Layer-4 SMTP Traffic to a Mail Server

Goal: Create un-authenticated, un-encrypted SMTP traffic to an email server.

This is a basic email traffic testing scenario. We start with an easy-to-construct scenario for a mail server (no user authentication or TLS configured). This testing scenario works when

- 1. the mail server accepts emails from a local network (E.G. 192.168.0.0/16)
- 2. or the email server allows incoming mail to its own domain.

The following scenario was tested against two postfix servers:

- LANforge sending to an email relay in an office firewall to a public email server. The public server permits the IP of the office firewall and all email addressed to example.com.
- LANforge sending emails directly to the example.com mail server, skipping the office gateway.

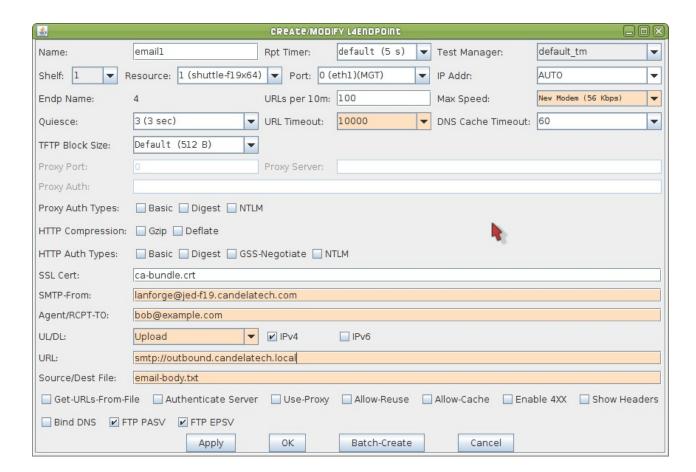


CAVEATS: This cookbook does not cover authenticated SMTP connections (E.G.: Postfix and SASL) or SSL/TLS certificates (E.G.: Postfix and TLS).



 Create a text file /home/lanforge/email-body.txt. We will send it as an email. We will use a minimum of RFC 822 specified fields: To, From and Subject

2. In the LANforge *Layer-4* tab, click **Create** and enter fields we will use to find the email body and where we will send it.



- A. Set the Name to email1
- B. Set SMTP-FROM to lanforge@jed-f19.candelatech.com
- C. The RCPT-TO address to bob@example.com
- D. For *UL/DL*, choose **Upload**
- E. Our mail relay is at outbound.candelatech.local. Enter the URL smtp://outbound.candelatech.local
- F. Set *Source/Dest* to email-body.txt. Double check that files actually exists at /home/lanforge/email-body.txt

For more information see GUI User Guide: Layer-4

- 3. To monitor your mail relay, open up a terminal, ssh to the relay and tail the mail-log. You will probably use the command sudo tail -f /var/log/maillog
- 4. In the Layer-4 tab, select connection email1 and click Start.