ZENECTED
THREAT DEFENSE VPN

ADMINISTRATOR GUIDE

v. 1.2

TABLE OF CONTENTS

PERUN WORKS

OVERVIEW

Zenected is a cloud based security threat protection service. Its delivered through a set of preconfigured services including a L2TP VPN over IPSEC, DNS, IDS and Proxy.
Once a user connects to Zenected, that users network traffic is filtered to keep the bad things out (e.g. phishing sites, malware). The only thing this a user has to configure on the endpoint device (be it a mobile device, a desktop or laptop or IoT device) is connection to your Zenected instance.

All services are updated every hour with a new set of threat indicators prepared by Perun Works.

The following diagram describes a typical ZENECTED setup:

INITIAL SETUP

We've worked hard to keep the initial setup as easy and as minimal as possible. Still there are a few steps you will need to take in order to customize your ZENECTED instance.

1. In order to start, you will need to connect via SSH to your ZENECTED server.
2. Once on the server, please run the following commands:

```
$ sudo apt-get update
$ sudo apt-get upgrade
$ sudo /opt/zenected/zenected_setup.zenx
```

3. This last command will bring up the initial setup screen:
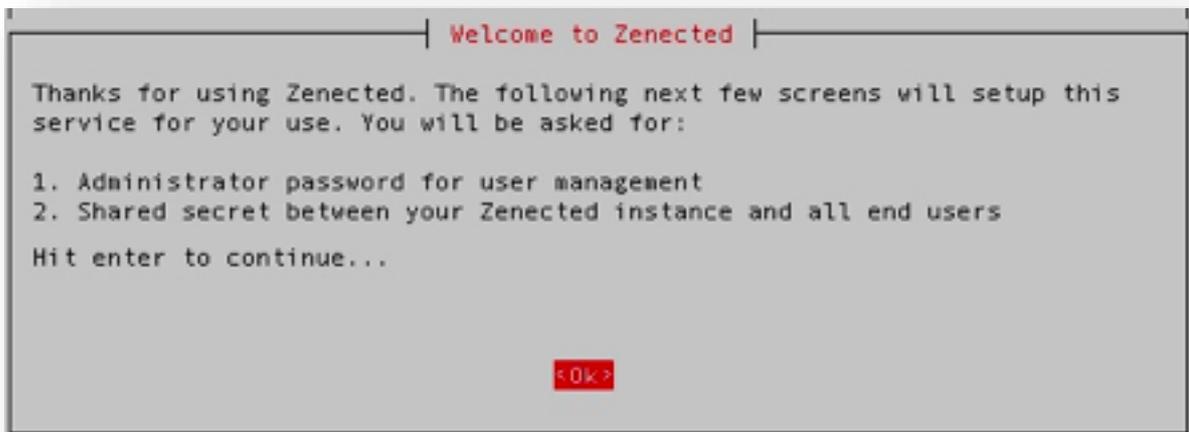
Just hit ENTER to move to the next screen.

4. Administrator password screen – this is where we ask you to enter your preferred administrator password. This password will be used for user management.

5. Shared secret screen – again we ask you to come up with a secret password. This time it will be shared with users of the service as they will need it to configure their devices using this "shared secret". Again, you will be asked twice to enter the same password:
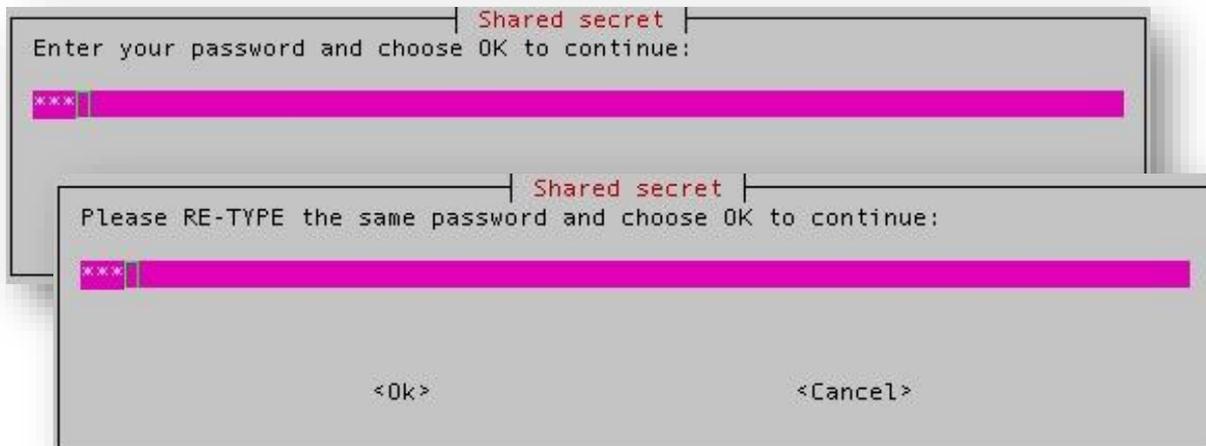
6. Summary screen – the last screen confirms the setup exited and reminds you how to add ZENECTED users:

7. One final command to run on the server is to just say Good Bye by typing:
   `$ exit`

USERS

Once you've completed the INITIAL SETUP you should go ahead and start adding users.

1. This is done by going to:
   `https://IP_address_of_your_instance/users`

2. Your browser will shout that the connection is not secure. This is expected, as the server uses a self-signed certificate.

   Confirm the security exception to move forward:

3. Once you add the exception, you will get to daloRADIUS login screen.

   The default login is "administrator". The password for that account is the one you defined during the INITIAL SETUP STEP 4.

4. Once you successfully log in, select MANAGEMENT from the menu. You should see a screen similar to this:

   Here you will be able to easily manage your ZENECTED instance users.

ADMIN PANEL

Oh yes – there is also an Admin Panel. You can use it to create and manage whitelists and and blacklists for domains and URLs.

ADMIN PANEL LOGIN

1. This is done by going to:
   `https://IP_address_of_your_instance/admin`

2. Your browser will shout that the connection is not secure. This is expected, as the server uses a self-signed certificate.

   Confirm the security exception to move forward:

3. After a successful login you will see a screen similar to this:
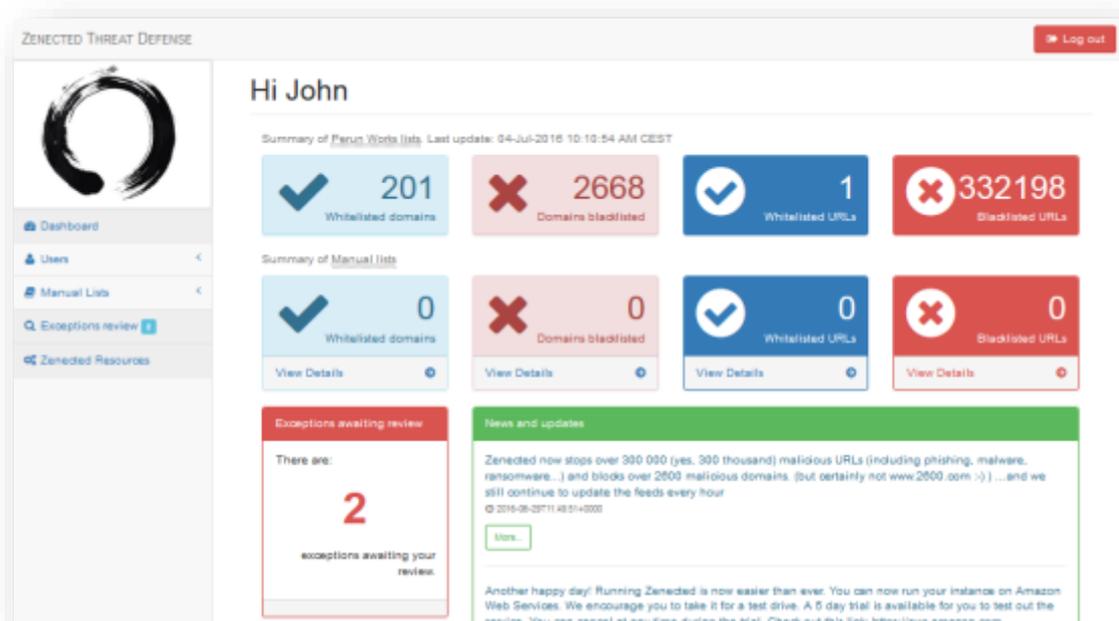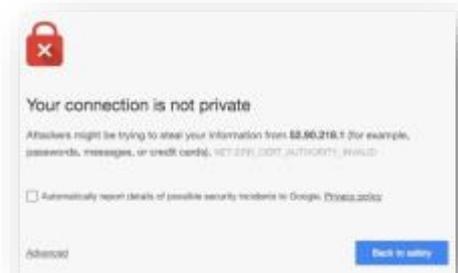

ADMIN PANEL USERS

4. You will see the login screen. Please note that both fields are case sensitive. The initial username is:
   `administrator`
   and the default password is:
   `ZenectedDefault`

5. As your first step, please go to the "Users > Register a new admin user" and create a new admin account for yourself.

PERUN WORKS
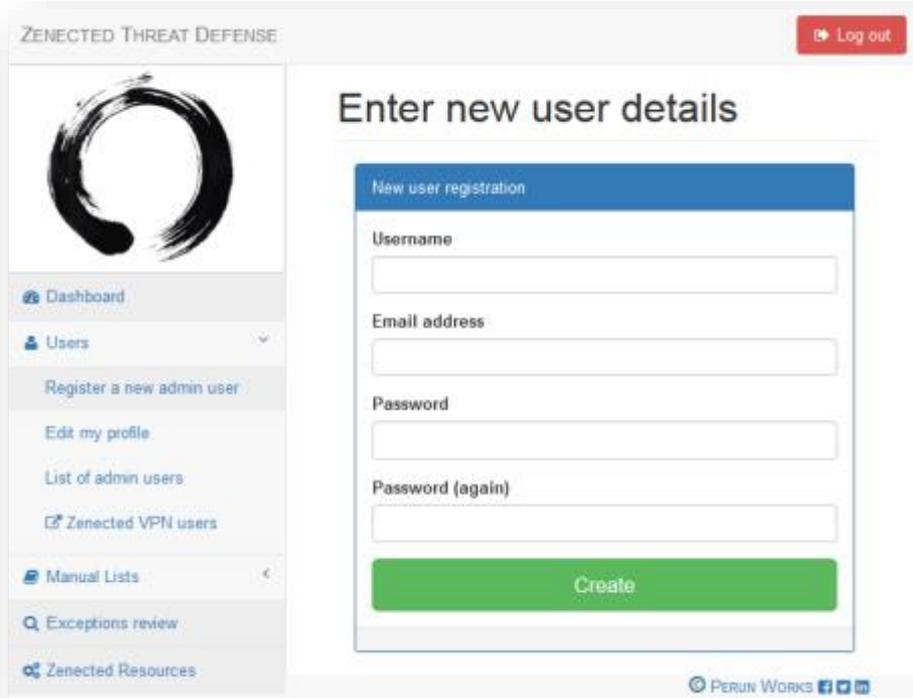
6. Once you complete creation of a new account, log out from the default user account (upper right corner >) and log in back again using your newly created user.

7. Due to security reasons, using the new account go to "Users > List of admin users" and delete the default account by clicking on the **x** in the Delete column:
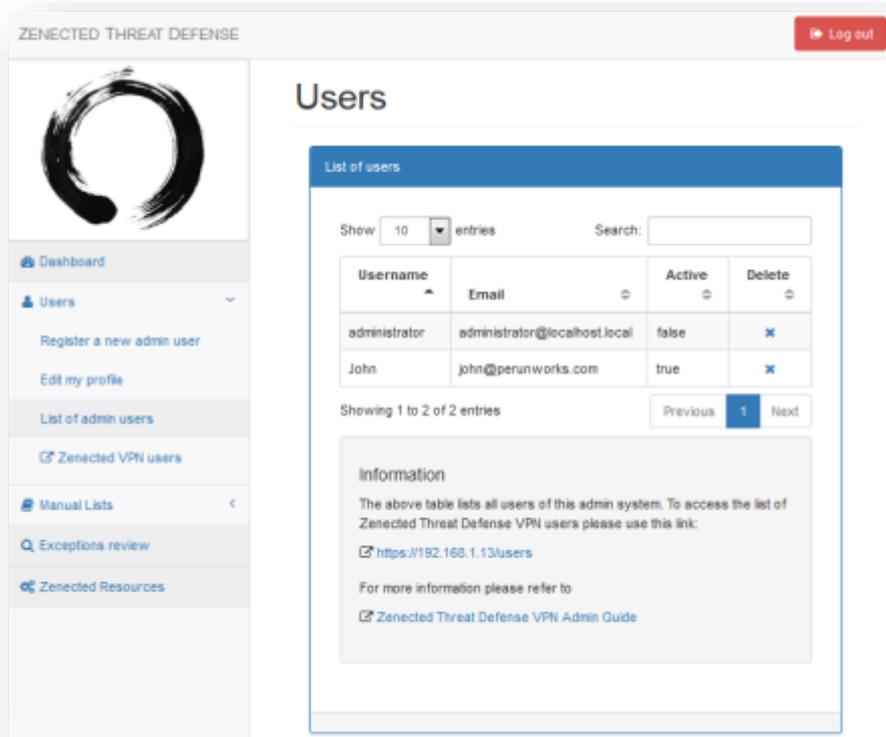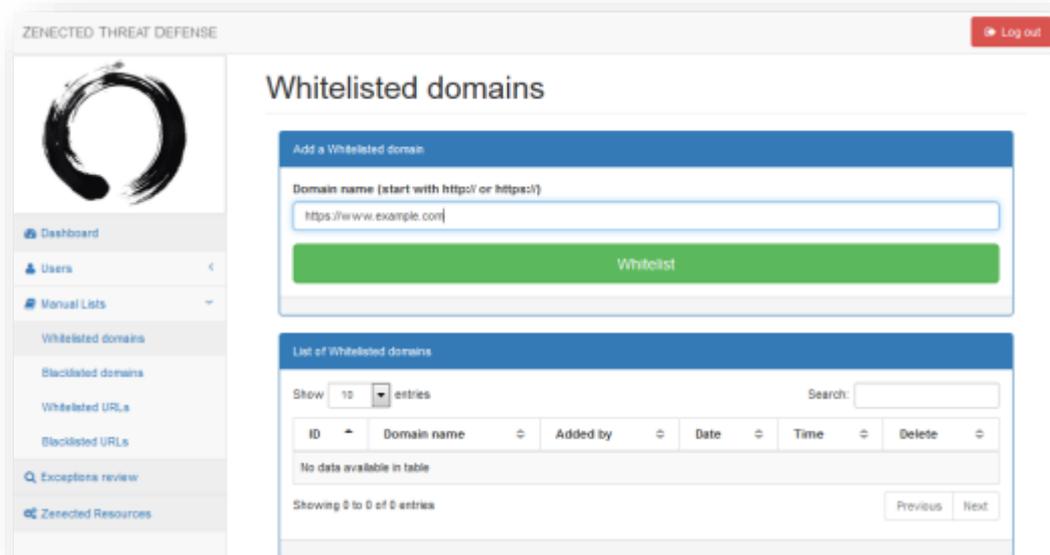
8. If needed, you can also change your new user settings in "Users > Edit my profile":
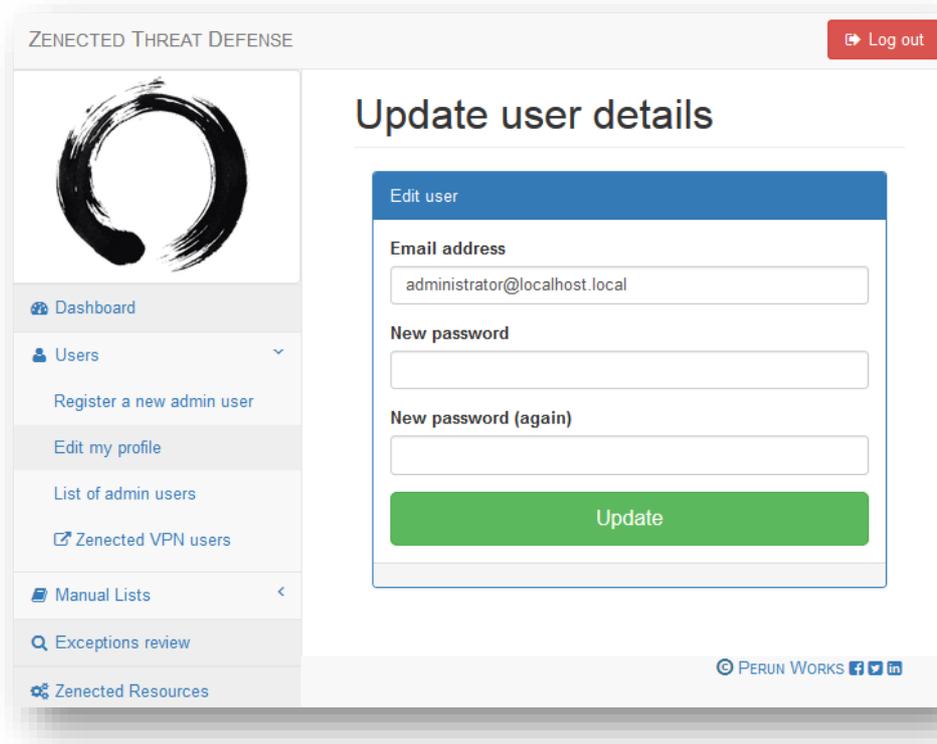
WHITELISTS AND BLACKLISTS OF DOMAINS AND URLS – MANUAL LISTS

9. The use of whitelists and blacklists for domains and URLs is for each of them very similar.
   Using an example of a domain whitelist entry – go to "Manual Lists > Whitelisted domains" you will get this screen:

a) Adding a new domain (URLs) to the list:
   Fill out the form "Add a Whitelisted domain" and press "Whitelist".
   This will add the domain you defined to the whitelist.

b) Deleting an entry (domain, URL) from a list:
This is simply done by pressing the **x** next to the entry name on the list:
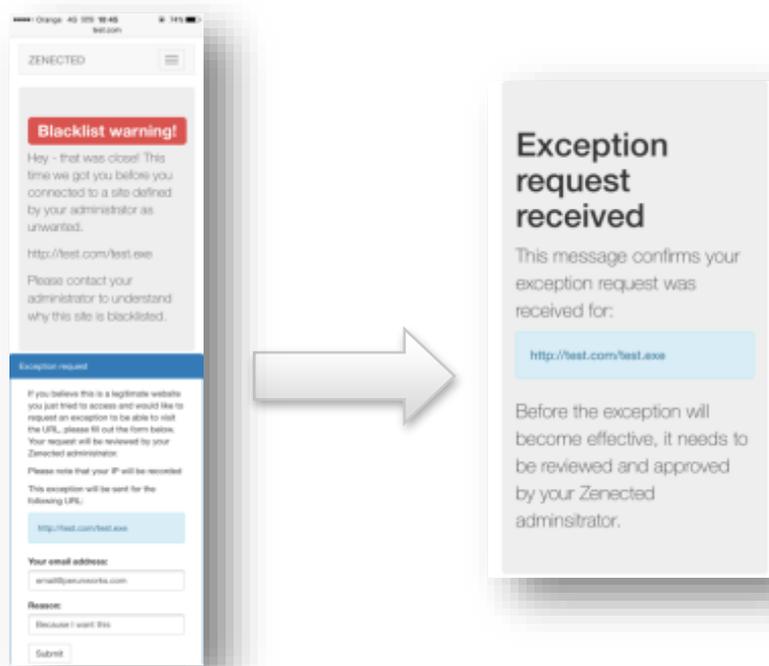

Please note that it will take about a minute for the changes you make to take effect.

EXCEPTIONS

Once an end user hits a page that is blocked by Zenected, they are presented a simple form, which they can fill to request an exception.
The following two screenshots are examples of what a end user would see on a mobile phone:

Exceptions allow Zenected your end users to request a certain resource to be whitelisted.

10. If you are a Zenected Administrator, you can decide on the fate of exceptions in the "Exceptions review" section.

Obviously, there are two possible choices – you can either approve an exception by clicking on the check "✓" or decline it by clicking on "✗".

11. If you approve and then change your mind - any approved exceptions after your approval are added to the URL whitelist, You can delete them from that list ("Manual Lists > Whitelisted URLs"):

CONFIGURATION SETTINGS

In case you want to perform some customization of your ZENECTED instance to better suit your needs, you might need to access relevant databases and other configuration settings. These are kept in:

`/etc/zenected/zenected.conf`

Please note:

- that the details in the file are unique to your instance. If you run multiple instances of ZENECTED, each of them will have different details in the file.
- the details change each time you run the INITIAL SETUP program.

CLIENT SETUP

We've prepared an overview of how the end users can setup their ZENECTED connection on their devices running different operating systems.

If you are a ZENECTED administrator please provide to your end users the following details, which they will need during the setup:

- A username
- A password
- Shared secret (see: INITIAL SETUP, point 5)
- IP or hostname of the ZENECTED instance

Detailed, step-by-step guides are located in the Resources page:
https://zenected.com/resources/

SOFTWARE USED

To keep the costs to a minimum but quality at maximum levels ZENECTED is using a number of great open-source solutions.

Please refer to appropriate web pages for additional information:

1. Ubuntu (http://www.ubuntu.com/)
2. PHP (https://secure.php.net/)
3. MySQL (http://www.mysql.com/)
4. daloRADIUS (http://www.daloradius.com/)
5. Dnsmasq (http://www.thekelleys.org.uk/dnsmasq/doc.html)
6. Squid (http://www.squid-cache.org/)
7. SquidGuard (http://www.squidguard.org/)

ADDITIONAL INFORMATION

ZENECTED is free. If you like it and are using it, please consider becoming part of our team by donating at:
https://www.paypal.me/zenected

For additional information please refer to ZENECTED website at:
https://zenected.com

In case of a support request, please use our Support website at:
https://support.perunworks.com

For more information on services provided by PERUN WORKS please visit us at:
https://www.perunworks.com

PERUN WORKS