Test Destination Controls in ESA Using Email Bombing

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Problem

Solution

- Python Script for Email Bombing
- Script Breakdown

Testing Destination Controls

Related Information

Introduction

This document describes the process of testing destination controls in the ESA appliance using Email Bombing.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Email Appliance
- Python Programming language

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Email Appliance
- Python 3.X

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Destination controls on the ESA appliance regulate email delivery to prevent overwhelming recipient domains. The ESA allows defining the number of connections the appliance can open and the number of messages sent to each destination domain. The destination controls table provides settings for connection and message rates when delivering emails to remote destinations, and also includes options for enforcing the use of TLS.

Further details on destination controls can be found here: Best Practice Guide for Bounce Verification and Destination Controls.

A mail bomb is a type of denial-of-service (DoS) attack designed to overwhelm an inbox or inhibit a server by sending a massive number of emails to a specific recipient. This method aims to either fill up disk space or overload the server, causing disruptions.

Problem

Testing the effectiveness of destination controls in preventing email flooding is crucial. Without proper configuration, excessive email delivery attempts can overwhelm the server, leading to performance degradation or service disruption.

Solution

A Python script can be used to simulate an email bomb and test the effectiveness of destination controls on the ESA appliance.

Python Script for Email Bombing

```
import smtplib subject = 'EMAIL BOMBER' body = 'I am bombing you!' message = f'Subject: {subject}\n\n{body}' server =
smtplib.SMTP("XXX.XXX.XXX.XXX", 25) i = 1 while i < 100: server.sendmail("SENDER_ADDR", "RECIPIENT_ADDR", message) i += 1
server.quit()
```

Note: You can substitute these sections of the code with your required information:

- XXX.XXX.XXX.XXX - IP address of your ESA.
- SENDER_ADDR - Sender Address
- RECIPIENT_ADDR - Recipient Address

Script Breakdown

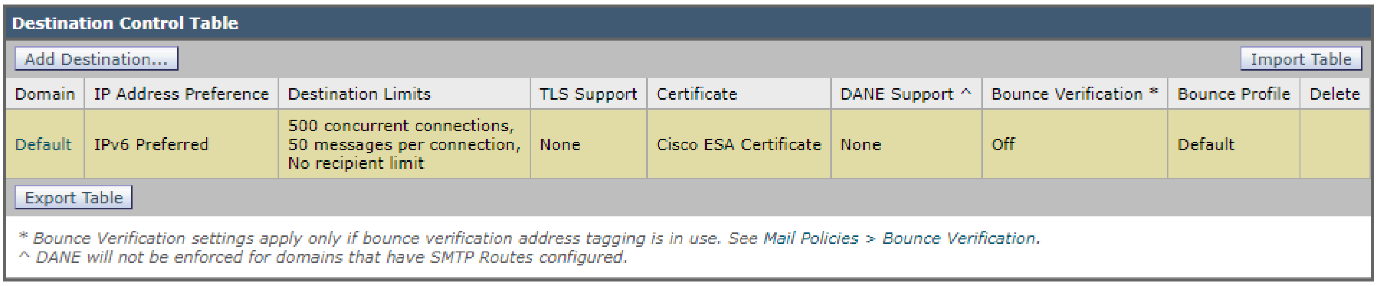
- The smtplib library is imported to send emails using the SMTP protocol.
- Subject and body define the email content.
- The server variable stores the SMTP server details, with the CES appliance IP and port 25 for connection.
- The while loop sends 99 emails using the provided sender and recipient email addresses.
- The **server.quit()** function terminates the connection to the SMTP server.

Testing Destination Controls

1. Open the GUI of the CES/ESA appliance and navigate to **Mail Policies -> Destination Controls**.

2. Click on **Default** settings.

Destination Controls



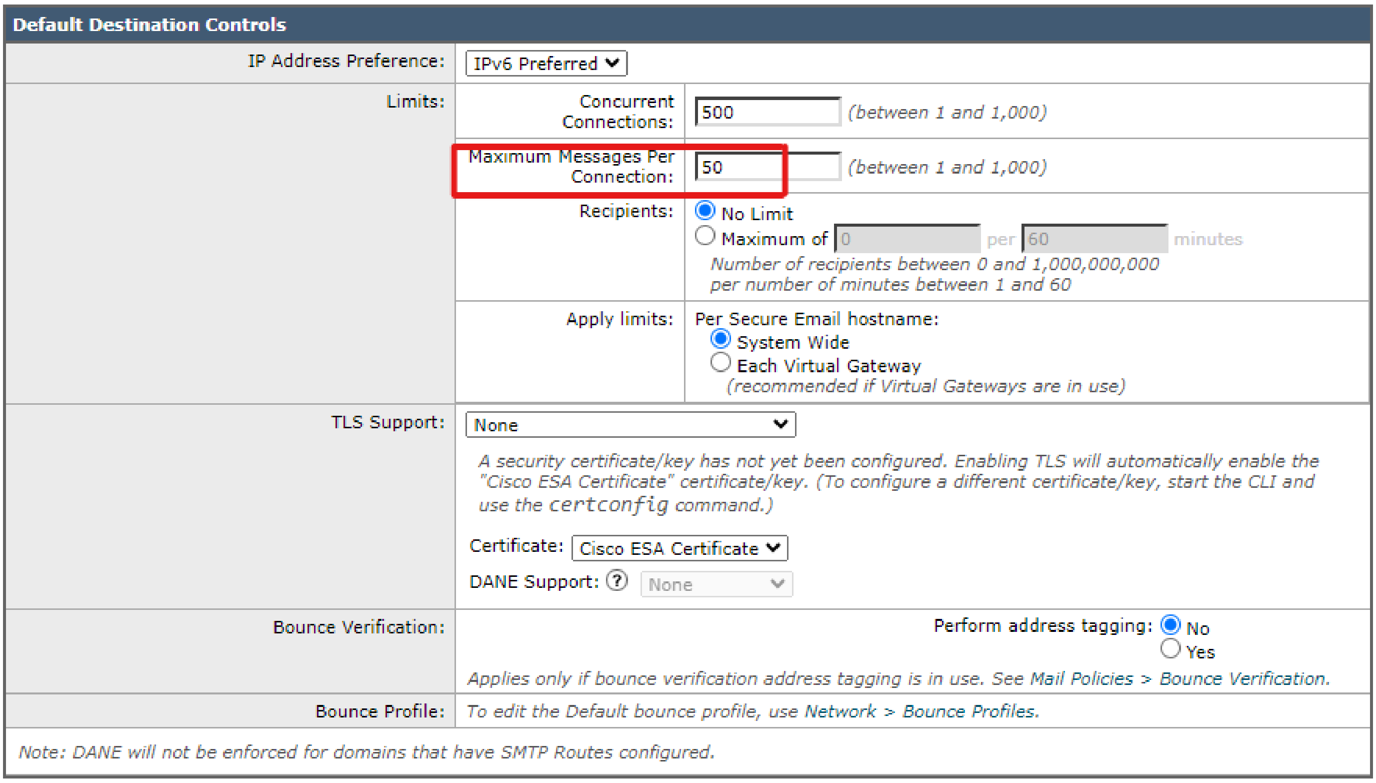
Destination Control Table

Domain	IP Address Preference	Destination Limits	TLS Support	Certificate	DANE Support ^	Bounce Verification *	Bounce Profile	Delete
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	Cisco ESA Certificate	None	Off	Default	

** Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

Destination Controls Table

3. Check the **Maximum Messages Per Connection** value.



Default Destination Controls

IP Address Preference: IPv6 Preferred

Limits:
- Concurrent Connections: 500 *(between 1 and 1,000)*
- Maximum Messages Per Connection: 50 *(between 1 and 1,000)*
- Recipients: ● 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 Secure Email hostname: ● System Wide ○ Each Virtual Gateway *(recommended if Virtual Gateways are in use)*

TLS Support: None

A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Cisco ESA Certificate" certificate/key. (To configure a different certificate/key, start the CLI and use the `certconfig` command.)

Certificate: Cisco ESA Certificate

DANE Support: ? None

Bounce Verification: Perform address tagging: ● No ○ Yes

Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

Bounce Profile: *To edit the Default bounce profile, use Network > Bounce Profiles.*

Note: DANE will not be enforced for domains that have SMTP Routes configured.

Edit Default Destination Controls

4. Ensure this value is lower than the number of emails set in the script. For instance, if the script is configured to send 100 emails and the appliance allows only 50 messages per connection, excessive connections are blocked.

5. Execute the script and observe the results in **Message Tracking**.

6. If more than 50 connections are attempted, the system blocks excessive emails and logs the attempt as too many connections.

7. Modify the script to send fewer than 50 emails and verify that all emails are successfully delivered.

Tip: For controlled testing, set the email bombing value to fewer than 10 emails. Even 50 emails can be considered a form of email bombing. Adjust the script as needed to test different thresholds without causing unintended disruptions.

Related Information

- Cisco ESA Destination Control Guide
- Cisco Technical Support & Downloads