HCIE-Security 备考指南

邮件过滤

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 邮件过滤需要掌握的知识点

- 熟悉邮件过滤关键技术
- 掌握邮件过滤技术的应用

邮件过滤简介

介绍邮件过滤特性的定义和目的。

定义

邮件过滤主要使用 IP 地址检查和邮件内容过滤技术，它可以帮助局域网用户提高邮件系统的安全性：

- IP 地址检查可以防止垃圾邮件在内网泛滥。
- 邮件内容过滤既可以过滤掉匿名邮件，也可以通过检查邮件内容控制内网用户的邮件发送或接收权限。

目的

随着互联网的发展，电子邮件已经成为人们沟通交流的主要途径，其安全问题也日益突出：

- 垃圾邮件泛滥：垃圾邮件是指未经用户许可强行发送的电子邮件，邮件包含广告、宣传资料、病毒等内容。对于用户来说，垃圾邮件除了会影响正常的邮件阅读，还可能包含病毒等有害信息；对服务提供商来说，垃圾邮件会造成邮件服务器拥塞，降低网络运行效率，甚至成为黑客攻击邮件服务器的工具。
- 匿名邮件非法传播：匿名邮件指发件人地址为空的电子邮件。从安全的角度考虑，匿名发送的邮件可能包含暴力、色情等对他人有危害的信息。
- 信息泄密：在一些企业，例如知识密集型高科技企业、金融公司、上市公司等，部分违法分子可能会通过邮件将机密信息非法传递到外部。

NGFW 可以帮助用户解决上述问题：

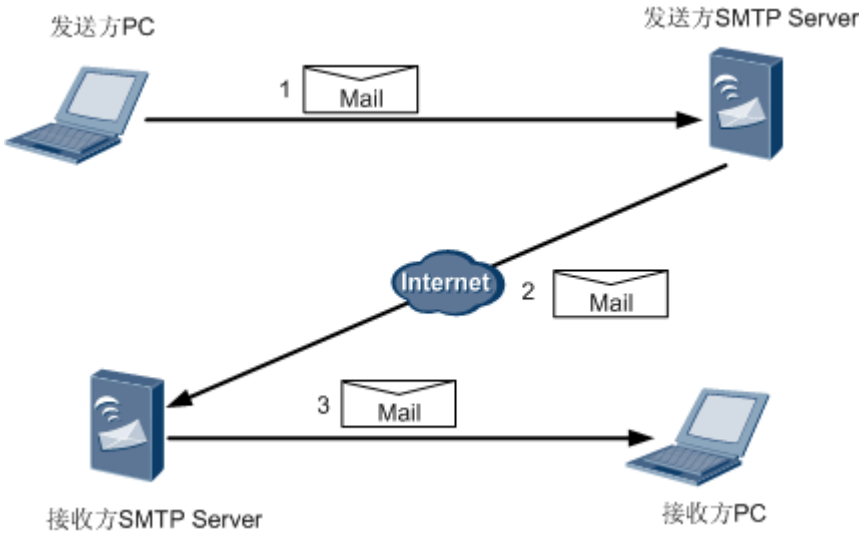
- 配置垃圾邮件防范，可以减少垃圾邮件造成的带宽浪费，并防止邮件服务器因频繁转发垃圾邮件被上一级因特网服务提供商加入黑名单。
- 配置匿名邮件检测，可以减少匿名邮件带来的信息干扰。
- 配置邮箱地址检查和配置邮件附件控制可以从邮件的发送权限、发送规模进行控制，防止信息泄密。

邮件发送/接收工作机制

本节介绍电子邮件的发送和接收机制。

邮件的传输需要经过 SMTP Server，SMTP Server 之间通过 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）协议来传递消息。

图 1 电子邮件传输过程



从图 1 可以看到，电子邮件的传输过程主要包括以下三步：

1. 发送方 PC 将邮件寄到指定的 SMTP Server。
2. 发送方 SMTP Server 根据邮件的目的地址，将邮件信息封装在 SMTP 消息中寄给接收方 SMTP Server。
3. 收件人下载邮件。

基于 SMTP/POP3/IMAP 的邮件收发机制

SMTP 定义了计算机如何将邮件发送到 SMTP Server，SMTP Server 之间如何中转邮件。

POP3（Post Office Protocol 3，邮局协议版本 3）和 IMAP（Internet Mail Access Protocol，交互式邮件存取协议）规定计算机如何通过客户端软件管理、下载邮件服务器上的电子邮件。

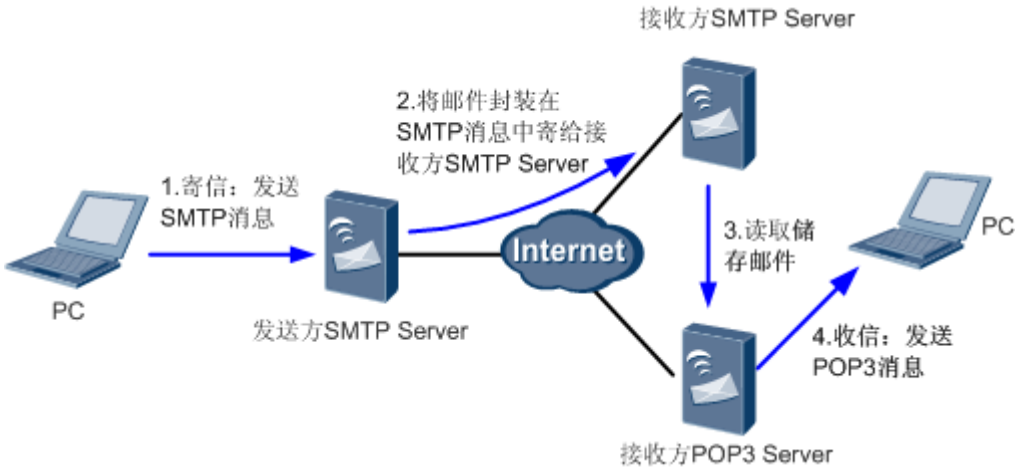
说明：

- SMTP Server、POP3 Server、IMAP 是为用户提供服务的管理软件，需要部署在硬件服务器上。

- IMAP 与 POP3 主要区别在于：使用 POP3，客户端软件会将所有未阅读邮件下载到计算机，并且邮件服务器会删除该邮件。使用 IMAP，用户直接对服务器上的邮件进行操作，不需要把所有邮件下载到本地再进行各项操作。

基于该种方式，网络管理员需要在邮件服务器上部署 SMTP 服务、POP3 服务（或 IMAP 服务）；终端用户需要在 PC 上安装邮件客户端软件（例如 MicroSoft OutLook、FoxMail 等邮件管理软件）。

图 2 基于 SMTP/POP3 的邮件收发机制



一个完整的邮件发送过程包括 4 步：

1. PC 将邮件内容封装在 SMTP 消息中寄给发送方 SMTP Server。
2. 发送方 SMTP Server 将邮件封装在 SMTP 消息中寄给接收方 SMTP Server，接收方 SMTP Server 储存起来。
3. POP3 Server 收到用户的请求后，读取 SMTP Server 储存的邮件。
4. POP3 Server 将邮件封装到 POP3 消息中发送给 PC。

垃圾邮件防范

垃圾邮件防范是基于 IP 的邮件过滤技术，通过检查发送方 SMTP Server 源 IP 的合法性来防止垃圾邮件泛滥。

背景介绍

电子邮件已经成为人们沟通和交流的重要途径，人们在享受电子邮件带来便利的同时，也被垃圾邮件所困扰。

垃圾邮件是指未经请求而发送的电子邮件。垃圾邮件的泛滥带来很多问题：

- 占用网络带宽，造成邮件服务器拥塞，进而降低整个网络的运行效率。
- 占用收件人的信箱空间，影响正常邮件的阅读和查看。
- 频繁转发垃圾邮件，导致邮件服务器被上级国际 Internet 服务提供商加入黑名单，无法发送邮件到国外。

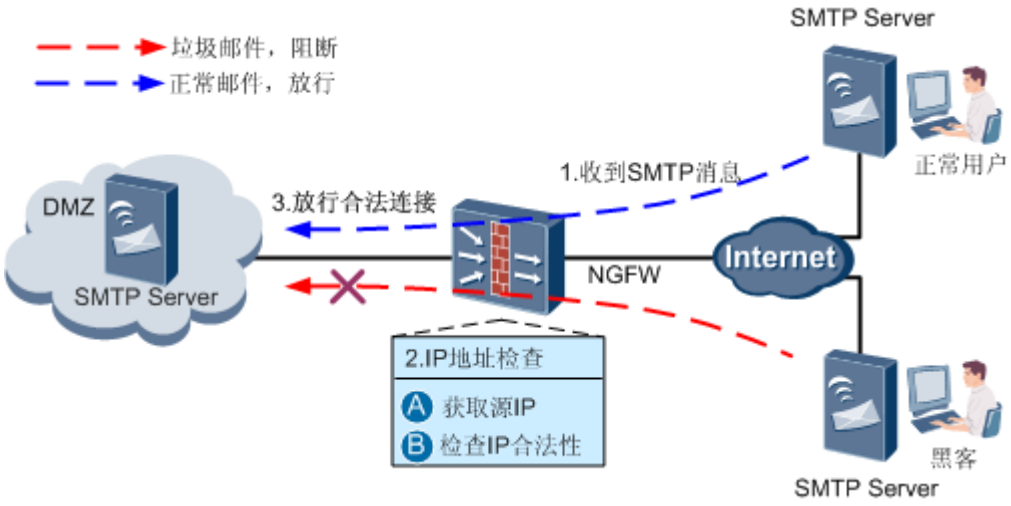
NGFW 作为安全网关时，所有外部邮件均需经过 NGFW 中转，通过检查发送方 SMTP Server 的 IP 地址，可以有效过滤垃圾邮件。

发送方 SMTP Server 源 IP 地址检查

从邮件发送/接收工作机制可以了解到，在整个邮件发送过程中，PC 与邮件服务器、邮件服务器与邮件服务器之间都不做认证，攻击者可以通过互联网上任意一台 SMTP Server 来发送邮件。

IP 地址检查是指 NGFW 对发送方 SMTP Server 的源 IP 进行检查，检查过程可参考图 1。

图 1 发送方 SMTP Server 源 IP 地址检查



1. NGFW 收到其他 SMTP Server 发送的 SMTP 消息，包括正常邮件和垃圾邮件。
2. NGFW 执行 IP 地址检查：
   a. 解析 SMTP 消息，从 SMTP 消息中获取发送方 SMTP Server 的源 IP。
   b. 检查源 IP 合法性。NGFW 将 IP 地址与黑名单、白名单进行比较，来判断 IP 地址的合法性。有本地白名单、本地黑名单和 RBL 黑名单。如果源 IP 命中了本地白名单，判定为合法邮件；否则查找本地黑名单，如果命中本地黑名单，判定为垃圾邮件；否则查询 RBL 黑名单，命中 RBL 黑名单判断为垃圾邮件，否则判定为合法邮件。

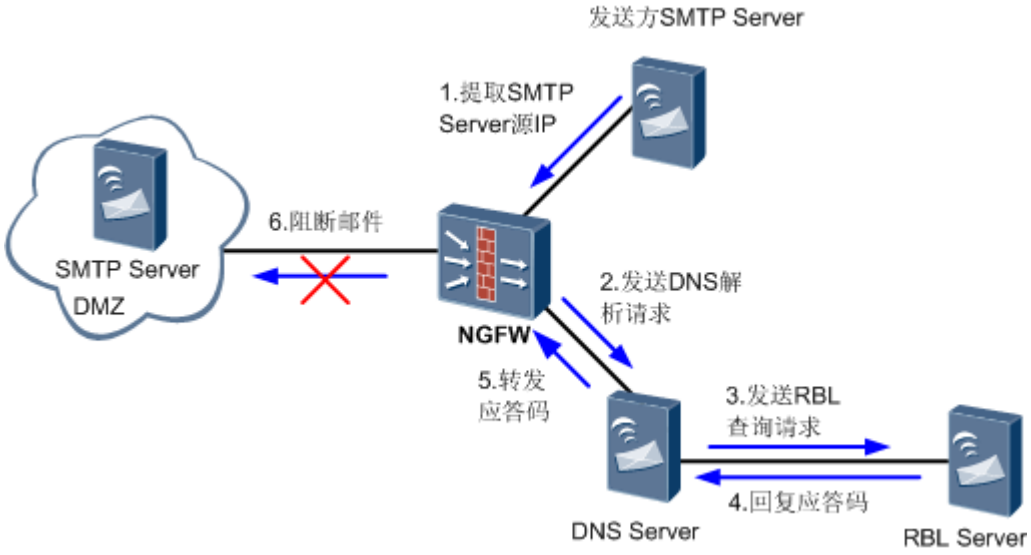
3. 放行合法邮件，阻断垃圾邮件。

RBL 黑名单查询机制

RBL 黑名单是由反垃圾邮件组织联合收集的一个庞大的在线数据库，收集、保存频繁发送垃圾邮件 SMTP Server 的 IP 地址。

NGFW 使用 RBL 黑名单进行邮件过滤的工作原理可参考图 2。

图 2 RBL 工作机制



1. NGFW 收到 SMTP 消息后，提取发送方 SMTP Server 的 IP 地址。
2. NGFW 将步骤 1 解析出来的 IP 地址和由第三方 RBL 服务器指定的 RBL 服务名放到一条信息中，向 DNS Server 发送解析请求。例如，SMTP Server 的源 IP 为 1.2.3.4，RBL 服务名为“sbl.spamhaus.org”，则 NGFW 将信息“4.3.2.1.sbl.spamhaus.org”发送给 DNS Server。
3. DNS Server 收到 NGFW 发送的信息后，读取 RBL 服务名，解析出 RBL 服务器对应的 IP 地址，将查询请求转发给 RBL 服务器。
4. RBL 服务器收到 DNS 服务器转发的查询请求后，将结果以应答码的形式反馈给 DNS Server。应答码是一个 IP 地址，标识此次 RBL 查询是否有结果。
5. DNS Server 将从 RBL 服务器获取的应答码转发给 NGFW。
6. NGFW 根据应答码判断来自该 SMTP Server 的邮件是否为垃圾邮件。
   - 如果从 RBL 服务器获得的应答码与 NGFW 上配置的应答码一致，该 SMTP 邮件将被视为垃圾邮件。

- 如果从 RBL 服务器获得的应答码与 NGFW 上配置的应答码不一致，该 SMTP 邮件将被放行。

从 NGFW 查询 RBL 黑名单的过程可以知道，要使用 RBL 黑名单，网络管理员需要配置 DNS 服务器、RBL 服务名和应答码，配置过程可参考配置垃圾邮件防范。

基于邮件内容的过滤

匿名邮件检测、邮箱地址检查、邮件附件控制都是基于邮件内容的过滤，通过检查发件人和收件人的邮箱地址、附件大小和附件个数来实现过滤。

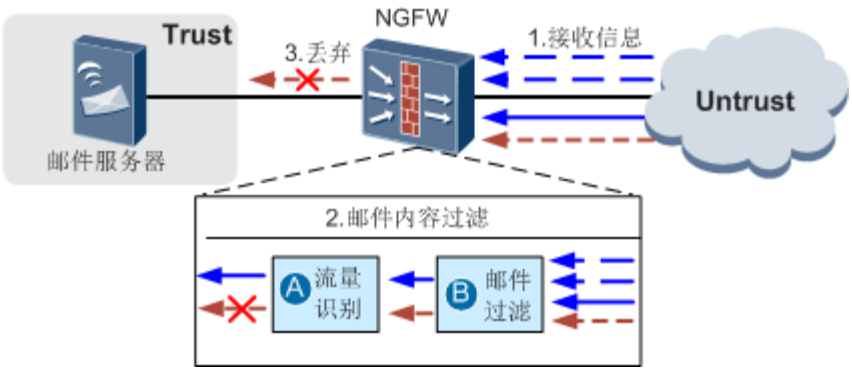
邮件内容过滤运行机制

NGFW 作为安全网关时，所有的数据信息都要经过 NGFW 中转，NGFW 在中转信息前，对信息进行检查，过滤掉包含非法邮件的信息。

图 1 展示了 NGFW 过滤来自外网非法邮件信息的过程，过滤来自内网非法信息的过程类似，在此不一一赘述：

1. 数据信息到达 NGFW。
2. NGFW 进行邮件内容过滤：
   a. 流量识别。NGFW 根据匹配条件（例如数据流量的源安全区域、目的安全区域、源地址、目的地址等）识别出要进行邮件过滤的流量。
   b. 邮件过滤。NGFW 分析出哪些流量包含邮件内容，检查邮箱地址、附件大小，识别出非法邮件。
3. 丢弃包含非法邮件的信息。

图 1 邮件内容过滤运行机制



配置匿名邮件检测、配置邮箱地址检查和配置邮件附件控制将会生成邮件过滤配置文件，配置文件定义如何进行邮件过滤。

配置安全策略定义流量识别条件，并引用邮件过滤配置文件。

检测方向

邮件内容过滤分为发送方向和接收方向：

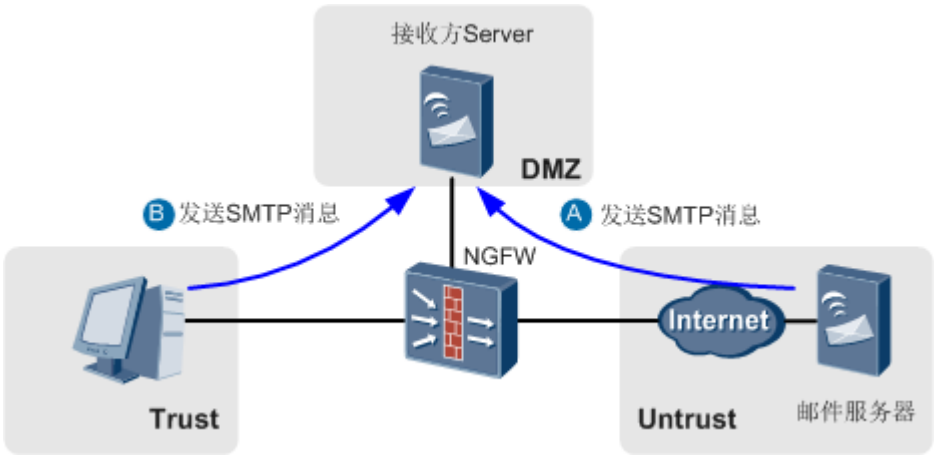
- 发送方向

  如果邮件内容封装在 SMTP 消息中，NGFW 执行发送方向检测。

  图 2 展示了发送方向检测的几个典型场景：

  - A.外网邮件服务器将邮件寄给位于 DMZ 区域的邮件服务器，NGFW 检测到了从 Untrust 区域发到 DMZ 区域的 SMTP 消息，执行发送方向的邮件内容检测。
  - B.内网用户使用 OutLook 等客户端发送邮件，将邮件寄给位于 DMZ 区域的邮件服务器，NGFW 检测到了从 Trust 区域发到 DMZ 区域的 SMTP 消息，执行发送方向的邮件内容检测。

  图 2 发送方向定义

- 接收方向

  如果邮件内容封装在 POP3 消息或 IMAP 消息中，NGFW 会判断为接收方向，执行接收方向的检测。

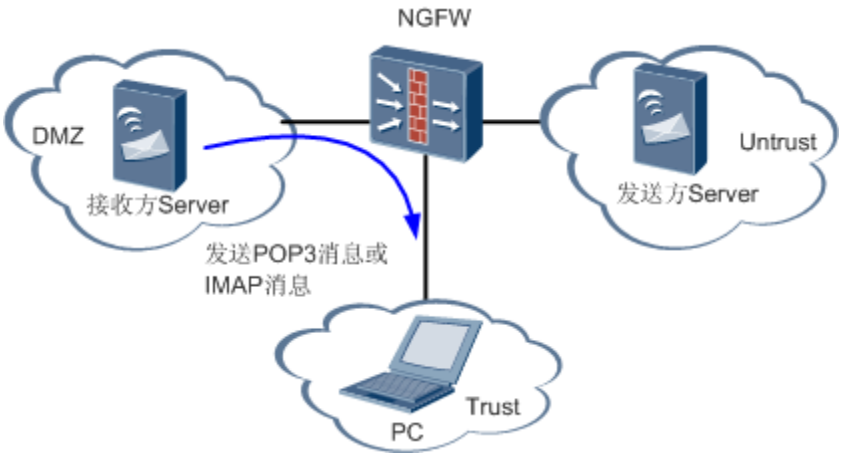
  图 3 展示了接收方向的典型场景，NGFW 检测到了从 DMZ 区域发到 Trust 区域的 POP3 消息或 IMAP 消息，执行接收方向的邮件内容检测。

说明：

- 检测到 POP3 消息时，如果判定为非法邮件，NGFW 的响应动作可以是发送告警信息或阻断邮件。

- 检测到 IMAP 消息时，如果判定为非法邮件，NGFW 的响应动仅支持发送告警信息，不会阻断邮件。

图 3 接收方向定义



应用场景

介绍邮件过滤的典型应用场景。

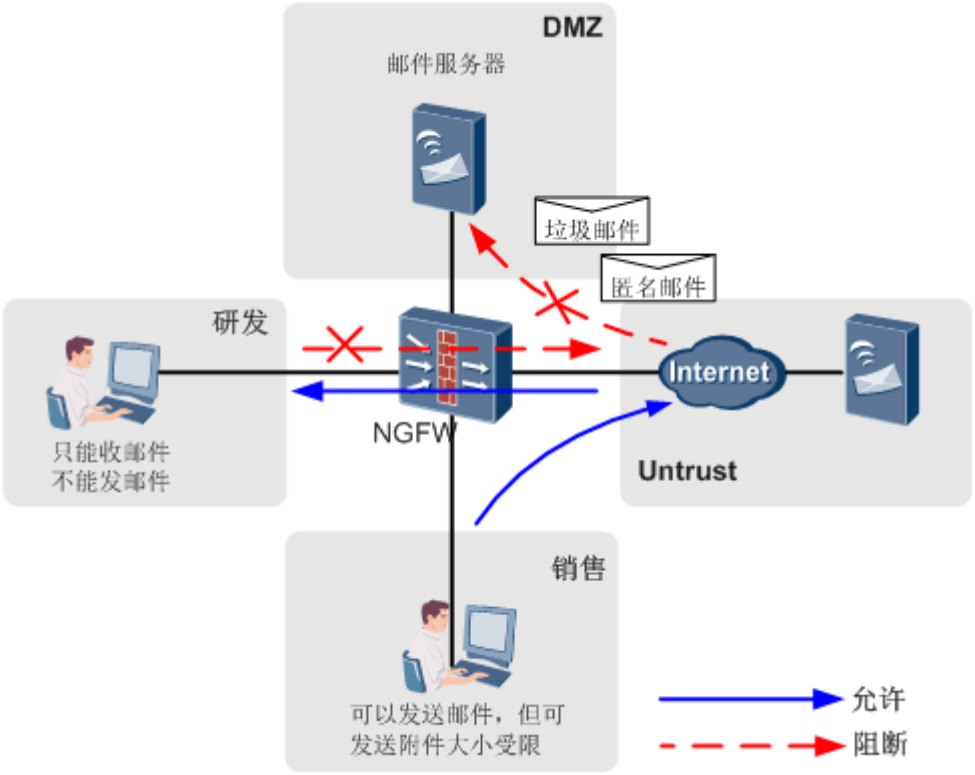
邮件服务器部署在内网

如图 1 所示，NGFW 作为一个办公网络的安全网关，邮件服务器部署在内网，内部网络用户通过部署在内网的 SMTP 服务器收发邮件。

在 NGFW 上配置邮件过滤，可以收到如下邮件安全保护效果：

- 开启垃圾邮件防范，防止内网的 SMTP 服务器收到大量垃圾邮件。
- 开启匿名邮件检查，防止违法信息通过匿名邮件方式在整个网络内部传播。
- 开启邮箱地址检查，只允许指定邮箱地址发送或接收电子邮件，从发送和接收权限上进行控制，防止内部用户泄露重要信息。
- 开启邮件附件控制，对附件的大小和个数进行控制，防止大量信息通过附件泄露出去。

图 1 邮件服务器部署在内网



邮件服务器部署在外网

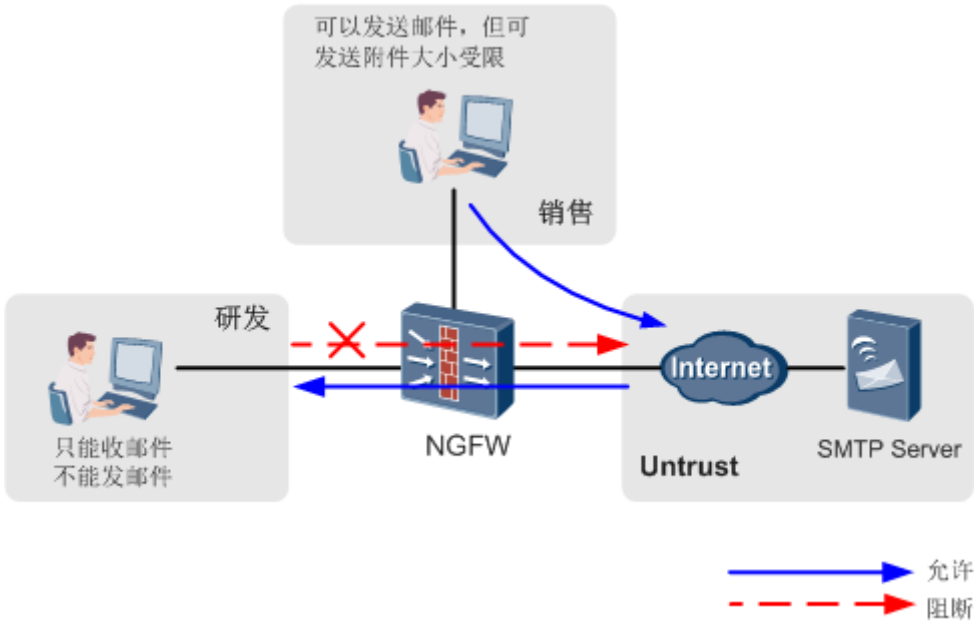
如图 2 所示，NGFW 作为一个办公网络的安全网关，邮件服务器托管到远程服务器中心。

在 NGFW 上配置邮件过滤，网络管理员可以收到如下邮件安全保护效果：

- 开启匿名邮件检查，防止违法信息通过匿名邮件方式在整个网络内部传播。
- 开启邮箱地址检查，只允许指定邮箱地址发送或接收电子邮件，从发送和接收权限上进行控制，防止内部用户泄露重要信息。
- 开启邮件附件控制，对附件的大小和个数进行控制，防止大量信息通过附件泄露出去。

此组网与第一种组网的最大区别在于：邮件服务器部署在 Internet 上，该邮件服务器与其他邮件服务器的通信消息不经过 NGFW，因此，无法通过检查 IP 地址进行垃圾邮件防范。

图 2 邮件服务器部署在外网



邮件过滤配置流程

介绍邮件过滤特性的配置流程。

在 NGFW 上开启哪种邮件过滤功能与组网、对邮件安全的要求有关，用户可参考表 1 选配。

表 1 邮件过滤配置流程

任务	子任务	配置说明
1、配置邮件过滤	配置垃圾邮件防范	当 NGFW 作为服务器群体的安全网关，为了防止邮件服务器受到垃圾邮件和匿名邮件的攻击，可以在 NGFW 上配置垃圾邮件防范和匿名邮件检测。
	配置匿名邮件检测	
	配置邮箱地址检查	当 NGFW 作为某个企业办公网络的安全网关，且该企业比较重视内部信息的保密性时，可以配置邮箱地址检查控制企业内网用户的邮件发送权限、邮件附件控制来防止内部员工将机密信息通过邮件方式泄露到外部。
	配置邮件附件控制	
2、 配置安全策略	-	步骤 1 仅配置了邮件过滤配置文件。要想启用邮件过滤，还需要配置安全策略，在安全策略中定义流量匹配规则、引用邮件过滤配置文件。

配置邮件地址组

配置 E-Mail 地址检查时会需要引用邮件地址组，可以将具有相同发送或接收权限的邮箱地址加入同一个邮件地址组。

操作步骤

1. 选择“对象 > 邮件地址组”。
2. 在“邮件地址组列表”区域框中，单击“新建”。
3. 配置地址组的组名和描述。

参数	说明
名称	输入地址组的名称。名称必须是唯一的，不能有重复的名称。
描述	输入地址组的描述信息。合理填写描述信息有助于管理员正确理解地址组都保存了哪些邮箱地址，便于地址组的选择、查找和维护。

4. 单击“新建”。
5. 依次输入各项参数。

说明：

当邮件地址组中有多个邮件地址时，被检查的邮件只要匹配其中的一个地址，就匹配此邮件地址组。

参数	说明
匹配方式	匹配方式。 • 前缀：表示匹配方式是前缀匹配，即待匹配的邮件地址要以配置的模式开头。例如：配置了内容为“bcd@ex.com”的邮件地址模式，“bcd@ex.com.cn”等以“bcd@ex.com”开头的邮件地址会被匹配到。 • 后缀：表示匹配方式是后缀匹配，即待匹配的邮件地址要以配置的模式结尾。例如：配置了内容为“bcd@ex.com”的邮件地址模式，“abcd@ex.com”等以“bcd@ex.com”结尾的邮件地址会被匹配到。 • 精确：表示匹配方式是精确匹配，即待匹配的邮件地址要与模式完全一致才会被匹配。例如：配置了内容为“bcd@ex.com”的邮件地址模式，只有“bcd@ex.com”这个邮件地址能被匹配。 • 关键字：表示匹配方式是关键字匹配，即待匹配的邮件地址中只要包含邮件地址模式，就会被匹配。例如：配置了内容为“bcd@ex.com”的邮件地址模式，“bcd@ex.com”、“bcd@ex.com.cn”、“abcd@ex.com”等邮件地址都会被匹配到。
内容	邮件地址在阻断范围之内的将被阻断，其他邮件允许通过。

6. 单击“确定”。
7. 单击“确定”。
8. 单击界面右上角的“提交”。

创建或修改邮件地址组后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对邮件地址组的操作后再统一进行提交。

配置垃圾邮件防范

通过检查发送方 SMTP Server 源 IP 的合法性来防范垃圾邮件。如果命中白名单直接转发、命中黑名单则被当做垃圾邮件处理。

前提条件

了解垃圾邮件防范工作机制。

背景信息

在 NGFW 上可以配置本地白名单、本地黑名单和 RBL 黑名单，它们的匹配优先级顺序为：

- 本地白名单

  当某个邮件的源地址命中了本地白名单，NGFW 直接认定其是合法邮件，本地黑名单和 RBL 黑名单不再对此源 IP 地址进行匹配。白名单的设置有利于提高匹配效率。

- 本地黑名单

  本地黑名单的优先级比 RBL 黑名单高，当某个邮件的源地址命中了本地黑名单，NGFW 直接认定其是垃圾邮件，RBL 黑名单不再对此源 IP 地址进行匹配。

- RBL 黑名单

  RBL 黑名单由第三方组织提供，第三方组织实时维护 RBL 并通过 RBL 服务器对外提供查询服务。

  当 RBL 黑名单不包含 SMTP 请求的源 IP 地址时，无法过滤该邮件。此时，可以通过补充本地黑名单来完成过滤。

说明：

- 本地白名单、本地黑名单、RBL 黑名单配置完毕后，还需创建邮件内容过滤配置文件、在安全策略中引用邮件内容过滤配置文件，配置才会生效。

- 如果需要同时配置本地白名单、本地黑名单、RBL 黑名单，可在这些功能全部配置完毕后，再统一创建邮件内容过滤配置文件、并在安全策略中引用邮件内容过滤配置文件。

配置本地黑名单/白名单

如果已经知道某些 SMTP Server 采取了很好的安全措施、肯定不会发送垃圾邮件，可以将这些 SMTP Server 的 IP 地址加入到本地白名单中；来自这些 SMTP Server 的邮件信息会优先通过，大大提高安全性和快捷性。

配置本地黑名单后，如果某个邮件的发送方源 IP 命中了黑名单，该邮件被直接阻断，不需要再执行 RBL 过滤。如果曾经收到过来自某些 SMTP Server 的垃圾邮件，或已经检测出部分 SMTP Server 专门发送垃圾邮件，可以将这些 SMTP Server 的 IP 地址加入到本地黑名单中；来自这些 SMTP Server 的邮件信息会直接丢弃，大大提高快捷性。

1. 选择“对象 > 安全配置文件 > 邮件过滤” 。
2. 选择进入“垃圾邮件过滤”页签。
3. 选中“垃圾邮件过滤功能”对应的“启用”复选框。
4. 配置黑名单和白名单。可以同时配置黑名单和白名单，也可以只配置其中的一项。
   - 在“白名单”文本框中输入要加入白名单 SMTP Server 的 IP 地址和掩码，可以输入多个 IP 地址，一个 IP 地址一行。
   - 在“黑名单”文本框中输入要加入黑名单 SMTP Server 的 IP 地址和掩码，可以输入多个 IP 地址，一个 IP 地址一行。
5. 单击“应用”。
6. 选择进入“邮件内容过滤”页签。
7. 单击“新建”。
8. 配置邮件内容过滤配置文件的名称和描述。

参数	描述
名称	输入邮件内容过滤配置文件的名称。名称必须是唯一的，不能有重复的名称。当配置安全策略时，名称会出现在“邮件过滤”的参数选择列表中。
描述	输入邮件内容过滤配置文件的描述信息。合理填写描述信息有助于管理员正确理解配置文件的功能，使配置文件变得方便选择、查找和维护。例如：配置 Trust 区域（源）到 DMZ 区域（目的）的邮件过滤策略。

9. 选中“垃圾邮件过滤”对应的复选框。
10. 单击“确定”。
11. 在安全策略中引用邮件过滤文件。
12. 单击“提交”。

创建或修改安全配置文件后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对安全配置文件的操作后再统一进行提交。

配置 RBL 黑名单

配置 RBL 黑名单，IP 地址检查时将使用第三方组织机构维护的黑名单，保证可以过滤最新的垃圾邮件。

1. 选择“对象 > 安全配置文件 > 邮件过滤” 。
2. 选择进入“垃圾邮件过滤”页签。
3. 选中“垃圾邮件过滤功能”对应的“启用”复选框。
4. 配置 DNS 服务器。
   a. 在“首选 DNS 服务器”文本框中输入 DNS 服务器的 IP 地址，配置查询 RBL 黑名单时使用的 DNS 服务器。
   b. **可选：**在“备用 DNS 服务器”文本框中输入备用 DNS 服务器的 IP 地址，首选 DNS 服务器出现网络连接问题时，将使用备用 DNS 服务器。

说明：

选择 DNS 服务器时需要注意：

- 需要保证 DNS 服务器没有被劫持，否则正常邮件可能会被误判为垃圾邮件。
- 需要保证 DNS 服务器使用递归查询方式。

5. 单击“应用”。
6. 配置垃圾邮件配置文件，垃圾邮件配置文件定义了 RBL 过滤使用的远程服务器。

说明：

如果同时配置了多个 RBL 服务器，NGFW 进行 IP 地址查询时，将向最后一个配置的 RBL 服务器发起查询

请求。

. 在“垃圾邮件配置文件”区域框中，单击“新建”。

a. 配置 RBL 服务器的各项参数。

参数	描述
名称	垃圾邮件配置文件名称。名称必须是唯一的，不能有重复的名称。
描述	垃圾邮件配置文件的描述信息。合理填写描述信息有助于管理员快速识别 RBL 服务器。
服务器查询集合	查询集合就是 RBL 服务域名，用来定位 RBL 服务器。查询集合由 RBL 服务提供商提供。一个策略只能配置一个查询集合。 例如：cbl.anti-spam.org.cn。
动作	邮件匹配策略后设备采取的动作。 • 阻断：阻断邮件传输。 • 告警：不阻断邮件传输，但是会发送告警信息。
应答码	应答码会因为 RBL 服务提供商的不同而不一样，具体请咨询 RBL 服务提供商。 • 若配置了指定的应答码，NGFW 会将 RBL 返回的应答码与 NGFW 上配置的应答码进行比较，如果应答码相同，那么视该邮件为垃圾邮件。回复的不是应答码或回复的应答码与在 NGFW 上配置的不一样，放行邮件。 • 如果不清楚应答码是什么时，可以配置为“任意应答码”，表示只要 RBL 服务器回复了应答码（如 127.0.0.1），就视该邮件为垃圾邮件。如果 RBL 服务器不回复应答码或回复的不是应答码（如 NXDOMAIN），放行邮件。 一个垃圾邮件配置文件中最多可以配置 16 条应答码。

b. 单击“确定”。

7. 选择进入“邮件内容过滤”页签。

8. 单击“新建”。

9. 配置邮件内容过滤配置文件的名称和描述。

参数	描述
名称	输入邮件内容过滤配置文件的名称。名称必须是唯一的，不能有重复的名称。当配置安全策略时，名称会出现在“邮件过滤”的参数选择列表中。
描述	输入邮件内容过滤配置文件的描述信息。合理填写描述信息有助于管理员正确理解配置文件的功能，使配置文件变得方便选择、查找和维护。例如：配置 Trust 区域（源）到 DMZ 区域（目的）的邮件过滤策略。

10. 选中“垃圾邮件过滤”对应的复选框。

11. 单击“确定”。
12. 在安全策略中引用邮件过滤文件。
13. 单击“提交”。

创建或修改安全配置文件后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对安全配置文件的操作后再统一进行提交。

后续处理

查看或解除安全策略与配置文件的引用关系。

1. 在配置文件的列表界面单击“引用计数”下的“查看”，可以看到配置文件被哪些安全策略引用。
2. 选中安全策略后，单击“解除”，可以解除安全策略与此配置文件的引用关系。

单击“解除所有”，在弹出的对话框中单击“确定”，解除所有安全策略对此配置文件的引用。

配置匿名邮件检测

匿名邮件指的是发件人为空的邮件，匿名邮件有可能包含暴力、色情等对他人有威胁的信息。配置匿名邮件检测，可以控制是否允许用户发送和接收匿名邮件。

前提条件

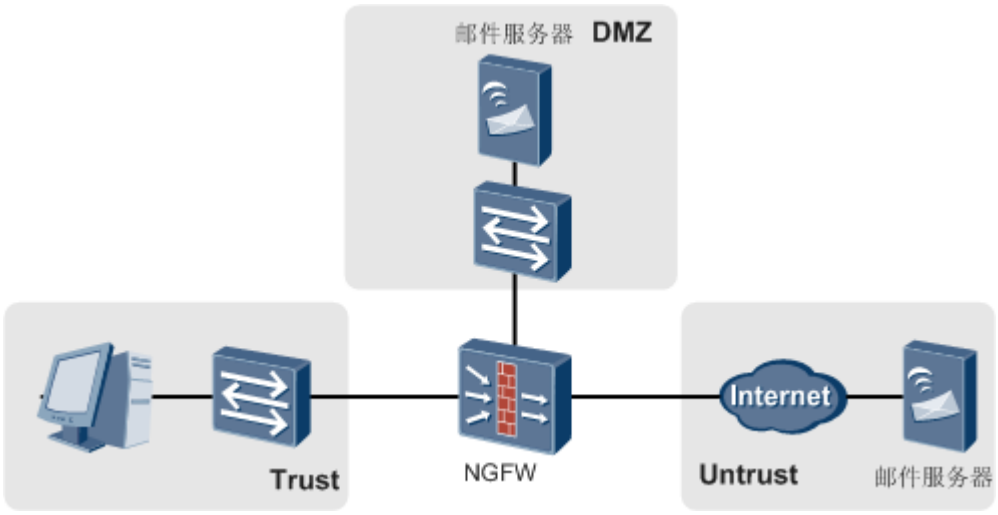
了解基于邮件内容的过滤工作机制。

背景信息

匿名邮件检测分为发送方向和接收方向：

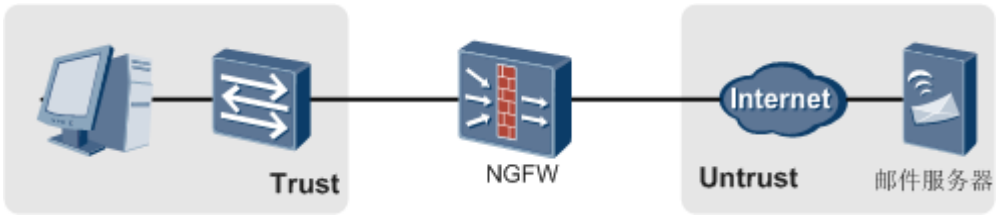
- 如果检测到封装在 SMTP 消息中的邮件信息，NGFW 执行发送方向的邮件过滤。典型应用如图 1 所示，在 Untrust 区域和 DMZ 区域之间开启发送方向匿名检测，可以防止邮件服务器受到匿名邮件的攻击。

图 1 邮件服务器在内网



- 如果检测到封装在 POP3 消息或 IMAP 消息中的邮件信息，NGFW 执行接收方向的邮件过滤。典型应用如图 2 所示，在 Trust 区域和 Untrust 区域之间开启接收方向匿名检测，可以防止内网 PC 下载匿名邮件。

图 2 邮件服务器在外网



说明：

内网用户使用 IMAP 方式下载邮件时，如果检测到匿名邮件，仅发送告警信息，不会阻断邮件。

操作步骤

1. 选择“对象 > 安全配置文件 > 邮件过滤”。
2. 单击“邮件内容过滤”。
3. 单击“新建”。
4. 配置邮件过滤策略的名称和描述。

参数	描述
名称	输入邮件过滤策略的名称。名称必须是唯一的，不能有重复的名称。当配置安全策略时，名称会出现在“邮件过滤”的参数选择列表中。
描述	输入邮件过滤配置文件的描述信息。合理填写描述信息有助于管理员正确理解配置文件的功能，使配置文件变得方便选择、查找和维护。例如：配置 Trust 区域（源）到 DMZ 区域（目的）的邮件过滤策略。

5. 配置发送方向匿名邮件检测。

   在“发送匿名邮件”中选择过滤动作。

参数	说明
允许	放行邮件。
告警	放行邮件，但是会发送告警信息。
阻断	阻断邮件。

6. 配置接收方向匿名邮件检测。

   在“接收匿名邮件”中选择过滤动作。

参数	说明
允许	放行邮件。
告警	放行邮件，但是会发送告警信息。
阻断	阻断邮件。

7. 单击“确定”，保存邮件内容过滤配置文件。

   说明：

   如需配置邮箱地址检查和配置邮件附件控制，可先继续配置邮箱地址检查和配置邮件附件控制，再统一保存配置文件、并在安全策略中对其引用 。

8. 在安全策略中引用邮件过滤文件。

9. 单击“提交”。

   创建或修改安全配置文件后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对安全配置文件的操作后再统一进行提交。

后续处理

查看或解除安全策略与配置文件的引用关系。

1. 在配置文件的列表界面单击“引用计数”下的“查看”，可以看到配置文件被哪些安全策略引用。
2. 选中安全策略后，单击“解除”，可以解除安全策略与此配置文件的引用关系。

   单击“解除所有”，在弹出的对话框中单击“确定”，解除所有安全策略对此配置文件的引用。

配置邮箱地址检查

邮箱地址是邮件用户注册的邮箱地址。配置邮箱地址检查，可以根据邮箱地址决定是否允许指定邮箱发送或接收邮件。

前提条件

了解基于邮件内容的过滤工作机制。

背景信息

邮箱地址检查主要是对局域网用户发送或下载邮件的权限进行控制。邮箱地址检查的配置项包括：

- 检测方向，包括发送方向和接收方向。
  - 如果检测到封装在 SMTP 消息中的邮件信息，NGFW 执行发送方向的邮件过滤。
  - 如果检测到封装在 POP3 消息或 IMAP 消息中的邮件信息，NGFW 执行接收方向的邮件过滤。

    说明：

    内网用户使用 IMAP 方式下载邮件时，如果检测到匿名邮件，仅发送告警信息，不会阻断邮件。
- 匹配条件，对发件人邮箱地址还是收件人邮箱地址进行过滤。

组网、检测方向和匹配条件共同决定是对发送权限还是对接收权限进行控制，邮件内容过滤主要有两种典型组网：

- 邮件服务器在内网，配置方法可参考图 1。

  图 1 邮件服务器在内网

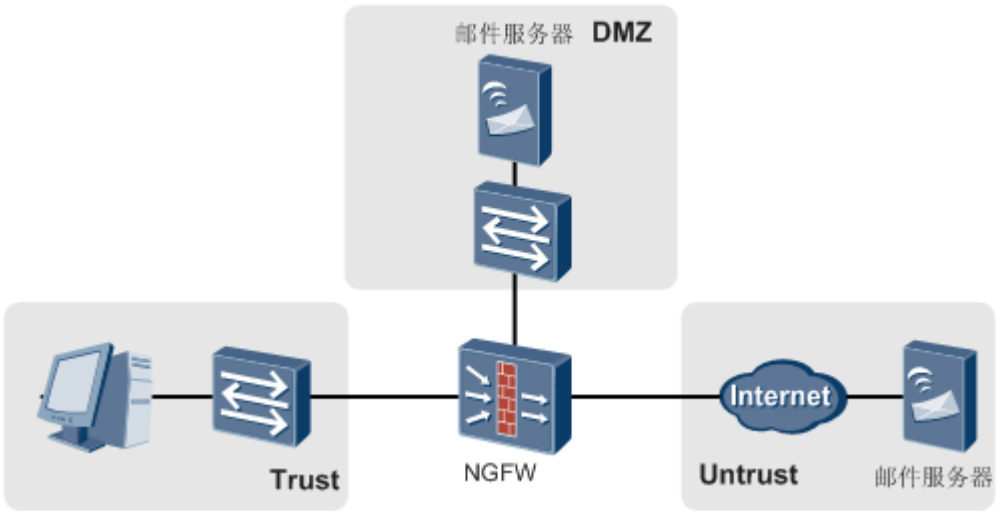


表 1 邮箱地址检查配置参考（邮件服务器在内网）	
需求	**配置方法**
过滤掉来自指定邮箱的电子邮件。 例如，如果检测到 abc@example.com 经常发送垃圾邮件，可以配置过滤掉发件人为“abc@example.com”的邮件。	在 Untrust 区域和 DMZ 区域之间开启发送方向地址检查，以发件人的邮箱地址为过滤条件。
配置内网用户可以下载来自哪些外网用户的邮件。 例如，配置内网用户只能下载来自“张三”和“李四”的邮件。	在 Trust 区域和 DMZ 区域之间开启接收方向地址检查，以发件人的邮箱地址为过滤条件。
配置哪些内网用户具有邮件下载权限。 例如，配置只有“张三”和“李四”才可以下载邮件。	在 Untrust 区域和 DMZ 区域之间开启发送方向地址检查，以收件人的邮箱地址为过滤条件。
	在 Trust 区域和 DMZ 区域之间开启接收方向地址检查，以收件人的邮箱地址为过滤条件。
配置哪些内网用户具有邮件外发权限。 例如，配置只有“张三”和“李四”具备邮件外发权限。	在 Trust 区域和 DMZ 区域之间开启发送方向地址检查，以发件人的邮箱地址为过滤条件。
配置内网用户可以向哪些外网用户发送邮件。 例如，配置内网用户只能把邮件发送给“张三”或“李四”。	在 Trust 区域和 DMZ 区域之间开启发送方向地址检查，以收件人的邮箱地址为过滤条件。

- 邮件服务器在外网，配置方法可参考图 2。

图 2 邮件服务器在外网

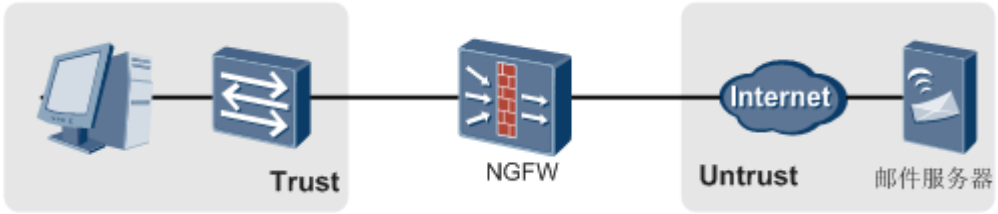


表 2 邮箱地址检查配置参考（邮件服务器在外网）	
需求	**配置方法**
配置哪些内网用户具有邮件外发权限。 例如，配置只有“张三”和“李四”具备邮件外发权限。	在 Trust 区域和 Untrust 区域之间开启发送方向地址检查，以发件人的邮箱地址为过滤条件。
配置内网用户可以向哪些外网用户发送邮件。 例如，配置内网用户只能把邮件发送给“张三”或“李四”。	在 Trust 区域和 Untrust 区域之间开启发送方向地址检查，以收件人的邮箱地址为过滤条件。
配置哪些内网用户具有邮件下载权限。 例如，配置只有“张三”和“李四”才可以下载邮件。	在 Trust 区域和 Untrust 区域之间开启接收方向地址检查，以收件人的邮箱地址为过滤条件。
配置内网用户可以下载来自哪些外网用户的邮件。 例如，配置内网用户只能下载来自“张三”和“李四”的邮件	在 Trust 区域和 Untrust 区域之间开启接收方向地址检查，以发件人的邮箱地址为过滤条件。

操作步骤

1. 选择“对象 > 安全配置文件 > 邮件过滤”。
2. 单击“邮件内容过滤”。
3. 单击“新建”。
4. 配置邮件内容过滤配置文件的名称和描述。

参数	描述
名称	输入邮件过滤策略的名称。名称必须是唯一的，不能有重复的名称。当配置安全策略时，名称会出现在“邮件过滤”的参数选择列表中。
描述	输入邮件过滤配置文件的描述信息。合理填写描述信息有助于管理员正确理解配置文件的功能，使配置文件变得方便选择、查找和维护。例如：配置 Trust 区域（源）到 DMZ 区域（目的）的邮件过滤策略。

5. 配置发送方向邮箱地址检查。
   a. 单击“发送邮件”中发件人地址、收件人地址对应的  。
   b. 选择处理动作。

参数	说明
允许	放行邮件的条件是发件人或收件人地址与邮件地址组匹配，不匹配的邮件将被阻断。

参数	说明
阻断	阻断邮件的条件是发件人或收件人地址与邮件地址组匹配，不匹配的邮件将得以放行。

c. 选择邮件地址组，配置使用哪些邮箱地址作为地址检查的匹配条件。

说明：

当邮件地址组中有多个邮件地址时，被检查的邮件只要匹配其中的一个地址，就匹配此邮件地址组。

可以引用已经创建的邮件地址组，步骤如下：

1. 单击，将邮件地址组移到“已选”区域框中。
2. 单击“确定”。

也可以新建邮件地址组，步骤如下：

3. 在“已选”区域框中，单击“新建”。
4. 配置地址组的组名和描述。

参数	说明
名称	输入地址组的名称。名称必须是唯一的，不能有重复的名称。
描述	输入地址组的描述信息。合理填写描述信息有助于管理员正确理解地址组都保存了哪些邮箱地址，便于地址组的选择、查找和维护。

5. 单击“新建”。
6. 依次输入各项参数。

参数	说明
匹配方式	匹配方式。 • 前缀：表示匹配方式是前缀匹配，即待匹配的邮件地址要以配置的模式开头。例如：配置了内容为“bcd@example.com”的邮件地址模式，“bcd@example.com.cn”等以“bcd@example.com”开头的邮件地址会被匹配到。 • 后缀：表示匹配方式是后缀匹配，即待匹配的邮件地址要以配置的模式结尾。例如：配置了内容为“bcd@example.com”的邮件地址模式，“abcd@example.com”等以“bcd@example.com”结尾的邮件地址会被匹配到。

参数	说明
	• 精确：表示匹配方式是精确匹配，即待匹配的邮件地址要与模式完全一致才会被匹配。例如：配置了内容为“bcd@example.com”的邮件地址模式，只有“bcd@example.com”这个邮件地址能被匹配。 • 关键字：表示匹配方式是关键字匹配，即待匹配的邮件地址中只要包含邮件地址模式，就会被匹配。例如：配置了内容为“bcd@example.com”的邮件地址模式，“bcd@example.com”、“bcd@example.com.cn”、“abcd@example.com”等邮件地址都会被匹配到。
内容	邮件地址在阻断范围之内的将被阻断，其他邮件允许通过。

7. 单击“确定”。
8. 单击“确定”。
9. 单击“确定”。

6. 配置接收方向邮箱地址检查。

a. 单击“接收邮件”中发件人地址、收件人地址对应的。

b. 选择处理动作。

参数	说明
允许	邮件地址不在允许范围之内的邮件将被禁止。
阻断	邮件地址在阻断范围之内的将被阻断，其他邮件允许通过。

c. 选择邮件地址组，配置使用哪些邮箱地址作为地址检查的匹配条件。

说明：

当邮件地址组中有多个邮件地址时，被检查的邮件只要匹配其中的一个地址，就匹配此邮件地址组。

可以引用已经创建的邮件地址组，步骤如下：

1. 单击，将邮件地址组移到“已选”区域框中。
2. 单击“确定”。

也可以新建邮件地址组，步骤如下：

3. 在“已选”区域框中，单击“新建”。
4. 配置地址组的组名和描述。

参数	说明
名称	输入地址组的名称。名称必须是唯一的，不能有重复的名称。
描述	输入地址组的描述信息。合理填写描述信息有助于管理员正确理解地址组都保存了哪些邮箱地址，便于地址组的选择、查找和维护。

5. 单击“新建”。

6. 依次输入各项参数。

参数	说明
匹配方式	匹配方式。 • 前缀：表示匹配方式是前缀匹配，即待匹配的邮件地址要以配置的模式开头。例如：配置了内容为“bcd@example.com”的邮件地址模式，“bcd@example.com.cn”等以“bcd@example.com”开头的邮件地址会被匹配到。 • 后缀：表示匹配方式是后缀匹配，即待匹配的邮件地址要以配置的模式结尾。例如：配置了内容为“bcd@example.com”的邮件地址模式，“abcd@example.com”等以“bcd@example.com”结尾的邮件地址会被匹配到。 • 精确：表示匹配方式是精确匹配，即待匹配的邮件地址要与模式完全一致才会被匹配。例如：配置了内容为“bcd@example.com”的邮件地址模式，只有“bcd@example.com”这个邮件地址能被匹配。 • 关键字：表示匹配方式是关键字匹配，即待匹配的邮件地址中只要包含邮件地址模式，就会被匹配。例如：配置了内容为“bcd@example.com”的邮件地址模式，“bcd@example.com”、“bcd@example.com.cn”、“abcd@example.com”等邮件地址都会被匹配到。
内容	邮件地址在阻断范围之内的将被阻断，其他邮件允许通过。

7. 单击“确定”。

8. 单击“确定”。

9. 单击“确定”。

7. 单击“确定”。

说明：

如需配置邮箱地址检查和配置邮件附件控制，可先继续配置邮箱地址检查和配置邮件附件控制，再统一保存配置文件、并在安全策略中对其引用 。

8. 在安全策略中引用邮件过滤文件。

9. 单击“提交”。

   创建或修改安全配置文件后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对安全配置文件的操作后再统一进行提交。

后续处理

查看或解除安全策略与配置文件的引用关系。

1. 在配置文件的列表界面单击“引用计数”下的“查看”，可以看到配置文件被哪些安全策略引用。
2. 选中安全策略后，单击“解除”，可以解除安全策略与此配置文件的引用关系。

   单击“解除所有”，在弹出的对话框中单击“确定”，解除所有安全策略对此配置文件的引用。

配置邮件附件控制

通过配置邮件附件控制，可以控制附件的大小、个数。

前提条件

了解基于邮件内容的过滤工作机制。

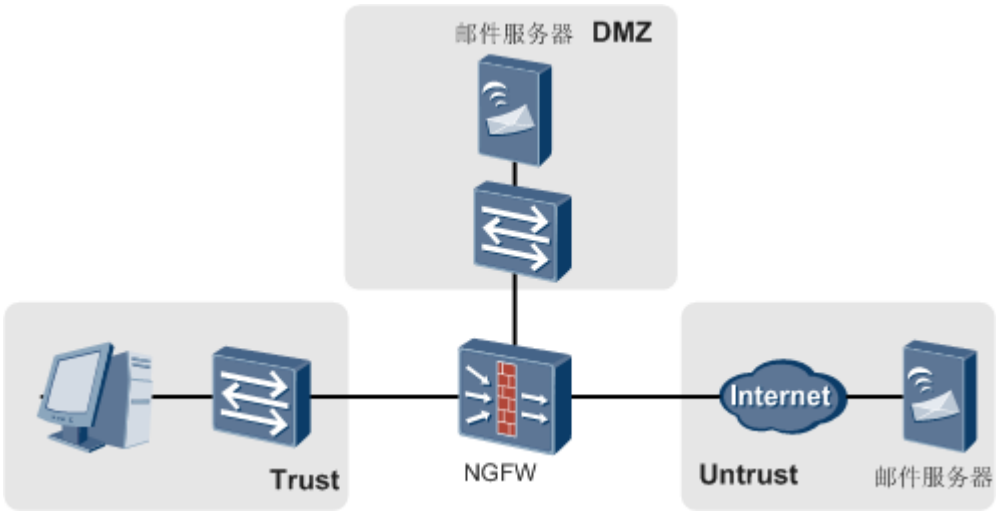
背景信息

一些组织机构比较重视内部信息的保密性，配置邮件附件控制，可以控制局域网用户可发送附件的大小和个数，一定程度上防止大量信息通过邮件泄露出去。

附件大小检测分为发送方向和接收方向：

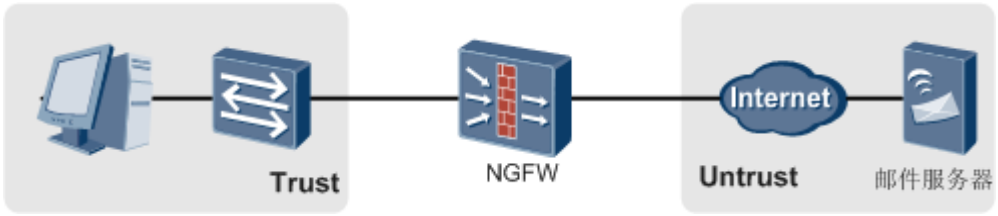
- 如果检测到封装在 SMTP 消息中的邮件信息，NGFW 执行发送方向的邮件过滤。典型组网如图 1 所示，在 Trust 区域和 DMZ 区域之间开启发送方向附件控制，可以防止机密信息通过邮件方式泄露到外网。

  图 1 邮件服务器在内网



- 如果检测到封装在 POP3 消息或 IMAP 消息中的邮件信息，NGFW 执行接收方向的邮件过滤。典型组网如图 2 所示，在 Trust 区域和 Untrust 区域之间开启接收方向附件控制，可以有效防止病毒入侵内网以及附件下载时占用过多的带宽资源。

图 2 邮件服务器在外网



说明：

- 用户使用 SMTP 和 POP3(IMAP)发送和接收邮件时，NGFW 可以执行附件过滤。
- 内网用户使用 IMAP 方式下载邮件时，如果检测到不符合要求的附件，仅发送告警信息，不会阻断邮件。

操作步骤

1. 选择“对象 > 安全配置文件 > 邮件过滤”。
2. 单击“邮件内容过滤”。
3. 单击“新建”。
4. 配置邮件内容过滤配置文件的名称和描述。

参数	描述
名称	输入邮件过滤策略的名称。名称必须是唯一的，不能有重复的名称。当配置安全策略时，名称会出现在“邮件过滤”的参数选择列表中。

参数	描述
描述	输入邮件过滤配置文件的描述信息。合理填写描述信息有助于管理员正确理解配置文件的功能，使配置文件变得方便选择、查找和维护。例如：配置 Trust 区域（源）到 DMZ 区域（目的）的邮件过滤策略。

5. 配置附件大小及个数控制。

   a. 单击“附件大小及个数控制”。

   b. 选择“发送附件个数上限”、“接收附件个数上限”、“发送附件大小限制”或“接收附件大小限制”，输入数值。

   c. 在“处理动作”中选择处理动作。

参数	说明
告警	放行邮件，但是会发送告警信息。
阻断	阻断邮件。

6. 单击“确定”。

7. 在安全策略中引用邮件过滤文件。关于安全策略的具体配置请参见安全策略。

8. 单击“提交”。

   创建或修改安全配置文件后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对安全配置文件的操作后再统一进行提交。

后续处理

查看或解除安全策略与配置文件的引用关系。

1. 在配置文件的列表界面单击“引用计数”下的“查看”，可以看到配置文件被哪些安全策略引用。

2. 选中安全策略后，单击“解除”，可以解除安全策略与此配置文件的引用关系。

   单击“解除所有”，在弹出的对话框中单击“确定”，解除所有安全策略对此配置文件的引用。

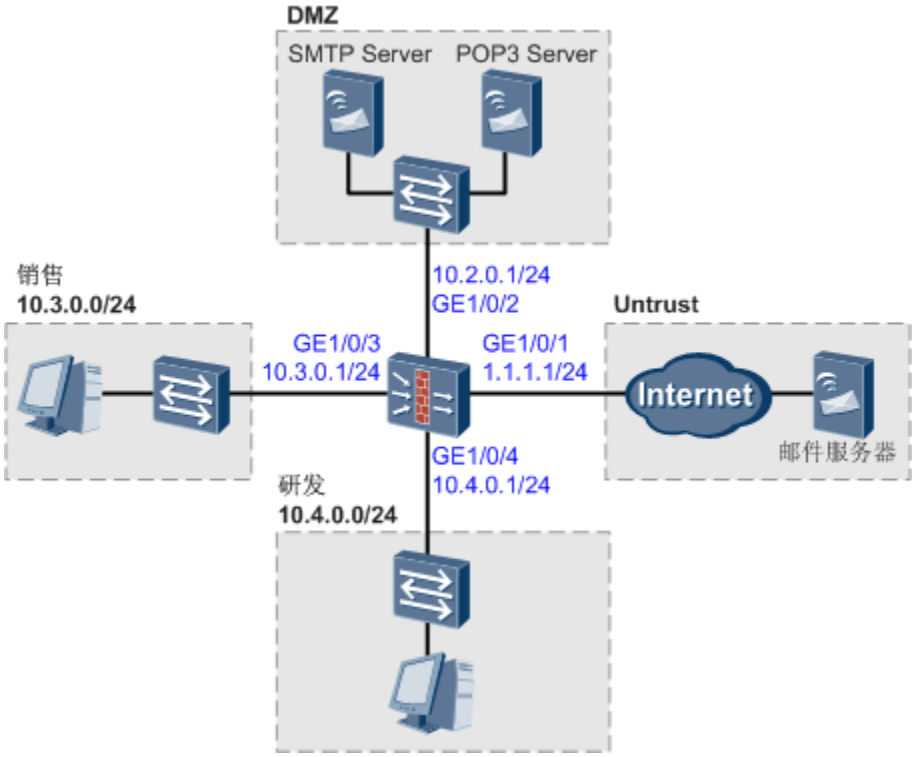
举例：配置邮件过滤

以 NGFW 作为分支机构安全网关为例，介绍邮件过滤的配置方法。

组网需求

某公司规模在 200 人左右，分为销售、研发两个大部门。该公司具有独立的邮件域名，并且在公司内部部署了邮件服务器。

图 1 邮件过滤组网



该公司对邮件安全的需求如下：

- 防止位于 DMZ 区域的邮件服务器收到大量垃圾邮件和匿名邮件，避免占用网络资源。
- 为了避免机密信息通过邮件方式泄露出去，对各部门人员的邮件发送权限进行控制。
  - 研发人员中只有张三、李四同时具有邮件发送、接收权限，其他人只能接收邮件，不能发送邮件。
  - 销售人员可以发送和接收邮件，但发送附件大小不能超过 10M。

配置思路

1. 构建公司局域网，将 NGFW 作为安全网关。
   - 将邮件服务器划分到 DMZ 区域。
   - 将销售部门员工划分到自定义“sale”安全区域。
   - 将研发部门员工划分到自定义“research”安全区域。

- 将 Internet 划分到 Untrust 区域。

2. 配置邮件过滤。

邮件配置文件是基于区域的，需要规划各区域之间的邮件过滤策略。

需求	配置思路
防止邮件服务器收到大量垃圾邮件，避免占用网络资源。	在 Untrust 和 DMZ 区域之间开启垃圾邮件防范，使用 RBL 服务器“cbl.anti-spam.org.cn”。
防止邮件服务器收到匿名邮件，避免占用网络资源。	在 Untrust 和 DMZ 区域之间配置匿名邮件检测。
研发人员中只有张三、李四同时具有邮件发送、接收权限，其他人只能接收邮件，不能发送邮件。	在“research”区域和 DMZ 区域之间配置发送方向邮件地址检查，按照发件人邮箱地址进行过滤，只允许张三和李四发送邮件。
销售人员可以发送和接收邮件，但发送附件大小不能超过 10M。	在“sale”区域和 DMZ 区域之间配置发送方向附件大小控制，将“sale”区域人员可发送附件大小控制在 10M 以内。

操作步骤

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。

a. 将接口 GE1/0/1 加入 Untrust 区域。

1. 选择“网络 > 接口”。

2. 选择 GE1/0/1 对应的，按如下参数配置。

安全区域	untrust
IP 地址	1.1.1.1/24

3. 单击“确定”。

b. 参考上述步骤，将接口 GE1/0/2 加入 DMZ 区域。

GE1/0/2 接口配置如下。

安全区域	dmz
IP 地址	10.2.0.1/24

c. 创建安全区域“sale”，将接口 GE1/0/3 加入“sale”区域。

1. 选择“网络 > 安全区域”。

2. 单击“新建”。

3. 按如下参数配置。

名称	sale
优先级	60

4. 在“未加入域的接口”中选择 GE1/0/3，单击  ，将 GE1/0/3 加入“sale”区域。

5. 单击“确定”。

6. 选择“网络 > 接口”。

7. 选择 GE1/0/3 对应的  ，按如下参数配置。

安全区域	sale
IP 地址	10.3.0.1/24

8. 单击“确定”。

d. 参考上述步骤，创建安全区域“research”，将接口 GE1/0/4 加入“research”区域。

“research”区域配置如下。

名称	research
优先级	70

“GE1/0/4”接口配置如下。

安全区域	research
IP 地址	10.4.0.1/24

2. 在 Untrust 和 DMZ 区域之间配置垃圾邮件防范和匿名邮件检测。

a. 选择“对象 > 安全配置文件 > 邮件过滤” 。

b. 选择进入“垃圾邮件过滤”页签。

c. 选中“垃圾邮件过滤功能”对应的“启用”复选框。

d. 配置首选 DNS 服务器，DNS 服务器的 IP 地址为“10.10.10.10”。

e. 单击“应用”。

f. 配置垃圾邮件配置文件，使用 RBL 服务器“cbl.anti-spam.org.cn”。

1. 在“垃圾邮件配置文件”区域框中，单击“新建”。

2. 配置 RBL 服务器的各项参数。

名称	rbl server
服务器查询集合	cbl.anti-spam.org.cn
动作	阻断
应答码	任意应答码

3. 单击“确定”。

g. 选择进入“邮件内容过滤”。

h. 单击“新建”。

i. 配置邮件内容过滤配置文件的名称和描述。

名称	profile_mail_untrust_dmz
描述	Untrust 区域到 DMZ 区域的邮件策略

j. 选中“垃圾邮件过滤”对应的复选框。

k. 在“发送匿名邮件”中将过滤动作配置为阻断。

l. 单击“确定”。

m. 配置 DMZ 区域和 Untrust 区域之间的安全策略。

1. 选择“策略 > 安全策略 > 安全策略”。

2. 单击“新建”，按如下参数配置从 Untrust 到 DMZ 的域间策略。

名称	policy_sec_untrust_dmz
描述	Untrust 区域到 DMZ 区域的安全策略
源安全区域	Untrust
目的安全区域	DMZ
动作	允许
内容安全	
邮件过滤	profile_mail_untrust_dmz

3. 单击“确定”。

3. 在“sale”区域和 DMZ 区域之间配置发送方向附件控制，将“sale”区域人员可发送附件大小控制在 10M 以内。

a. 选择“对象 > 安全配置文件 > 邮件过滤”。

b. 选择“邮件内容过滤”。

c. 单击“新建”。

d. 配置邮件过滤策略的“名称”和“描述”。

名称	profile_mail_sale_dmz
描述	sale 区域到 DMZ 区域的邮件过滤策略

e. 单击“附件大小及个数控制”。

f. 在“发送附件大小限制”中，输入 10240。

g. 在“处理动作”中将处理动作配置为阻断。

h. 单击“确定”。

i. 配置 sale 区域和 DMZ 区域之间的安全策略。

1. 选择“策略 > 安全策略 > 安全策略”。

2. 单击“新建”，按如下参数配置从 sale 到 DMZ 的域间策略。

名称	policy_sec_sale_dmz
描述	sale 区域到 DMZ 区域的安全策略
源安全区域	sale
目的安全区域	DMZ
动作	允许
内容安全	
邮件过滤	profile_mail_sale_dmz

3. 单击“确定”。

4. 在“research”区域和 DMZ 区域之间配置发送方向邮件地址检查，按照发件人邮箱地址进行过滤，只允许张三和李四具备邮件发送权限。

a. 选择“对象 > 安全配置文件 > 邮件过滤”。

b. 单击“邮件内容过滤”。

c. 单击“新建”。

d. 配置邮件内容过滤配置文件的“名称”和“描述”。

名称	profile_mail_research_dmz

描述	Research 区域到 DMZ 区域的邮件过滤策略

e. 单击“发送邮件”中发件人地址对应的  。

f. 选择处理动作，配置为“允许”。

g. 在“已选”区域框中，单击“新建”。

h. 配置地址组的“名称”和“描述”。

名称	mail_group_research
描述	Resarch 区域具有发送权限的邮箱地址列表。

i. 在“邮件地址列表”中单击“新建”。

j. 依次输入各项参数。

匹配方式	精确
内容	zhangsan@huawei.com

k. 单击“确定”。

l. 参考步骤 h、步骤 i 和步骤 j，将李四的邮箱地址“lisi@huawei.com”加入到地址组中。

m. 单击“确定”。

n. 单击“确定”。

o. 单击“确定”。

p. 配置 research 区域和 DMZ 区域之间的安全策略。

1. 选择“策略 > 安全策略 > 安全策略”。

2. 单击“新建”，按如下参数配置从 research 到 DMZ 的域间策略。

名称	policy_sec_research_dmz
描述	research 区域到 DMZ 区域的安全策略
源安全区域	research
目的安全区域	DMZ
动作	允许
内容安全	
邮件过滤	profile_mail_research_dmz

3. 单击“确定”。

5. 单击“提交”。

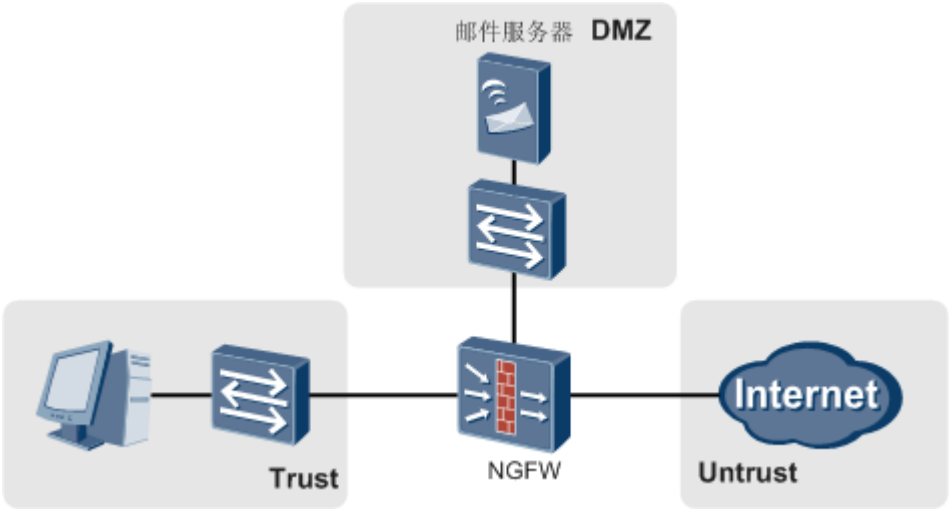
用户收到大量垃圾邮件

内网用户收到大量垃圾邮件。

现象描述

如图 1 所示，NGFW 上配置了垃圾邮件防范功能，但内网用户仍然收到大量垃圾邮件。

图 1 网络环境示意图



定位思路

诊断现象	可能原因	定位处理方法
内网用户收到大量垃圾邮件。	1：配置错误。	参考配置垃圾邮件防范，检查是否存在配置错误。
	2：垃圾邮件发送方 SMTP Server 的 IP 地址不在黑名单内。	将发送垃圾邮件 SMTP Server 的源 IP 加入本地黑名单，配置方法参见配置垃圾邮件防范。

如果以上原因均已排查无误，问题仍然没有解决，请联系技术支持工程师处理。

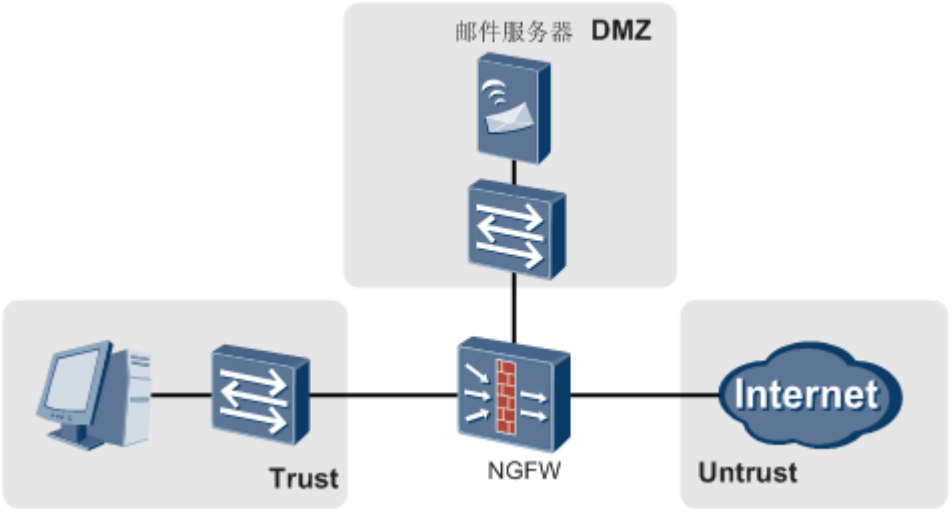
正常邮件被误判为垃圾邮件

用户反馈无法收到邮件。

现象描述

如图 1 所示，NGFW 上配置了垃圾邮件防范功能后，正常邮件被误判为垃圾邮件。

图 1 网络环境示意图



定位思路

诊断现象	可能原因	定位处理方法
查看日志，正常邮件被误判为垃圾邮件。	使用被劫持了的 DNS 服务器。	DNS 劫持是指服务提供商为引导用户访问其增值站点或合作站点，对 DNS 查询结果做修改，在接收到一个不存在结果的 DNS 查询时，总是返回一些特定的 IP 地址，使用户访问到这些增值站点。 需要保证 DNS 服务器没有被劫持，否则正常邮件可能会被误判为垃圾邮件。 1. 使用 Windows 自带的 nslookup 工具测试 DNS 服务器：在“开始 > 运行”中输入 nslookup，单击“确定”，启用 nslookup 工具。 2. 使用 RBL 服务提供商提供的测试地址进行测试（该测试地址在黑名单列表中）。如果返回的应答码与 RBL 服务提供商提供的应答码一致时，表示该 DNS 服务器可用。 举个例子，假设，DNS 服务器为 165.87.13.129，RBL 服务提供商的 RBL 服务名为 cbl.anti-spam.org.cn、测试地址为 127.0.0.2、应答码为 127.0.8.2。 **> server 165.87.13.129** //输入要测试的 DNS 服务器地址 Default Server: nscache.prserv.net Address: 165.87.13.129 **> 2.0.0.127.cbl.anti-spam.org.cn** //将测试地址进行逆转，与 RBL 服务名拼成一个字符串，输入拼接后的字符串 Server: nscache.prserv.net Address: 165.87.13.129 Non-authoritative answer: Name: 2.0.0.127.cbl.anti-spam.org.cn Address: **127.0.8.2** **//预期的结果：返回的应答码与 cbl.anti-spam.org.cn 提供的应答码一致，该 DNS 服务器可用**

<table>
<tr><th>诊断现象</th><th>可能原因</th><th>定位处理方法</th></tr>
<tr><td></td><td></td><td>3. 使用不属于 RBL 黑名单的 IP 地址进行测试。192.168.0.1 这个 IP 地址一般不会被列入 RBL 黑名单，可用使用这个 IP 地址进行测试。
4. > server 165.87.13.129//输入要测试的 DNS 服务器地址
5. Default Server: nscache.prserv.net
6. Address: 165.87.13.129
7. > 1.0.168.192.cbl.anti-spam.org.cn//将测试地址进行逆转，与 RBL 服务名拼成一个字符串，输入拼接后的字符串
8.
9. Server: nscache.prserv.net
10. Address: 165.87.13.129
11.
12. *** nscache.prserv.net can't find 1.0.168.192.cbl.anti-spam.org.cn: Non-existent domain
//反馈结果为 Non-existent domain，表示 DNS 服务器没有被劫持；反馈 IP 地址表示该 DNS 服务器被劫持</td></tr>
<tr><td></td><td>DNS 服务器使用迭代查询方式。</td><td>DNS 有两种查询方式，递归查询和迭代查询。DNS 服务器必须使用递归查询方式，使用迭代查询时，正常邮件可能会被误判为垃圾邮件。
1. 使用 Windows 自带的 nslookup 工具测试 DNS 服务器：在“开始 > 运行”中输入 nslookup，单击“确定”，启用 nslookup 工具。
2. 打开 Debug 开关。
3. > set debug //打开 debug 开关
4. 使用 RBL 服务提供商提供的测试地址进行测试（该测试地址在黑名单列表中）。如果提示 recursion avail，表示支持递归查询。
举个例子，假设，DNS 服务器为 165.87.13.129，RBL 服务提供商的 RBL 服务名为 cbl.anti-spam.org.cn、测试地址为 127.0.0.2。
> server 165.87.13.129 //输入要测试的 DNS 服务器地址

Got answer:
HEADER:
opcode = QUERY, id = 3, rcode = NOERROR
header flags: response, want recursion, recursion avail.
questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:
129.13.87.165.in-addr.arpa, type = PTR, class = IN
ANSWERS:
-> 129.13.87.165.in-addr.arpa
name = nscache.prserv.net
ttl = 86203 (23 hours 56 mins 43 secs)</td></tr>
</table>

诊断现象	可能原因	定位处理方法
		------------ Default Server: nscache.prserv.net Address: 165.87.13.129 ------------ Default Server: nscache.prserv.net Address: 165.87.13.129 **> 2.0.0.127.cbl.anti-spam.org.cn** //将测试地址进行逆转，与 RBL 服务名拼成一个字符串，输入拼接后的字符串 Server: nscache.prserv.net Address: 165.87.13.129 ------------ Got answer: HEADER: opcode = QUERY, id = 4, rcode = NOERROR header flags: response, want recursion, **recursion avail.** questions = 1, answers = 1, authority records = 7, additional = 7 QUESTIONS: 2.0.0.127.cbl.anti-spam.org.cn, type = A, class = IN ANSWERS: -> 2.0.0.127.cbl.anti-spam.org.cn internet address = 127.0.8.2 ttl = 9999 (2 hours 46 mins 39 secs) AUTHORITY RECORDS: -> cbl.anti-spam.org.cn nameserver = ns2.anti-spam.org.cn ttl = 9999 (2 hours 46 mins 39 secs) -> cbl.anti-spam.org.cn nameserver = ns4.anti-spam.org.cn ttl = 9999 (2 hours 46 mins 39 secs) -> cbl.anti-spam.org.cn nameserver = ns5.anti-spam.org.cn ttl = 9999 (2 hours 46 mins 39 secs) -> cbl.anti-spam.org.cn nameserver = ns3.anti-spam.org.cn ttl = 9999 (2 hours 46 mins 39 secs)

诊断现象	可能原因	定位处理方法
		-> cbl.anti-spam.org.cn nameserver = ns8.anti-spam.org.cn ttl = 9999 (2 hours 46 mins 39 secs) -> cbl.anti-spam.org.cn nameserver = ns1.anti-spam.org.cn ttl = 9999 (2 hours 46 mins 39 secs) -> cbl.anti-spam.org.cn nameserver = ns7.anti-spam.org.cn ttl = 9999 (2 hours 46 mins 39 secs) ADDITIONAL RECORDS: -> ns2.anti-spam.org.cn internet address = 113.11.200.186 ttl = 4633 (1 hour 17 mins 13 secs) -> ns4.anti-spam.org.cn internet address = 204.15.82.90 ttl = 4633 (1 hour 17 mins 13 secs) -> ns5.anti-spam.org.cn internet address = 161.69.225.9 ttl = 4633 (1 hour 17 mins 13 secs) -> ns3.anti-spam.org.cn internet address = 113.11.204.130 ttl = 4633 (1 hour 17 mins 13 secs) -> ns8.anti-spam.org.cn internet address = 202.106.182.243 ttl = 4634 (1 hour 17 mins 14 secs) -> ns1.anti-spam.org.cn internet address = 211.157.2.94 ttl = 4633 (1 hour 17 mins 13 secs) -> ns7.anti-spam.org.cn internet address = 202.106.182.244 ttl = 4633 (1 hour 17 mins 13 secs) ------------ Non-authoritative answer: Name: 2.0.0.127.cbl.anti-spam.org.cn Address: 127.0.8.2 5. 使用不属于 RBL 黑名单的 IP 地址进行测试。1.1.1.1 这个 IP 地址一般不会被列入 RBL 黑名单，可用使用这个 IP 地址进行测试。如果提示 recursion avail，表示支持递归查询。 > 1.1.1.1.cbl.anti-spam.org.cn //将 IP 地址逆转后与 RBL 服务名拼成一个字符串，输入拼接后的字符串 Server: nscache.prserv.net Address: 165.87.13.129

诊断现象	可能原因	定位处理方法
		------------ Got answer: HEADER: opcode = QUERY, id = 5, rcode = NXDOMAIN header flags: response, want recursion, recursion avail. questions = 1, answers = 0, authority records = 1, additional = 0 QUESTIONS: 1.1.1.1.cbl.anti-spam.org.cn, type = A, class = IN AUTHORITY RECORDS: -> cbl.anti-spam.org.cn ttl = 2811 (46 mins 51 secs) primary name server = cbl.anti-spam.org.cn responsible mail addr = wxy.anti-spam.org.cn serial = 2011050306 refresh = 14400 (4 hours) retry = 3600 (1 hour) expire = 14400 (4 hours) default TTL = 3600 (1 hour) ------------ ------------ Got answer: HEADER: opcode = QUERY, id = 6, rcode = NXDOMAIN header flags: response, want recursion, recursion avail. questions = 1, answers = 0, authority records = 1, additional = 0 QUESTIONS: 1.1.1.1.cbl.anti-spam.org.cn, type = A, class = IN AUTHORITY RECORDS: -> cbl.anti-spam.org.cn ttl = 2811 (46 mins 51 secs) primary name server = cbl.anti-spam.org.cn responsible mail addr = wxy.anti-spam.org.cn serial = 2011050306 refresh = 14400 (4 hours)

诊断现象	可能原因	定位处理方法
		retry = 3600 (1 hour) expire = 14400 (4 hours) default TTL = 3600 (1 hour) ------------ *** nscache.prserv.net can't find 1.1.1.1.cbl.anti-spam.org.cn: Non-existent dom ain

如果以上原因均已排查无误，问题仍然没有解决，请联系技术支持工程师处理。

邮件过滤 FAQ

邮件过滤特性常见疑问的回答。

开启邮件过滤后，仍无法查杀邮件中的病毒

仅开启邮件过滤功能是无法查杀邮件病毒的，需要开启反病毒功能。

什么是应答码

垃圾邮件防范是通过检查邮件发送方源 IP 合法性来实现的，如果源 IP 命中黑名单，NGFW 将会认为这是一封垃圾邮件。当 NGFW 使用 RBL 黑名单进行源 IP 地址检查时，会向远程 RBL 服务器发送查询请求，并根据 RBL 服务器反馈的应答码来判断邮件的合法性。

应答码通常是一个 IP 地址，仅仅标识查询结果，并不具有实际意义，可以是一个保留 IP 段的地址，如 127.0.0.1、127.0.0.2 等。

要使用 RBL 黑名单，需要事先从 RBL 服务提供商获取应答码，并在 NGFW 上完成应答码的配置。NGFW 发起 RBL 查询请求后，会将 RBL 服务器反馈的应答码与网络管理员配置的应答码进行比较，如果两者一致，NGFW 会判断这是一封垃圾邮件。

HCIE-Security 模拟面试问题及面试建议

1. 邮件过滤原理是什么？