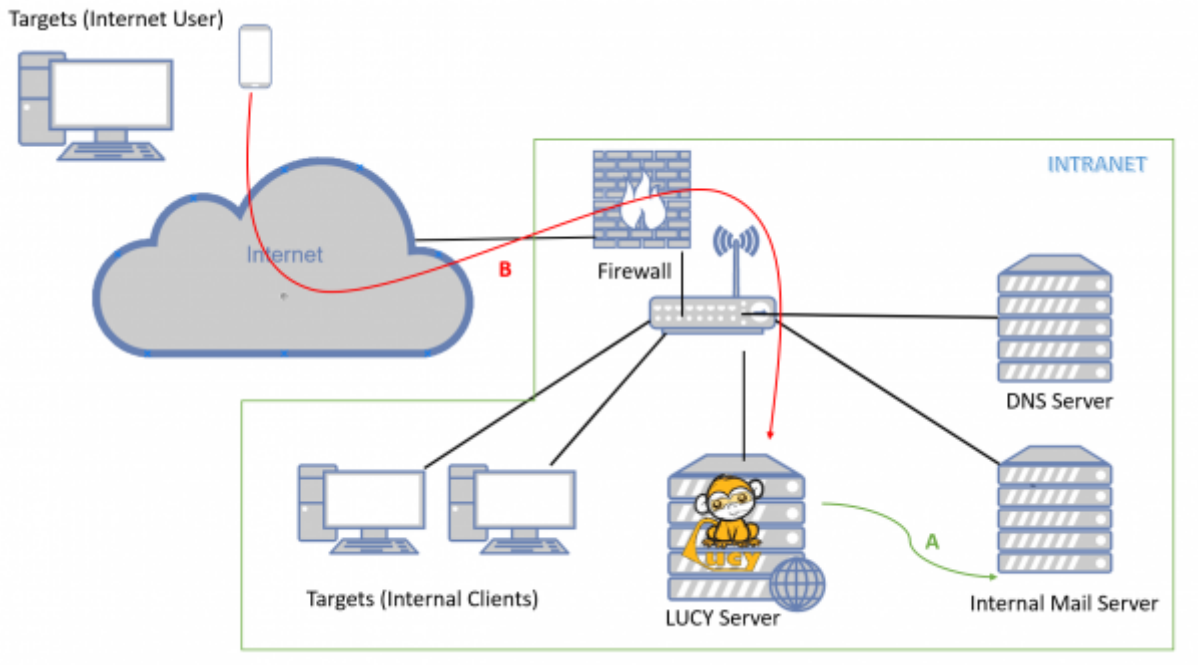
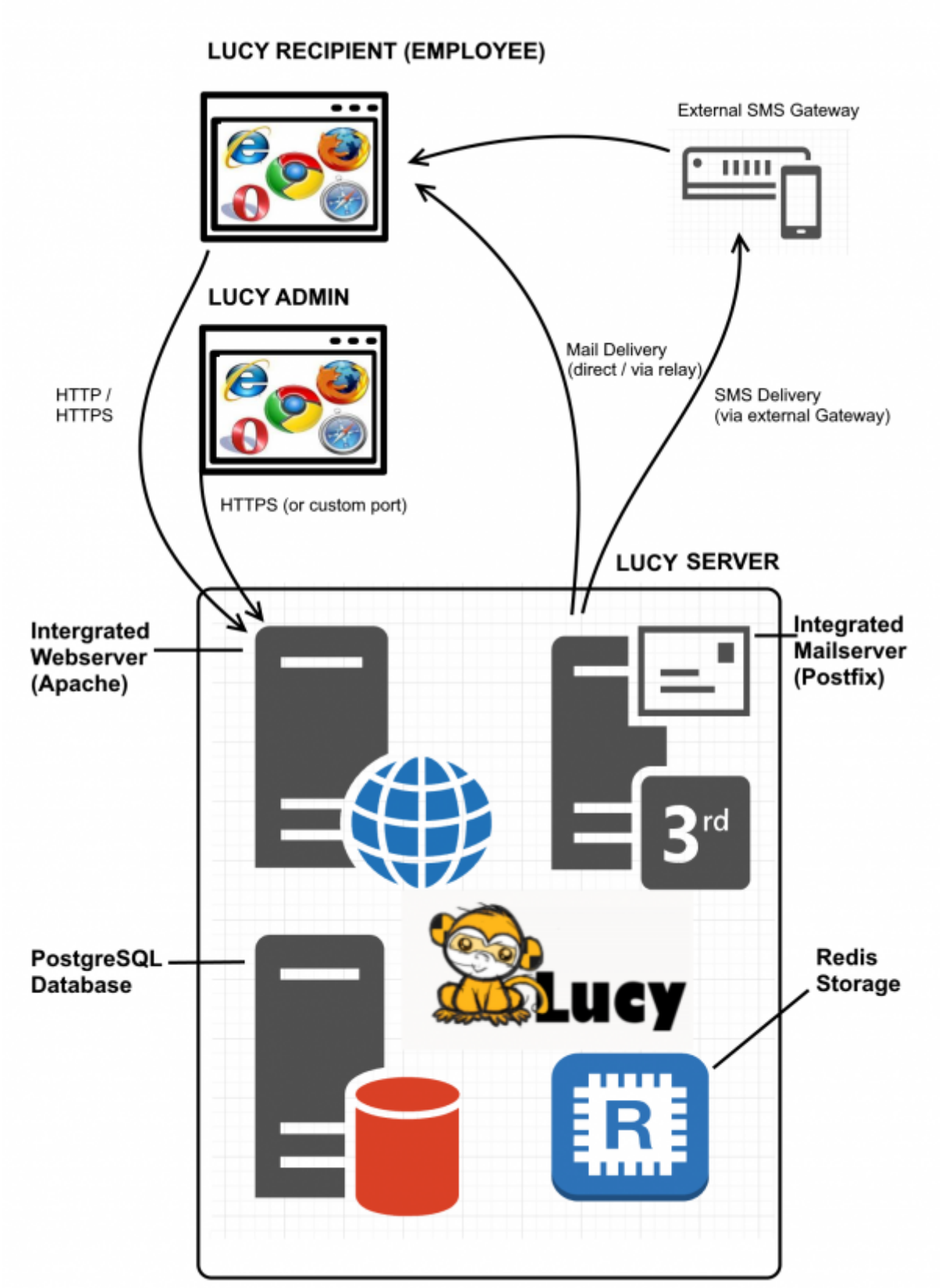
Introduction

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:



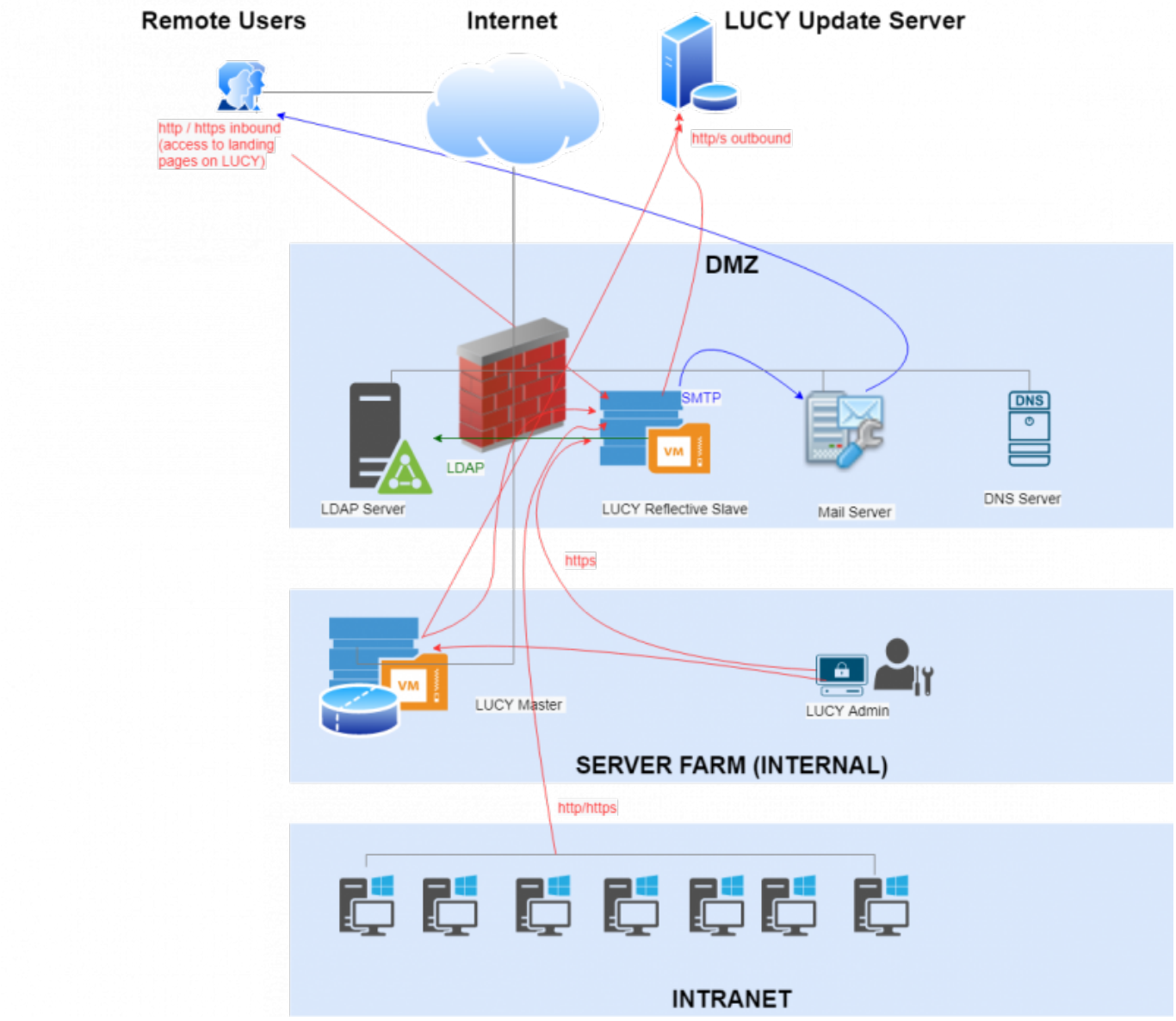
A secure design requires that the web service which is accessible from the internet (untrusted network) can be segregated from the internal network (trusted network) and moved to a DMZ. If you do so, please keep in mind that LUCY has different communication channels that depend on the specific use:



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.

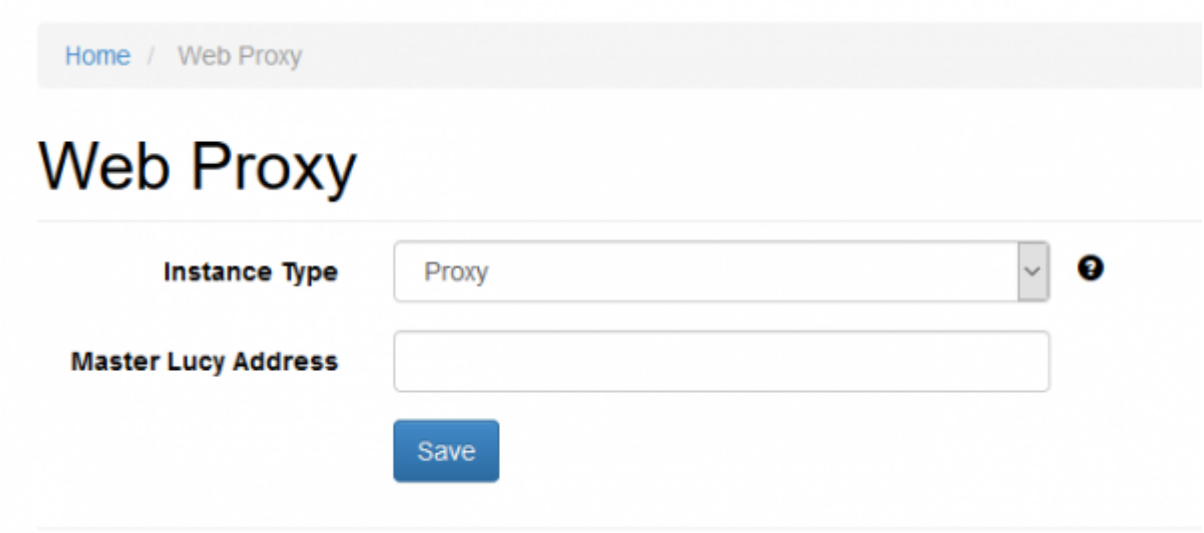
- **Master/Slave**: When a proxy mode is enabled, Lucy acts as a reverse proxy and pushes all HTTP/S requests to the "master" address, without analyzing the traffic in any way, except the /admin part. You can still access the proxy's admin panel when the proxy is enabled, all other (scenario/static) 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 system domain name:



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.

Integration with other services Master and Slave

- End-User portal and all end-users must be configured on the Master since Lucy in Proxy mode forwards all traffic (except Admin console page /admin) to Master.
- SSO Settings and LDAP Settings must be applied to the Master server.
- Mail Server is running on the Master server. In the Proxy mode, SMTP traffic is intercepted by the Slave server and forwarded to the Master server. That means that your domain name used in the sender email address must have an MX record pointed to the Slave server.
- Incident Plugin Settings is configured on the Master and Slave server in the same way. The slave server forwards (SMTP & HTTP) traffic directly to the Master. Incidents are not saved on the Slave server.

Integration with other services Reflective Master and Slave

- End-User portal and all end users must be configured on the Slave server. In case of the option "Do not send emails" you must import all end users to the Slave server manually. But note that the statistics in the End User portal for each recipient will be available while the campaign is running. Once you stop the campaign, the statistics will be stored on the Master server only.
- Only running campaigns are available on the End User portal. To allow users to see their progress and entire statistics you may give access to the End User portal on the Master server.
- In case of "Direct Login" and\or "SSO for Awareness" options, the SSO Settings and LDAP Settings must be also configured on the Slave server. To access the End User portal for the LDAP-based users on the Slave server you must configure LDAP Settings there. To access Admin Console for LDAP-based and SSO users on the Slave server you must configure LDAP Settings and SSO Settings accordingly.
- Mail Server is running on the Slave server. SMTP traffic is intercepted by the Slave server only, later the statistics are synchronized with the Master.
- SMTP Settings must be the same on both, Master and Slave server.
- Incident Plugin Settings are configured on the Slave server. Incidents are saved on both the Master and Slave server. Slave synchronize each incident with Master.

Master and Slave common information

- Custom admin Port and IP should not limit the communication between the two servers.
- Adapt should be configured on Master.
- LUCY Admin users (including End Users) are not replicated between the Master and Slave server.
- If the option "Do not send emails" is enabled for awareness, the end-users will be created automatically on the Slave server when sending an email. Otherwise, all end-users should be imported first on the Slave server.

Master and Slave domain info

The following is applicable for both type of Web Proxy configuration (Master \ Proxy configuration and Reflection Master \ Reflection Slave configuration):

- SMTP hostname (Mail Settings) must point to the Slave server
- All domain names used for landing page and sender email must point to the Slave server.
- Master server may have (or may not have) their own domain name for the Admin Console.
- Slave server (in case of use of the End User portal) should have a domain name for the Admin Console that point to that server.

Troubleshooting

Please contact support in case if you have any questions.

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

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

Last update: **2020/09/21 08:55**