

Esenzione di indirizzi IP/domini/indirizzi e-mail dalla configurazione ESA Bounce

Sommario

[Introduzione](#)

[Esenzione di indirizzi IP/domini/indirizzi e-mail dalla configurazione ESA Bounce](#)

[Posta in uscita](#)

[Posta in arrivo](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare la posta in entrata e in uscita in modo da esentare indirizzi IP, domini o indirizzi e-mail per Cisco Email Security Appliance (ESA).

Esenzione di indirizzi IP/domini/indirizzi e-mail dalla configurazione ESA Bounce

È possibile specificare i domini dei destinatari su cui disabilitare la verifica del rimbalzo quando l'ESA recapita a tali domini. Sarà necessario configurare sia la posta in uscita che quella in entrata.

Posta in uscita

1. Andare a Mail Policies > Destination Controls.
2. Selezionare "Add destination..." (Aggiungi destinazione).
3. Chiamare la nuova destinazione "example.com".
4. Nelle impostazioni, impostare "Verifica rimbalzo" su No.
5. Inviare e confermare le modifiche.

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>

Nota: per la posta in uscita, puoi fare riferimento solo al dominio di destinazione e non a un indirizzo IP o a un indirizzo e-mail.

Posta in arrivo

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> <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
DMARC Verification:	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
	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>

Note: Se non riesci a configurare la posta in arrivo, l'ESA potrebbe eliminare i messaggi validi.

Note: per verificare che la verifica dei rimbalzi sia disabilitata per questo dominio, è possibile abilitare i "log di debug del dominio" e impostare la coda dei log da verificare.

Informazioni correlate

- [Cisco Email Security Appliance - Guide per l'utente](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)