

配置β ESA接收生产ESA数据流

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[配置β工具](#)

[β ESA的监听程序配置](#)

[β ESA的发送方组](#)

[β ESA的简单邮件传输协议\(SMTP\)路由](#)

[β ESA的流入中继](#)

[Enable \(event\)捕获在邮件日志内的垃圾邮件判决的日志报头](#)

[配置生产工具](#)

[生产ESA的SMTP路由](#)

[跳动配置文件创建](#)

[目的地控制配置文件创建](#)

[消息生产ESA的过滤器建筑](#)

[跳动配置文件创建](#)

[目的地控制配置文件创建](#)

[Verify](#)

[Troubleshoot](#)

[其他信息](#)

[Related Information](#)

Introduction

本文描述如何配置β Cisco电子邮件安全工具(ESA)为了通过消息过滤器接收生产ESA数据流。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 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β工具

β ESA的监听程序配置

最初的监听程序配置将完成在β ESA。

1. 从GUI，请连接给**网络>监听程序**。
2. 点击**添加监听程序...**
3. 名字和设置在TCP端口25运作的公共监听程序。
4. 点击**提交**为了保存对公共监听程序的更改。
5. 重复同样步骤并且添加第二监听程序。
6. 名字和设置在TCP端口26运作的专用的监听程序。(此监听程序使用outbound邮件。)如果有为您的环境，可用和配置的一个额外接口您可以使用端口25。CES主机的β环境为outbound保留了端口587。
7. **提交**保存对监听程序的更改。
8. 保存全部的**进行变成配置**。

β ESA的发送方组

对于被传递的数据流或出局的消息，请添加在β ESA的适当的IP地址为了接受和从生产ESA的中转消息。

1. 从GUI，请连接**邮寄策略>帽子概述**。
2. 选择适当地已命名中继发送方组。(这通常被命名中继或者RELAYLIST。)
3. 点击**添加发送方...**
4. 对于发送方，请使用生产ESA的IP地址。
5. 输入所有管理备注，当必要时。
6. **提交**保存对中继发送方组的更改。
7. 保存全部的**进行变成配置**。

β ESA的简单邮件传输协议(SMTP)路由

在β ESA需要做的SMTP路由更改如下：

1. 从GUI，请连接到**网络> SMTP路由**。
2. 如果有当前SMTP路由，您可能需要选择那些和**删除**，在您进行前。(请保证查看β实验室设置指南。)
3. 点击**添加路由...**
4. 设置接受域作为**cisco.com**和目的地作为**USEDNS**。
5. 单击 **submit**。
6. 重复同样步骤并且添加在秒钟SMTP路由。
7. 设置接受**ironport.com**的域和目的地作为**USEDNS**。
8. 单击 **submit**。
9. 最后，请选择**其他域**从接受域。
10. 设置目的地作为**/dev/null**。(这防止路由邮件从没被配置的所有域的β工具。)
11. 单击 **submit**。
12. 保存全部的**进行变成配置**。

如镜像所显示，此时，在β工具上的SMTP路由是：

Receiving Domain	Destination Hosts	All Delete
.ironport.com	usedns	<input type="checkbox"/>
cisco.com	usedns	<input type="checkbox"/>
All Other Domains	/dev/null	<input type="checkbox"/>

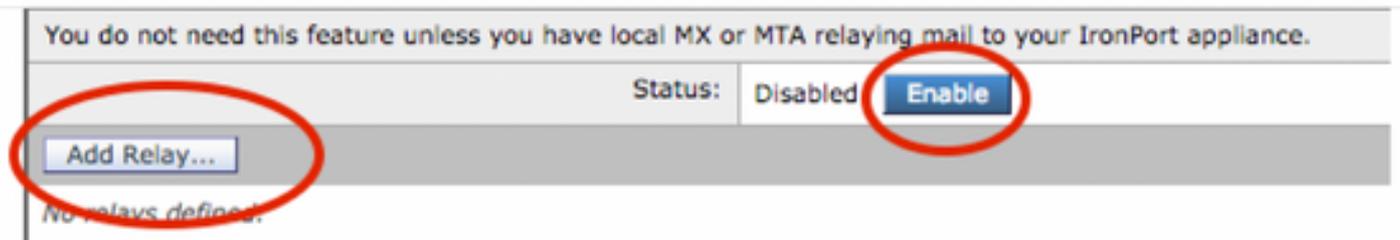
Note: 添加适当的路由传送电子邮件为域测试终端用户当必要时。

β ESA的流入中继

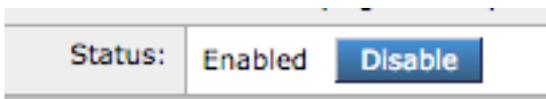
流入中继配置允许β检索生产ESA的SBRs评分beyond。

多数配置将工作用一次跳跃。

1. GUI，连接到网络流入中继。
2. 启用它的Click "Enable"空白在颜色。
3. 点击添加中继。
4. “名字”选择名字。
5. “传送到β ESA的生产ESA的IP地址”值。如果多台主机传送，部分主机名-是可接受的。
6. “跳跃：” 1
7. 提交并且确认更改



流入中继：禁用状态。



流入中继：允许状态，变色的白色。

Add Relay

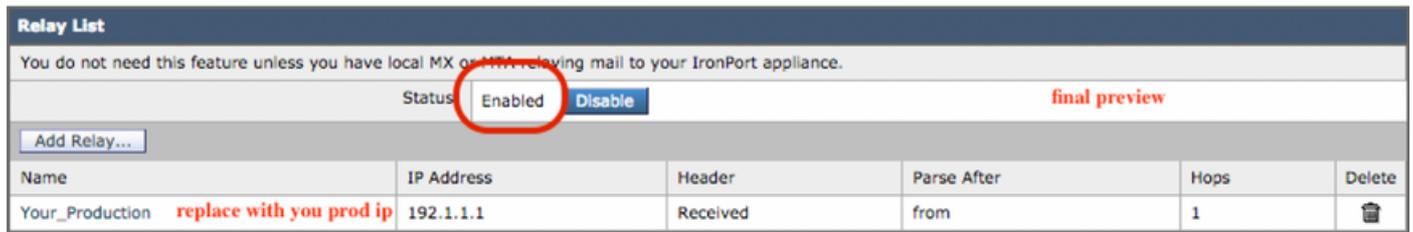
Name: Your_Production

IP Address: 102.1.1.1 **YOUR Production ESA IP ADDRESS**

Header: Parse the "Received" header

Hop: 1 **This will retrieve the sbrs score, one HOP beyond the connecting ip address**

流入中继：示例模板



Name	IP Address	Header	Parse After	Hops	Delete
Your_Production	replace with you prod ip	192.1.1.1	Received	from	1

流入中继：概略的视图以后提交。

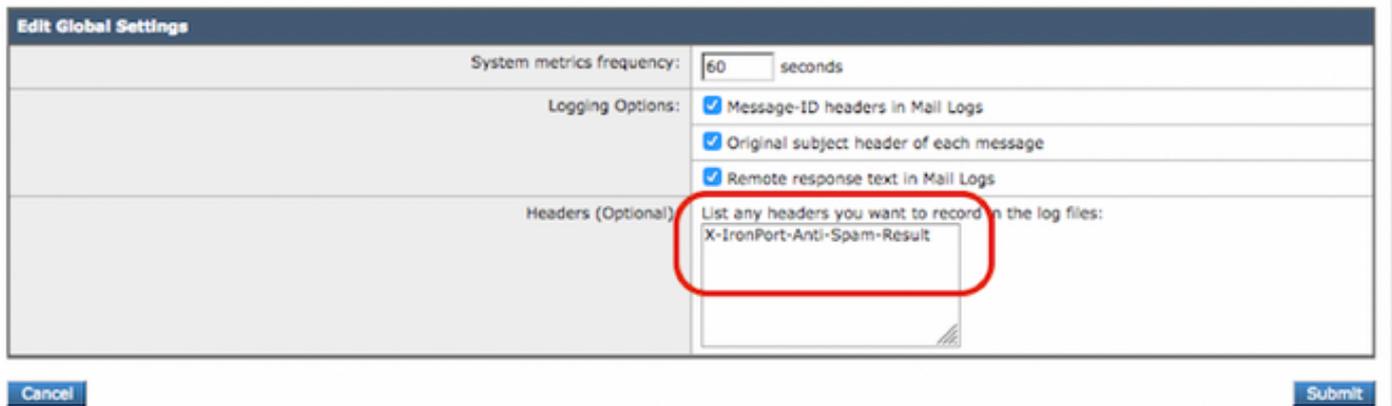
示例邮件日志条目：

Mon Apr 8 12:48:28 2019信息：MID 2422822 IncomingRelay(PROD_hc2881-52)：收到找到的报头，IP使用的54.240.35.22，SBRS 3.5国家美国

Enable (event)捕获在邮件日志内的垃圾邮件判决的日志报头

- Webui > System Administration >>() >> () X IronPort

Log Subscriptions Global Settings



System metrics frequency: 60 seconds

Logging Options:

- Message-ID headers in Mail Logs
- Original subject header of each message
- Remote response text in Mail Logs

Headers (Optional): List any headers you want to record in the log files:

X-IronPort-Anti-Spam-Result

Cancel Submit

BETA边配置END。

配置生产工具

警告：您将做对生产ESA的变动。保证您备份当前配置。

1. 从GUI，请连接对**系统管理>配置文件**。
2. 从当前配置部分，请选择其中一个选项备份当前配置作为文件：下载文件到本地计算机查看或保存。给文件发电子邮件对：< your_email_address@domain.com >
3. 单击 **submit**。

生产ESA的SMTP路由

必须添加SMTP路由为了允许所有入站和outbound电子邮件的BCC从生产ESA到β ESA。对于此示例，使用inbound.beta.com和outbound.beta.com。

1. 从GUI，请连接到**网络> SMTP路由**。
2. 点击**添加路由...**

3. 设置接受域作为与目的地的inbound.beta.com作为β工具公共监听程序的IP地址创建前，端口设置到25。
4. 点击**提交**保存对此新的SMTP路由的更改。
5. 重复同样步骤，**添加路由...**
6. 设置接受域作为outbound.beta.com，目的地主机作为β工具专用的监听程序的IP地址被创建前和端口到26。
7. **提交**保存对此新的SMTP路由的更改。
8. 保存全部的**进行**变成配置。

此时，在生产ESA的SMTP路由如镜像所显示：

SMTP Routes List		Items per page 20
Add Route...		Clear All Routes Import Routes...
Receiving Domain	Destination Hosts	All Delete
cisco.com		<input type="checkbox"/>
esatest.onmicrosoft.com	smtp.office365.com:587	<input type="checkbox"/>
inbound.beta.com	172.18.250.222	<input type="checkbox"/>
ironport.com		<input type="checkbox"/>
outbound.beta.com	172.18.250.222:26	<input type="checkbox"/>
All Other Domains	/dev/null	<input type="checkbox"/>
Export Routes...		Delete

跳动配置文件创建

组合跳动配置文件和目的地控制配置文件将保护生产邮件流量免受与延迟或疏忽产生关联的复杂化提供消息到β主机。此配置只将适用于β消息。

1. 从GUI，请连接对网络>跳动Profiles>**添加跳动配置文件**。
2. 重试次数的最大数量：**15**
3. 最大排队的时间：**130**
4. 初期时刻每个消息等待：**60**
5. 最大时间每个消息等待：**60**
6. 发硬信号反跳信息：**无**
7. 传送延迟警告消息：**无**
8. 请使用签字域的键跳动并且延迟消息：**无**
9. **提交**保存对此新的跳动配置文件的更改。
10. **Committo**保存全部变成配置。

Add Bounce Profile

Profile Name:

Maximum Number of Retries:
(between 0 and 10000)

Maximum Time in Queue: seconds
(between 0 and 3000000)

Initial Time to Wait per Message: seconds
(between 60 and 86400)

Maximum Time to Wait per Message: seconds
(between 60 and 86400)

Hard Bounce and Delay Warning Messages:

Send Hard Bounce Messages:

Use Default (Yes) Yes No

Use DSN format for bounce messages:

Use Default (Yes) Yes No

Message Composition

Message Subject:

Parse DSN "Status" field from bounce responses: Use Default (No) Yes No

Notification Template: *Bounce Notification Template can be defined at Mail Policies > Text Resources.*

Message Language	Template	Preview	Delete
Default	System Generated		

Send Delay Warning Messages:

Use Default (No) Yes No

Message Composition

Message Subject:

Notification Template: *Bounce Notification Template can be defined at Mail Policies > Text Resources.*

Message Language	Template	Preview	Delete
Default	System Generated		

Minimum Interval Between Messages: seconds

Maximum Number of Messages to Send:

Recipient for Bounce and Warning Messages:

Message sender

Alternate:

Use Domain Key Signing for Bounce and Delay Messages:

Use Default (No) Yes No

There is no signing profile matching bounce.com address MAILER-DAEMON@bluedevil.rtp. Bounce messages will not be signed until you create appropriate signing profile.

跳动配置文件创建

Note: 非常积极地配置以上的编号值防止发运队列备份在发运中断情形下到β主机。值可能被修改成首选。通知设置故意地设对不防止所有用户通知被传送从BCC过滤器。

目的地控制配置文件创建

1. 从GUI，请连接邮寄策略>目的地控制>Add目的地。
2. 目的地：**inbound.beta.com**
3. 跳动验证：>请执行地址标记：没有>或默认值(不)
4. 跳动配置文件：**BETA_BOUNCE**
5. 其他值可能根据管理员的首选被配置。
6. 提交保存对此新建目标控制配置文件的更改。
7. 重复第2步-第6步使用目的地：**outbound.beta.com**
8. 提交保存对此新建目标控制配置文件的更改。
9. 保存全部的进行变成配置。

Destination Controls

Destination:

IP Address Preference:

Limits:

- Concurrent Connections: Use Default (500) Maximum of (between 1 and 1,000)
- Maximum Messages Per Connection: Use Default (50) Maximum of (between 1 and 1,000)
- Recipients: Use Default (No Limit) Maximum of per minutes
Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60
- Apply limits: Per ESA hostname: System Wide Each Virtual Gateway (recommended if Virtual Gateways are in use)

TLS Support:

DANE Support:

Bounce Verification: Perform address tagging: Default (No) No Yes

Bounce Profile:

添加目标控制配置文件。

Destination Control Table Items per page 20

Domain ▲	IP Address Preference	Destination Limits	TLS Support	DANE Support	Bounce Verification *	Bounce Profile	All <input type="checkbox"/>	Delete <input type="checkbox"/>
<input type="text" value="inbound.beta.com"/>	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Default	Default	Off	BETA_BOUNCE	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="outbound.beta.com"/>	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Default	Default	Off	BETA_BOUNCE	<input type="checkbox"/>	<input type="checkbox"/>

新建目标控制配置文件概略的视图。

消息生产ESA的过滤器建筑

从在生产ESA的CLI，请修建能BCC电子邮件给β ESA的适当的监听程序的消息过滤器。

1. 连接对过滤器>NEW。
2. 复制和插入此消息过滤器示例并且做变动适当：

```

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. 请返回，直到您是回到主要CLI提示。
4. 保存全部的进行变成配置。

Note: 限制在消息过滤器复制的数据流根据sendergroup、rcv监听程序、mail-from、或者其他可用的规则和语法。参见全部的消息的过滤规则和概略的过滤规则的ESA用户指南。

重新启动配置文件创建

目的地控制配置文件创建

Verify

使用本部分可确认配置能否正常运行。

此时，β工具接收从生产工具的电子邮件数据流。为了从在β工具上的CLI验证，请运行尾标 `mail_logs`：

```
Wed Mar 23 17:28:43 2016 Info: New SMTP ICID 2 interface Management (172.18.250.222) address 172.18.250.224 reverse dns host dhcp-172-18-250-224.cisco.com verified yes
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: <robsherw@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 outbound table
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 delivery'
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 (β工具)设立。数据流被发送的地址从是172.18.250.224 (生产工具)。

接受通信的发送方组是中继，从172.18.250.1/24网络的被传递的数据流。

其余是TEST 2消息的通信。

在生产工具上，请验证并且运行尾标`mail_logs`。在生产处理的MID将显示：

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

这是一清楚分裂电子邮件消息如被接受和BCC'd对β工具并且测试终端用户按照计划为收据。

Troubleshoot

目前没有针对此配置的故障排除信息。

Additional Information

内容过滤器可能考虑为了帮助区分生产与测试终端用户的β电子邮件数据流。

1. 从在β ESA的GUI，请连接**邮寄策略>流入内容过滤器**或**邮件策略>流出的内容过滤器**。
2. 修建一台基本的内容过滤器为了进行Add的动作/编辑报头。

3. 点击**提交**为了保存对被修建的内容过滤器的更改。
4. **邮寄策略>流入的邮件策略或邮件策略>流出的邮件策略**， enable (event)并且添加新的内容过滤器到策略名称。
5. 点击**提交**为了保存内容过滤器到该策略。
6. 点击**进行**为了保存对配置的所有更改。

如镜像所显示，此时，在β ESA的内容过滤器是：

Content Filter Settings

Name:	<input type="text" value="Bellagio_Subject_Tagging"/>
Currently Used by Policies:	Default Policy
Description:	<input style="width: 90%;" type="text" value="Prepend BETA PROCESSED tag to subject line for all emails processed through this ESA"/>

Conditions

Add Condition...

There are no conditions, so actions will always apply.

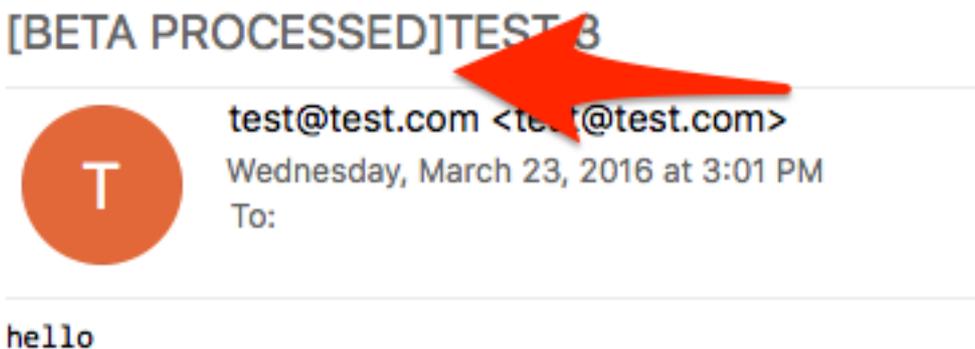
Actions

Add Action...

Order	Action	Rule	Delete
1	Add/Edit Header	edit-header-text("Subject", "(.*)", "[BETA PROCESSED]\\1")	

Cancel
Submit

现在，当电子邮件消息在β ESA时收到您在电子邮件的标题栏能看到此一次被处理如镜像所显示：



Related Information

- [如何配置演出的更新的ESA/SMA](#)
- [Technical Support & Documentation - Cisco Systems](#)