Configuración ESA beta para validar el tráfico de la producción ESA

Contenido

Introducción

Este documento describe cómo configurar un dispositivo de seguridad beta del correo electrónico de Cisco (ESA) para validar el tráfico de la producción ESA vía un filtro del mensaje.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configure el dispositivo beta

Configuración del módulo de escucha para el ESA beta

La configuración inicial del módulo de escucha debe ser completada en el ESA beta.

1. Del GUI, navegue a la **red > a los módulos de escucha**.
2. El tecleo **agrega al módulo de escucha…**
3. Nombre y puesto un módulo de escucha público que se ejecuta en el puerto TCP 25.
4. El tecleo **somete** para salvar los cambios al módulo de escucha público.
5. Relance los mismos pasos y agregue a un segundo módulo de escucha.
6. Nombre y puesto un módulo de escucha privado que se ejecuta en el puerto TCP 26. (Utilizan a este módulo de escucha para el correo saliente.) Usted puede utilizar el puerto 25 si hay una interfaz adicional disponible y configurada para su entorno. El entorno beta recibido CES ha reservado el puerto 587 para saliente.
7. **Someta** para salvar los cambios al módulo de escucha.
8. **El cometer** para salvar todo cambia a la configuración.

Grupo del remitente para el ESA beta

Para el tráfico o los mensajes de salida retransmitidos, agregue en la dirección IP apropiada para el ESA beta para validar y los mensajes de retransmisión de la producción ESA.

1. Del GUI, navegue **para enviar las directivas > la descripción del SOMBRERO**.
2. Seleccione el grupo apropiadamente Nombrado del remitente de la retransmisión. (Esto generalmente se nombra RETRANSMISIÓN, o RELAYLIST.)
3. El tecleo **agrega el remitente…**
4. Para el remitente, utilice la dirección IP de la producción ESA.
5. Ingrese cualquier comentario administrativo, según lo necesitado.
6. **Someta** para salvar los cambios al grupo del remitente de la retransmisión.
7. **El cometer** para salvar todo cambia a la configuración.

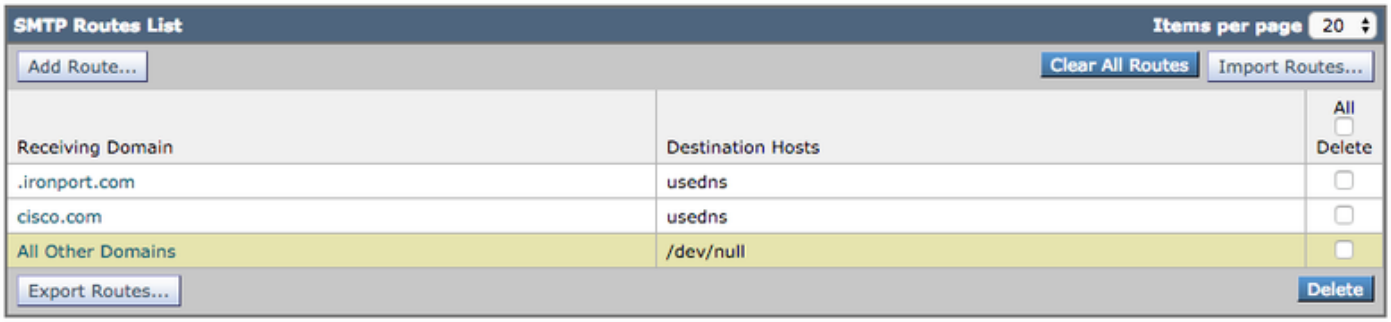
Rutas del Simple Mail Transfer Protocol (SMTP) para el ESA beta

Los cambios de ruta S TP que necesitan ser realizados en el ESA beta son como sigue:

1. Del GUI, navegue a la **red > a las rutas S TP**.
2. Si hay rutas actuales S TP, usted puede necesitar seleccionar ésos y la **cancelación** antes de que usted proceda. (Asegure para revisar el guía beta de la configuración de laboratorio.)
3. El tecleo **agrega la ruta…**
4. Fije el dominio de recepción como **cisco.com** y el destino como **USEDNS**.
5. Haga clic en Submit (Enviar).
6. Relance los mismos pasos y agregue en una segunda ruta S TP.

7. Fije la recepción del dominio para **ironport.com** y del destino como **USEDNS**.
8. Haga clic en Submit (Enviar).
9. Finalmente, seleccione **el resto de los dominios de** recibir el dominio.
10. Fije el destino como **/dev/null**. (Esto evita el rutear del correo del dispositivo beta para cualquier dominio no configurado.)
11. Haga clic en Submit (Enviar).
12. **El cometer** para salvar todo cambia a la configuración.

Ahora, las rutas S TP en el dispositivo beta están tal y como se muestra en de la imagen:



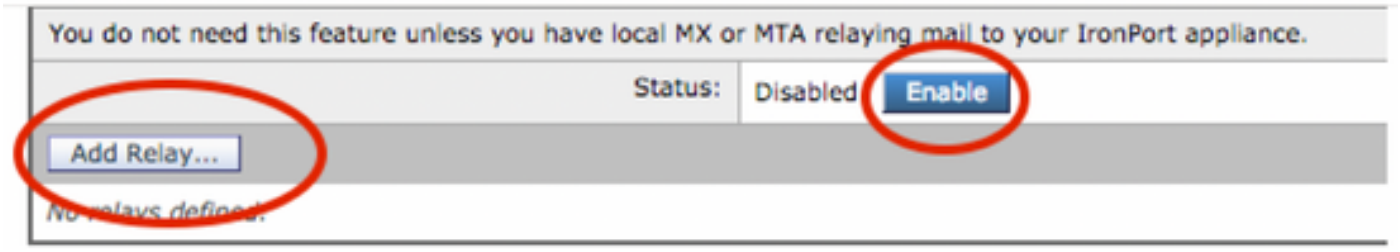
Nota: Agregue las rutas apropiadas para entregar los correos electrónicos para probar a los usuarios finales para los dominios según las necesidades.

Retransmisión entrante para el ESA beta

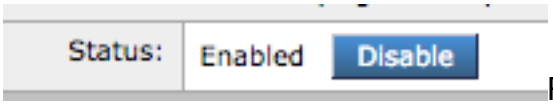
La configuración de Relay entrante permite que el beta extraiga el beyone de la calificación SBR que de la producción ESA.

La mayoría de las configuraciones trabajarán con un salto.

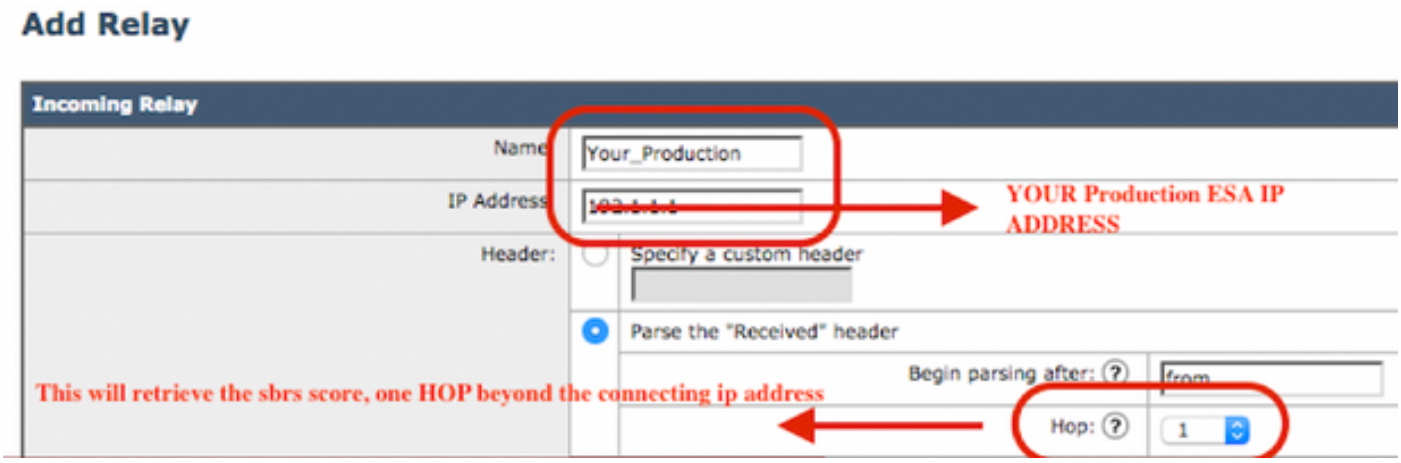
1. El GUI, navega a la retransmisión Entrante de red.
2. “enable” del tecleo que le da vuelta blanco en el color.
3. El tecleo agrega la retransmisión.
4. El “nombre” elige un nombre.
5. Valor de la “dirección IP” de la producción ESA que entrega al ESA beta. El nombre de host parcial es aceptable si los host múltiples están entregando.
6. “Salto: ” 1
7. Someta y confíe los cambios



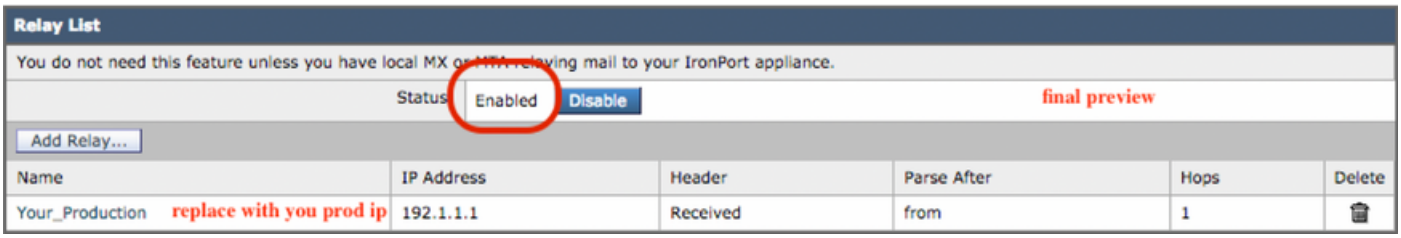
Retransmisión entrante: Estado inhabilitado.



Retransmisión entrante: Estado habilitado, blanco coloreado.



Retransmisión entrante: Plantilla de la muestra



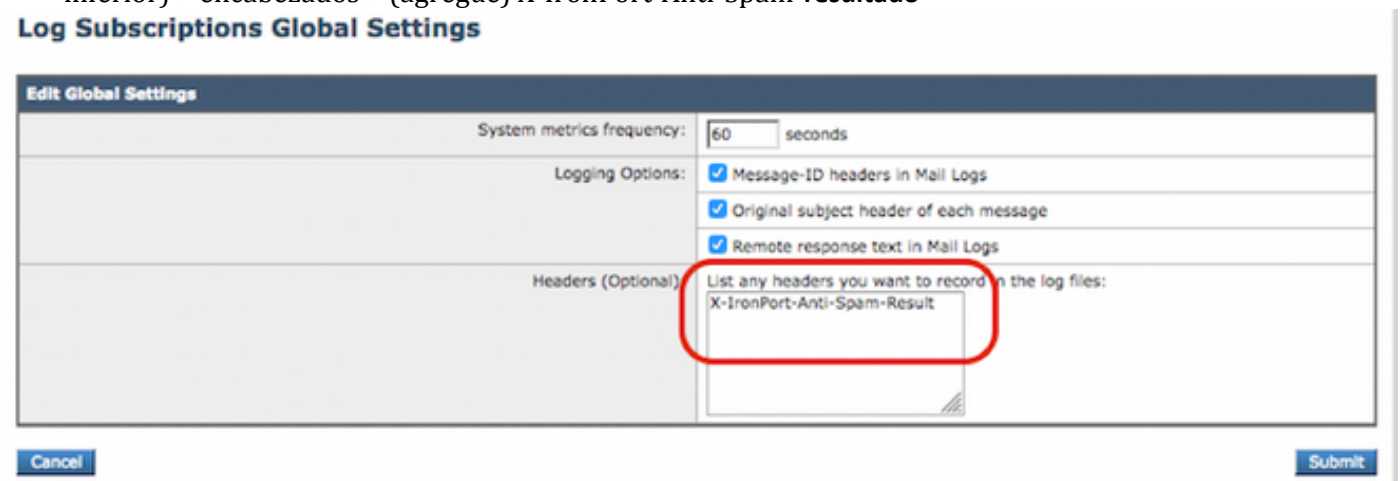
Retransmisión entrante: La visión sumaria después de somete.

Entrada de registro del correo de la muestra:

Lunes información 2019 del 8 de abril 12:48:28: MEDIADOS DE 2422822 **IncomingRelay(PROD_hc2881-52)**: Encabezado recibida encontrada, IP 54.240.35.22 que es utilizado, país Estados Unidos SBR 3.5

Encabezados del registro del permiso para capturar el veredicto del Spam dentro de los registros del correo

- Webui > suscripciones de la administración del sistema > del registro > configuraciones globales (parte inferior) > encabezados > (agregue) X-IronPort-Anti-Spam-**resultado**



Registre las encabezados del Spam para enviar los registros

FINAL DE LA CONFIGURACIÓN LATERAL BETA.

Dispositivo de la producción de la configuración

Precaución: Usted está a punto de realizar los cambios a una producción ESA. Asegúrese de que usted respaldo la configuración actual.

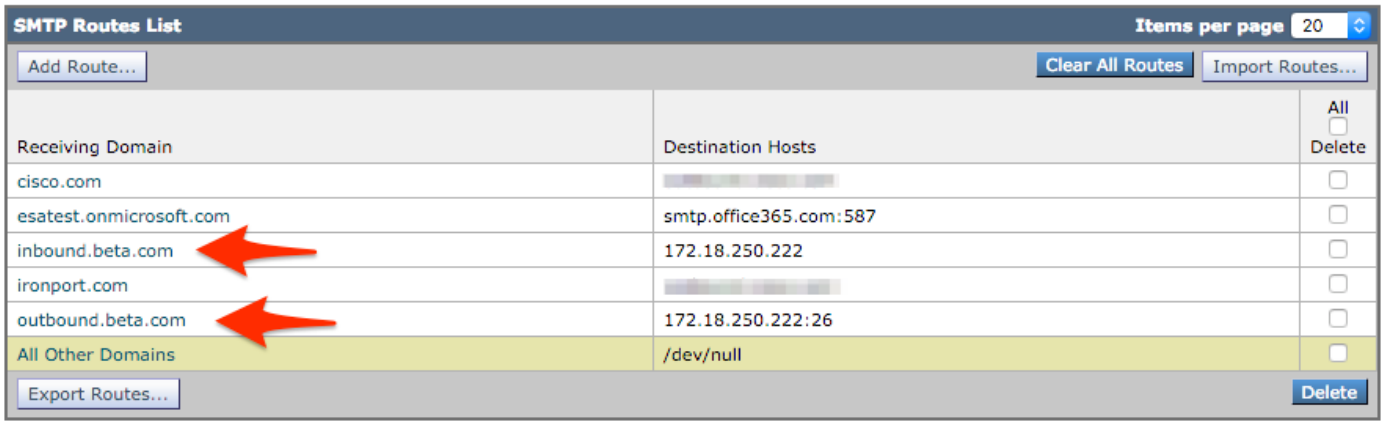
1. Del GUI, navegue a la **administración del sistema > al archivo de configuración**.
2. De la sección de configuración actual, seleccione una de las opciones para sostener la configuración actual como archivo: Descargue el archivo a la computadora local para ver o para salvar.Envíe por correo electrónico el archivo a: < your_email_address@domain.com >
3. Haga clic en Submit (Enviar).

Rutas S TP para la producción ESA

Las rutas S TP se deben agregar para permitir el BCC para todos los correos electrónicos entrantes y salientes de la producción ESA al ESA beta. Por este ejemplo, se utilizan **inbound.beta.com** y **outbound.beta.com**.

1. Del GUI, navegue a la **red > a las rutas S TP**.
2. El tecleo **agrega la ruta…**
3. Fije la recepción del dominio como **inbound.beta.com** con el destino como la dirección IP del módulo de escucha público del dispositivo beta creado anterior, con el puerto fijado a 25.
4. El tecleo **somete** para salvar los cambios a esta nueva ruta S TP.
5. Relance los mismos pasos, **agregue la ruta…**
6. Fije el dominio de recepción como **outbound.beta.com**, las computadoras principales de destino como la dirección IP del módulo de escucha privado del dispositivo beta creado anterior, y el puerto a 26.
7. **Someta** para salvar los cambios a esta nueva ruta S TP.
8. **El cometer** para salvar todo cambia a la configuración.

Ahora, rutas S TP en la producción ESA tal y como se muestra en de la imagen:

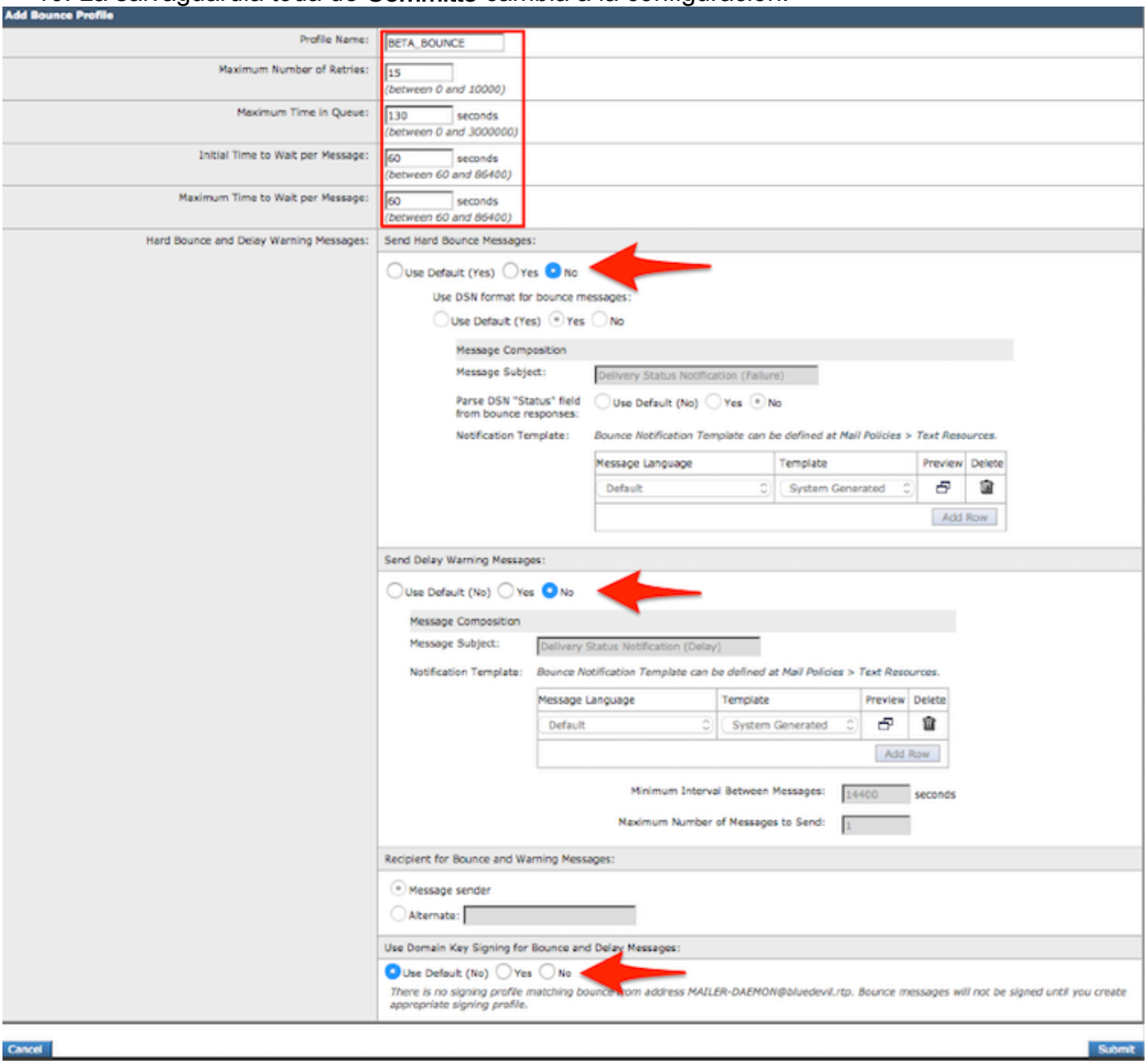


Creación del perfil de la despedida

Un perfil de la despedida de la combinación y el perfil del control del destino protegerán el flujo de correo de la producción contra las complicaciones asociadas a los retardos o a los errores de entregar los mensajes a los host beta. Esta configuración se aplicará solamente a los mensajes beta.

1. Del GUI, navegue al **perfil de la despedida de los** perfiles de la red > de la despedida > Add.
2. Número máximo de Retries: **15**

3. Tiempo máximo en la cola: **130**
4. Hora inicial de esperar por el mensaje: **60**
5. Tiempo máximo para esperar por el mensaje: **60**
6. Envíe los mensajes de despedida duros: **NO**
7. Envíe los mensajes de advertencia del retardo: **NO**
8. Utilice la clave del dominio que firma para la despedida y retrase los mensajes: **NO**
9. **Someta** para salvar los cambios a este nuevo perfil de la despedida.
10. La salvaguardia toda de **Committo** cambia a la configuración.

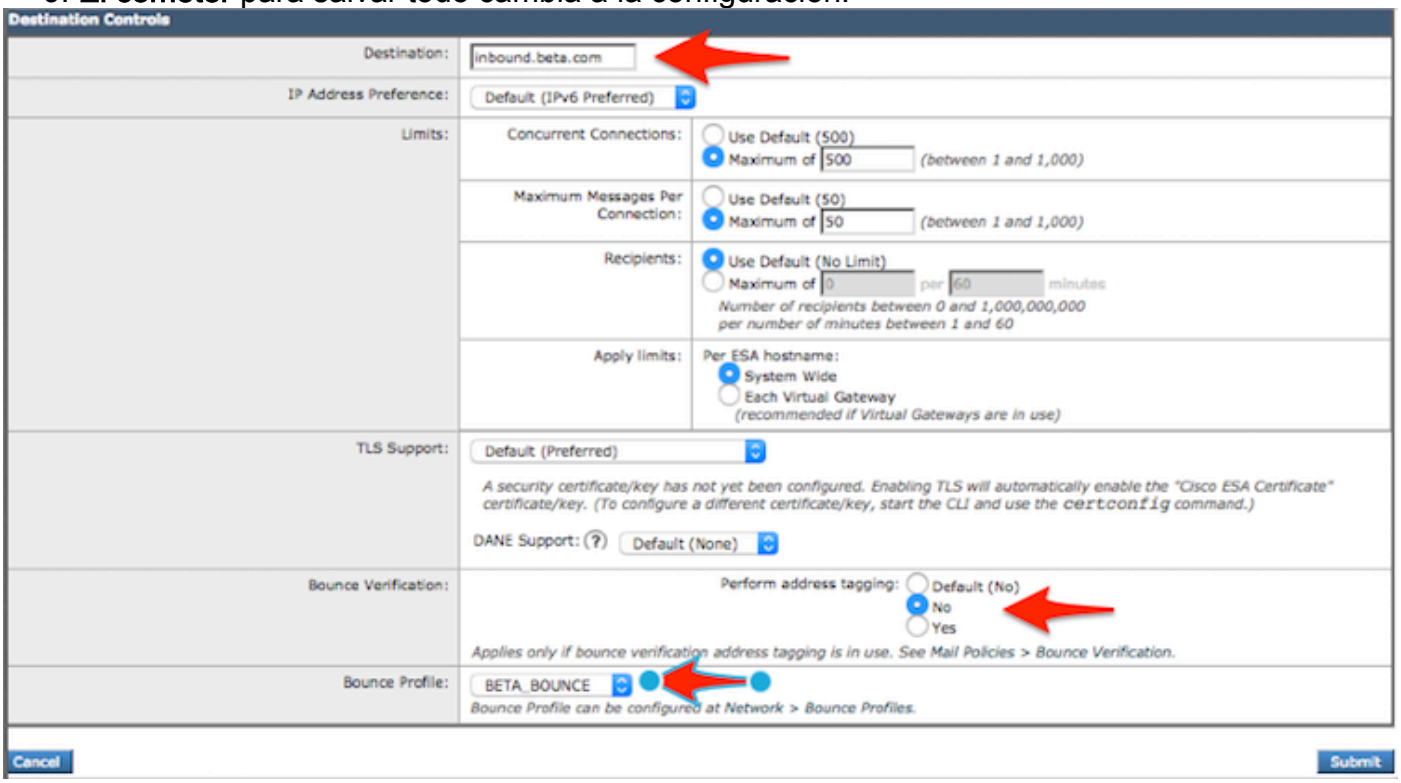


Creación del perfil de la despedida

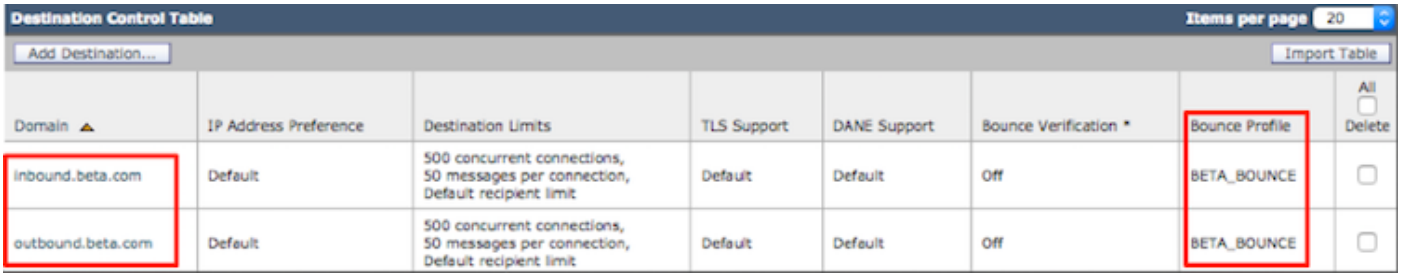
Nota: Los valores numerados antedichos se configuran muy agresivamente para prevenir los respaldos de la cola de la salida en caso de interrupción de la salida a los host beta. Los valores se pueden modificar a la preferencia. Las configuraciones de la notificación se fijan intencionalmente a NO para evitar que cualquier notificación de usuario sea entregada de los filtros BCC.

El destino controla la creación del perfil

1. Del GUI, navegue para enviar las directivas > el destino de los controles del destino > Add.
2. Destino: **inbound.beta.com**
3. Verificación de la despedida: **> realice marcar con etiqueta del direccionamiento: NINGÚN >** o valor por defecto (NO)
4. **Perfil de la despedida: BETA_BOUNCE**
5. Los otros valores se pueden configurar sobre la base de la preferencia del administrador.
6. **Someta** para salvar los cambios a este nuevo perfil del control del destino.
7. **Relance los** pasos 2 - 6 usando el destino: **outbound.beta.com**
8. **Someta** para salvar los cambios a este nuevo perfil del control del destino.
9. **El cometer** para salvar todo cambia a la configuración.



Agregue los perfiles del control del destino.



Vista sumaria de los nuevos perfiles del control del destino.

Construcción del filtro del mensaje para la producción ESA

Del CLI en la producción ESA, construya un filtro del mensaje que pueda los correos electrónicos BCC al módulo de escucha apropiado en el ESA beta.

1. Navegue a los **filtros > NUEVO**.
2. La copia y pega este ejemplo del filtro del mensaje y realiza los cambios dondequiera que apropiados:

```
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. **Vuelva** hasta que usted esté de nuevo al prompt principal CLI.
4. **El cometer** para salvar todo cambia a la configuración.

Nota: Limite el tráfico copiado en el filtro del mensaje basado en el sendergroup, el recv-módulo de escucha, correo-de, o las otras reglas y sintaxis disponibles. Consulte el guía del usuario ESA para las reglas para filtros del mensaje Complete y las reglas para filtros sumarias.

Despida la creación del perfil

El destino controla la creación del perfil

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Ahora, el dispositivo beta valida el tráfico del correo electrónico del dispositivo de la producción. Para verificar del CLI en el dispositivo beta, ejecute los **mail_logs de la cola**:

```
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
```

La comunicación SMTP establece en 172.18.250.222 (dispositivo beta). El direccionamiento del cual se envía el tráfico es de es 172.18.250.224 (dispositivo de la producción).

El grupo del remitente que recibe la comunicación es RETRANSMISIÓN, tráfico retransmitido de la red 172.18.250.1/24.

El resto es la comunicación del mensaje TEST2.

En el dispositivo de la producción, verifique y ejecute los **mail_logs de la cola**. El MEDIADOS DE procesada en la producción mostraría:

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

Éste sería el astillar claro del correo electrónico según lo recibido y BCC'd encima al dispositivo beta y probaría al usuario final según lo previsto para el recibo.

Troubleshooting

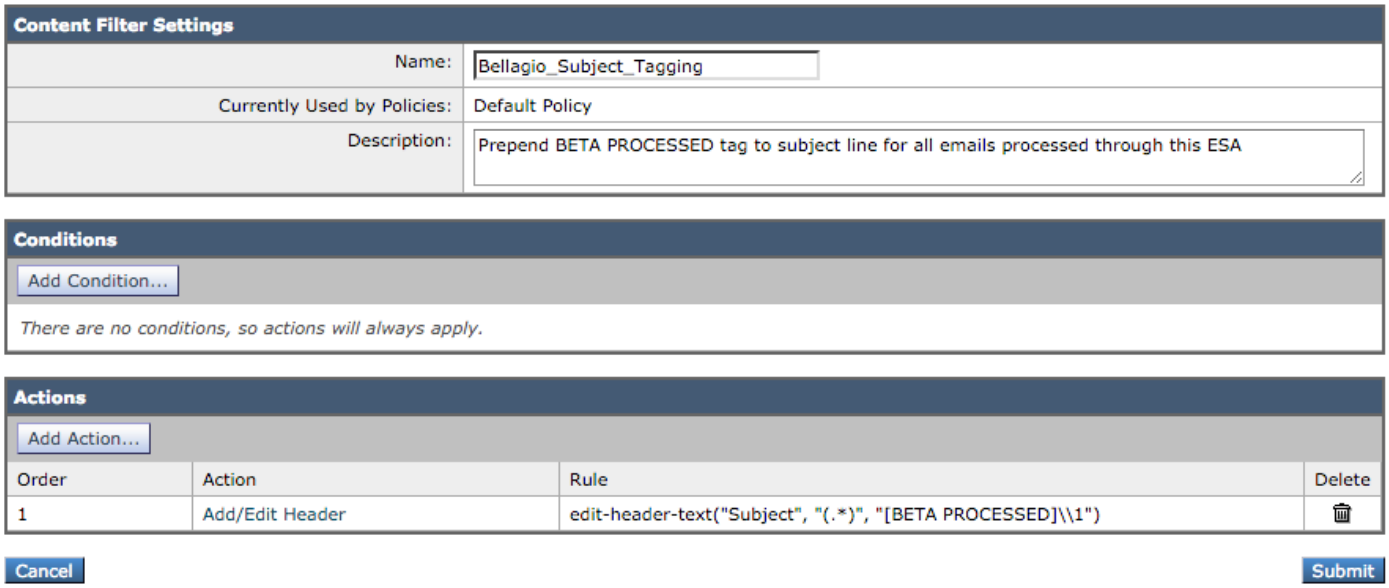
Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información adicional

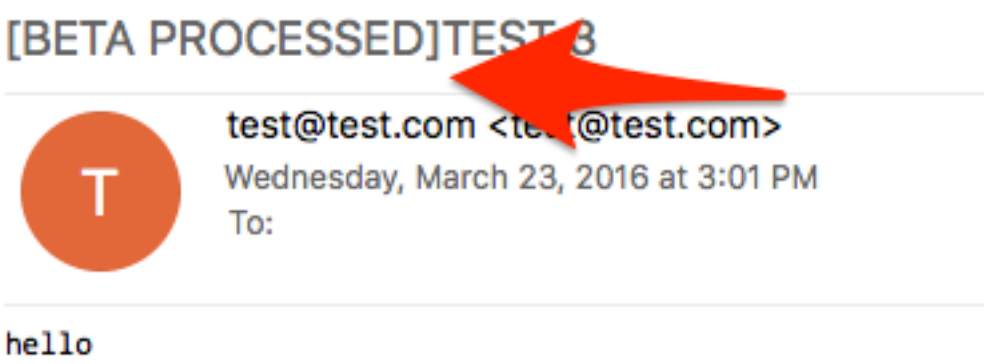
Un filtro contento se puede considerar para ayudar a distinguir la producción contra el tráfico beta del correo electrónico para los usuarios finales de la prueba.

1. Del GUI en el ESA beta, navegue **para enviar las directivas > los filtros contentos entrantes** o las **directivas del correo > los filtros contentos salientes**.
2. Construya un filtro contento básico para realizar una acción Add/edite la encabezado.
3. El tecleo **somete** para salvar los cambios al filtro contento construido.
4. **Las directivas del correo > las directivas del correo entrante** o las **directivas del correo > las directivas salientes del correo**, permiso y agregan el nuevo filtro contento al nombre de la directiva.
5. El tecleo **somete** para salvar el filtro contento a esa directiva.
6. Haga clic el **cometer** para salvar todos los cambios a la configuración.

Ahora, el filtro contento en el ESA beta está tal y como se muestra en de las imágenes:



Ahora, cuando un correo electrónico se recibe en el ESA beta usted puede ver esto en el asunto del correo electrónico procesado una vez tal y como se muestra en de la imagen:



Información Relacionada

- Cómo configurar un ESA/SMA para las actualizaciones que efectúan
- Soporte Técnico y Documentación - Cisco Systems