Exempt IP Addresses/Domains/Email Addresses from the ESA Bounce Configuration

Contents

Table of Contents

Introduction

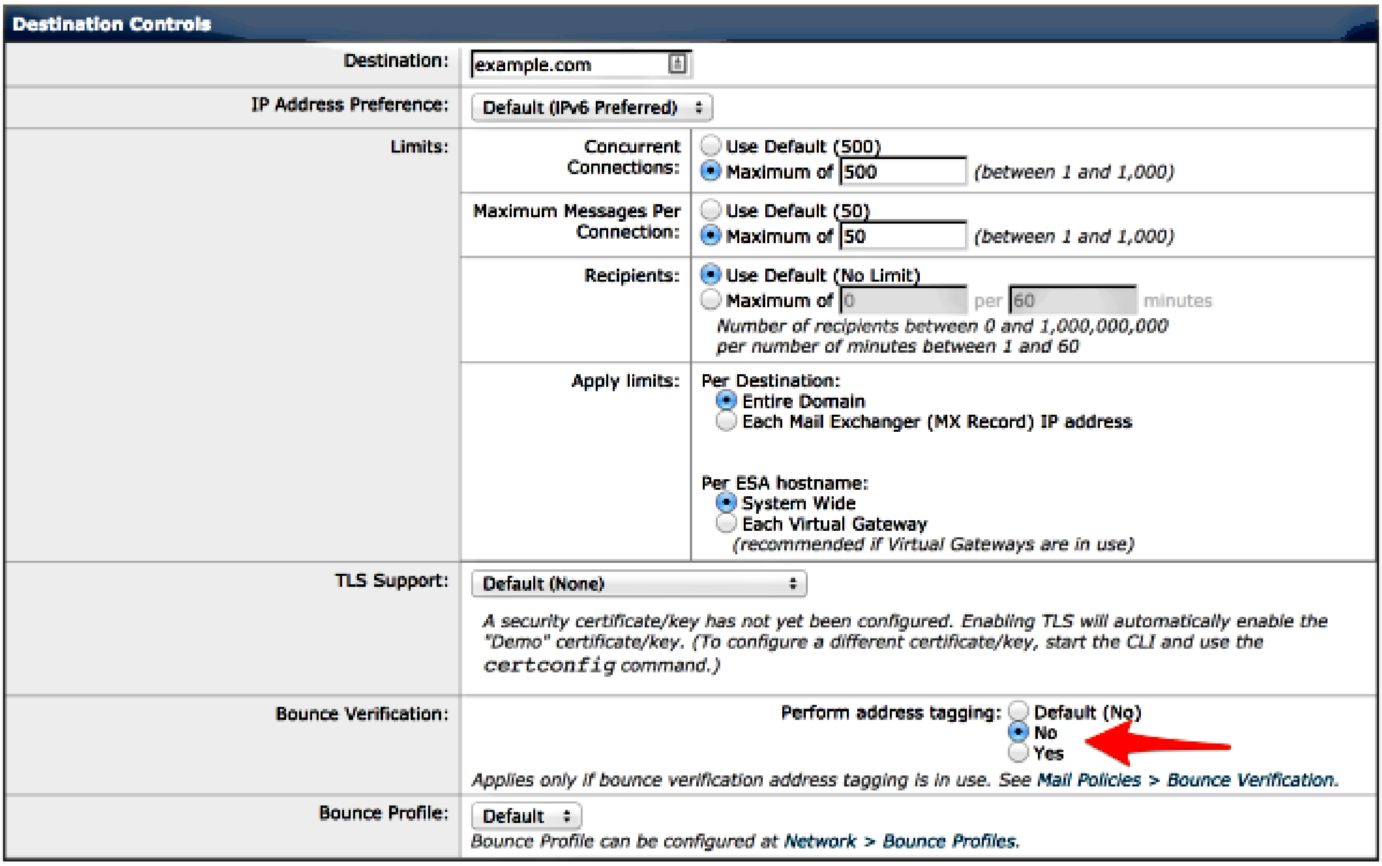
This document describes how to configure inbound and outbound mail to exempt IP addresses, domains, or email addresses for the Cisco Email Security Appliance (ESA).

Exempt IP Addresses/Domains/Email Addresses from the ESA Bounce Configuration

You can specify recipient domains on which to disable Bounce Verification when the ESA delivers to those domains. You will need to configure both outbound and inbound mail.

Outbound Mail

1. Go to Mail Policies > Destination Controls.
2. Select "Add destination...".
3. Call the new destination "example.com".
4. In the settings, set "Bounce Verification" to No.
5. Submit and Commit changes.



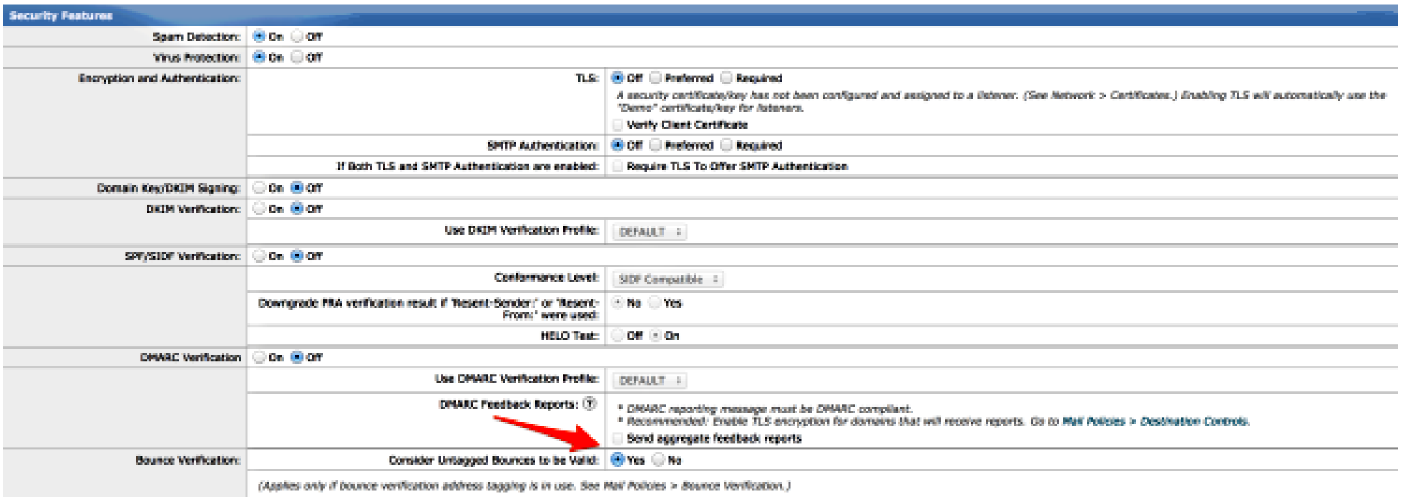
Destination Controls

Destination:		example.com
IP Address Preference:		Default (IPv6 Preferred)
Limits:	Concurrent Connections:	○ Use Default (500) ● Maximum of 500 (between 1 and 1,000)
	Maximum Messages Per Connection:	○ Use Default (50) ● Maximum of 50 (between 1 and 1,000)
	Recipients:	● Use Default (No Limit) ○ Maximum of 0 per 60 minutes Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60
	Apply limits:	Per Destination: ● Entire Domain ○ Each Mail Exchanger (MX Record) IP address Per ESA hostname: ● System Wide ○ Each Virtual Gateway (recommended if Virtual Gateways are in use)
TLS Support:		Default (None) 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.)
Bounce Verification:		Perform address tagging: ○ Default (No) ● No ○ Yes Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.
Bounce Profile:		Default Bounce Profile can be configured at Network > Bounce Profiles.

Note: For outbound mail, you can only refer to the destination domain and not an IP address or email address.

Inbound Mail

1. From **Mail Policies > Mail Flow Policies**, use an exisiting Mail Flow Policy or create a new Mail Flow Policy, and set the Bounce Verification/"Consider Untagged Bounces to be valid" to Yes.
2. From **Mail Policies > Hat Overview**, add the domain to a Sender Group that uses the modified or created Mail Flow Policy.



Security Features

Spam Detection:		● On ○ Off
Virus Protection:		● On ○ Off
Encryption and Authentication:	TLS:	● Off ○ Preferred ○ Required 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. □ Verify Client Certificate
	SMTP Authentication:	● Off ○ Preferred ○ Required
	If Both TLS and SMTP Authentication are enabled:	□ Require TLS To Offer SMTP Authentication
Domain Key/DKIM Signing:		○ On ● Off
DKIM Verification:		○ On ● Off
	Use DKIM Verification Profile:	DEFAULT
SPF/SIDF Verification:		○ On ● Off
	Conformance Level:	SIDF Compatible
	Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:	● No ○ Yes
	HELO Test:	○ Off ● On
DMARC Verification		○ On ● Off
	Use DMARC Verification Profile:	DEFAULT
	DMARC Feedback Reports:	* DMARC reporting message must be DMARC compliant. * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies > Destination Controls. □ Send aggregate feedback reports
Bounce Verification:	Consider Untagged Bounces to be Valid:	● Yes ○ No
		(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)

Notes: Failure to configure your inbound mail may cause your ESA to drop valid bounce messages for messages.

✎ **Notes**: To verify that Bounce Verification is disabled for this domain, you can enable "domain debug logs" and tail the logs to verify.

Related Information

- **Cisco Email Security Appliance - End-User Guides**
- **Technical Support & Documentation - Cisco Systems**