

Bèta ESA configureren om productie ESA verkeer te accepteren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Bèta-applicatie configureren](#)

[Configuratie van luisteraar voor Bèta ESA](#)

[Sender Group voor Beta ESA](#)

[Simple Mail Transfer Protocol \(MTP\)-routers voor BESA](#)

[Inkomende relay voor Bèta ESA](#)

[Koppen voor inloggen inschakelen om het Samsung-vonnis in de postlogbestanden op te nemen](#)

[Productie-applicatie configureren](#)

[MTP-routes voor de productie van het ESR](#)

[Profielcreatie starten](#)

[Creatie van profiel van besturing van de bestemming](#)

[Berichtfilter Bouw van productie ESA](#)

[Profielcreatie starten](#)

[Creatie van profiel van besturing van de bestemming](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Aanvullende informatie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een Bèta Cisco e-mail security applicatie (ESA) kunt configureren om ESA-verkeer te verwerken via een berichtfilter.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Bèta-applicatie configureren

Configuratie van luisteraar voor Bèta ESA

De eerste configuratie van de Lijstconfiguratie moet worden voltooid op de Beta ESA.

1. Vanuit de GUI, navigeer naar **Netwerk > Lijsten**.
2. Klik op **Luisteraar toevoegen...**
3. Naam en instelling een openbare Lijstserver die op TCP poort 25 draait.
4. Klik op **Inzenden** om de wijzigingen in de openbare lijst op te slaan.
5. Herhaal de zelfde stappen en voeg een tweede luisteraar toe.
6. Naam en instelling een privé-luisteraar die op TCP poort 26 draait. (Deze luisteraar wordt gebruikt voor uitgaande mail.) U kunt poort 25 gebruiken als er een extra interface beschikbaar en ingesteld is voor uw omgeving. CES Hosted Bèta-omgeving heeft poort 587 gereserveerd voor uitzending.
7. **Indienen** om wijzigingen in de Luisteraar op te slaan.
8. **Verbind** om alle veranderingen in de configuratie op te slaan.

Sender Group voor Beta ESA

Vermeld voor omgekeerde of uitgaande berichten het passende IP-adres(en) van de Beta ESA om berichten van de Production ESA te aanvaarden en door te geven.

1. Vanuit de GUI, navigeer naar **Mail Policy > HAT - Overzicht**.
2. Selecteer de juiste naam Relay Sender Group. (Deze naam wordt gewoonlijk RELAY of RELAYLIST genoemd.)
3. Klik op **Eender toevoegen...**
4. Gebruik voor Zender het IP-adres van het ProductieESA.
5. Voer indien nodig alle administratieve opmerkingen in.
6. **Indienen** om wijzigingen in de Relay Sender Group op te slaan.
7. **Verbind** om alle veranderingen in de configuratie op te slaan.

Simple Mail Transfer Protocol (MTP)-routers voor BESA

Op de Beta ESA's moeten volgende routewijzigingen worden aangebracht:

1. Vanuit de GUI, navigeer naar **Netwerk > Routes**.
2. Als er huidige TCP-routes zijn, kunt u deze moeten selecteren en **verwijderen** voordat u doorgaat. (Verzeker u ervan dat u de setup-gids van het bèta-label opnieuw bekijkt.)
3. Klik op **Toevoegen route...**
4. Stel het ontvangende domein in als **cisco.com** en Destination als **USEDNS**.
5. Klik op **Inzenden**.
6. Herhaal de zelfde stappen en voeg in een tweede route toe TCP.
7. Instellen Ontvangend Domein voor **Aironport.com** en Bestemming als **USEDNS**.

8. Klik op **Inzenden**.
9. Tenslotte selecteert u **Alle andere velden** uit ontvangstdomein.
10. Stel de bestemming in als **/dev/nul**. (Dit voorkomt het versturen van e-mail van het Bèta-apparaat voor gebieden die niet zijn geconfigureerd.)
11. Klik op **Inzenden**.
12. **Verbind** om alle veranderingen in de configuratie op te slaan.

Op dit moment zijn MTP-routers op het Bèreapparaat zoals in de afbeelding:

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

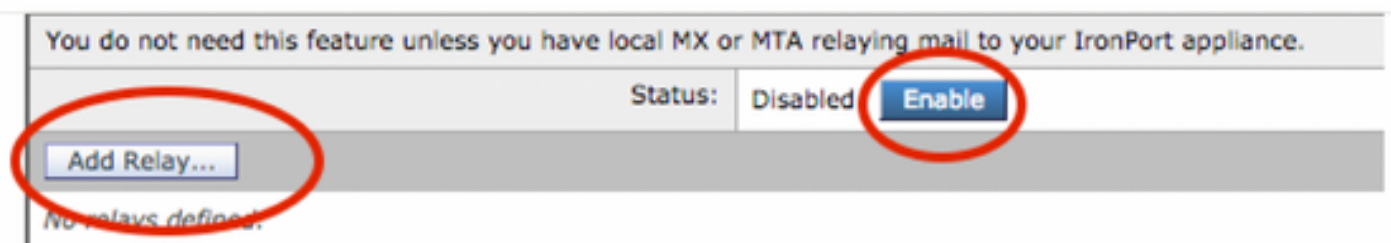
Opmerking: Voeg de juiste routes toe om e-mails te leveren om eindgebruikers voor domeinen te testen waar nodig.

Inkomende relay voor Bèta ESA

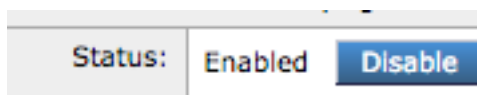
Met behulp van de inkomende relaisconfiguratie kan de bèta de SBRS-score boven die van de Productie ESA herstellen.

De meeste configuraties werken met één agent.

1. GUI, navigeer naar Network Inkomend Relay.
2. Klik op "Inschakelen" om het wit in kleur te draaien.
3. Klik op Relay toevoegen.
4. "Naam" kiest een naam.
5. "IP-adreswaarde" van de productie ESA die levert aan de Beta ESA. De gedeeltelijke hostname is aanvaardbaar als de meerdere gastheren leveren.
6. "Hop:" 1
7. Wijzigingen indienen en beloven



inkomende relay: Uitgeschakelde staat.



inkomende relay: Ingeschakeld, gekleurd wit.

Add Relay

Incoming Relay

Name:

IP Address:

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

Begin parsing after:

Hop:

YOUR Production ESA IP ADDRESS

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

inkomende relay: Monstersjabloon

Relay List

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

Status:

final preview

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

inkomende relay: Summary View na Submit.

Ingang postlogboek van voorbeeld:

8 maart 2019 Info: MID 2422822 inkomendeRelay (PROD_hc2881-52): Gevonden header, IP 54.240.35.22 gebruikt, SBRS 3.5 land Verenigde Staten

Koppen voor inloggen inschakelen om het Samsung-vonnis in de postlogbestanden op te nemen

- Webei > Systeembeheer > Log abonnementen > Global Settings (onder) > Koppen > (add/drop) **X-IJzeren poort-anti-SPAM-resultaat**

Log Subscriptions Global Settings

Edit Global Settings

System metrics frequency: seconds

Logging Options:

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

Headers (Optional):

Log spamkoppen op postlogboek

EINDTIJD VAN DE BETA-CONFIGURATIE.

Productie-applicatie configureren

Voorzichtig: U staat op het punt wijzigingen aan te brengen in een ESA. Zorg ervoor dat u back-up maakt van de huidige configuratie.

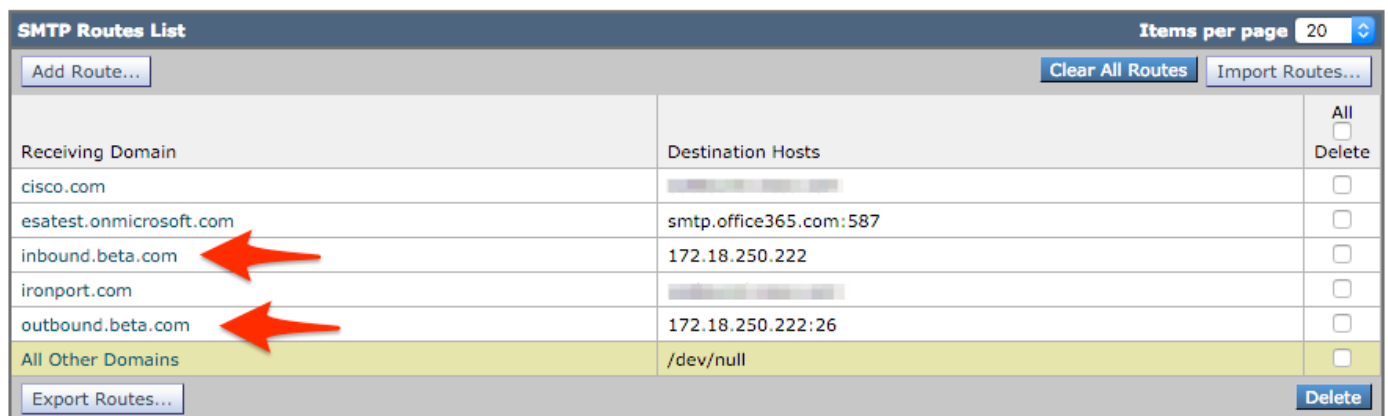
1. Vanuit de GUI, navigeer naar **Systeembeheer > Configuratiebestand**.
2. Selecteer in het gedeelte Huidige configuratie een van de opties om een back-up van de huidige configuratie als bestand te maken: Downloadbestand naar lokale computer om te bekijken of op te slaan. E-mailbestand naar: <your_email_address@domain.com>
3. Klik op **Inzenden**.

MTP-routes voor de productie van het ESR

Er moeten mtp-routes worden toegevoegd om BCC voor alle inkomende en uitgaande e-mails van de Productie ESA naar de Beta ESA toe te staan. Bijvoorbeeld, **inbound.bèta.com** en **outbound.bèta.com** worden gebruikt.

1. Vanuit de GUI, navigeer naar **Netwerk > Routes**.
2. Klik op **Toevoegen route...**
3. Stel Domeinondersteuning in als **inbound.beta.com** met Destination in als het IP-adres van de openbare Luisteraar van het Beta-apparaat dat eerder gemaakt werd, met de poort ingesteld op 25.
4. Klik op **Indienen** om wijzigingen in deze nieuwe route op te slaan.
5. Herhaal dezelfde stappen, **voeg route toe...**
6. Stel het Ontvangende Domein in als **outbound.bèta.com**, Destination Hosts in als het IP adres van de Beta toestel privé Luisteraar die eerder werd gemaakt, en de haven aan 26.
7. **Indienen** om de veranderingen in deze nieuwe route op te slaan.
8. **Verbind** om alle veranderingen in de configuratie op te slaan.

Op dat moment worden de MTP-routes op de Productie ESA aangegeven zoals in de afbeelding:



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"/>

Profielcreatie starten

Een combinatie van een stuitprofiel en een profiel van doelcontrole zal de productie-mailstroom beschermen tegen complicaties die gepaard gaan met vertragingen of mislukkingen om berichten aan de Bèta Hosts te leveren. Deze configuratie is alleen van toepassing op de bèta-berichten.

1. Vanuit de GUI, navigeer naar **Network > Bounce profielen > Bounce Profile** toevoegen.
2. U kunt maximaal aantal keren proberen: 15
3. Max. tijd in wachtrij: 130

4. Eerste tijd om per bericht te wachten: 60
5. Max. tijd om per bericht te wachten: 60
6. Harde bounce sturen: NEE
7. Waarschuwingen voor vertraging verzenden: NEE
8. Domain Key Signing voor Bounce en Delay Messaging: NEE
9. Indienen om de wijzigingen in dit nieuwe Bounce Profile op te slaan.
10. Om alle wijzigingen in de configuratie op te slaan.

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 from address MAILER-DAEMON@bluedevil.rtp. Bounce messages will not be signed until you create appropriate signing profile.

Creatie van profiel voor bellen

Opmerking: de bovenstaande genummerde waarden zijn zeer agressief geconfigureerd om back-ups van de bezorging te voorkomen in het geval van een onderbreking van de bezorging in de bèta-hosts. De waarden kunnen worden aangepast aan de voorkeur. De berichtinstellingen worden opzettelijk op NO ingesteld om te voorkomen dat er gebruikersmeldingen vanuit de BCC-filters worden ontvangen.

Creatie van profiel van besturing van de bestemming

1. Vanuit de GUI, navigeer naar postbeleid > Bestemmingscontroles > Bestanden toevoegen.
2. Bestemming: **inbound.beta.com**
3. Bounce verificatie: > **Voer adresmarkering uit: NEE** > of Standaard (NEE)
4. **Bounce profiel: BETA_BOUNCE**
5. De andere waarden kunnen worden ingesteld op basis van de voorkeur van de beheerder.
6. **Indienen** om de wijzigingen in dit nieuwe doelcontroleprofiel op te slaan.
7. **Herhaal** stap 2 - 6 op de bestemming: **outbound.beta.com**
8. **Indienen** om de wijzigingen in dit nieuwe doelcontroleprofiel op te slaan.
9. **Verbind** om alle veranderingen in de configuratie op te slaan.

Destination Controls configuration page showing the following settings:

- Destination: inbound.beta.com
- IP Address Preference: Default (IPv6 Preferred)
- Limits:
 - Concurrent Connections: Maximum of 500 (between 1 and 1,000)
 - Maximum Messages Per Connection: Maximum of 50 (between 1 and 1,000)
 - Recipients: Use Default (No Limit)
- Apply limits: System Wide
- TLS Support: Default (Preferred)
- DANE Support: Default (None)
- Bounce Verification: Perform address tagging: No
- Bounce Profile: BETA_BOUNCE

Bestemmingscontroleprofielen toevoegen.

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"/>

Summary View of New Destination Control Profiles.

Berichtfilter Bouw van productie ESA

Vanuit de CLI op de Productie ESA, bouw een berichtfilter dat BCC e-mails naar de juiste Luisteraar op de Bèta ESA kan sturen.

1. Navigeer naar **filters > NIEUW**.
2. Kopieer en plak dit voorbeeld van het berichtfilter en wijzig de gewenste instellingen indien nodig:

```
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. **Ga terug** tot u terug bent naar de hoofdlocatie van CLI.
4. **Verbind** om alle veranderingen in de configuratie op te slaan.

Opmerking: Beperk het verkeer dat in het berichtfilter wordt gekopieerd op basis van sendergroep, recv-luisteraar, mail-from of andere beschikbare regels en syntax. Raadpleeg de ESA-gebruikershandleiding voor een volledige samenvatting van de berichtfilterregels en de filterregels.

Profielcreatie starten

Creatie van profiel van besturing van de bestemming

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Op dit moment accepteert het Beta-apparaat e-mailverkeer van Productieapparaat. Laat CLI op het Beta-apparaat om het volgende te controleren **per tail mail_logs**:

```
Wed Mar 23 17:28:43 2016 Info: New SMTP ICID 2 interface Management (172.18.250.222) address  
172.18.250.224 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
```

In de MTP-mededeling wordt vastgesteld op 172.18.250.222 (Beta-apparaat). Het adres waar het verkeer wordt verstuurd, is 172.18.250.224 (Productieapparaat).

De verzendende Groep die de mededeling ontvangt is RELAY, het indirecte verkeer van het 172.18.250.1/24 netwerk.

De rest is de communicatie van het TEST 2 bericht.

Controleer en voer in het productieapparaat **mail_logs** op. Uit de op productie verwerkte MID's

zou blijken:

Wed Mar 23 14:50:10 2016 Info: MID 242 was generated based on MID 241 by bcc filter 'bcc-EFT'
Dit zou een duidelijke splitsing zijn van het e-mailbericht zoals ontvangen en BCC zou naar het Beta-apparaat overstappen en de eindgebruiker testen zoals bedoeld voor ontvangst.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Aanvullende informatie

Een inhoudfilter kan worden overwogen om productie te differentiëren naar het e-mailverkeer van de testeindgebruikers.

1. Vanuit de GUI op de Bèta ESA, navigeer naar **postbeleid > Inkomend contentfilters of postbeleid > Uitgaande contentfilters**.
2. Maak een basisfilter om een actie van Kop toevoegen/bewerken uit te voeren.
3. Klik op **Inzenden** om wijzigingen in het geconstrueerde inhoudfilter op te slaan.
4. **Mail Policies > inkomend Mail beleid of Mail beleid > Outdoorlopend Mail beleid** , schakelt het nieuwe content filter in en voegt deze toe aan de Policy name.
5. Klik op **Inzenden** om het contentfilter in dat beleid op te slaan.
6. Klik op **Commit** om alle wijzigingen in de configuratie op te slaan.

Het inhoudfilter van de Beta ESA is op dat moment zoals in de beelden wordt getoond:

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")	

Wanneer een e-mailbericht wordt ontvangen op de Beta ESA, zie je dit in de Onderwerp regel van de e-mail zodra verwerkt zoals in de afbeelding:

[BETA PROCESSED]TEST 3



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

Wednesday, March 23, 2016 at 3:01 PM

To:

hello

Gerelateerde informatie

- [Een ESA/SMA configureren voor updates](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)