NAME

ftp-proxy - Internet File Transfer Protocol proxy daemon

SYNOPSIS

ftp-proxy [**-6Adrv**] [**-a** *address*] [**-b** *address*] [**-D** *level*] [**-m** *maxsessions*] [**-P** *port*] [**-p** *port*] [**-q** *queue*] [**-R** *address*] [**-T** *tag*] [**-t** *timeout*]

DESCRIPTION

ftp-proxy is a proxy for the Internet File Transfer Protocol. FTP control connections should be redirected into the proxy using the pf(4) *rdr* command, after which the proxy connects to the server on behalf of the client.

The proxy allows data connections to pass, rewriting and redirecting them so that the right addresses are used. All connections from the client to the server have their source address rewritten so they appear to come from the proxy. Consequently, all connections from the server to the proxy have their destination address rewritten, so they are redirected to the client. The proxy uses the pf(4) *anchor* facility for this.

Assuming the FTP control connection is from $client to $server, the proxy connected to the server using the $proxy source address, and $port is negotiated, then **ftp-proxy** adds the following rules to the various anchors. (These example rules use inet, but the proxy also supports inet6.)

In case of active mode (PORT or EPRT):

```
rdr from $server to $proxy port $port -> $client
pass quick inet proto tcp \
    from $server to $client port $port
```

In case of passive mode (PASV or EPSV):

```
nat from $client to $server port $port -> $proxy
pass in quick inet proto tcp \
    from $client to $server port $port
pass out quick inet proto tcp \
    from $proxy to $server port $port
```

The options are as follows:

-6 IPv6 mode. The proxy will expect and use IPv6 addresses for all communication. Only the extended FTP modes EPSV and EPRT are allowed with IPv6. The proxy is in IPv4 mode by default.

-A Only permit anonymous FTP connections. Either user "ftp" or user "anonymous" is allowed.

-a *address*
The proxy will use this as the source address for the control connection to a server.

-b *address*
Address where the proxy will listen for redirected control connections. The default is 127.0.0.1, or ::1 in IPv6 mode.

-D *level*
Debug level, ranging from 0 to 7. Higher is more verbose. The default is 5. (These levels correspond to the syslog(3) levels.)

-d Do not daemonize. The process will stay in the foreground, logging to standard error.

-m *maxsessions*
Maximum number of concurrent FTP sessions. When the proxy reaches this limit, new connections are denied. The default is 100 sessions. The limit can be lowered to a minimum of 1, or raised to a maximum of 500.

-P *port* Fixed server port. Only used in combination with **-R**. The default is port 21.

-p *port* Port where the proxy will listen for redirected connections. The default is port 8021.

-q *queue*
Create rules with queue *queue* appended, so that data connections can be queued.

-R *address*
Fixed server address, also known as reverse mode. The proxy will always connect to the same server, regardless of where the client wanted to connect to (before it was redirected). Use this option to proxy for a server behind NAT, or to forward all connections to another proxy.

-r Rewrite sourceport to 20 in active mode to suit ancient clients that insist on this RFC property.

-T *tag* The filter rules will add tag *tag* to data connections, and not match quick. This way alternative rules that use the *tagged* keyword can be implemented following the **ftp-proxy** anchor. These rules can use special pf(4) features like route-to, reply-to, label, rtable, overload, etc. that **ftp-proxy** does not implement itself.

-t *timeout*

Number of seconds that the control connection can be idle, before the proxy will disconnect. The maximum is 86400 seconds, which is also the default. Do not set this too low, because the control connection is usually idle when large data transfers are taking place.

-v Set the ’log’ flag on pf rules committed by **ftp-proxy**. Use twice to set the ’log-all’ flag. The pf rules do not log by default.

CONFIGURATION

To make use of the proxy, pf.conf(5) needs the following rules. All anchors are mandatory. Adjust the rules as needed.

In the NAT section:

```
nat-anchor "ftp-proxy/*"
rdr-anchor "ftp-proxy/*"
rdr pass on $int_if proto tcp from $lan to any port 21 -> \
    127.0.0.1 port 8021
```

In the rule section:

```
anchor "ftp-proxy/*"
pass out proto tcp from $proxy to any port 21
```

SEE ALSO

ftp(1), pf(4), pf.conf(5)

CAVEATS

pf(4) does not allow the ruleset to be modified if the system is running at a securelevel(7) higher than 1. At that level **ftp-proxy** cannot add rules to the anchors and FTP data connections may get blocked.

Negotiated data connection ports below 1024 are not allowed.

The negotiated IP address for active modes is ignored for security reasons. This makes third party file transfers impossible.

ftp-proxy chroots to "/var/empty" and changes to user "proxy" to drop privileges.