邮件头扫描，勾选邮件头分析



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”。



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

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。

连接设置
输入0来关闭检查

限制每个客户端的连接数为 每 分钟

每个客户端只能连接 次并发

限制总连接数为

丢掉连接，在 秒用户不活动

展开发件人信誉，取消允许发件人信誉检查

发件人信誉

允许发件人信誉检查

认证：如果用户使用客户端软件(outlook 等)收发邮件，需要配置认证。如果只使用 Web 收发邮件不需要配置。

在认证—POP3 中点击新建，服务器 IP: 输入保护的邮件服务器地址。勾选 Server Requires Domain，存在多个域时有效。

新建POP3服务器

内容表名称

服务器名称/IP

服务器端口

Server Requires Domain

SSL Enable

安全认证 Enable

TLS Enable

步骤四：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：从邮件服务器(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

Authentication And Access: 选择步骤三中定义好的认证表

New/Edit Policy User

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

Authentication And Access

Authentication profile

Use for SMTP authentication

Allow different SMTP sender identity

Allow POP3 for SPAM access

Allow Web Mail for SPAM access

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