配置Beta ESA以接受来自生产ESA的流量

目录

简介

背景信息

先决条件

- 环境
- 要求
- 使用的组件

配置Beta设备

- Beta ESA的监听程序配置
- 测试版ESA的发件人组
- Beta ESA的简单邮件传输协议(SMTP)路由
- Beta ESA传入中继（可选）
- 启用日志信头以捕获邮件日志中的垃圾邮件判定（可选）

配置生产设备

- 生产ESA的SMTP路由
- 退回配置文件创建
- 目标控制配置文件创建
- 面向生产ESA的消息过滤器结构

验证

故障排除

其他信息（可选）

相关信息

简介

本文档介绍如何配置Beta思科邮件安全设备(ESA)以接收生产ESA的复制邮件流进行测试。

背景信息

此过程配置Beta ESA侦听程序、中继权限和简单邮件传输协议(SMTP)路由，然后配置Production ESA邮件过滤器以将邮件的BCC副本发送到Beta ESA，并验证mail_logs中的传送。预期结果：beta ESA接受来自生产ESA的复制入站和出站流量以进行测试。

先决条件

环境

- 一个生产思科邮件安全设备(ESA)和一个测试版ESA。

- Beta ESA侦听程序：TCP端口25上的公共侦听程序；TCP端口26上的专用侦听程序（或仅当有其他接口可用时才使用端口25）。 在CES托管版测试版中，端口587保留用于出站邮件。
- 通过使用生产ESA邮件过滤器(BCC)，适用于从生产ESA到Beta ESA的已复制入站和出站邮件流。

要求

需要对ESA GUI和CLI进行管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置Beta设备

Beta ESA的监听程序配置

初始监听程序配置将在Beta ESA上完成。

1. 在GUI中，导航到网络>侦听器。
2. 选择Add Listener....
3. 输入侦听程序名称并在TCP端口25上配置公共侦听程序。
4. 选择 Submit。
5. 重复步骤2至4以添加第二个监听程序。
6. 输入监听程序名称并在TCP端口26上配置专用监听程序。此监听程序用于出站邮件。仅当为环境提供并配置了其他接口时，才能使用端口25。在CES托管版测试版中，端口587保留用于出站邮件。
7. 提交以将更改保存到监听程序。
8. 提交以保存对配置的所有更改。

测试版ESA的发件人组

对于中继流量或出站消息，请为Beta ESA添加适当的IP地址，以便其接受并中继来自生产ESA的消息。

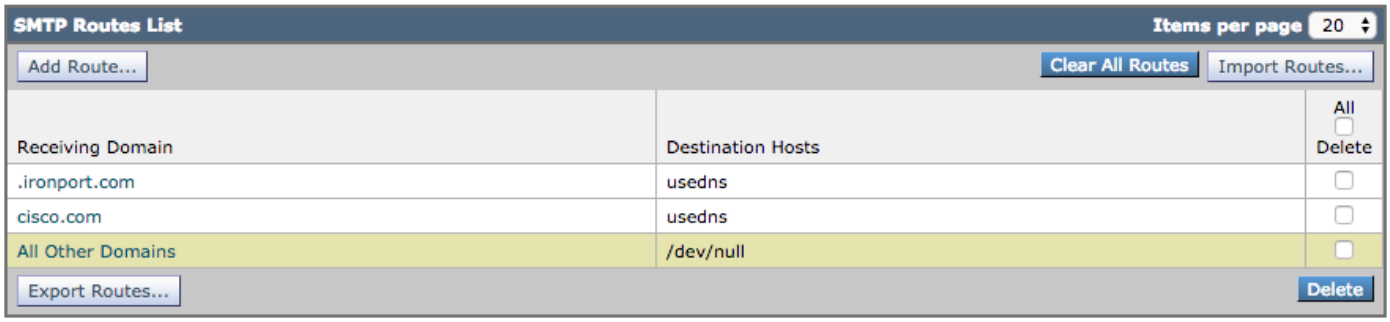
1. 在GUI中，导航到邮件策略> HAT概述。
2. 选择相应名称的中继发件人组。（通常命名为RELAY或RELAYLIST。）
3. 选择Add Sender....
4. 对于发送方，使用生产ESA的IP地址。
5. 根据需要输入任何管理注释。
6. 提交以保存对中继发件人组的更改。
7. 提交以保存对配置的所有更改。

Beta ESA的简单邮件传输协议(SMTP)路由

在Beta ESA上配置此SMTP路由。

1. 在GUI中，导航到网络> SMTP路由。
2. 如果当前SMTP路由存在，则您需要先选择它们并删除它们，然后再继续。确保您阅读测试版实验室设置指南。
3. 选择Add Route...
4. 输入cisco.com作为接收域，输入USEDNS作为目标。
5. 选择 Submit。
6. 重复步骤3至5以添加第二个SMTP路由。
7. 输入ironport.com作为接收域，输入USEDNS作为目标。
8. 单击 submit。
9. 选择All Other Domains以接收域。
10. 为Destination输入/dev/null。这可以防止从未配置的任何域从Beta ESA路由邮件。
11. 选择 Submit。
12. 提交以保存对配置的所有更改。

Beta ESA上的SMTP路由如下图所示。



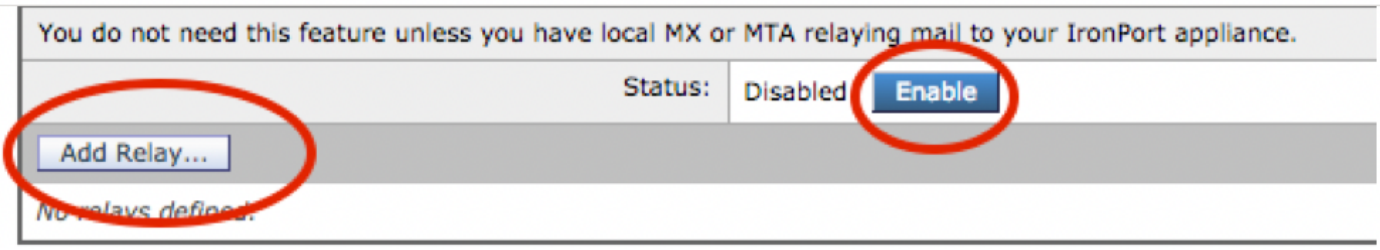
注意： 添加适当的路由以根据需要发送电子邮件以测试最终用户是否拥有域。

Beta ESA传入中继（可选）

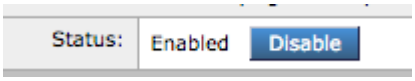
传入中继允许Beta ESA评估连接的IP地址并检索SenderBase信誉得分(SBRS)，该得分超出了生产ESA提供的得分。

大多数部署都需要一跳。

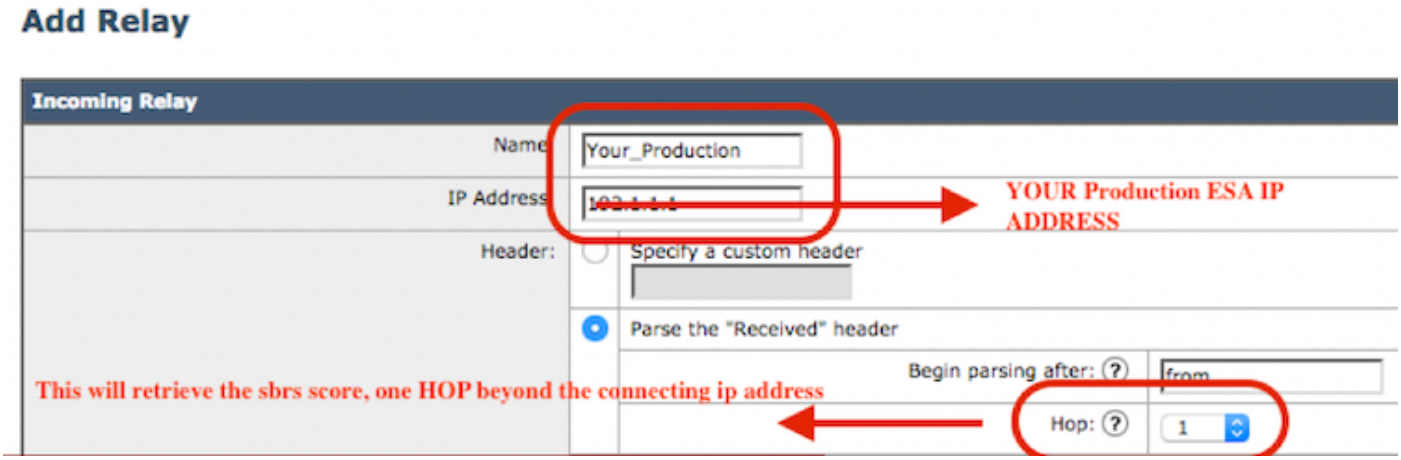
1. 在GUI中，导航到网络>传入中继。
2. 选中Enable复选框。
3. 选择Add Relay。
4. 在名称字段中，输入描述性名称。
5. 在IP Address字段中，输入将邮件传送到Beta ESA的生产ESA的IP地址。仅当多台主机传送邮件时才使用部分主机名。
6. 在Hop字段中，输入1。
7. 单击Submit，然后单击Commit。



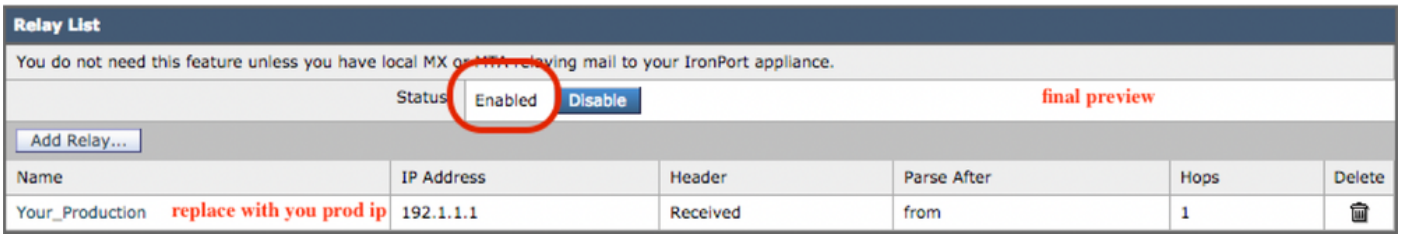
传入中继：禁用状态。



传入中继：Enabled State，彩色白色。



传入中继：示例模板



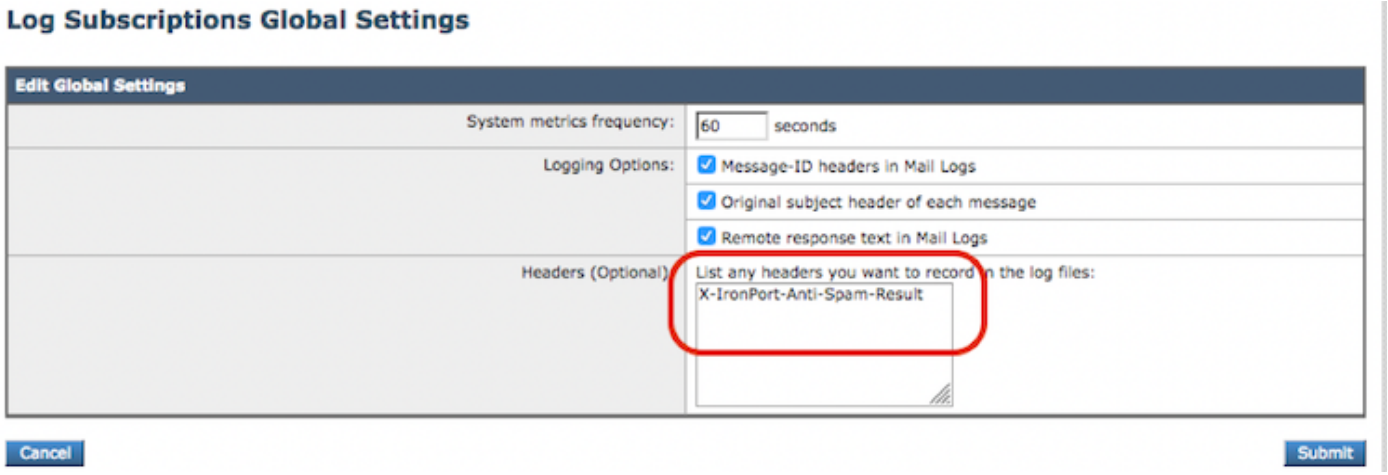
传入中继：提交后的摘要视图。

邮件日志条目示例：

```
Mon Apr 8 12:48:28 2019 Info: MID 2422822 IncomingRelay(PROD_hc2881-52): Header Received found, IP 10.1
```

启用日志信头以捕获邮件日志中的垃圾邮件判定（可选）

1. 在GUI中，导航到系统管理>日志订阅。
2. 选择页面底部的Global Settings。
3. 在Headers部分中，选择Add。
4. 输入X-IronPort-Anti-Spam-Result。
5. 选择 Submit。
6. 单击Commit。



将垃圾邮件信头记录到邮件日志

Beta端配置结束。

配置生产设备

⚠ 警告：您即将对生产ESA进行更改。确保备份当前配置。

1. 从Web UI导航到系统管理>配置文件。
2. 在“当前配置”部分中，选择将当前配置备份为文件的选项之一：
   - 将文件下载到本地计算机以查看或保存。
   - 通过电子邮件将文件发送到：<your_email_address@domain.com>
3. 单击 submit。

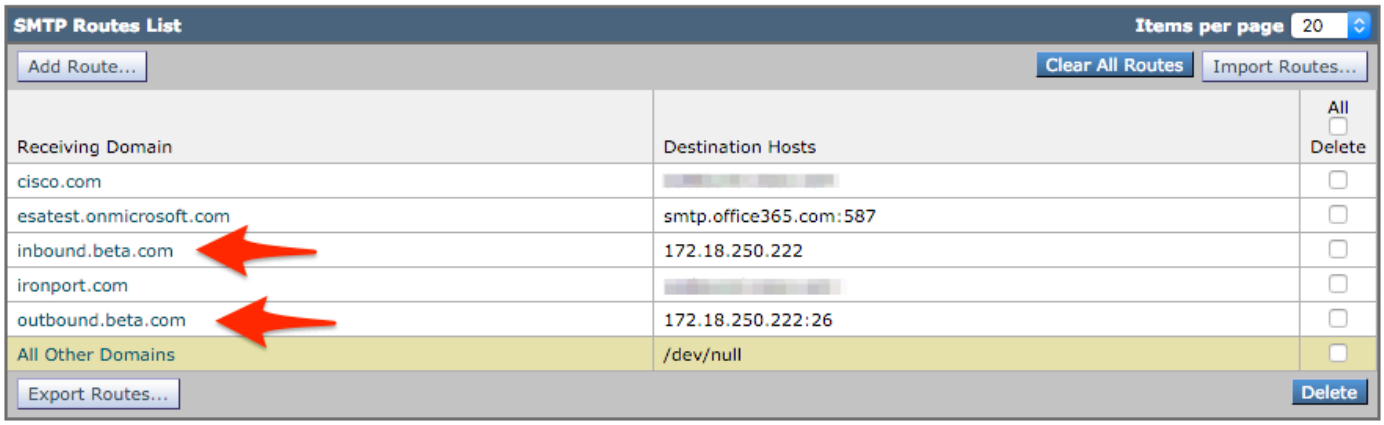
生产ESA的SMTP路由

添加SMTP路由以允许从生产ESA到测试版ESA的所有入站和出站电子邮件的BCC副本。在本示例中，使用inbound.beta.com和outbound.beta.com。

1. 在GUI中，导航到网络> SMTP路由。
2. 选择Add Route...
3. 输入inbound.beta.com作为接收域。
4. 输入之前为目标主机创建的Beta ESA公共侦听程序的IP地址。

5. 输入25作为端口。
6. 选择 Submit。
7. 重复步骤2至5以添加第二条路由。
8. 输入outbound.beta.com作为接收域。
9. 输入之前为目标主机创建的Beta ESA专用侦听程序的IP地址。
10. 输入26作为端口。
11. 选择 Submit。
12. 提交以保存对配置的所有更改。

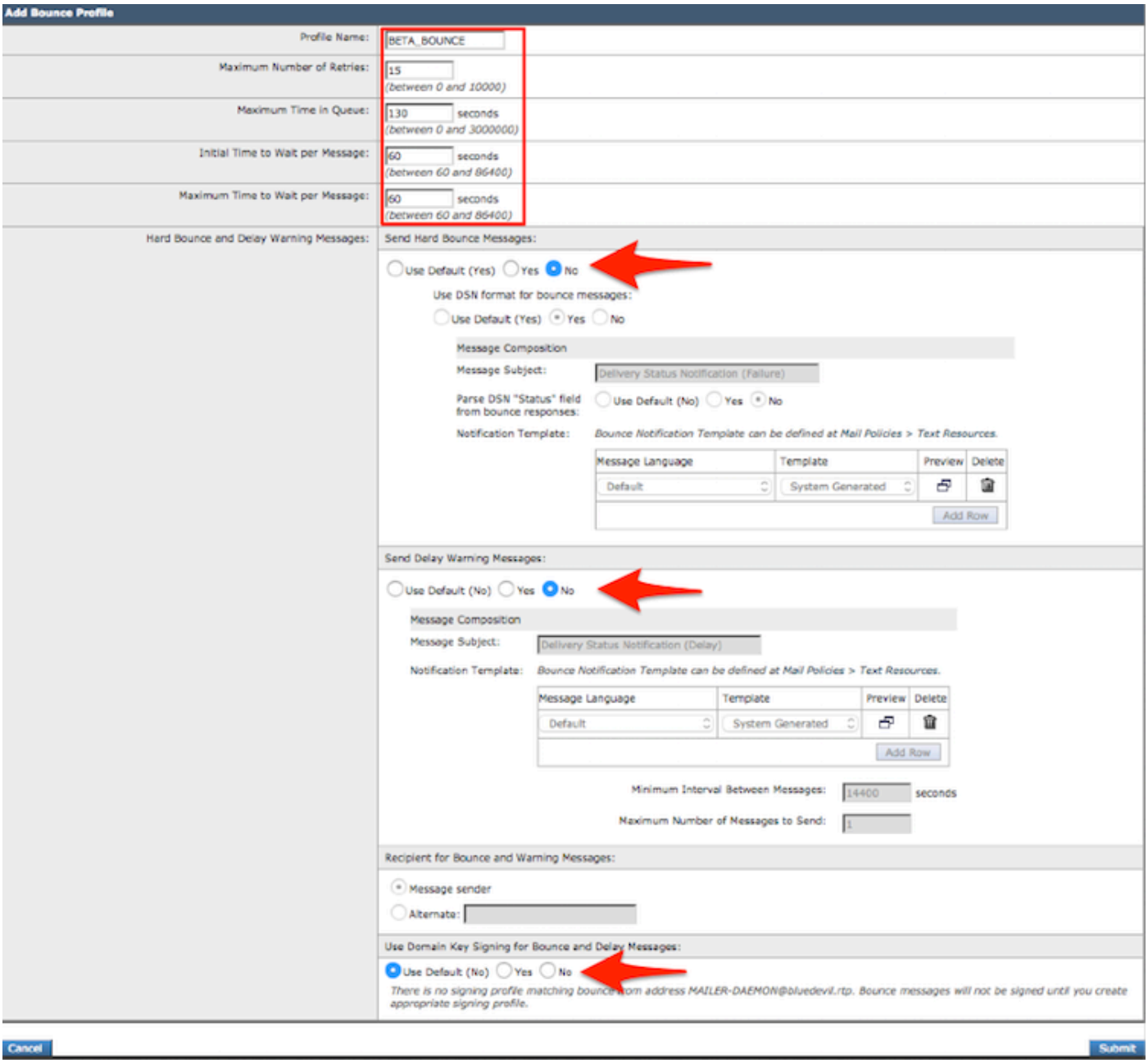
生产ESA上的SMTP路由如下图所示。



退回配置文件创建

退回配置文件和目标控制配置文件的组合可保护生产邮件流，防止邮件发送到Beta主机时延迟或失败。此配置仅适用于测试版消息。

1. 从Web UI导航到网络>退回配置文件>添加退回配置文件。
2. 最大重试次数：15
3. 队列中的最大时间：130
4. 每封邮件的初始等待时间：60
5. 每封邮件的最大等待时间：60
6. 发送硬退回邮件：否
7. 发送延迟警告消息：否
8. 对退回和延迟邮件使用域密钥签名：否
9. 提交以保存对此新退回配置文件的更改。
10. 选择Commit以保存对配置的所有更改。



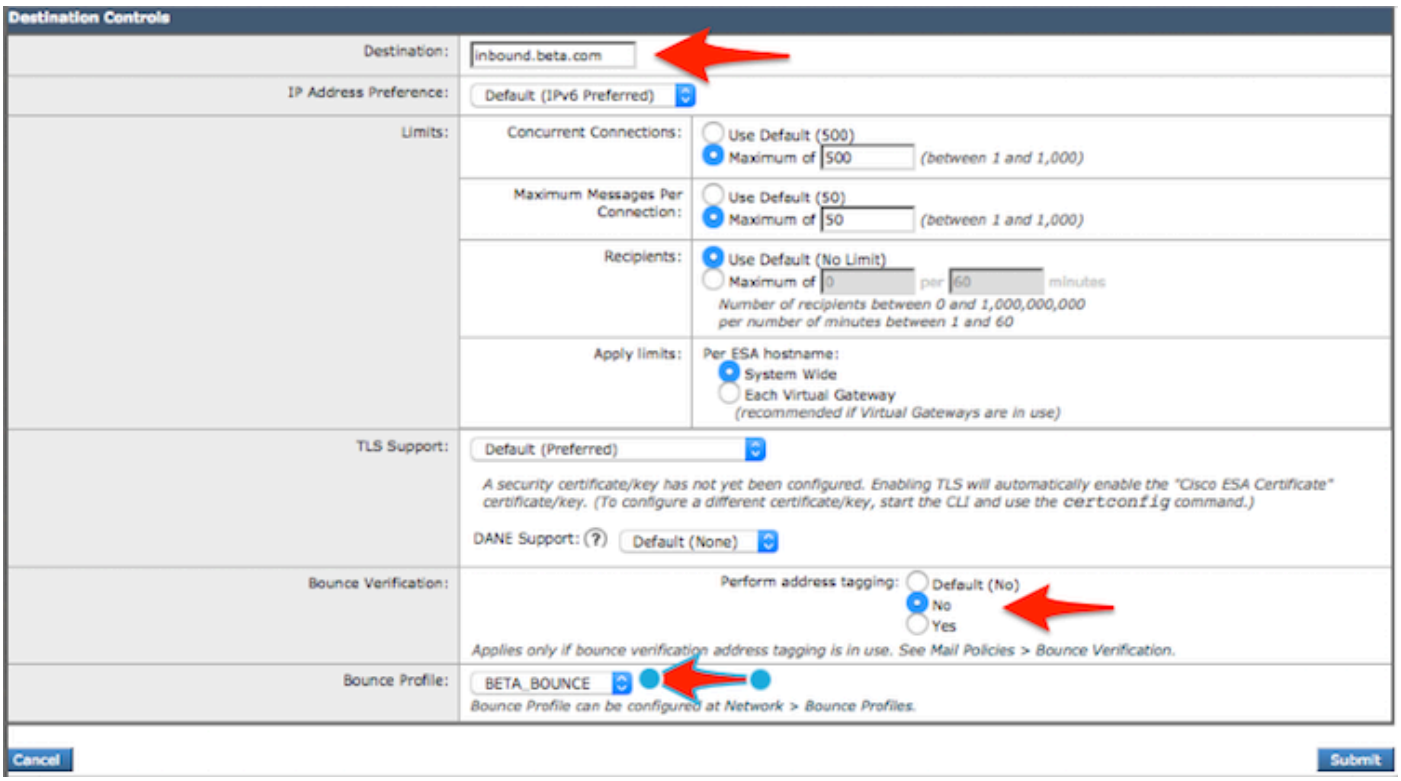
退回配置文件创建

注意：编号值配置得非常严格，以防止在测试版主机的传送中断时进行传送队列备份。值可以修改为首选项。通知设置有意设置为NO，以防止从BCC过滤器传送任何用户通知。

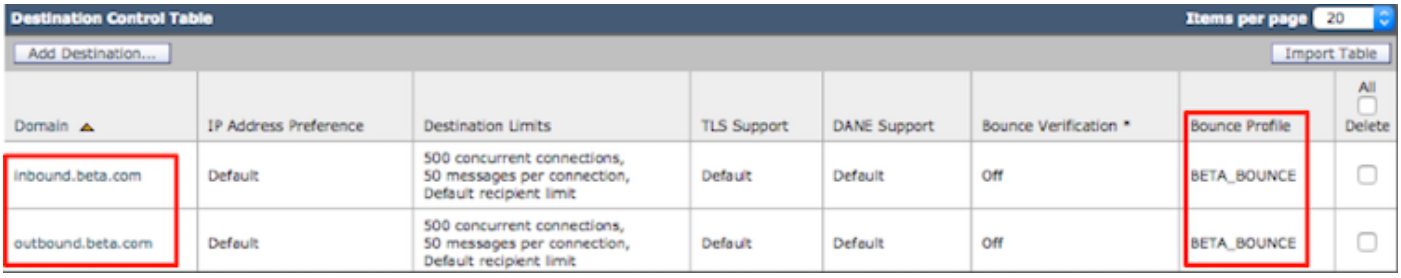
目标控制配置文件创建

1. 从Web UI导航到邮件策略>目标控制>添加目标。
2. 目的地：inbound.beta.com
3. 退回验证：> 执行地址标记：否>或默认（否）
4. 退回配置文件：BETA_BOUNCE
5. 根据管理员首选项配置其余值。
6. 提交以保存对此新的目标控制配置文件的更改。

7. 重复步骤2至6，将outbound.beta.com用于Destination。
8. 提交以保存对此新的目标控制配置文件的更改。
9. 提交以保存对配置的所有更改。



添加目标控制配置文件。



新目标控制配置文件的摘要视图。

面向生产ESA的消息过滤器结构

从生产ESA的命令行界面(CLI)创建邮件过滤器，将邮件的BCC副本发送到Beta ESA上的相应侦听程序。

1. 导航到过滤器>新建。
2. 复制并粘贴此邮件过滤器示例，并根据需要更新值：

```
bcc-EFT: if sendergroup == "RELAY" {
 bcc ("$enveloperecipients", "$Subject", "$EnvelopeFrom", "outbound.beta.com");
 log-entry("<=====BCC COPY TO BETA ESA=====>");
 } else {
```

```
 bcc ("$enveloperecipients", "$Subject", "$EnvelopeFrom", "inbound.beta.com");
 log-entry("<=====BCC COPY TO BETA ESA=====>");
}
.
```

3. 返回，直至返回到主CLI提示符。
4. 提交以保存对配置的所有更改。

注意： 根据sendergroup、recv-listener、mail-from或其他可用的规则和语法,限制在邮件过滤器中复制的流量。请参阅《ESA用户指南》以了解完整的邮件过滤器规则和过滤器规则摘要。

验证

使用此部分来确认配置是否按预期工作。

要验证Beta ESA是否接受来自生产ESA的电子邮件流量，请从Beta ESA上的CLI运行此命令：

<#root>

tail mail_logs

```
Wed Mar 23 17:28:43 2016 Info: New SMTP ICID 2 interface Management (172.18.250.222) address 172.18.250
Wed Mar 23 17:28:43 2016 Info: ICID 2 RELAY SG RELAY match 172.18.250.1/24 SBRS not enabled
Wed Mar 23 17:28:43 2016 Info: Start MID 2 ICID 2
Wed Mar 23 17:28:43 2016 Info: MID 2 ICID 2 From: <test@test.com>
Wed Mar 23 17:28:43 2016 Info: MID 2 ICID 2 RID 0 To: <example@ironport.com>
Wed Mar 23 17:28:43 2016 Info: MID 2 Message-ID '<a033ed$2@9.9.5-038.local>'
Wed Mar 23 17:28:43 2016 Info: MID 2 Subject 'TEST 2'
Wed Mar 23 17:28:43 2016 Info: MID 2 ready 320 bytes from <test@test.com>
Wed Mar 23 17:28:43 2016 Info: MID 2 matched all recipients for per-recipient policy DEFAULT in the outb
Wed Mar 23 17:28:43 2016 Info: MID 2 queued for delivery
Wed Mar 23 17:28:43 2016 Info: New SMTP DCID 3 interface 172.18.250.222 address 173.37.93.161 port 25
Wed Mar 23 17:28:43 2016 Info: Delivery start DCID 3 MID 2 to RID [0]
Wed Mar 23 17:28:44 2016 Info: Message done DCID 3 MID 2 to RID [0]
Wed Mar 23 17:28:44 2016 Info: MID 2 RID [0] Response '2.0.0 u2NHSipG018673 Message accepted for delive
Wed Mar 23 17:28:44 2016 Info: Message finished MID 2 done
Wed Mar 23 17:28:48 2016 Info: ICID 2 close
Wed Mar 23 17:28:49 2016 Info: DCID 3 close
```

SMTP通信在172.18.250.222（Beta设备）上建立。 流量从172.18.250.224（生产设备）发送。

接收通信的发送方组为来自172.18.250.1/24网络的中继流量的RELAY。

其余条目显示TEST 2消息的处理。

在Production ESA上，运行此命令以验证已处理的MID:

<#root>

```
tail mail_logs
```

Production ESA显示以下输出：

```
Wed Mar 23 14:50:10 2016 Info: MID 242 was generated based on MID 241 by bcc filter 'bcc-EFT'
```

此输出确认报文的清晰重复，并显示该报文按照预期被BCC复制到Beta ESA和测试最终用户。

故障排除

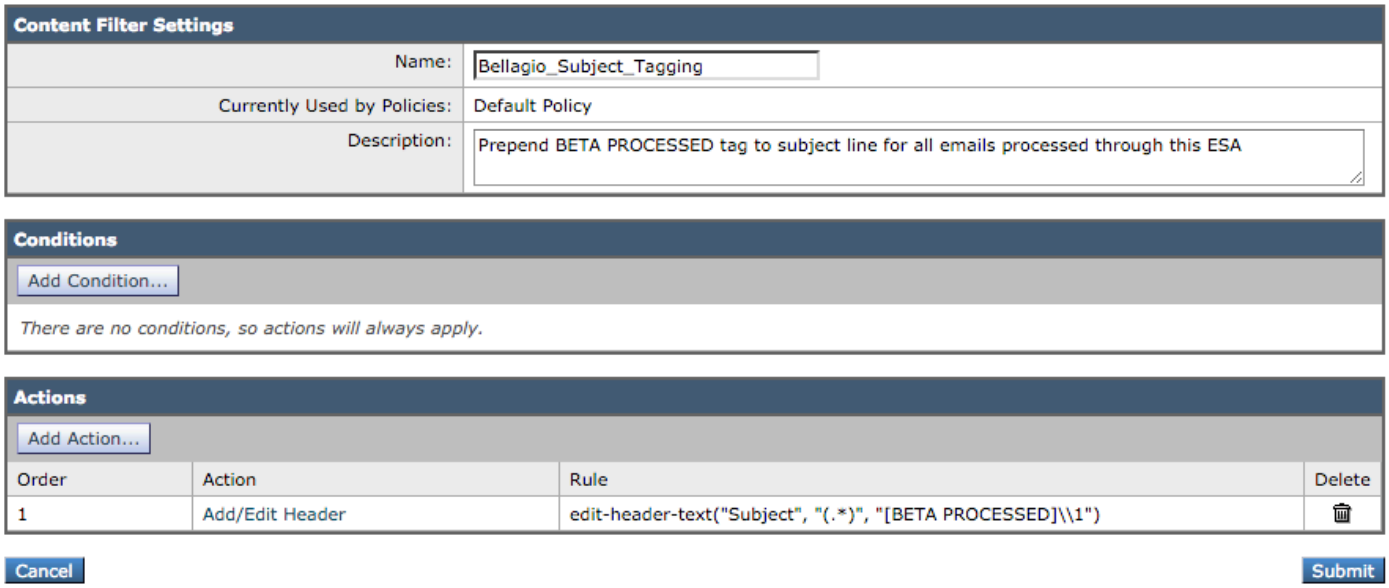
如果验证失败，请查看两个ESA上的侦听程序配置、发件人组条目、SMTP路由、传入中继设置和邮件过滤器配置。还要检查两台设备上的mail_logs，以确认连接、中继和传送事件。

其他信息（可选）

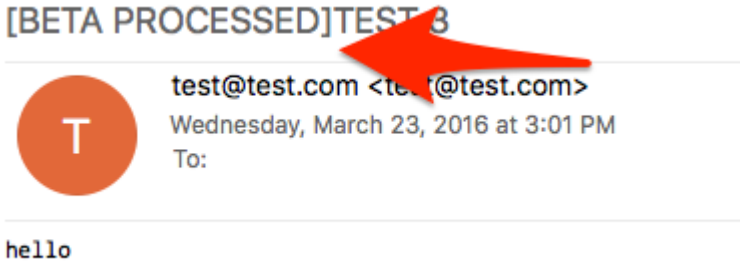
您可以使用内容过滤器来帮助区分测试最终用户的生产和Beta电子邮件流量。

1. 从Beta ESA上的Web UI导航到邮件策略>传入内容过滤器或邮件策略>传出内容过滤器。
2. 创建执行Add/Edit Header操作的基本内容过滤器。
3. 选择 Submit。
4. 导航到邮件策略(Mail Policies)>传入邮件策略(Incoming Mail Policies)或邮件策略(Mail Policies)>传出邮件策略(Outgoing Mail Policies)。
5. 启用新的内容过滤器并将其添加到策略。
6. 选择 Submit。
7. 单击Commit以保存对配置的所有更改。

完成此步骤后，Beta ESA上的内容过滤器会如图所示。



在Beta ESA处理电子邮件后，Subject（主题）行显示在此图像中。



相关信息

- 如何为分段更新配置ESA/SMA
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。