Introduction

Lucy can be installed on premise or in the internet.

Reasons for installing on an external server in the internet are:

- **Public IP address outside your network range**: Prevents your infrastructure from being blacklisted.
- **Direct access**: The server will not be blocked by any security products already in place within your own infrastructure.
- **Less possible conflicts with integration**: A LUCY server placed directly in the internet will be setup very fast as it does not require a complex integration process with your mail, DNS and firewall infrastructure
- **Smaller attack surface**: As the LUCY server requires a web based access for end users from the internet (e.g. accessing their mails from mobile devices), you might need to punch a hole in your firewall and allow inbound access to a LUCY server. If you place LUCY in the intranet (see this chapter), your might violate your zone concept.

Reasons for installing LUCY on premises are:

- **Legal**: Some laws might not allow you to store sensitive data on an external server outside your network or outside your country. Especially with the new data protection law in Europe (GDPR) you need to make sure any personalized or sensitive data is secured.
- **Integration with certain features**: LUCY comes with different API's such as the LDAP API, the REST API etc. which are common for backend applications that are usually not exposed to the internet.
- **Security**: LUCY might store sensitive data like windows login, user names, emails etc. within the database. Integrating the LUCY server in the internal protection layers (IDS, FW etc.) will minimize the risks of successful attacks.

On premise installation

Download: If you have decided to do an on premise installation you will first need to download LUCY from our webpage. Please choose one of our installers or images:

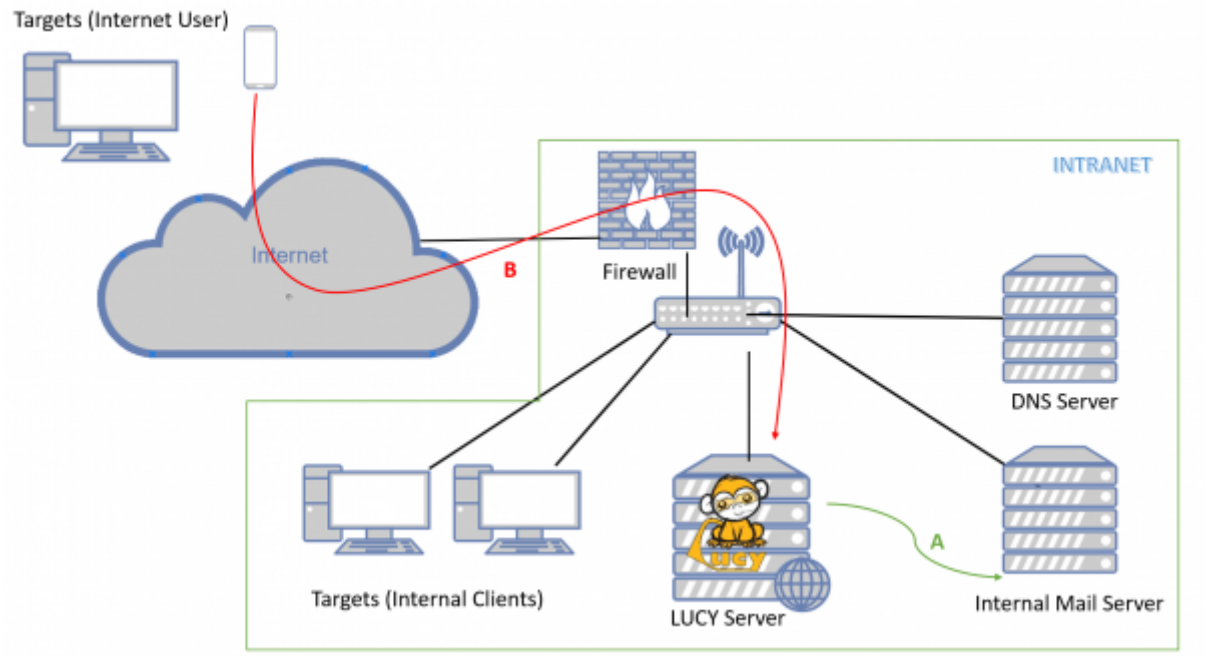
- **Virtual Box**: http://download.phishing-server.com/dl/lucy-latest/virtualbox.zip
- **Linux Installer**: http://download.phishing-server.com/dl/lucy-latest/install.sh
- **ESX/ESXi**: http://download.phishing-server.com/dl/lucy-latest/esxi.ova
- **Vmware Image**: http://download.phishing-server.com/dl/lucy-latest/vmware.zip
- **Amazon**: http://www.lucysecurity.com/PS/doc/dokuwiki/doku.php?id=installing_lucy_in_amazon

If you require a different format (e.g. ovf), search for the according converter (e.g. search for "convert ova to ovf"). All downloads are automatically treated as a community edition.

License: For testing purposes please send us the workstation ID (http://www.lucysecurity.com/PS/doc/dokuwiki/doku.php?id=how_to_activate_lucy&s[]=#where_to_find_the_workstation_id). This will allows us to issue you a test license. If you want to directly purchase LUCY please consult this article.

Where to place LUCY in an onsite installation? You can place LUCY in the intranet or within a secured zone (DMZ). If you setup LUCY within the intranet you will have to consider the following challenges:

- Mail integration: LUCY has different mail delivery methods. See this chapter. If you use the build in mail server, LUCY would need to be able to resolve the MX record and then deliver the mails to that public accessible server. As a result you probably need to open SMTP communication outbound. An easier method is using the internal mail server as a relay. In such a case LUCY would communicate with the internal mail server (A). You also need to allow relaying for the LUCY IP address on your internal mail server.



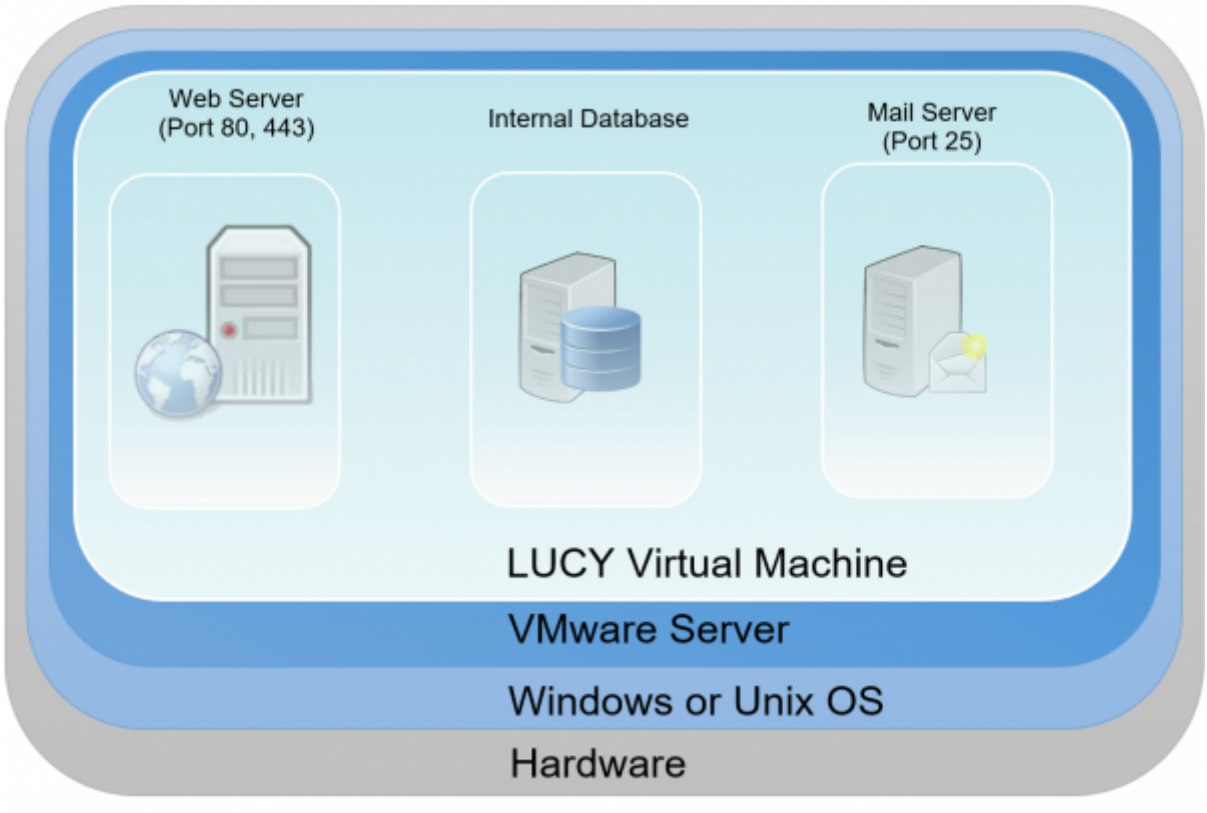
- DNS integration: You can quickly setup new domains in LUCY. Details are described here. Those domains could be used for the landing pages (Phishing or E-learning) or the mail sender. The internal clients will need to resolve those domains. Therefore, you need to create the according DNS entries also on your internal DNS server and point the records to LUCY. If the landing pages need to be access from users in the internet directly (without VPN), you need to make sure that the DNS records are also created on an external accessible DNS server.
- HTTP/HTTPS access: The landing pages and the E-learning needs to be accessible via http or https (see this chapter for SSL configuration). If users from the internet have to access those pages, you need to make sure that you have setup an according port forwarding rule on your firewall together with a NAT entry, that points to LUCY.
- Security products and whitelisting: You need to ensure that the LUCY IP is whitelisted on all your security products (mainly the SPAM filters). Otherwise you might end up blocking legitimate infrastructure elements within your own infrastructure.
- Securing the access: Once you finished the setup, you might want to prevent users from accessing the web based administration. In this chapter we discuss a few tips on how to secure LUCY.

If you setup LUCY in a DMZ, you could as well consider using a LUCY instance only as a reverse proxy

in the secured zone, and install the main application within the intranet as a "master instance". This configuration is described here. Other than that, the challenges in a DMZ installation are the same as the ones described in the intranet installation above.

LUCY Vmware technical components

When you download and boot the VMware Image, all software components are integrated in that image. There is no need to install any additional software. All components (DB, mail server, web server etc,) are bundles within the VMware images and controlled by the internal LUCY software, which runs transparently in the background. The updating of those components is also done within the LUCY software through internal processes, which are not visible to the end user.



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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=network_design_-_where_to_setup_lucy&rev=1527757804

Last update: **2019/07/25 12:51**