Vermillion FTP Daemon
User Manual

Contents

1. Feature Highlights

- Powerful, sleek, intuitive interface.
- High security, with per-user ip checking!
- Detailed system-wide and per-client status reporting.
- "Hides" to a taskbar icon, staying out of your way but still easily accessible.
- Ability to edit, examine, or disconnect individual clients.
- Handy quick info screen.
- Highly configurable logging
- Complete FTP compliance, including passive mode and resuming interrupted transfers.
- UNIX look and feel, works with any client.
- Fast! optimized for high speed networks.
- CPU-friendly, even with many simultaneous connections.
- User templates for easy configuration.
- Directory-change messages.
- Flexible, unlimited guest (anonymous) accounts.
- Stable and secure, can't be crashed remotely like other servers.
- Very inexpensive.

2. Requirements

Windows 95 or Windows NT 4.0
Winsock 1.1 or higher.

3. Background Information

VFTPD was originally conceived to address the problem of security with existing ftp servers. Since the FTP protocol specifies that usernames and passwords travel "in the clear", sensitive account information is vulnerable to packet sniffing, and other simple attacks. VFTPD adds IP-checking to allow you to specify which computers a given account may accessed from, preventing access even when an account has been compromised.

From its initial focus on security, the design focus shifted to provide the most powerful, intuitive, and convenient interface imaginable. VFTPD includes many unique interface features, such as "shrinking" to a task-bar icon. This truly puts VFTPD in the background, removing it from the ALT-TAB menu, and freeing valuable desktop real estate. A single click on the task-bar icon pops up a handy quick-info box, with general information about the current number of clients and the total data transfer rate. A double click brings the full program back to the desktop for more detailed status and configuration information.

To complete the package, VFTPD combines this with a efficient, high-speed network kernel, easily handling the fastest transfers with many simultaneous users, all without hogging your CPU.

The VFTPD project has so far taken over 600 hours of programming, beginning in January 1996. As of this initial public release, it contains 5241 lines of tight, optimized Visual C++ code. Also, as of this initial release I have received $0 for my efforts. If you enjoy VFTPD, please considering paying the modest registration fee to make this effort worthwhile and to help plans for future additions become a reality.

Thanks for trying Vermillion,

Matte Kalinowski
(i.e. Arcane Software)

If you have any comments about VFTPD, I'd love to hear them. You can contact me by email at mbk@jhu.edu, on the web at "http://jhunix.hcf.jhu.edu/~mbk".

4. Working with Vermillion

VFTPD is setup differently than most windows applications because instead of having one main window with pull-down menus, it has four "pages", each containing a different aspect of the server's configuration. To switch between pages, click on the tabs at the top of the window.

The first page, "status", is concerned primarily with providing the current status of the server. On this page, there are two windows, and two groups of buttons. The top window, "server log", provides a history of the last 1000 events. To find out how to filter what type of events should appear here, read section "4. System Setup. The bottom window, "connected clients", shows a list of who is currently connected to your system. The left column shows the unique session id code, which can be matched with a corresponding code in the "server log" window to identify which user is responsible for the event shown. The middle column lists the account under which the client has logged in, and the right column shows the address (or hostname if available) of the computer from which the client is connected.

By selecting a client from the "connected clients" window, and clicking one of the top three buttons, you can perform several useful tasks.

The first button, "examine", brings up a window contains a variety of useful information relating to the client. Among the information is a log of the commands and replies sent over the control connection, time online, idle time, total number and size of files received and stored, and the status of the current transfer, including file name, size, current position, and transfer rate.

The second button, "edit", brings up the user editor and allows you to make any changes to the account. Note that most changes do not take effect until the user's next login.

The third button, "disconnect", does just that, sending a "server shutting down" message to the client and closing the control connection.

The last button, "hide", has nothing to do with connected clients, but is one of most useful features of VFTPD. If you are finished examining the system status and wish to put the server window aside while you work on other things, clicking "hide" makes the window disappear, leaving only a tiny icon at the far right of the task bar. This is very handy, because it keeps the program out of way, but allows you to bring it back any time you wish. A single click on this icon provides a quick status report, providing information on the current number of users online, percent of capacity, and the combined data transfer rate of all clients. Double-clicking the icon, "un-hides" the main program window and allows you to get a more detailed view of system activity, change configuration options, or edit user accounts.

5. System Setup

Most of the system configuration takes place on page two, "setup". This page contains all the information which applies to the system as a whole. No changes made on this page are saved or become active until you click the "ok" button in the lower right corner. If you make a mistake, you can restore the last saved configuration by clicking "cancel". The following options can be set on this page:

"ftp port number": port number on which VFTPD should listen for connections.

"max. connections": limit to the number of simultaneous clients.

"timeout seconds": how long VFTPD should wait before disconnecting an idle user.

"start hidden": whether to start VFTPD "hidden". (see "hide" in section 3).

"use DNS": whether to use DNS to resolve remote remote addresses into hostnames.

"logging": filter which events to show in the "server log" and/or to save to disk.
- Level 0: none
- Level 1: security messages, including successful and failed logins.

Level 2: file writes (created, modified, deleted, etc.)
Level 3: file reads (retrieved, etc.)
Level 4: all other actions, including directory changes.
Level D: debug-level logging, includes commands and replies.

"welcome" and "goodbye" banners: change the messages displayed to users.
Use control-enter to advance to the next line in either window. If you prefer a larger workspace, you can create the messages using a program such as notepad and "paste" them into the window.

There are four types of message files which can be displayed by users. The "welcome banner" is the first thing displayed to a connecting user, even before logging in. The "goodbye banner" is displayed when a client logs off gracefully (issues the QUIT command). The other two messages are read from files. The first, "WELCOME.MSG" should be placed in the home directory of a user and will be displayed as part of the "user logged in" message. The second, ".message" (note the initial period), is placed in an directory and is displayed when a user changes to a directory. All messages should be limited to 75 characters per line to be displayed correctly.

Any of the four types of messages can contain special "tokens" which are replaced with system information, allowing you to create more personalized or informative messages. The following tokens are available (they are not case-sensitive):

%T: Current time and date, e.g. "Fri Apr 12 05:34:16 1996".
%F: Megabytes of free space in current directory, e.g. "212".
%C: Current directory, e.g. "/pub/incoming/".
%R: Remote host, e.g. "ppp123.rmt.college.edu".
%L: Local host, e.g. "jhunix.hcf.jhu.edu".
%U: User name, e.g. "anonymous".
%%: Percent character, e.g. "%".

Note that not all tokens are valid in all situations, such as "%U" in the "welcome banner", in those situations, the token is ignored. For convenience, a quick reference of available tokens appears at the bottom of the "setup" page.

6. Account Setup

The user account editor is available from either page three, "accounts", or from the "edit" button on page one, "status". The "accounts" page is much more flexible however because it allows you to create, delete, and edit any user or template.

To create a new account, type a name for the user or template in the edit box at the top of the window, and click to "add" button. If you wish to create a user or template based on an existing account, select the existing account and click the "clone" button. To edit an account, select account and click "edit", or simply double-click on the account name.

In the event that you add, clone, or edit an account, an "edit" window will appear where you can specify the following information:

"username": the name of the account, enter a new name if you wish to rename the account.
"password": specifies a password for the account (users only).
"template": select from a list of templates (users only).
"disable account": disable any logins to this account (users only).
"guest account": this is a guest user and doesn't require a password (users only).
"priority login": ignore "max. connections", handy for administrators (users only).
"file security": list of directory permissions, see below.
"ip security": list of remote systems which connect using this account, see below.

In order for a user to login, you must specify "file" and "ip" security permissions. The easiest way to do this is to create a template and setup the user as a member of that template. The permission lists display where the permissions are specified with the letter "s" for system defaults, "t" for template, and "u" for user. As you change templates for a user, the permission lists are updated to prevent mistakes in configuration. To setup permissions, simply click the appropriate buttons to the right of the list, "add", "edit", or "delete". Add and edit bring up the appropriate permissions edit window.

The file permissions edit window contains a number of check boxes with which you can grant or remove rights for a pathname, specify the home directory, etc. Each permission is assigned a letter which will appear next to the

pathname in the list if that permission is granted. The syntax for specifying directories is very specific, so be sure to follow the instructions given in the file permissions edit window.

The ip permissions edit window contains just one check box, "allow". If the ip mask that you specify should be allowed access using the current account, set the check box. If the ip mask should be denied access, clear the check box. The system default is to deny all access, so for the account to become active you must set at least one ip permission. "allow *.*.*.*" is fine, and is appropriate for anonymous access, but for user accounts it is beneficial to be more restrictive.

When a question of permissions arises, each setting is ranked according to how closely it matches the situation. For example, if a user wants to create a file in a directory called "/c:/ftp/pub/games/arcade/", and there are different permissions given for "/c:/ftp/pub/" and "/c:/ftp/pub/games/", both match, but since the second is a closer match, it takes priority. A similar rule works with ip security. If a user connects from a computer with ip "123.4.5.6", and there are settings to "deny 123.*.*.*", "allow 123.4.5.*", and deny "128.4.5.4-8", each setting registers as a match, but the user is denied access, because the third permission is the most specific match, and specifies a "deny".

If there is a conflict in permissions because a match is found in both the user's settings the settings inherited from the template, the user's settings take priority even if the template's settings provide a better match.

Unlike other servers, there are no "hard-coded" accounts for anonymous access. However, it is very easy to configure your server to accept anonymous logins. The simplest way is to set the desired permissions in a template, e.g. "guest", and create two users belonging to that template, "ftp" and "anonymous". Make sure that "guest account" is checked for both accounts and the ip permissions are sufficient.

One feature of VFTPD which causes some confusion is that if an ip is rejected for login, the message printed to the client says "User <name> unknown.", exactly as if the user really is "unknown". This is by design, and although it may be confusing at first, it makes it more difficult for hackers and doesn't reward them for trying random names in their attempts to gain access.

The user setup may sound difficult, but it's actually very simple. VFTPD was designed with the intelligence necessary to make this part of the job easy. The only "rules" you need to really need to remember is that VFTPD uses the best information you have given it to make its decisions, and that user settings always override their template's settings.

7. Acknowledgments

I'd like to thank the following people for helping to contribute to the release of VFTPD:

Mike Prados, for letting me test on his system virtually every day since this project began and feigning interest at the slightest new feature, after everyone else was long tired of hearing about VFTPD.

Nat Fellows, for moral support and encouragement during that slow interface development phase, for lots of great suggestions, for making me track down and fix even the most esoteric bugs, and for helping out with the documentation.

Jon Polimeni, for scaring the hell out of me by asking me how "my ftp server is coming along."

Margaret Murphy, for coming up with the name "Vermillion", which by the way is the name of a color very similar to scarlet.

Amanda Yancy, for being the most wonderful and supportive girlfriend possible, and especially for putting up with my week-long explanation of "how VFTPD works".

My beta testers, especially "hex", who possessed a remarkable talent for bringing VFTPD to its knees and finding subtle quirks that probably would have made it into the release otherwise.

Hank, Brendan, Kevin, Markham, Kito, Mimi, Kurt, Melena, Liz, Debbie, Sandy, Olga, Manas, Kate, Beta, Laura, Steve, Chris, and everyone else who heard more hype about VFTPD than any human should ever have to endure.