

IP-Adressen/Domänen/E-Mail-Adressen aus der ESA-Bounce-Konfiguration entfernen

Inhalt

[Einführung](#)

[IP-Adressen/Domänen/E-Mail-Adressen aus der ESA-Bounce-Konfiguration entfernen](#)

[Ausgehende Mails](#)

[Eingehende E-Mails](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie eingehende und ausgehende E-Mails so konfiguriert werden, dass IP-Adressen, Domänen oder E-Mail-Adressen für die Cisco E-Mail Security Appliance (ESA) nicht berücksichtigt werden.

IP-Adressen/Domänen/E-Mail-Adressen aus der ESA-Bounce-Konfiguration entfernen

Sie können Empfängerdomänen angeben, auf denen die Bounce-Verifizierung deaktiviert werden soll, wenn die ESA für diese Domänen bereitstellt. Sie müssen sowohl ausgehende als auch eingehende E-Mails konfigurieren.

Ausgehende Mails

1. Gehen Sie zu Mail-Policys > Zielsteuerelemente.
2. Wählen Sie "Ziel hinzufügen..".
3. Rufen Sie das neue Ziel "beispiel.com" auf.
4. Legen Sie in den Einstellungen "Bounce-Verifizierung" auf "Nein" fest.
5. Änderungen senden und bestätigen.

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>

Hinweis: Bei ausgehenden E-Mails können Sie nur auf die Zieldomäne und nicht auf eine IP-Adresse oder E-Mail-Adresse verweisen.

Eingehende E-Mails

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 <i>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.</i>
	SMTTP Authentication: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTTP Authentication
	Verify Client Certificate: <input type="checkbox"/>
Domain Key/DMK 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 type="radio"/> Yes
	HELO Test: <input type="radio"/> Off <input checked="" type="radio"/> On
DMARC Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Use DMARC Verification Profile: DEFAULT
	DMARC Feedback Reports: <input checked="" type="checkbox"/> Send aggregate feedback reports <i>* DMARC reporting message must be DMARC compliant.</i> <i>* Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies > Destination Controls.</i>
Bounce Verification:	Consider Unlagged Bounces to be Valid: <input checked="" type="radio"/> Yes <input type="radio"/> No <i>(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)</i>

Hinweise: Wenn Sie Ihre eingehende E-Mail nicht konfigurieren, kann Ihre ESA gültige Bounce-Nachrichten für Nachrichten verwerfen.

Hinweise: Um zu überprüfen, ob die Bounce-Verifizierung für diese Domäne deaktiviert ist, können Sie "Domain Debug-Protokolle" aktivieren und die Protokolle zum Überprüfen zurückstellen.

Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)