FU - The Funneling Unit Documentation

Release 1.0.0

Daniel Waardal

November 14, 2012

CONTENTS

Info Read the documentation hosted at readthedocs.

Author Daniel Waardal

DNSBL checking *SMTP-Proxy*

FU is a simple yet powerful SMTP Proxy that checks the incoming connections against a list of preconfigured DNSBL's. Based on the weights assigned to the lists and a threshhold it makes a decision weather it should proxy the email to the upstream or hang up (close) the connection.

FU is optimized to run in a virtual machine environment. It should be able to handle a couple of hundred incoming connections per second on a single core system/vm.

CHAPTER

ONE

FEATURES

- Round Robin Load Balancing of Backends.
- Ability to check multiple blacklists.

OPTIONS AND ARGUMENTS

Options accepted by the `fu` command.

-h, --help	Show a help message and exit.
-c, --config	Configuration file.
-t, --test	A IPv4-address to run a test against based on the provided configuration file.

CHAPTER

THREE

EXAMPLES

3.1 Configuration File

```
settings:
    loglevel: notice
    predicate: 2
    threshhold: 1.0
    bind:
        localhost: 2525
    upstream:
        - localhost: 1026
        - localhost: 1025


providers:
    bl.spamcop.net: {weight: 0.3}
    ix.dnsbl.manitu.net: {weight: 1.0}
    rhsbl.ahbl.org: {weight: 0.3}
    truncate.gbudb.net: {weight: 1.0}
    zen.spamhaus.org: {weight: 0.5}
```

3.2 Example of a Dry Run

```
$fu --config /etc/fu.yml --test 201.8.3.1
Negative response from 1.3.8.201.ix.dnsbl.manitu.net.
Negative response from 1.3.8.201.truncate.gbudb.net.
Negative response from 1.3.8.201.rhsbl.ahbl.org.
DNSBL reply: 11 (Predicate is: 2).
Positive response from zen.spamhaus.org adding 0.5 to weight
Negative response from 1.3.8.201.bl.spamcop.net.
0.5 is below the threshhold (1.0) - NOT SPAM!
```

CHAPTER

FOUR

INSTALLATION AND DEPLOYMENT

FU is dependent on gevent to harness the power of libevent.

4.1 Debian and Ubuntu

A one-liner to install on a fresh system.

```
sudo apt-get update; sudo apt-get install python-pip python-gevent python-yaml; sudo pip install fu
```

You then need to create the configuration file.

CHAPTER

FIVE

REFERENCES

- RFC5782
- Wikipedia Comparison of DNS blacklists

CHAPTER

SIX

PYTHON API

6.1 API

DNSBL checking SMTPD-Proxy on gevent steroids

`fu.`**`resolve`**`(`*zone*`)`

Checks if the name resolves and if the last part of the reply is >= the predicate.

Parameters **zone** (*string*) – A valid zone for lookup ex: '234.52.218.89.ix.dnsbl.manitu.net.'

Return type integer

`fu.`**`as_reversed`**`(`*ip*, *suffix*`)`

Reverses the ipv4 so that it can be checked >>> as_reversed(ip='89.218.52.234', suffix='ix.dnsbl.manitu.net') '234.52.218.89.ix.dnsbl.manitu.net.'

Parameters

- **ip** (*string*) – A IPv4 address.
- **suffix** – The FQDN of the DNSBL Provider.

Return type string

`fu.`**`check_lists`**`(`*ip*, *providers*, *threshhold*, *predicate=2*`)`

Checks a ip against a list of DNSBL providers.

Parameters

- **ip** (*string*) – A IPv4 address to be checked.
- **providers** (*Mapping*) – A mapping (dict) containing FQDN's as keys and weights as values (floats).
- **threshhold** (*float*) – If the combined results >= this value, we deem it as spam.
- **predicate** (*integer*) – The DNSBL-reply must be equal to this or higher.

Return type bool

`fu.`**`is_spam`**`(`*ip*, *provider*, *predicate=2*`)`

Returns either True or False depending on if the last digits in the reply is >= the predicament. 2 is the default as per RFC.

Parameters

- **ip** (*string*) – A IPv4 address to be checked.
- **provider** (*string*) – The FQDN of the DNSBL Provider.

- **predicate** (*integer*) – The DNSBL-reply must be equal to this or higher.

Return type bool

PYTHON MODULE INDEX