perdition: Mail Retrieval Proxy

Horms (Simon Horman)
Verge Networks – horms@verge.net.au
VA Linux Systems Japan, K.K. – horms@valinux.co.jp

January 2003

http://www.verge.net.au/linux/perdition/

What is Perdition?

/pɜdɪˈʃən/ *noun* **1.** a condition of final spiritual ruin or damnation. **2.** the future state of the wicked. **3.** hell. **4.** utter destruction or ruin. [Middle English, from Latin: act of destroying]

Source: Macquarie Concise Dictionary www.macquariedictionary.com.au

What is this Perdition?

Non-Caching POP and IMAP proxy server

Proxies connections to a real-server based on:

- popmap lookup
- user-supplied server-name
- round-robin server pool

Popmap lookup is implemented as a module with an open API

Arbitrary lookup mechanisms may be defined

Perdition: Some of its Uses

Load balancing

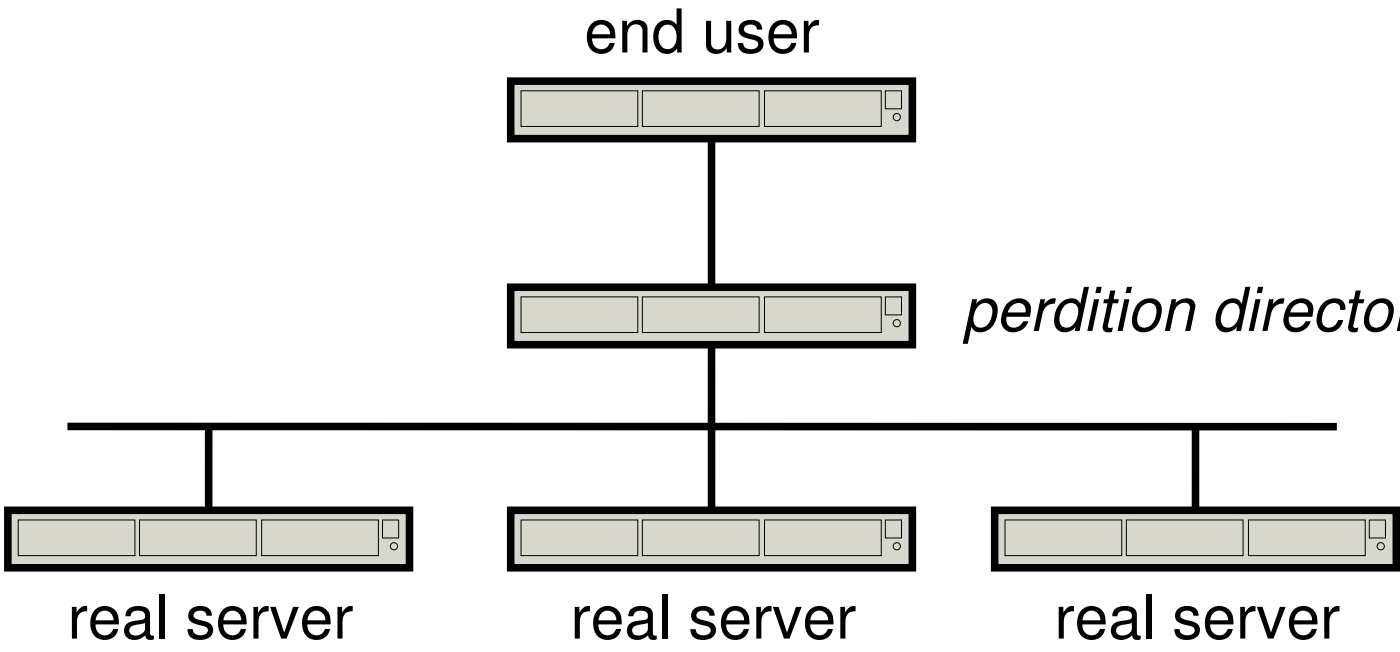
Integration

Migration

Bridging plain-text, SSL and TLS services

Firewall

Basic Architecture


end user
perdition directo
real server
real server
real server

Perdition handles the authentication phase of a connection

It then pipes data between the end-user and the real-server

Authentication Phase

User may query the capabilities of the server

User may request a TLS connection

User inputs their username and password

Perdition selects the real-server for the connection

Real-Server Connection

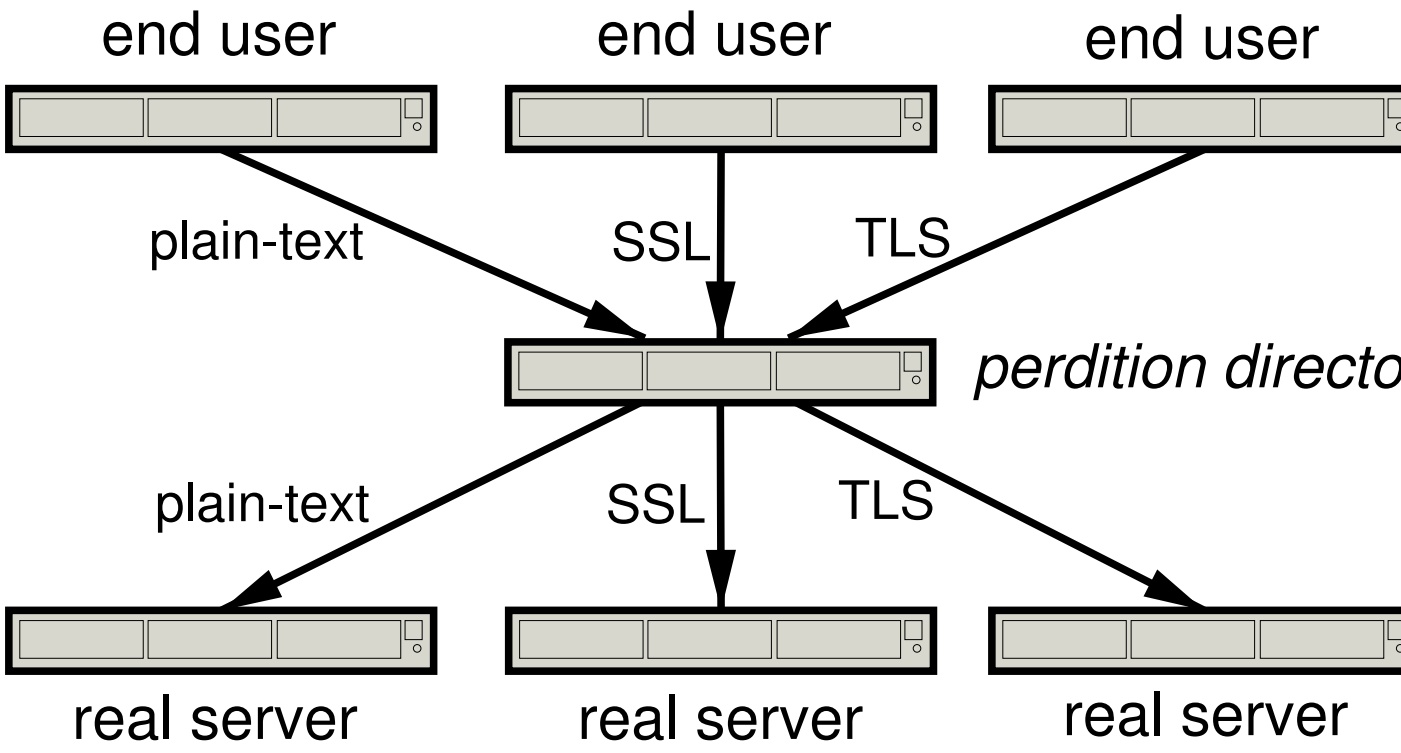
Perdition uses the end-user supplied username and password to authenticate with the real-server.

If unsuccessful, an error is returned to the end-user who may try again.

If successful, data is piped between the end-user and real-server.

Perdition does not integrate the IMAP/POP commands after the authentication phase.

Plain-Text, SSL and TLS


end user
end user
end user
plain-text
SSL
TLS
perdition directo
plain-text
SSL
TLS
real server
real server
real server

Plain-Text, SSL and TLS

Perdition may bridge Plain-Text, SSL and TLS services.

In: Plain-Text, SSL or TLS

Out: Plain-Text, SSL or TLS

Useful when using a POP or IMAP daemon that does not support SSL or TLS.

N.B: POP in $\longrightarrow$ POP out, IMAP4 in $\longrightarrow$ IMAP4 out

Popmap

Database that perdition may use to determine an end-user's real-server.

Lookup is done by a map-library that is loaded at run-time.

Modules in the current distribution are: LDAP, ODBC, MySQL, PostgreSQL, GDBM, Berkeley DB, POSIX Regular Expression and NIS.

By defining a new map-library, the real-server can be determined by any means desired.

- Database: Key-Value, SQL...
- Algorithmic: Regular Expression, Hash...
- External Programme: Dynamic Feedback...

Popmap: Input

The key for the popmap lookup is provided by the end-user.

The username supplied by the end-user is referred to as the long username.

This is split by the domain delimiter into the short username and the domain.

Long Username	Short Username	Domain
mary@verge.net.au	mary	vergenet.net
bob	bob	-

The domain delimiter is configurable at run-time. The default is @.

Popmap: Query Key

A list of keys used to query the popmap can be built using escape sequences and string literals.

Escape Sequence	Entity
\U	long username
\u	short username
\D	domain delimiter
\d	domain
\i	source IP address
\I	destination IP address
\p	source port
\P	destination port
\\	Literal \

The resulting query-key is a comma (,) delimited list of keys to query the popmap.

e.g. `\u\D\I,\u\Ddefault`

The result from the first successful lookup will be used.

Popmap: Result

The result is the real-server to connect to.

It may be suffixed by a colon (:) and the port to connect to.

A username and the domain delimiter may also be prepended.

Result	Username	Server	Port
pop0.verge.net.au	-	pop0.verge.net.au	-
pop0.verge.net.au:110	-	pop0.verge.net.au	110
mary@pop0.verge.net.au	mary	pop0.verge.net.au	-
mary@pop0.verge.net.au:110	mary	pop0.verge.net.au	110

If a username is provided it may be used as the username to use when authenticating with the real-server.

If a port is given it will override the default.

Popmap: No Result

All is not lost!*

A comma delimited list of default servers may be supplied.

These servers will be used in a round-robin fashion.

Optionally, each server may be appended with a colon and the port to connect to.

If a port is supplied it will override the default.

If all connections are to be forwarded to these default servers, then a database lookup can be avoided by specifying the map-library to use as the empty string ("").

*"*Poor Morpheus. Without him we're lost.*" The Matrix

Relaying Email

Allowing anonymous hosts to use a mail server as a relay is generally undesirable.

It provides a Spam gateway.

However is is desirable to allow authorised end-users to relay mail on the fly.

SMTP Auth (RFC 2554) is a good solution to this.

POP/IMAP Before SMTP is an alternative if SMTP Auth is not available.

POP/IMAP Before SMTP

Record the IP address of end-users that are authenticated for POP/IMAP access.

These IP addresses are allowed to relay email.

Typically the IP addresses are expired from the list after a time.

This provides a window where end-users can relay mail.

If the end-user continues to access their email through POP/IMAP then the window is extended.

Perdition-PBS

Perdition provides POP/IMAP before SMTP support as a separate daemon, Perdition-PBS.

Monitors the perdition log files.

Adds and expired entries to a local Berkeley DB database.

May be modified to use other databases – TDBRepl* would allow information to be shared between hosts without significant overhead.

As IMAP connections may last for a long time, perdition periodically relogs sessions to keep the relaying window open.

Perdition-PBS can also be used with other POP/IMAP before SMTP implementations.

*TDBRepl: http://tdbrepl.inodes.org/

Perdition-PBS and MTAs

MTA uses the information in the database to allow relaying from authenticated hosts.

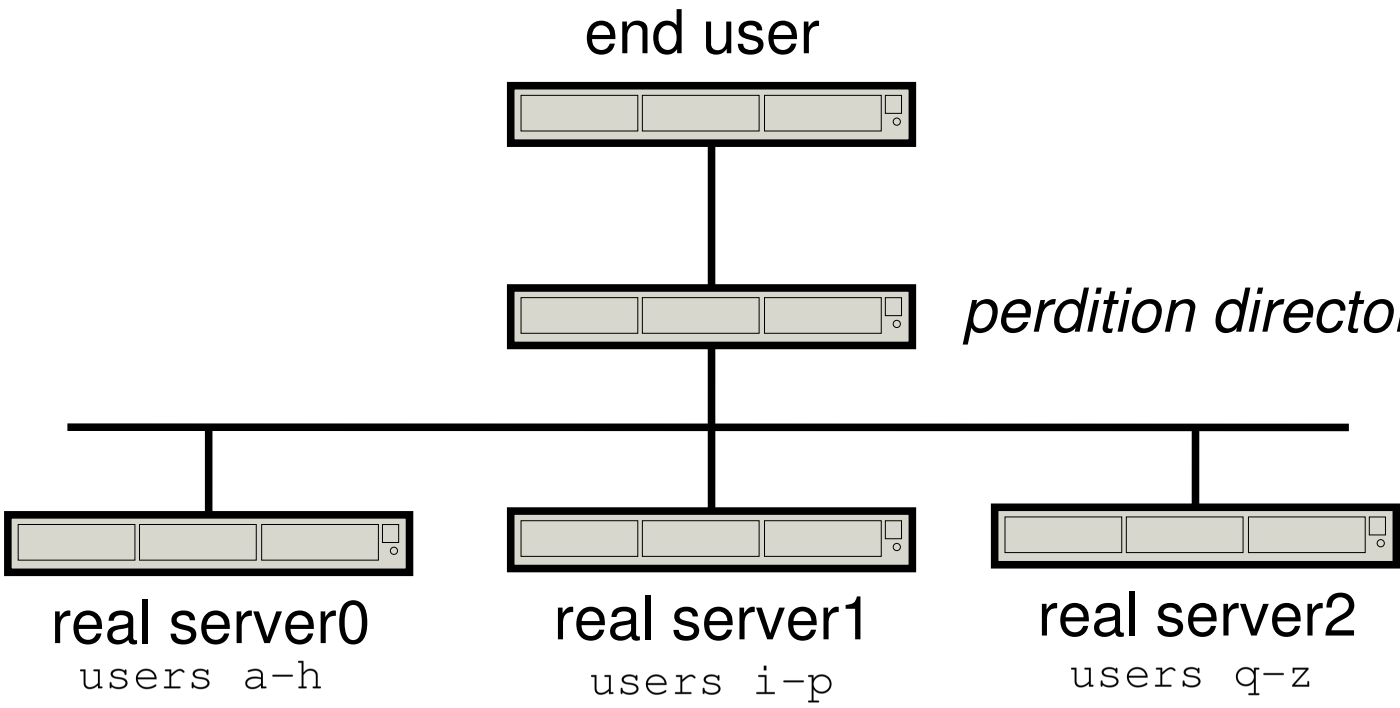
- Sendmail: Is able to access the Berkeley DB directly.
- Qmail: A wrapper reads the database and sets the RELAYCLIENT environment variable accordingly.
- Postfix: Some modifications are required, but it should also be able to read the Berkeley DB directly.

Applications

Because of Perdition's flexibility it can be used for a variety of applications.

- Load Balancing
- Integration
- Migration
- Firewall

Load Balancing


end user
perdition directo
real server0
users a–h
real server1
users i–p
real server2
users q–z

Load Balancing

For large email systems it is desirable to grow beyond a single machine.

One way to do this is to split end-users between different real-servers.

This can be done transparently by having the end-users connect to a perdition-director.

The perdition-directors can scale horizontally using Layer 4 Switching.
(or round-robin DNS, urgh!)

Load Balancing: Splitting Users

Suppose users are split: a-h to real-server0, i-p to real-server1 and q-z to real-server2.

This can be done simply in perdition using a regular expression popmap.

```
^[a-h]: real-server0
^[i-p]: real-server1
^[q-z]: real-server2
```

A database map-library may be used instead of regular expressions to give more fine-grained control over user allocations.

A custom map-library may be written to take into account system-specific parameters.

Integration

When organisations merge is can be desirable to consolidate email infrastructure.

This can result in username clashes.

Perdition can resolve this problem by mapping usernames to different internal mail-box names.

e.g.

`bob@foo.com` $\longrightarrow$ `bob1`

`bob@bar.com` $\longrightarrow$ `bob2`

Integration: Determing the Domain Name

The domain name of an end-user need to be determined to form part of the key for the popmap lookup.

If end-user's supply their domain-name as part of their username when authenticating, this can be used.

Otherwise, the perdition-director can be assigned multiple IP addresses.

Each IP address maps to a different hostname in DNS.

e.g.

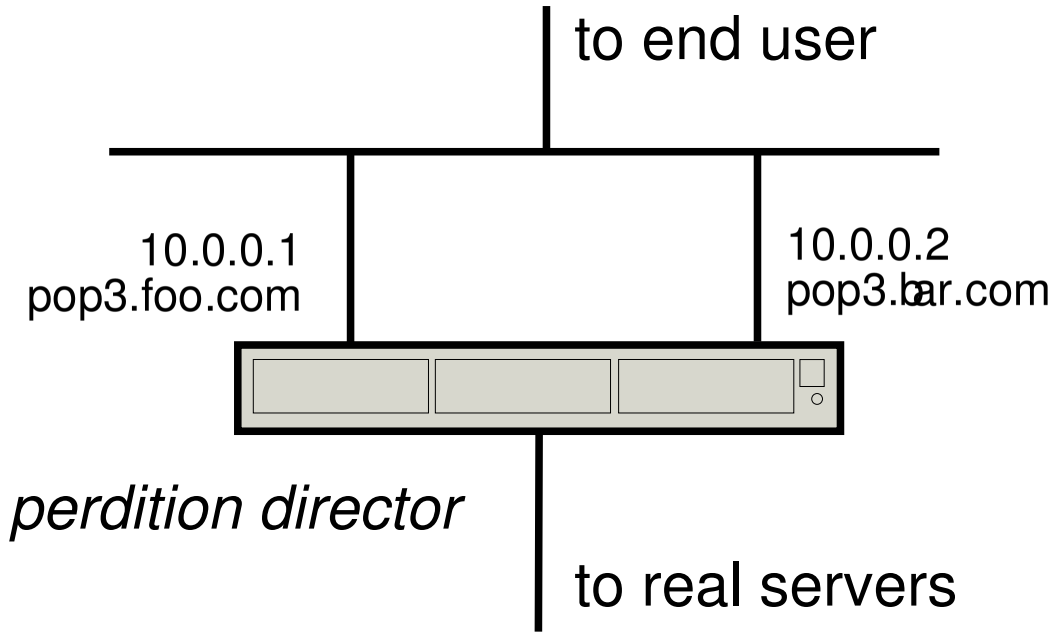
`pop3.foo.com` $\longleftrightarrow$ `10.0.0.1`

`pop3.bar.com` $\longleftrightarrow$ `10.0.0.2`

Thus, end-users connecting to the pop-server for different domains will connect to different IP addresses.

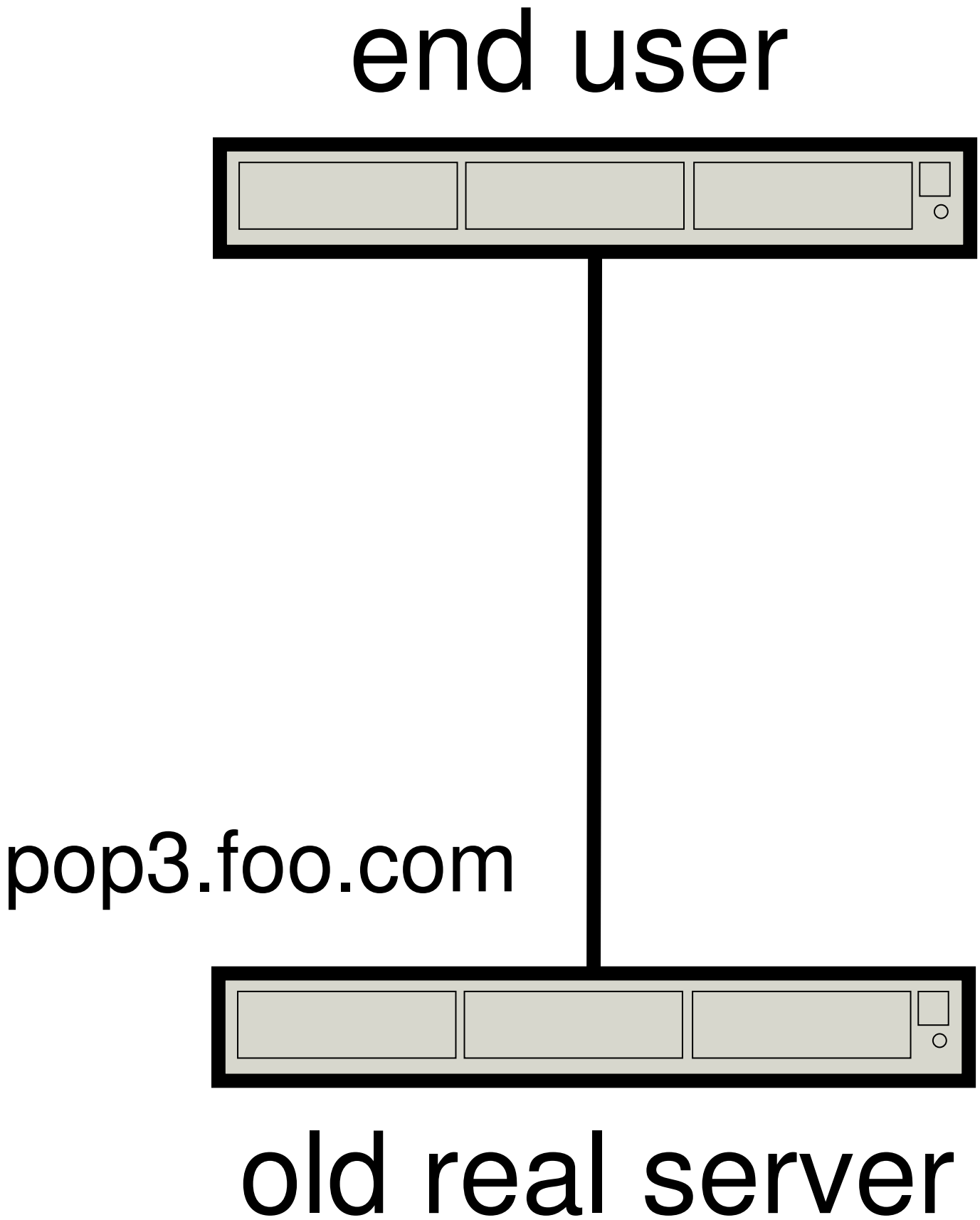
Perdition can use this IP address as part of the key for the popmap lookup.

Integration: Multiple IP Addresses


to end user
10.0.0.1
pop3.foo.com
10.0.0.2
pop3.bar.com
perdition director
to real servers

Migration

Perdition may be used to gradually migrate users to a new real-server.


end user
pop3.foo.com
old real server

Migration

Suppose that a replacement for pop3.foo.com is needed.

A new server is commissioned, but for some reason it is desirable to move users over gradually.

This can be done by putting a perdition in front of both the old and new real-server.

Perdition may run on a separate host or on one of the real-servers.

The perdition-director should assume the IP address for pop3.foo.com.

Users are directed to the old or new real server by perdition.

Once the migration is compete, perdition can be removed and the new real-server can assume the IP address for pop3.foo.com.

Firewall

Perdition may be used to proxy POP and IMAP requests as part of a firewall.

It may forward end-user's connections passed on a popmap, default server or an end-user supplied hostname.

e.g. End user supplied hostname

`bob@pop3foo.com` $\longrightarrow$ `connect as bob to pop3.foo.com`

End-User may be authenticated by perdition. But this is very limited as the password must be the same as that on the real-server.

Perdition does not understand or verify POP or IMAP commands after the authentication phase. So it may not offer much protection.

Availability

Implemented in C.

Primary development platform is Linux. But it is known to work well on Solaris and FreeBSD and should work on other Unixes.

It have been developed for several years now, and should be considered quite stable.

Available under the terms of the GNU General Public Licence from
`http://www.verge.net.au/linux/perdition/`

Also available as part of Debian GNU/Linux and FreeBSD.

Version 1.11 will be released soon. 1.11beta series is available for testing.

Contributions are always welcome. (I ♡ patches!)

Deployments

Perdition is currently in use in many production systems.

Some of the larger ones that are public knowledge are:

- Pipex, ISP in the UK, 260,000 accounts
- NetCologe, ISP in Germany, 110,000 accounts
- Ohio State University, USA, 60,000 accounts
- SoVerNet, ISP in the USA, 40,000 accounts
- Belgacom Skynet, largest ISP in Belgium, 7,500,000 connections/day
- Fastmail.FM, large IMAP provider

Sources listed at: www.vergenet.net/linux/perdition/

perdition: Mail Retrieval Proxy

Horms (Simon Horman)
Verge Networks – horms@verge.net.au
VA Linux Systems Japan, K.K. – horms@valinux.co.jp

January 2003

http://www.verge.net.au/linux/perdition/