FortiMail 故障排错

版本	1.0
时间	2011 年 10 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FortiMail v4.2.2
状态	草稿

目录

1.目的

本文对 Fortimail 基于 CLI 与 Web 模式下一般故障排错方法及特殊情况的提示进行说明。一些在 CLI 命令行下提供的信息在 Web 管理界面下无法提供。

2.系统基准与故障定义

在明确具体故障之前,我们需要了解系统正常状态是如何运行的,所以,作为系统管理员在日常维护时,需要记录日志,定期了解系统状态并运行相关命令收集信息保存,当发生故障时,常规数据能帮助你什么地方出现了变化和改动。

周期备份 Fortimail 配置是最有效的方法,一旦系统更改出现故障,备份能够最快最安全的恢复至运营状态。

在解决问题之前,了解并清楚下列问题:

- 发生故障的时间;
- 设备在故障之前是否正常工作;
- 连接是否正常,Fortimail 是否能连接 internet,是否能与 DNS 通讯;
- 服务器的相关策略工作是否正常;
- 是否同时涉及多个故障点;
- 故障是否能重现;
- 系统配置做过哪些改动;
- 通过系统资源查看系统是否过载;

3.收集系统信息

FortiMail 提供多种功能来帮助故障排除及性能检测,Web 界面中的高级管

理模式中,可以通过监控来查看系统信息和所有邮件传递信息,也可以通过 CLI 诊断命令来排查硬件和软件问题。

4.常见故障解决办法

4.1 磁盘故障

故障描述:事件日志显示 RAID errors regarding a degraded array event on multiple HD dev(ref./dev/md2 and /dev/md3).

解决方法:

磁盘故障,磁盘阵列中的某块磁盘无法正常工作.

4.2 Web 与 CLI 连接故障

4.2.1 故障描述:管理员账户可以连接 Web 界面高级管理模式,但是不能连接基本模式或 CLI 命令行.

解决方法:

将管理员账户从域管理员改成系统管理员,如果需要限制账号的操作权限,可以定义访问内容表应用与相应的管理员.

4.2.2 故障描述:管理员无法登陆 Web 管理界面或者 CLI 界面

解决方法:

1.检查用户名及密码; 2.检查接口配置的管理服务是否开启; 3. 检查管理员信任主机是否允许当前 IP

4.3 FortiGaurd 连接故障

4.3.1 故障描述:Fortimail 无法连接至 FDN 服务器获取 AV 及 AntiSpam 服务

解决方法:

1.在 https://support.fortinet.com 注册 Fortimail; 2. 获取试用或购买 FortiGuard 服务合同; 3. 检查 Fortimail DNS 配置,是否能正常解析; 4. 配置 Fortimail 静态路由,确定能够连接 Internet.

4.4 MTA 故障

4.4.1 故障描述:smtp 客户端接收到信息提示 550 5.7.1 Relay access denied.

解决方法:

该提示客户端由于未被允许中继而拒绝.

a. 对于进站连接,访问控制默认自动允许中继,除非明确拒绝;

b. 对于出站连接,只有认证后或访问控制列表通过后才允许中继,如果需要认证,请确认 smtp 客户端配置认证信息并且正确.

如果接收到 5.7.1 错误信息并没有提到 Relay access,请检查 fortimail 是否开启发件人或终端声望,smtp 客户端是否因超过声望阀值被拒绝。

4.4.2 故障描述:Fortimail 被 bypass

解决办法:

在一个复杂的网络环境中,如果网络规划或部署不合理,smtp 流量没有被 NAT 设备正确的路由,那么有可能发生 Fortimail bypass(即 smtp 流量未经过 fortimail)。

如果 Fortimail 执行垃圾邮件的出战扫描,那么所有出站邮件必须被路由至 Fortimail,如果邮件用户或者被保护服务器通过其他 MTA 中继出站,那么 Fortimail 将被 bypass.

同时,垃圾邮件的发送者能够判断决定使用优先级最低(即最高的 preference)的邮件服务器来避免有效的垃圾邮件防御措施。

如何保证垃圾邮件无法绕开 Fortimail:

1. 配置防火墙和路由器确保 smtp 流量路由至 Fortimail 进行扫描;
2. 如果 Fortimail 工作在 Gateway 模式,通过修改邮件服务器的 MX 记录或防火墙映射至 Fortimail;
3. 检查所有可能的连接的策略,默认如果无策略匹配,那么该连接将被允许且不会被扫描(为防止这种情况,可以在 IP 策略的底部添加一条策略拒绝所有未匹配策略的连接。)
4. 检查策略中选中反垃圾邮件的内容表,并开启反垃圾邮件扫描。

4.4.3 故障描述:反垃圾邮件(以下简称 AS)和反病毒 AV(以下简称 AV)被 bypass

解决方法:

如果邮件未被 Fortimail bypass,但却未被 AS 与 AV 扫描,检查访问控制规则是否过于宽松,现有策略是否匹配这些邮件连接,内容表中是否启用 AV 与 AS。

4.4.4 故障描述:反垃圾邮件(以下简称 AS) 被 bypass

解决方法:

如果 AV 扫描生效,但是 AS 未生效,请检查白名单和被保护域中的白名单发送

者,如果开启白名单,那么将忽略 AS 扫描。另外,也需要检查“放行已经过 SMTP 认证的邮件”选型是否启用。

4.4.5 故障描述:收件人地址校验到达 SMTP 失败

解决方法:

如果启用了邮件保护域服务器的收件人地址校验,但是收件人校验失败,可能由以下原因导致:

- SMTP 服务器不可用;
- Fortimail 与 SMTP 服务器直接的网络连接不稳定;
- SMTP 服务器不支持 ESMTP.EHLO;
- SMTP 服务器为 Microsoft Exchange 服务器,SMTP 的收件人校验未开启或配置。

当 SMTP 服务器收件人验证服务不可用时,Fortimail 将返回 451 错误码,并将邮件保留在邮件队列中等待下次发送。

4.4.6 故障描述:smtp 客户端收到 451 Try again later

解决方法:

- 灰名单遇到未知的发送者或者灰名单列表中的条目已经过期,这种情况是预期而且合理的行为,如果是合法的邮件,smtp 客户端将会在灰名单的时间窗内重发该邮件。
- 另一种情况是启用了收件人地址校验,但是 Fortimail 却无法通过连接 SMTP 服务器校验该收件人,此时需要检查服务器配置是否正确以及是否支持收件

人地址校验。

4.4.7 故障描述:Fortimail 回应 temporary failure SMTP reply code,且事件日志显示 Milter (fas_milter): timeout before data read.

解决方法:

由于 Fortimail 在 4 分钟内未响应造成 Timeout. 反应延迟较大或者无反应的 DNS 对于 DNSBL 和 SURBL 的扫描造成 AS 的扫描在 Timeout 时间之前未能完成,如果问题一直持续,请检查与 DNSBL 和 SURBL 服务器的连接是否正常。

4.4.8 故障描述:在 Exchange 服务器开启收件人校验,所有邮件被拒绝。

解决方法:

默认情况下,Exchange 服务器将不会校验收件人,建议配置 Fortimail 使用 LDAP 用于收件人校验,或者开启 Exchange 的 smtp 收件人校验。

4.5 反垃圾邮件相关故障

4.5.1 故障描述: 垃圾邮件检测率低

解决方法:

- 确认没有 smtp 流量没有由于错误的路由策略导致被 Fortimail bypass;
- 谨慎使用白名单,尤其在使用通配符,如*.edu 将允许所有.edu 的邮件 bypass 反垃圾邮件检查;
- 不要将被保护域加入白名单,由于白名单 bypass 反垃圾邮件扫描,垃圾邮件发送者有可能使用被保护域的发件地址来欺骗,达到绕过检测的目的;

- 检查所有的被保护域匹配相关策略并开启相关的保护内容表;
- 考虑开启合适的反垃圾邮件功能如灰名单或者发送人声望。

4.5.2 故障描述: 邮件用户并未发送垃圾邮件但却被 DSN 认为是垃圾邮件发送者

解决方法:

垃圾邮件发送者通常会利用传递状态通知(DSN)机制 bypass 反垃圾邮件检测,这种攻击通常被称为 Backscatter,其原理为,当一个垃圾邮件制造者使用虚假的发送者地址(该地址真实存在,但被发送者假冒利用)往不可能抵达的目标地址发送邮件,以期达到收件人的服务器返回大量的 DSN 邮件给真实的发件人地址。

如何检测 Backscatter:

1. 在反垃圾邮件选项中开启退信校验功能并激活密钥;
2. 在邮件设置的邮件域设置与会话保护内容表中关闭 bypass 退信校验和跳过退信校验检查选项;
3. 检查所有的进站与出站邮件经过 Fortimail,否则 Fortimail 无法识别标记邮件或合法的 DSN。

4.5.3 故障描述: 邮件用户无法通过邮件释放或删除隔离邮件

解决方法:

- 收件人邮件地址的域名无法被 DNS 解析为 Fortimail 主机(即 Fortimail 主机,如 release-ctrl@fortimail.example.com);
- 隔离邮件中的发送者邮件地址不同于发送释放或删除隔离邮件的发件者地址。

4.5.4 故障描述: 邮件附件小于配置的 10M 限值却无法发送

解决方法:

邮件限制传送大小是指整个被传送邮件的内容:邮件,邮件头,所有的附件及编码,所以在可以传送的附件时应该小于实际 10M 的大小。

4.5.5 故障描述: 事件日志显示 DNSBL 查询错误

解决方法:

日志信息如下

RblServer::check 20.4.90.202.zen.spamhaus.org error=2 : 'Host name lookup failure'

该日志表明查询可能由于超过 DNSBL 提供商的限制而被拒绝,如果用户需要大量邮件流量需要进行 DNSBL 查询,尽量建立本地 DNSBL 并提供服务。

4.5.6 故障描述: 邮件隔离报告延迟

解决方法:

大多数情况,该故障由隔离账号过多导致隔离报告的延迟,当邮件被认定为垃圾邮件时,Fortimail 自动创建隔离账号。Netbots 与 spam harvest 扫描能够引起创建大量的虚假隔离账号。

通过邮件设定-邮件域设定避免该情况

1. 启用收件人地址校验;
2. 启用自动移除非法隔离账号功能。

默认自动清除非法隔离账号开始于每天的凌晨 4:00,可以通过以下命令修改

```
config antispam settings
    set system option backend_verify <hh:mm:ss>
end
```

5.参考

Fortimail 管理员使用手册