

Configurar o beta ESA para aceitar o tráfego da produção ESA

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar o beta dispositivo](#)

[Configuração do ouvinte para o beta ESA](#)

[Grupo do remetente para o beta ESA](#)

[Rotas do Simple Mail Transfer Protocol \(SMTP\) para o beta ESA](#)

[Relé entrante para o beta ESA](#)

[Permita encabeçamentos do log de capturar a sentença do Spam dentro dos logs do correio](#)

[Configurar o dispositivo da produção](#)

[Rotas S TP para a produção ESA](#)

[Criação do perfil do salto](#)

[O destino controla a criação do perfil](#)

[Construção do filtro da mensagem para a produção ESA](#)

[Criação do perfil do salto](#)

[O destino controla a criação do perfil](#)

[Verificar](#)

[Troubleshooting](#)

[Additional Information](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar beta Cisco envia por correio eletrónico a ferramenta de segurança (ESA) a fim aceitar o tráfego da produção ESA através de um filtro da mensagem.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar o beta dispositivo

Configuração do ouvinte para o beta ESA

A configuração inicial do ouvinte deve ser terminada no beta ESA.

1. Do GUI, navegue à **rede > aos ouvintes**.
2. O clique **adiciona o ouvinte...**
3. Nome e setup um ouvinte público que seja executado na porta TCP 25.
4. O clique **submete-se** a fim salvar as mudanças ao ouvinte público.
5. Repita as mesmas etapas e adicionar um segundo ouvinte.
6. Nome e setup um ouvinte privado que seja executado na porta TCP 26. (Este ouvinte é usado para o correio de partida.) Você pode usar a porta 25 se há uma interface adicional disponível e configurada para seu ambiente. O beta ambiente hospedado CES reservou a porta 587 para de partida.
7. **Submeta** para salvar mudanças ao ouvinte.
8. **Comprometa** para salvar todas as mudanças à configuração.

Grupo do remetente para o beta ESA

Para o tráfego ou mensagens externa retransmitidos, adicionar no endereço IP de Um ou Mais Servidores Cisco ICM NT apropriado para o beta ESA a fim aceitar e em mensagens de relé da produção ESA.

1. Do GUI, navegue **para enviar políticas > vista geral do CHAPÉU**.
2. Selecione o grupo apropriadamente Nomeado do remetente do relé. (Isto é nomeado geralmente RELÉ, ou RELAYLIST.)
3. O clique **adiciona o remetente...**
4. Para o remetente, use o endereço IP de Um ou Mais Servidores Cisco ICM NT da produção ESA.
5. Incorpore todos os comentários administrativos, como necessários.
6. **Submeta** para salvar mudanças ao grupo do remetente do relé.
7. **Comprometa** para salvar todas as mudanças à configuração.

Rotas do Simple Mail Transfer Protocol (SMTP) para o beta ESA

As alterações de rota S TP que precisam de ser feitas no beta ESA são como segue:

1. Do GUI, navegue à **rede > às rotas S TP**.
2. Se há rotas atuais S TP, você pode precisar de selecionar aqueles e a **supressão** antes que você continue. (Assegure para rever o o beta guia da instalação de laboratório.)
3. O clique **adiciona a rota...**
4. Ajuste o domínio de recepção como **cisco.com** e o destino como **USEDNS**.
5. Clique em Submit.
6. Repita as mesmas etapas e adicionar num segundo a rota S TP.

7. Ajuste a recepção do domínio para **ironport.com** e do destino como **USEDNS**.
8. Clique em Submit.
9. Finalmente, selecione **todos domínios restantes** de receber o domínio.
10. Ajuste o destino como **/dev/null**. (Isto impede distribuir o correio do beta dispositivo para todos os domínios não configurados.)
11. Clique em Submit.
12. **Comprometa** para salvar todas as mudanças à configuração.

Neste tempo, as rotas S TP no beta dispositivo são segundo as indicações da imagem:

SMTP Routes List		Items per page 20
Add Route...		Clear All Routes Import Routes...
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"/>
Export Routes...		Delete

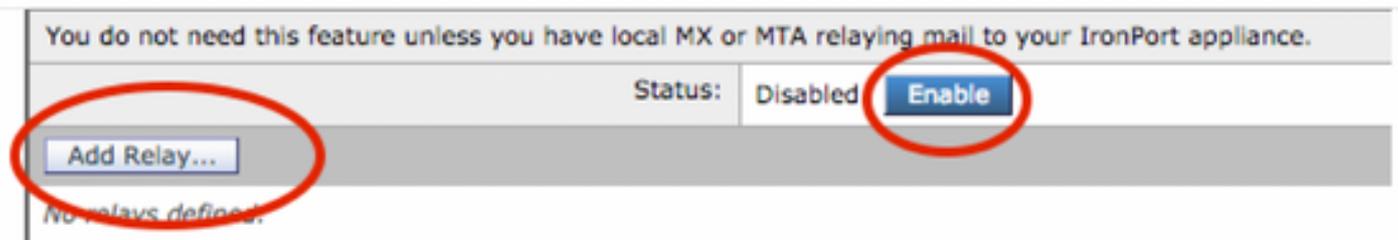
Nota: Adicionar as rotas apropriadas para entregar email para testar utilizadores finais para domínios como necessários.

Relé entrante para o beta ESA

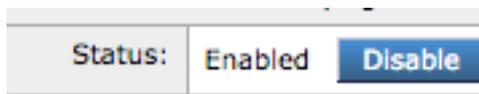
A configuração de Frame Relay entrante permite que o beta recupere o beyone da contagem SBR que da produção ESA.

A maioria de configurações trabalharão com um salto.

1. O GUI, navega ao relé do Recebimento de rede.
2. "habilitar " do clique que gerencie o branco na cor.
3. O clique adiciona o relé.
4. O "nome" escolhe um nome.
5. Valor do "endereço IP de Um ou Mais Servidores Cisco ICM NT" da produção ESA que entrega ao beta ESA. O hostname parcial é aceitável se os host múltiplos estão entregando.
6. "Salto: " 1
7. Submeta e comprometa mudanças



Relé entrante: Estado desabilitado.



Relé entrante: Estado permitido, branco colorido.

Add Relay

Incoming Relay

Name: Your_Production

IP Address: 192.1.1.1

Header: Specify a custom header
 Parse the "Received" header

Begin parsing after: from

Hop: 1

YOUR Production ESA IP ADDRESS

This will retrieve the sbrs score, one HOP beyond the connecting ip address

Relé entrante: Molde da amostra

Relay List

You do not need this feature unless you have local MX or MTA relaying mail to your IronPort appliance.

Status: **Enabled** Disable

final preview

Add Relay...

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

Relé entrante: A vista sumária após submete-se.

Entrada de registro do correio da amostra:

Segunda-feira informação 2019 do 8 de abril 12:48:28: 2422822 IncomingRelay(PROD_hc2881-52) MEADOS DE: Encabeçamento recebido encontrado, IP 54.240.35.22 que está sendo usado, Estados Unidos do país SBR 3.5

Permita encabeçamentos do log de capturar a sentença do Spam dentro dos logs do correio

- Webui > assinaturas da administração do sistema > do log > configurações globais (parte inferior) > encabeçamentos > (adicionar) X-IronPort-Anti-Spam-resultado

Log Subscriptions Global Settings

Edit 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

Registre encabeçamentos do Spam para enviar logs

FIM DA BETA CONFIGURAÇÃO LATERAL.

Configurar o dispositivo da produção

Cuidado: Você está a ponto de fazer mudanças a uma produção ESA. Assegure-se de que você backup a configuração atual.

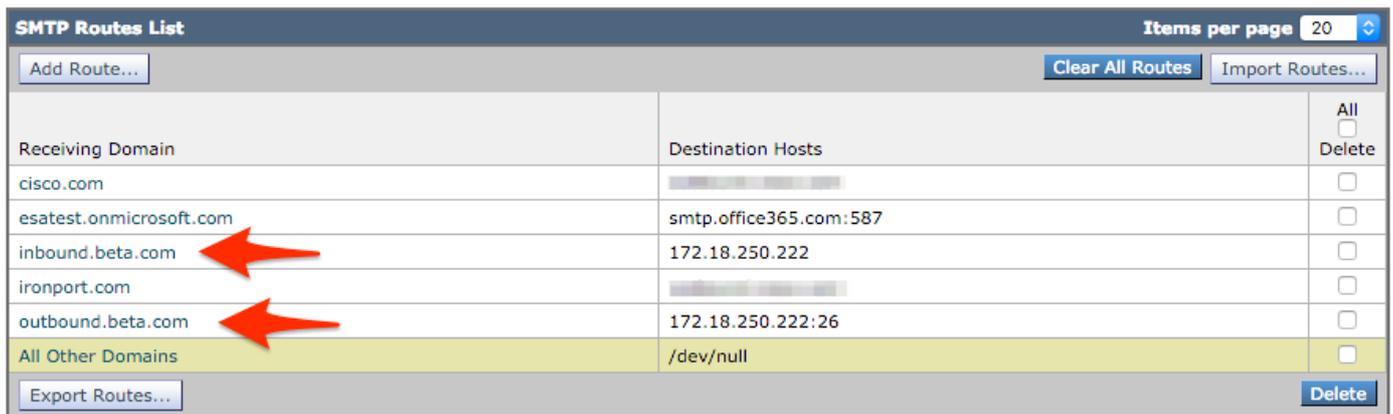
1. Do GUI, navegue à **administração do sistema > ao arquivo de configuração**.
2. Da seção de configuração atual, selecione uma das opções para suportar a configuração atual como um arquivo: Transfira o arquivo ao computador local para ver ou salvar. Envie por correio eletrônico o arquivo a: < your_email_address@domain.com >
3. Clique em Submit.

Rotas S TP para a produção ESA

As rotas S TP devem ser adicionadas a fim permitir o BCC para todos os email de entrada e de partida da produção ESA ao beta ESA. Para este exemplo, **inbound.beta.com** e **outbound.beta.com** são usados.

1. Do GUI, navegue à **rede > às rotas S TP**.
2. O clique **adiciona a rota...**
3. Ajuste a recepção do domínio como **inbound.beta.com** com o destino como o endereço IP de Um ou Mais Servidores Cisco ICM NT do ouvinte público do beta dispositivo criado mais cedo, com a porta ajustada a 25.
4. O clique **submete-se** para salvar mudanças a esta rota nova S TP.
5. Repita as mesmas etapas, **adicionar a rota...**
6. Ajuste o domínio de recepção como **outbound.beta.com**, host de destino como o endereço IP de Um ou Mais Servidores Cisco ICM NT do ouvinte privado do beta dispositivo criado mais cedo, e a porta a 26.
7. **Submeta** para salvar as mudanças a esta rota nova S TP.
8. **Comprometa** para salvar todas as mudanças à configuração.

Neste tempo, rotas S TP na produção ESA segundo as indicações da imagem:



Receiving Domain	Destination Hosts	All <input type="checkbox"/> 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"/>

Criação do perfil do salto

Um perfil do salto da combinação e o perfil do controle do destino protegerão o fluxo de correio da produção das complicações associadas com os atrasos ou as falhas entregar mensagens aos beta anfitriões. Esta configuração aplicar-se-á somente às beta mensagens.

1. Do GUI, navegue ao **perfil do salto do > Add dos perfis da rede > do salto**.
2. Número máximo de Retries: **15**

3. Tempo máximo na fila: **130**
4. Hora inicial de esperar pela mensagem: **60**
5. Tempo máximo esperar pela mensagem: **60**
6. Envie mensagens de salto duras: **NO**
7. Envie mensagens de advertência do atraso: **NO**
8. Use a chave do domínio que assina para o salto e atrase mensagens: **NO**
9. **Submeta** para salvar as mudanças a este perfil novo do salto.
10. A salvaguarda toda de **Committo** muda à configuração.

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.

Criação do perfil do salto

Nota: Os valores numerados acima são configurados muito agressivamente para impedir backup da fila da entrega no caso de uma interrupção da entrega aos beta anfitriões. Os valores podem ser alterados à preferência. Os ajustes da notificação são ajustados intencionalmente a NÃO para impedir que todas as notificações de usuário estejam entregadas dos filtros BCC.

O destino controla a criação do perfil

1. Do GUI, navegue para enviar políticas > destino do > Add dos controles do destino.
2. Destino: **inbound.beta.com**
3. Verificação do salto: > **execute a colocação de etiquetas do endereço: NENHUM** > ou padrão (NÃO)
4. **Perfil do salto: BETA_BOUNCE**
5. Os outros valores podem ser configurados com base na preferência do administrador.
6. **Submeta** para salvar as mudanças a este perfil novo do controle do destino.
7. **Repita** etapas 2 - 6 usando o destino: **outbound.beta.com**
8. **Submeta** para salvar as mudanças a este perfil novo do controle do destino.
9. **Comprometa** para salvar todas as mudanças à configuração.

Adicionar perfis do controle do destino.

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

Ideia sumária de perfis novos do controle do destino.

Construção do filtro da mensagem para a produção ESA

Do CLI na produção ESA, construa um filtro da mensagem que possa email BCC ao ouvinte apropriado no beta ESA.

1. Navegue aos **filtros > NOVO**.
2. A cópia e cola este exemplo do filtro da mensagem e faz as mudanças onde apropriadas:

```
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. **Retorne** até que você esteja de volta à alerta principal CLI.
4. **Comprometa** para salvar todas as mudanças à configuração.

Nota: Limite o tráfego copiado no filtro da mensagem baseado no sendergroup, o RECV-ouvinte, correio-de, ou as outras regras e sintaxe disponíveis. Consulte o Guia do Usuário ESA para as regras de filtro do mensagem completa e as regras de filtro sumárias.

Salte a criação do perfil

O destino controla a criação do perfil

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Neste tempo, o beta dispositivo aceita o tráfego do email do dispositivo da produção. A fim verificar do CLI no beta dispositivo, execute **mail_logs da cauda**:

```
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
```

A comunicação de SMTP estabelece em 172.18.250.222 (beta dispositivo). O endereço de que o tráfego é enviado é de 172.18.250.224 (dispositivo da produção).

O grupo do remetente que recebe a comunicação é RELÉ, tráfego retransmitido da rede 172.18.250.1/24.

O resto é a comunicação da mensagem TEST2.

No dispositivo da produção, verifique e execute **mail_logs da cauda**. O MEADOS DE processado na produção mostraria:

Esta seria uma lasca bem defenida do mensagem de Email como recebido e BCC'd sobre ao beta dispositivo e testaria o utilizador final como pretendido para o recibo.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Additional Information

Um filtro satisfeito pode ser considerado a fim ajudar a diferenciar a produção contra o beta tráfego do email para utilizadores finais do teste.

1. Do GUI no beta ESA, navegue **para enviar políticas > filtros satisfeitos entrantes ou políticas do correio > filtros satisfeitos que parte**.
2. Construa um filtro satisfeito básico a fim executar uma ação Add/edite o encabeçamento.
3. O clique **submete-se** a fim salvar mudanças ao filtro satisfeito construído.
4. **As políticas do correio > as políticas do correio recebido** ou **as políticas do correio > políticas que parte do correio**, permitem e adicionam o filtro satisfeito novo ao nome da política.
5. O clique **submete-se** a fim salvar o filtro satisfeito a essa política.
6. O clique **compromete** a fim salvar todas as mudanças à configuração.

Neste tempo, o filtro satisfeito no beta ESA é segundo as indicações das imagens:

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

Conditions			
<input type="button" value="Add Condition..."/>			
<i>There are no conditions, so actions will always apply.</i>			

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Add/Edit Header	edit-header-text("Subject", "(.*)", "[BETA PROCESSED]\\1")	<input type="button" value="Delete"/>

Agora, quando um mensagem de Email é recebido no beta ESA você pode ver este na linha de assunto do email processado uma vez segundo as indicações da imagem:

[BETA PROCESSED]TEST 3



test@test.com <test@test.com>

Wednesday, March 23, 2016 at 3:01 PM

To:

hello

Informações Relacionadas

- [Como configurar um ESA/SMA para atualizações de encenação](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)