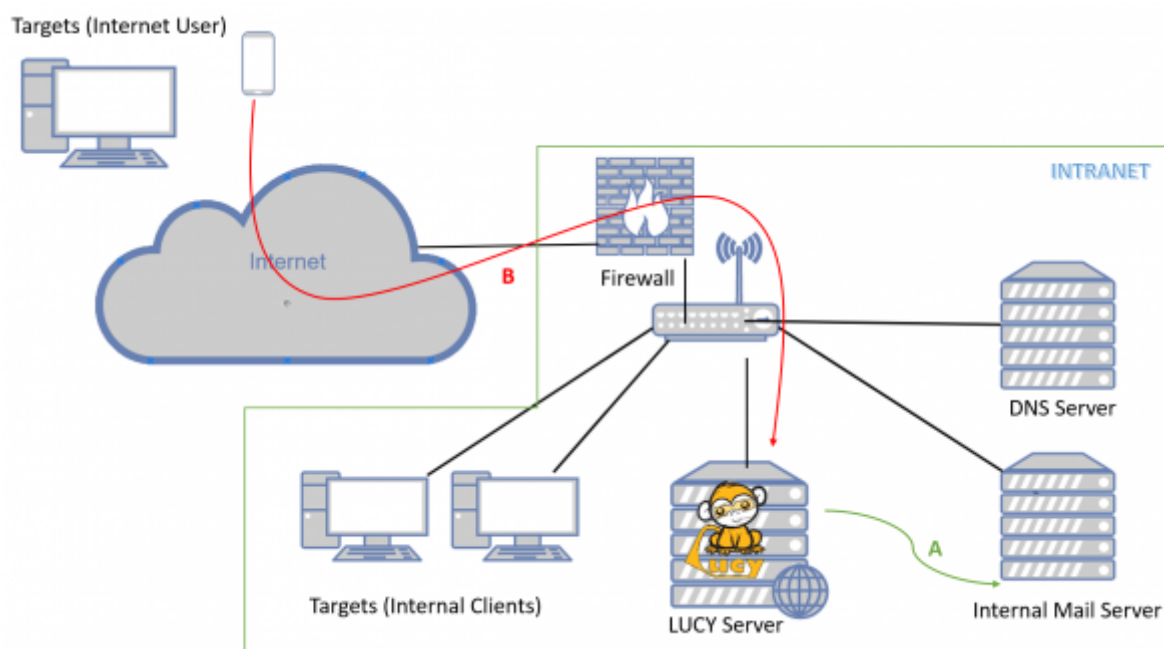# Introduction

If you setup LUCY within your own infrastructure you don't want users from the internet to access the phishing simulation directly within your intranet. If the server gets compromised, the attacker would have an entry point to the internal network:

A secure design requires that the web service which is accessible from the internet (untrusted network) can be segregated from the internal network (trusted network) and moved to a DMZ. If you do so, please keep in mind that LUCY has different communication channels that depend on the specific use:
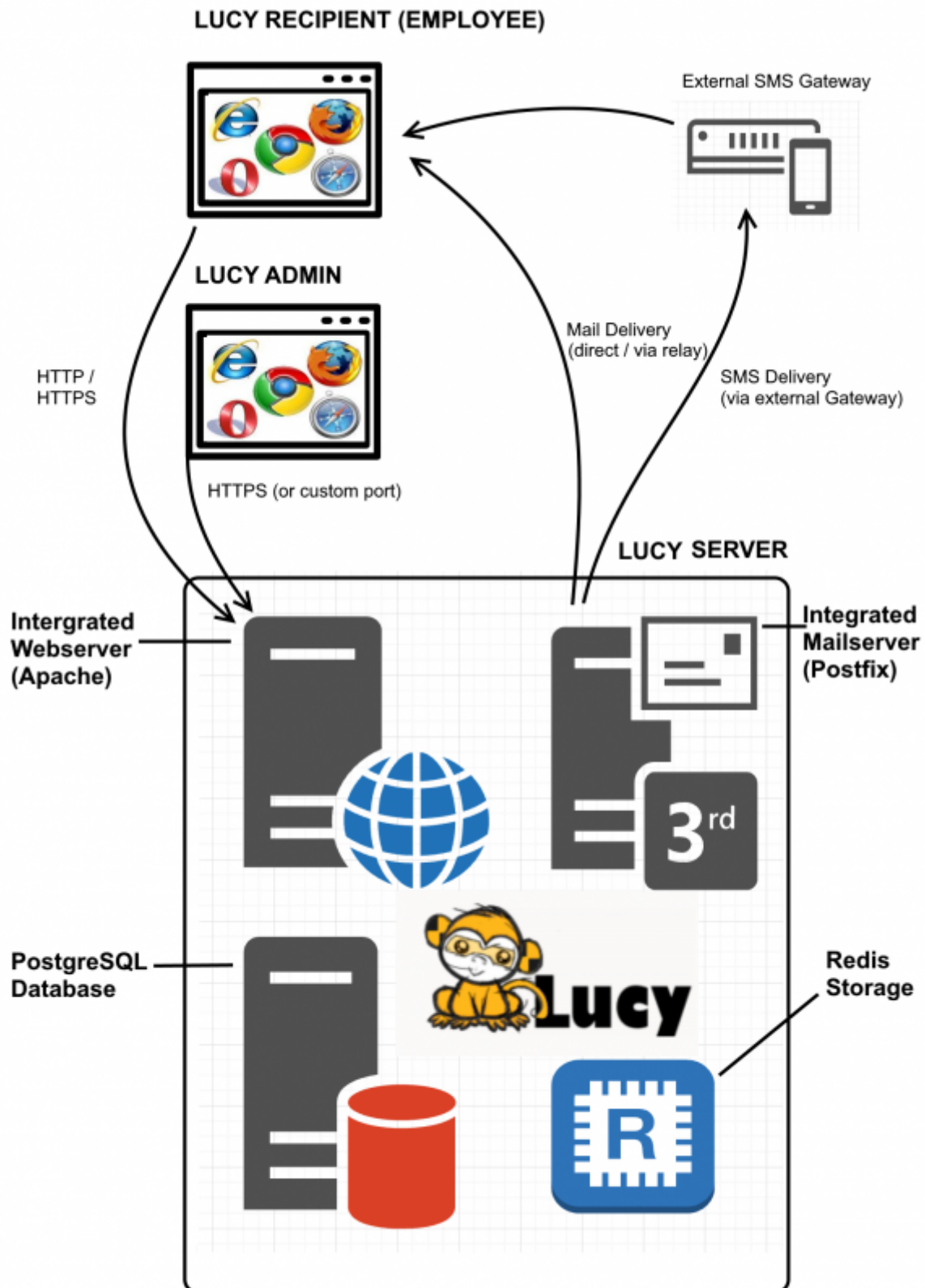
What is a master/slave?

LUCY's master/slave configuration enables the administrator to create such segregation by
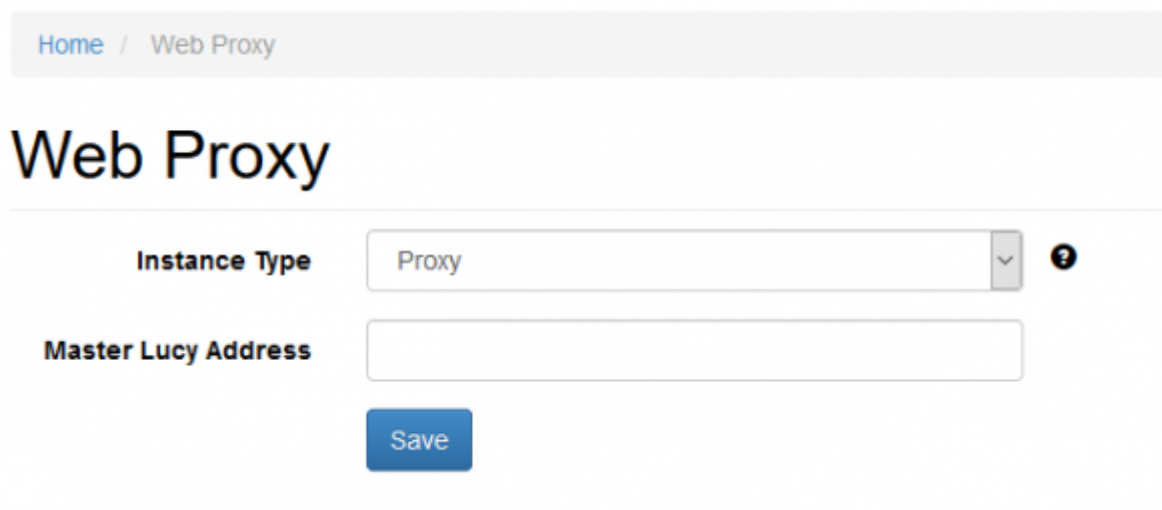
associating a "slave" role to a LUCY instance.

- **Master/Slave**: When a proxy mode is enabled, Lucy acts as a reverse proxy and pushes all HTTP/S requests to the "master" address, without analyzing the traffic in any way, except the /admin part. You can still access the proxy's admin panel when the proxy is enabled, all other (scenario/static) URLs get forwarded to master. The master is a regular Lucy instance, it just allows proxified requests. So you configure all campaigns on the master, send emails from the master and do nothing on proxy except enabling proxy mode. The master will push all running campaigns to the slave (SSL, virtual hosts, configuration, etc) and get statistics from the slave automatically. When the campaign is stopped, all data is removed from the slave.

- **Reflective Master/Slave**: All campaigns & recipients are configured on Master, when launched, the Master pushes everything to the Slave, and pulls the stats from the Slave to the Master. "Victims (end users)" access only the Slave. Only running campaigns are published on the Slave, then when a campaign is stopped, it gets wiped from the Slave and stored only on the Master. All mails in such a reflective mode are sent from the slave!

Please note: There is a caveat with HTTPS - if you generate SSL on master, you have to put it to proxy by hands, as the proxy doesn't automatically interact with master in any way and doesn't exchange information with it.

Configuration

The Master/Slave can be configured admin/settings/proxy. If you run LUCY as an external proxy within the DMZ (facing the internet) then you need to choose "the instance type "proxy" and define LUCY's master IP address:

Please contact our support for further help on this topic (support@lucysecurity.com).

Ports and Updates

Both master-slave approaches (reverse proxy and DMZ-based) use only HTTPS port (443). A "recipient" is an end user. For a **proxy**, the firewall configuration would be:

- master should allow connections from slave to port 443
- master should allow connections from slave to port 25 (if the SMTP method selected for the incidents reporting)
- master should allow connections from Lucy admin computers to port 443
- slave should allow connections from "recipients" to ports 443, 80
- master must be able to send emails via port 25

For "**reflective scheme**", the firewall should be configured as follows:

- slave should allow connections from "recipients" to ports 443, 80
- slave should allow connections from master to port 443
- master should allow connections from Lucy admin computers to port 443
- slave must be able to send emails via port 25

Updates: both workstations are updated separately and should have access to Lucy Update/License Server.

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=setting_up_a_lucy_master_slave&rev=1572244752

Last update: **2019/10/28 07:39**