

Uitgebreide IP-adressen/domeinen/e-mailadressen van de ESA Bounce Configuration

Inhoud

[Inleiding](#)

[Uitgebreide IP-adressen/domeinen/e-mailadressen van de ESA Bounce Configuration](#)

[Uitgaande post](#)

[inkomende e](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u inkomende en uitgaande mail kunt configureren om IP-adressen, domeinen of e-mailadressen te openen voor Cisco Email Security Appliance (ESA).

Uitgebreide IP-adressen/domeinen/e-mailadressen van de ESA Bounce Configuration

U kunt ontvangende domeinen specificeren waarop u Bounce Verification kunt uitschakelen wanneer het ESA aan deze domeinen levert. U zult zowel uitgaande als inkomende post moeten configureren.

Uitgaande post

1. Ga naar postbeleid > Bestemmingscontroles.
2. Selecteer "Toevoeging toevoegen...".
3. Bel de nieuwe bestemming "voorbeeld.com".
4. Stel in de instellingen "Bounce Verification" in op Nee.
5. Wijzigingen indienen en beloven.

Destination Controls	
Destination:	<input type="text" value="example.com"/>
IP Address Preference:	Default (IPv6 Preferred) ▾
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <i>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</i>
	Apply limits: Per Destination: <input checked="" type="radio"/> Entire Domain <input type="radio"/> Each Mail Exchanger (MX Record) IP address Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <i>(recommended if Virtual Gateways are in use)</i>
TLS Support:	Default (None) ▾ <i>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)</i>
Bounce Verification:	Perform address tagging: <input type="radio"/> Default (No) <input checked="" type="radio"/> No <input type="radio"/> Yes <i>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</i>
Bounce Profile:	Default ▾ <i>Bounce Profile can be configured at Network > Bounce Profiles.</i>

Opmerking: voor uitgaande mail kunt u alleen naar het doeldomein verwijzen en niet naar een IP-adres of e-mailadres.

Inkomende e

Security Features	
Spam Detection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Virus Protection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Encryption and Authentication:	TLS: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required <small>A security certificate/key has not been configured and assigned to a listener. (See Network > Certificates.) Enabling TLS will automatically use the "Demo" certificate/key for listeners.</small> <input type="checkbox"/> Verify Client Certificate
	SMTP Authentication: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required If Both TLS and SMTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTP Authentication
	Domain Key/DMARC Signing: <input type="radio"/> On <input checked="" type="radio"/> Off
	DKIM Verification: <input type="radio"/> On <input checked="" type="radio"/> Off Use DKIM Verification Profile: DEFAULT ▾
SPF/SIDF Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off Conformance Level: SIDF Compatible ▾ Downgrade PRA verification result if "resent-sender:" or "resent-from:" were used: <input type="radio"/> No <input checked="" type="radio"/> Yes HELO Test: <input type="radio"/> Off <input checked="" type="radio"/> On
	Use DMARC Verification Profile: DEFAULT ▾ DMARC Feedback Reports: ⓘ <input type="checkbox"/> Send aggregate feedback reports <small>* DMARC reporting message must be DMARC compliant. * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies > Destination Controls.</small>
	Bounce Verification: Consider Unlagged Bounces to be Valid: <input checked="" type="radio"/> Yes <input type="radio"/> No <small>(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)</small>

Opmerkingen: Wanneer u de inkomende e-mail niet aanpast, kan de ESA's de geldige Bounce voor berichten laten vallen.

Opmerkingen: Om te controleren of de Bounce Verificatie voor dit domein uitgeschakeld is, kunt u "domeindebug" inschakelen en de logbestanden staren om te controleren.

Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)