freeshell.de

FREE SHELLS FOR A FREE WORLD

User Manual

Date: 2016-05-15 - Version 1.3

Table of contents

Author

Contact private:
Sebastian Krajenski
Im Gehren 24/1
73732 Esslingen
Germany
Tel: +49-162-8741288 (SMS possible / only for emergencies like: “server down”)
E-Mail: sk@freeshell.de

Contact business:
mars solutions GmbH
Robert-Bosch-Str. 8
73037 Goeppingen
Germany
Tel: +49-7161-6549250 (Mon-Fri)
E-Mail: sebastian.krajenski@ mars-solutions.de

Business proposals welcome. I'm a certified RHCE7, LPIC-3 (security) with >20 years of Linux experience.

The project is called “**freeshell.de**”, like the homepage and main domain name. The old name of “Nic.Nac.Project” is not in use anymore.

Server

The system in use is a Intel-based 64-bit-system with the following specs:

- 1x Intel Xeon E3-1241 V3 3.5 GHz (8 cores)
- 32.0 GB RAM
- 2x 500GB WD SATA HDD

Description of base setup

The setup as such is a single-server system. Regarding the HDDs a software RAID1 (md device) is used. Both HDD get monitored using “smartd”. Daily tests (“short-test”) as well as weekly tests (“long-test”) assure, that possible SMART-Errors are detected as quickly as possible.

Nameservers of “freeshell.de”:
NS1: ns1.nic-nac-project.de, NS2: ns2.nic-nac-project.de

In detail:
ns1.nic-nac-project.de = freeshell.de (the server itself, the MASTER-DNS)
ns2.nic-nac-project.de = 50.30.38.228 (a vServer in USA , exclusively used as SLAVE-DNS)

The old legacy domain “nic-nac-project.de” itself is served from those nameservers:
nsa5.schlundtech.de
nsb5.schlundtech.de
nsc5.schlundtech.de
nsd5.schlundtech.de

A backup MX-record doesn't exist at the moment, but is planned.

The hardware- and software-situation as well as the DNS-setup is permanent work-in-progress. There may be regular updates and improvements.

Backup

The system is saved to another data centre on a daily basis using “duplicity”.
The data is gpg-encrypted. The command I am using is:

```
# duplicity incremental --encrypt-key <Key-ID> --full-if-older-than 30D -v3 / file:///backup
```

365 restore points are saved at the moment. In case you need a restore, please always name the exact and absolute path as well as a best-estimate regarding the date the data was still intact. The mount point /backup is mounted using sshfs:

```
# sshfs -o reconnect source:/backup /backup
```

Old restore points get cleaned up using:

```
# duplicity remove-older-than 1Y --force file:///backup
```

User resources

Disk space

There are different quotas for you depending on what services we're talking about:

- Linux base home directory quota (incl. Maildir/) → 512 MB
- MySQL database → +256 MB (technically: none; but you'd set an alarm off :-)
- Zarafa-Groupware mailbox→ +512 MB
- OwnCloud service → +2048 MB

Processes and RAM

Here is an overview on what resources to expect on the shell:

```
$ ulimit -a

data seg size           (kbytes, -d) 256000
file size               (blocks, -f) unlimited
pending signals                 (-i) 63359
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) 256000
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) 300
max user processes              (-u) 50
virtual memory          (kbytes, -v) 512000
file locks                      (-x) unlimited
```

Account lock

Basically this is covered in the "terms and conditions".
For short: Misuse of any kind as well as illegal content will lead to deletion of that content as well as account lock. I don't spy into your files, but there is an automated process using commercial AV snake oil to find virus and trojaned files. They get automatically deleted. Trojaned files e.g. in a “public_html” directory, served publicly, directly affects the ip/hostname reputation for all users!
For optimal privacy I recommend you to use dm-crypt, TrueCrypt, Veracrypt, gpg or similar software here.

Servername and network addresses

IPV4

Assigned: 94.247.40.144 – 94.247.40.159

In use:
(94.247.40.145 – Default Gateway)
94.247.40.147 – DNS-Name: ssh.freeshell.de aka work.ham.to (Port 443 alternative for SSH)
94.247.40.152 – DNS-Name: zarafa.freeshell.de (Zarafa Groupware)
94.247.40.153 – dns2tcp service address (source: http://www.hsc.fr/ressources/outils/dns2tcp/)
94.247.40.155 – DNS-Name: secure.freeshell.de (mainly for Zarafa WebApp)
94.247.40.156 – DNS-Name: **freeshell.de** (IPV4 main address)
94.247.40.157 – DNS-Name: gate.freeshell.de (GateOne SSH over HTML5)
94.247.40.158 – DNS-Name: pad.freeshell.de (EtherPad text collaboration)

IPV6

Assigned: 2a01:360:106::2 / 48

In use:
2a01:360:106::2 – DNS-Name: **freeshell.de** (IPV6 main address)

Connectivity

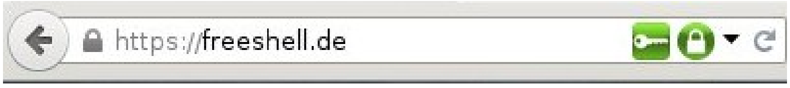
The server is connected by a 1000 Mbit/s symmetric link to the internet.
In case of a D(D)oS-attack the system automatically gets disconnected from the infrastructure.
Likewise it is automatically connected back when an attack stops.

System identification and certificates

DNSSEC

The DNS of the main domain “freeshell.de” is secured with DNSSEC.
I recommend the following tools to check out the zone:
URL: http://dnssec-debugger.verisignlabs.com/freeshell.de (manually)

URL: https://www.dnssec-validator.cz/ (automatically for your browser)
There you'll find a neat **Browser-Plugin** that checks for a couple of things. The availability of DNSSEC for that domain (key symbol), as well as the validity of TLSA-entries.



At the moment I maintain **TLSA** entries for the following names and services:

_443._tcp.freeshell.de.
_443._tcp.www.freeshell.de.
_443._tcp.secure.freeshell.de.
_25._tcp.freeshell.de. → So "postfix" is configured DANE-compatible here
_465._tcp.freeshell.de.
_587._tcp.freeshell.de.

SSH fingerprint

SSH Fingerprint freeshell.de (RSA): **0c:39:00:1a:11:4a:1c:09:4d:7c:06:6e:19:15:7a:c7**
SSH Fingerprint freeshell.de (ED25519): **92:61:df:85:1b:07:1b:6a:04:34:96:be:49:cf:9e:f0**

Hint: For untrusted or mobile situations like connecting from an Internet Cafe, hotel etc.
I deeply recommend you to print out the fingerprints on a piece of paper and carry them with you. You detect "man-in-the-middle" attacks this way!

SSL aka https

The webserver uses “**certificate pinning**”. Modern browsers may know this way if the certificate delivered is the right one. This technique relies on "trusted first visit", of course.

Technical background info: https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21
Implementation hints: https://developer.mozilla.org/en-US/docs/Web/Security/Public_Key_Pinning

PGP - public key

This is my public key for safe email communication. My address: sk@freeshell.de

URL: http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xB9C569CCC8EADFC4
Long-ID: B9C569CCC8EADFC4
Key fingerprint = 7249 FAFF 240A DA30 CD76 FB70 B9C5 69CC C8EA DFC4

S/MIME - public key

If you prefer that...

Download-URL: https://freeshell.de/smime.txt
Copy-Paste-variant:

```
-----BEGIN CERTIFICATE-----
MIIErzCCA5egAwIBAgIQZrRVwxe9sOu13VlGowUlKDANBgkqhkiG9w0BAQsFADBd
MQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU2lnbiBudi1zYTEzMDEGA1UE
AxMqR2xvYmFsU2lnbiBQZXJzb25hbFNpZ24gMSBDQSAtIFNIQTI1NiAtIEcyMB4X
DTE0MDUzMDE0NDMxNloXDTE3MDUzMDE0NDMxNlowOjEYMBYGA1UEAwwPc2tAZnJl
ZXNoZWxsLmRlMR4wHAYJKoZIhvcNAQkBFg9za0BmcmVlc2hlbGwuZGUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB++yJoWokc6ui9TSqSZ/+OS83FKal
FXIWuK1Mw4yN3MKiSt3VUke7qRXbnyMth6WrN9WcvoSs+0/NnpiRBwmjgtuTFOd3
WDlnz/Ni8J9JfplbvdPwjyl1YH42MBU5WmcV3ZQ4AruXxjWwSISn2Qy6GlDLszKB
cddUlq4y5MhPQUdEayprhmmmllKZCIQK1YJ+B3RUdBxGUvcCrZ8Jj6vgC+4dbX33
C/E9NxhiLewqZY/Me5YHfVf7gL+CLuNyo4HNaFTKtn4DY9D6XUy+q0rzCD1c/H/O
71EW7HvTR891fBb498OWDjBqgPIV9FiqpzddpXHc1hwk1DVIKQ1se/PdAgMBAAGj
ggGMMIIBiDAOBgNVHQ8BAf8EBAMCBaAwTAYDVR0gBEUwQzBBBgkrBgEEAaAyASgw
NDAyBggrBgEFBQcCARYmaHR0cHM6Ly93d3cuZ2xvYmFsc2lnbi5jb20vcmVwb3Np
dG9yeS8wGgYDVR0RBBMwEYEPc2tAZnJlZXNoZWxsLmRlMAkGA1UdEwQCMAAwHQYD
VR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEcGA1UdHwRAMD4wPKA6oDiGNmh0
dHA6Ly9jcmwuZ2xvYmFsc2lnbi5jb20vZ3MvZ3NwZXJzb25hbHNpZ24xc2hhMmcy
LmNybDBZBggrBgEFBQcBAQRNMEswSQYIKwYBBQUHMAKGPWh0dHA6Ly9zZWN1cmUu
Z2xvYmFsc2lnbi5jb20vY2FjZXJ0L2dzcGVyc29uYWxzaWduMXNoYTJnMi5jcnQw
HQYDVR0OBBYEFPmW20op7NINlKE6zT3zQ+LwJIL9MB8GA1UdIwQYMBaAFP4pqbj/
nFvJ7ULZbnfYNFdBp20FMA0GCSqGSIb3DQEBCwUAA4IBAQBpmSlGxcutBHIb28sk
XdF9I1x342jPMIYmsDNVs0XulKe2gVhGngsD9NO9cWrk8zbc0j+jVb+U3PzopMuc
id5m9X8ti2UOAzyjNNm67QXjsN++oQxcUIBmGm38xfAC51Oaqfo0U9AUr6LVlMQd
owHC5/7hfsXgblZ2q/OZeXnNGVnekcOalS5VPlAn1kYov87k9Vofw4TBfRMGTbNz
sdkLlVWbZ4FHYypnxtAiGuuC4oHB0fV3pnQqalBaGCi5NFObfFouQOM0867s06pP
YPo4eQGL77j0HCSqz7TA5AOw/+7zA5KXIQuQVylBvl9RcijysAc5IluEdVqd/QYy
Idzo
-----END CERTIFICATE-----
```

Authentication and access

SSH

OpenSSH server here accepts connections to “freeshell.de” on the default port (TCP/22) for interactive sessions. With Linux and MacOS I recommend you “ssh” on the terminal. With MS Windows “putty” is the favored client:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
When you connect from a computer for the first time, please always check the fingerprint!

Password

Your first login will be password-based. After that, there are a couple of possible enhancements or variants:

Public Key

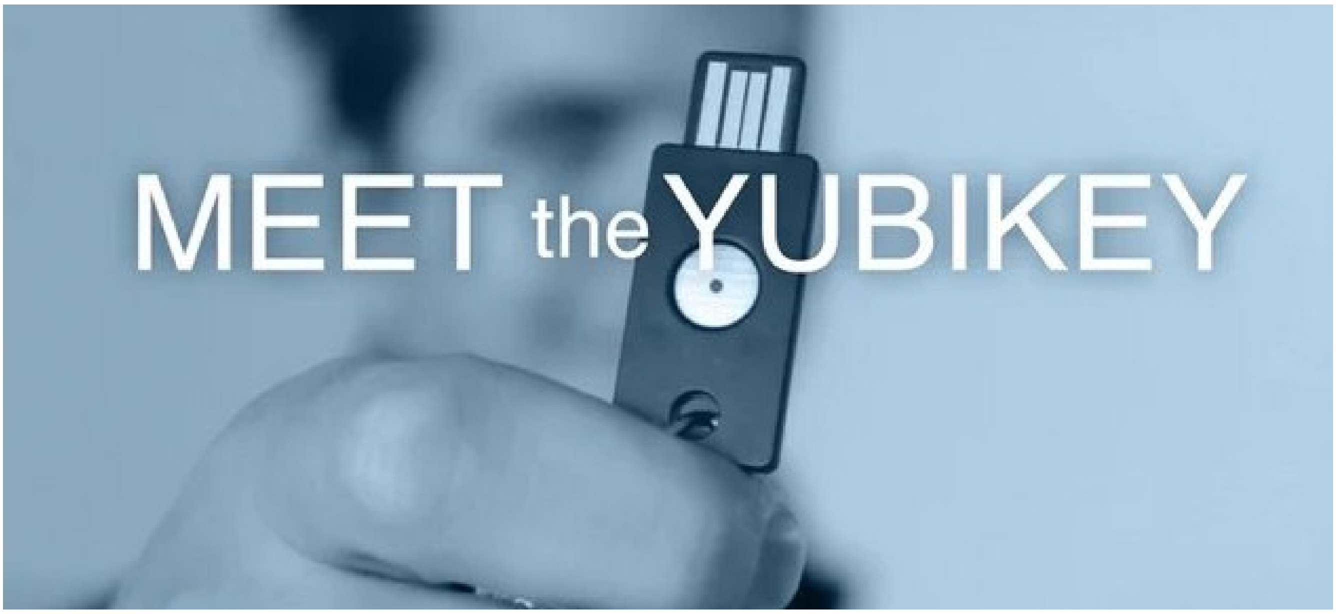
You already have a public key identity for SSH (type: RSA or ED25519) ?
Just fill
$HOME/.ssh/authorized_keys

…with your public key to login with a keyfile in the future. In case you don't have one yet – have a look here: https://help.ubuntu.com/community/SSH/OpenSSH/Keys

If you additionaly like to improve the SSH secrecy I recommend this article:
https://stribika.github.io/2015/01/04/secure-secure-shell.html

Hint: File transfer to the server is only possible using SFTP or SCP.
Classic FTP is **not** possible anymore. All major ftp clients support SFTP backend nowadays.

Yubikey



URL: https://www.yubico.com/products/

Another possibility to login is the Yubikey. It's basically a USB-Device that emulates a keyboard. It generates throw-away one-time-passwords. Set it up like this:

```
$ cd $HOME
$ mkdir .yubico
$ cd .yubico
$ cat >authorized_yubikeys
<activate your yubikey by pressing the sensor>
<Ctrl-D>
```

Now take a text editor and modify the file according to this schema:

yourlogin:first_12_chars_of_yubi_output

The first 12 chars are the public identity of your key. Just remove anything beyond character No.12.

Example result after editing:

thisisyou:ccclksjehdzu

Two-Factor-Login (forced)

You'd like to be forced to use two ways of authentication when logging into the system? Just use the homepage request form and tell me about that. I'll then add you to the "Force Two-Factor"-Group.

The login procedure is then the following:
- Login with SSH-Public-Key (!must!)
- Then you'll see:

```
Authenticated with partial success.
Password:
```

Here you now have two possibilities: Enter your normal text-based password **OR** hit the yubikey!

The server-side setup of that part - by the way - looks like this in /etc/ssh/sshd_config:

```
…
Match Group mfagroup
   AuthenticationMethods publickey,keyboard-interactive
…
```

OTP (one time password) / OPIE auth

URL: https://en.wikipedia.org/wiki/OPIE_Authentication_System
There is also OTP/OPIE available here. You generate one-time-passwords, which in this case are typed into the keyboard. No special hardware needed.

Setup (at the moment you are logged into freeshell.de – this is your server side setup part)

```
$ opiepasswd -c -f
```

Now you're asked for a at least 10 digit passphase, the output then looks like this:

```
ID yourlogin OTP key is 499 fr0761
TEN BILE MAID BARE SICK ABE
```

What does that mean?
“499” is the sequence number of the password
“fr0761” is the “seed” - so to say - the initializing vector for your one time passwords

Now for the client side. You need a piece of software to generate the passwords. In case of some older Debian (squeeze at best) you just install the package “opie-client”. Assuming you run a modern Linux client, this if for your **/etc/apt/sources.list** (works on Debian, Ubuntu and Mint)

```
…
deb  http://snapshot.debian.org/archive/debian/20121004T111800Z/  squeeze  main
…
# apt-get install opie-client
```

Let's use it!

Usage goes for example like this (you now are on your local Linux machine) :

```
$ ssh thisisyou@freeshell.de
Password: [ENTER]
otp-md5 497 fr0761 ext, Response:
```

In another terminal window you generate your one-time-password quickly:

```
$ opiekey 497 fr0761
```

Now, after entering your passphrase you are provided with the OTP for login:

```
WALK NEWS NE COAL MUFF BEAD
```

Voila – you're in!

Hint: You can generate OTPs in advance!

Example:

```
$ opiekey -n 10 497 fr0761
```

(generates the next 10 valid OTPs)

Accessing the system from censored or limited internet connections

So you are limited in some way regarding your internet connection? It's still likely that you can connect anyway. Let me show you some alternative ways to get into the system.

1) Use an alternative SSH port to login:

```
$ ssh ssh.freeshell.de -p443
$ ssh work.ham.to -p443       (same IP, but more unsuspicous name)
```

Other ports available for that same purpose: 32768 and 94.247.40.147:80

2) If your only limitation is not being able to run SSH client software - use the browser variant:
https://gate.freeshell.de

3) If all else fails, use dns2tcp (encapsulates your tcp stream within innocent DNS packets)
If you have access to a linux client simply install the package “dns2tcp”.

With this method the TCP packets for SSH are sent out covered in "normal" DNS requests.

Usage:

```
$ dns2tcpc -z tcp.ham.to -l 12345 -r ssh
```

(Tunnels SSH through DNS and port-forwards freeshell.de to your localhost:12345)
Keep that one running in background. Now:

```
$ ssh thisisyou@localhost -p12345 -D1080
```

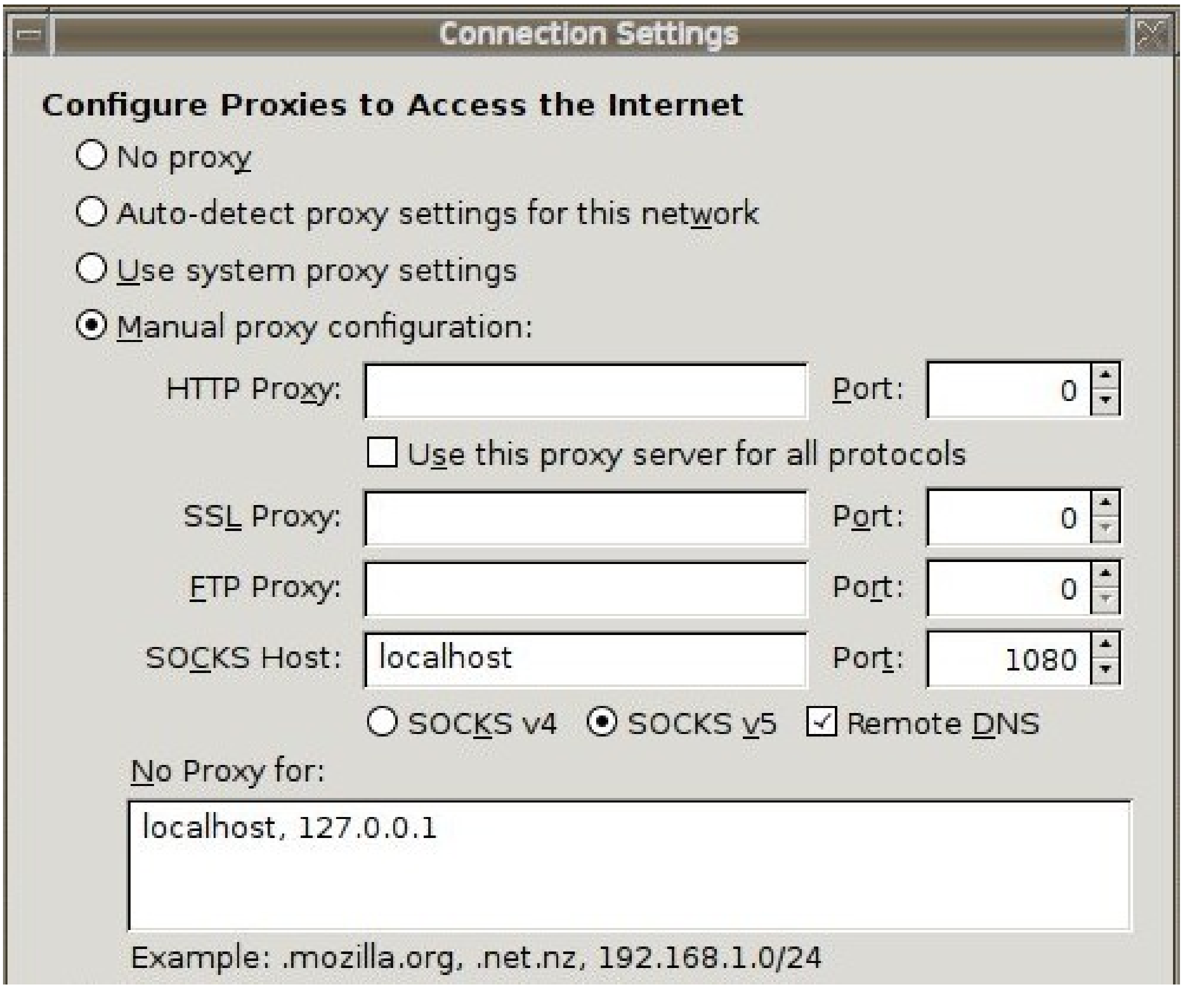
<u>Now you achieved two goals</u>:

- Getting into the system with SSH
- option “-D1080” also opened a local socks proxy that lets you now surf unrestricted!

Please check out the picture on the next page on how to setup your browser settings:

This is how to setup e.g. your firefox to use that proxy quite safely:

It's imperative to check the “Remote DNS” box. Otherwise your "evil" ISPs DNS might get a clue to where you surf.



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: Port: 0

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: localhost Port: 1080

○ SOCKS v4 ● SOCKS v5 ☑ Remote DNS

No Proxy for:

localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

What to expect: This method will be slow because of the dns2tcp overhead in general.

Anyway, even if you can “normally” connect to freeshell.de without hazzle, you are welcome to use the socks-proxy-technique as well.

Software and services

OS

The server runs Debian 8 (Jessie) 64-Bit-version. In irregeluar intervals the distribution gets updated the the latest "stable" release. There are 3rd-party software-dependencies that normally lead to 3-4 months of delay until I'm able to upgrade (after initial release). Please be patient.

Installation of additional packages

In case you miss a package just ask for it using the request form on the homepage. I will install almost any package that is available to official channels (in respect to the running release) :
https://www.debian.org/distrib/packages
http://backports.debian.org/Packages/

Firewall

This system uses a packet-filtering "iptables"-firewall. All ports (from the outside) to non-standard services are closed. In case you need a private port please let me know through the request form on the homepage.

Mailsystem

Postfix

The MTA on the server is postfix. The following services are configured.

Servername: freeshell.de
Port 25 (SMTP) sending email (Relaying) with auth. (STARTTLS forced)
Port 587 (Submission) sending email with auth. (TLS forced)
Port 465 (SMTPS) sending email with auth. (TLS forced)

The mailbox format used on the system is “Maildir”.
So your email resides in:
$HOME/Maildir/ (...)

Domain names
You are reachable with the following addresses:
you@freeshell.de (primary)
secondary: @freeshell.ch, @freeshell.at, @nic-nac-project.de
More domain names may follow.

Anti-Spam / Anti-Virus

Email on the system is passed through a couple of techniques (inbound and outbound)

- ips.backscatterer.org in “safe mode”
- policyd-spf (freeshell.de uses “hard fail” and strict with its own DNS entries)
- policyd-weightd (RBL-list checks)
- DKIM check (OpenDKIM in “safe mode” receiving side, otherwise mailing-lists would break)
- BATV (you get automated BATV envelope-adresses to your sent mails)
- commercial antivirus check (it checks for known malware and trojans)

Hint: Maximum element size (per mail element) is 50MB.

Dovecot - Receive mail

Dovecot provides your mailbox through **POP3** and **IMAP** on the following ports:

Servername: **freeshell.de**
Port 110 (POP3) STARTTLS (forced)
Port 143 (IMAP) STARTTLS (forced)
Port 995 (POP3S) TLS
Port 993 (IMAPS) TLS

On the shell you can run preconfigured “mutt” or “pine” to access your mailbox.

There are also webinterfaces in place:

URL: https://freeshell.de/squirrelmail/
SquirrelMail. Type: plain HTML – functional - and even works with lynx

URL: https://freeshell.de/rc/
RoundCube. Type: modern and good looking

Zarafa - Groupware

URL: http://www.zarafa.com

In case you want full collaboration experience and simple email is not enough for you. Zarafa is a AGPL3 groupware solution that provides additionally things like:

- Calendaring (also via ActiveSync aka “Exchange-Mailbox” for your mobile, see below)
- Tasks
- Notes
- Contacts (address books)

Zarafa is in permanent co-existence with the "normal" mail system. On the shell you can at any time migrate to Zarafa.
$ **move-in.sh**
…moves your current mail to into the Zarafa mailbox using "imapsync" in the background.

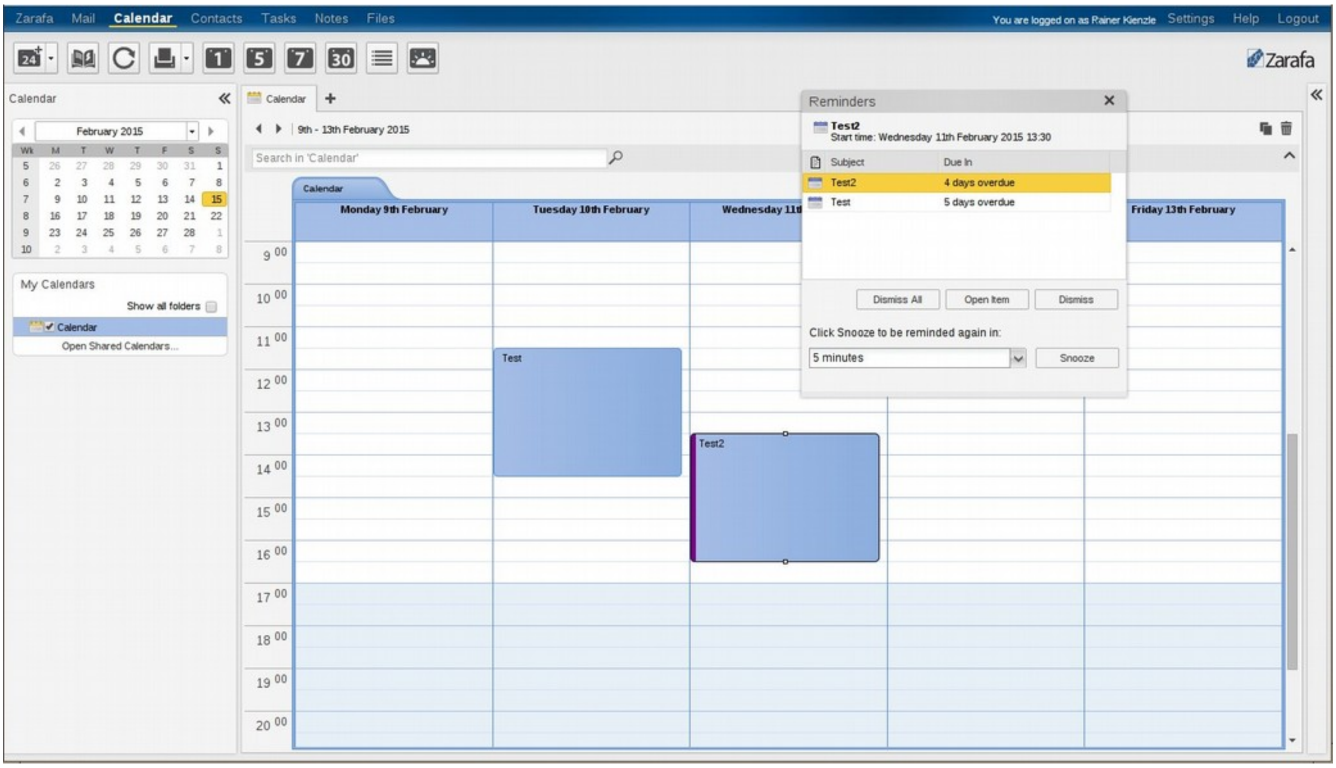
In case you just want to look around without migrating for real you can login into Zarafa WebApp anyway. The account is automatically in existence, just unused (empty).

Classic IMAP or POP to the zarafa account works also:
Servername: **zarafa.freeshell.de**
- Port 995 (POP3S) TLS
- Port 993 (IMAPS) TLS

Sending email (SMTP) with a mailclient of your choice:
Not different from the normal SMTP – it is simply the same. Zarafa uses postfix.
Servername: **freeshell.de**

Visit this URL for the groupware web-client "Zarafa WebApp"
URL: https://secure.freeshell.de/

(Please zoom in with your PDF viewer to see the details.)



Wk	M	T	W	T	F	S	S
5	26	27	28	29	30	31	1
6	2	3	4	5	6	7	8
7	9	10	11	12	13	14	15
8	16	17	18	19	20	21	22
9	23	24	25	26	27	28	1
10	2	3	4	5	6	7	8

Test2
Start time: Wednesday 11th February 2015 13:30

Subject	Due In
Test2	4 days overdue
Test	5 days overdue

Click Snooze to be reminded again in:
5 minutes

Of course there is always a way back. In case the Zarafa account doesn't fit your needs:
Just delete your $HOME/**.forward** file afterwards.
Now, new mail will arrive in your classic "Maildir/" style mailbox again.
Mail from the Zarafa account can be moved back using a mailclient of your choice.

ActiveSync – push services

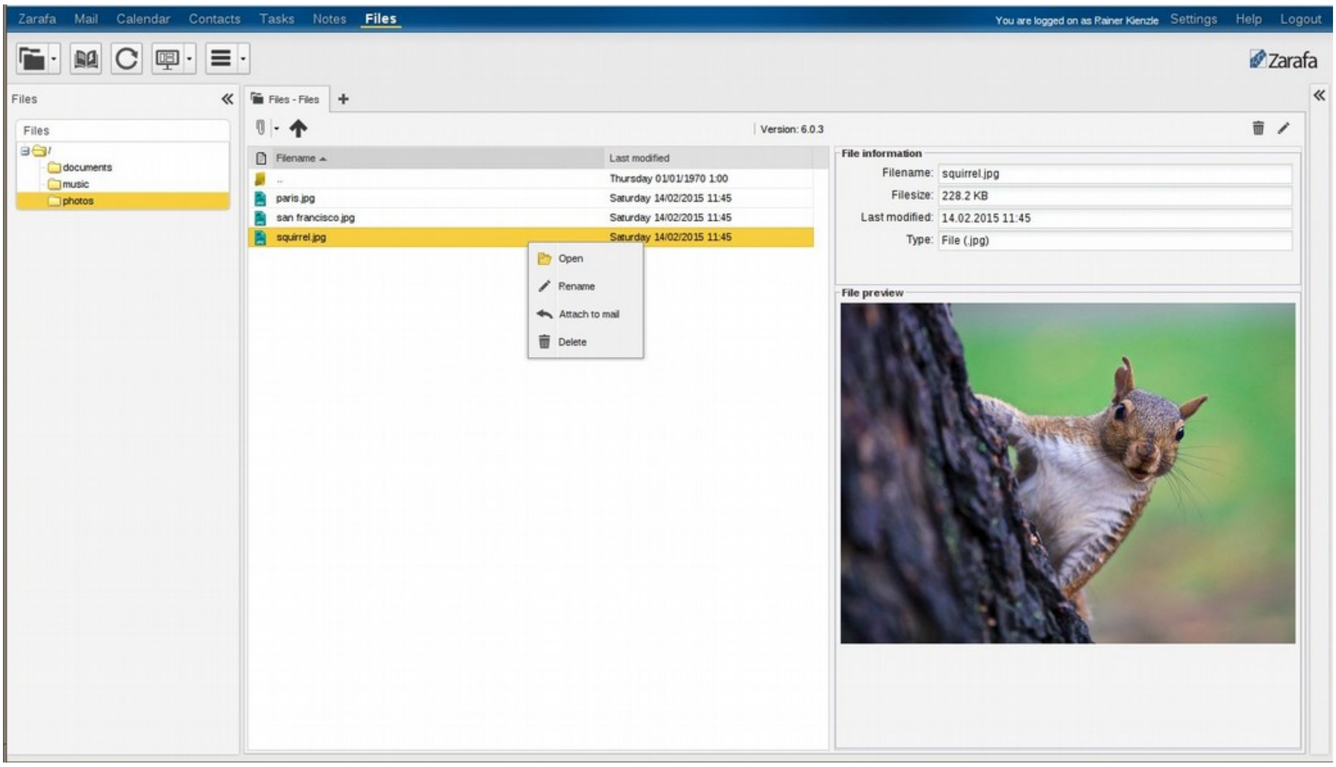
In case you use your Zarafa account, you can configure your mobile devices to sync with it. Choose “Exchange account" type and sync contacts, tasks, calendar and mail with it.

Servername: **freeshell.de**
Login and password: Just as with SSH...
Domain field: (leave empty – not mandatory)

Owncloud

URL: https://freeshell.de/owncloud/
Your account here is automatically equipped with some local owncloud storage. It's usable by browser or the native client. By the way: I mainly only support the file sharing features. All other fancy owncloud features are officially unsupported by me.

You can also configure your Zarafa Webapp to automatically use your owncloud storage:



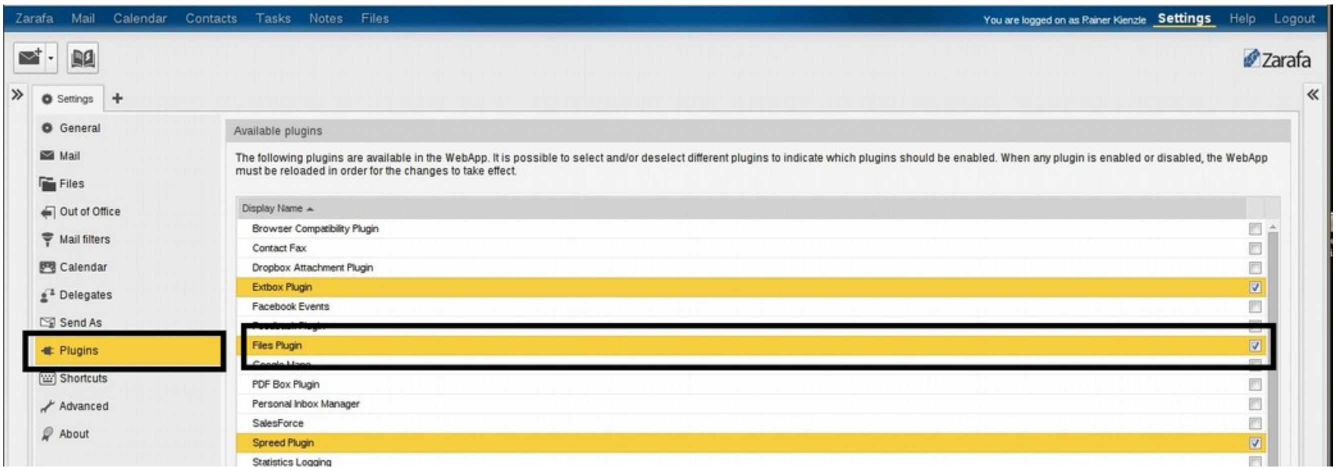
Filename	Last modified
..	Thursday 01/01/1970 1:00
paris.jpg	Saturday 14/02/2015 11:45
san francisco.jpg	Saturday 14/02/2015 11:45
squirrel.jpg	Saturday 14/02/2015 11:45

File information
Filename: squirrel.jpg
Filesize: 228.2 KB
Last modified: 14.02.2015 11:45
Type: File (.jpg)

In case the "Files"-feature in Zarafa-WebApp is not automatically enabled, here is how to do it:

- Login to Zarafa WebApp: https://secure.freeshell.de/

(Please zoom in with your PDF viewer to be able to read the instruction details.)

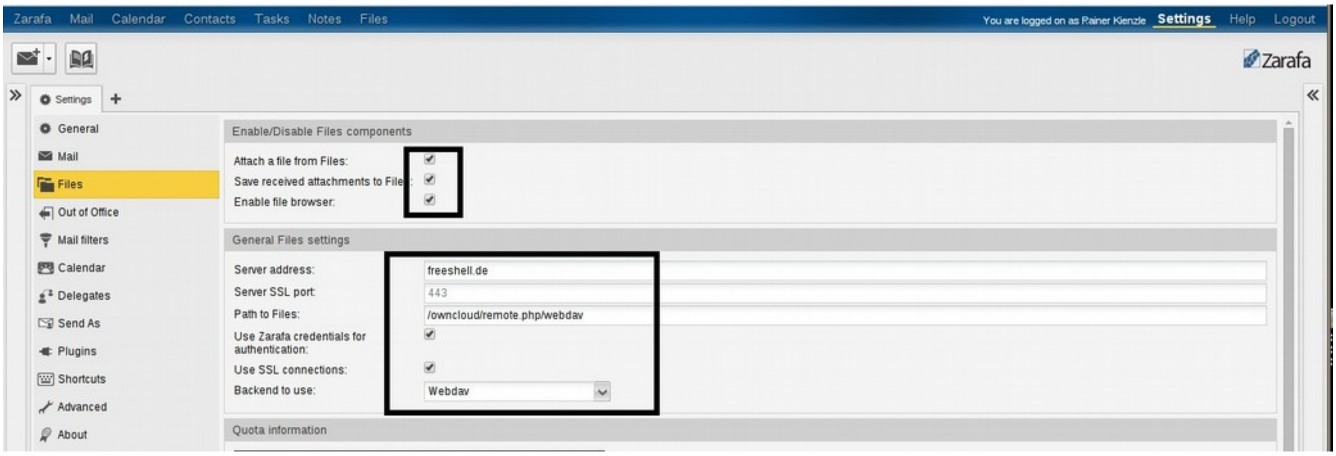


Available plugins

The following plugins are available in the WebApp. It is possible to select and/or deselect different plugins to indicate which plugins should be enabled. When any plugin is enabled or disabled, the WebApp must be reloaded in order for the changes to take effect.

Display Name ▲	
Browser Compatibility Plugin	☐
Contact Fax	☐
Dropbox Attachment Plugin	☐
Extbox Plugin	☑
Facebook Events	☐
Files Plugin	☑
PDF Box Plugin	☐
Personal Inbox Manager	☐
SalesForce	☐
Spreed Plugin	☑
Statistics Logging	☐

After that login/logoff **twice** and head back for the "Settings":



Enable/Disable Files components

Attach a file from Files: ☑
Save received attachments to Files: ☑
Enable file browser: ☑

General Files settings

Server address: freeshell.de
Server SSL port: 443
Path to Files: /owncloud/remote.php/webdav
Use Zarafa credentials for authentication: ☑
Use SSL connections: ☑
Backend to use: Webdav

Quota information

After that login/logoff **twice** again. Now owncloud storage is usable in your zarafa groupware account as well. Have fun.

Homepage / PHP / permissions

Your account automatically provides a directory where you can publish your homepage.
The URL is as follows:
http://freeshell.de/~yourlogin/
...which by the way gets automatically redirected to the secure: **https://freeshell.de/~yourlogin/**

To put content into it, that should be reachable from the outside, put it into this directory:
$HOME/public_html/
This is so to say your “document_root”.

Scripting languages

PHP v5.6.xx is installed and available; Perl (.pl / .cgi) and Python (.py) as well.

Permissions

Your base home directory (and public_html directory below that folder) are equipped with the correct minimal permissions: “**0711”** aka **drwx—x—x**
!! More won't work – less won't work !!
File permissions: PHP files need exactly “chmod 644” permissions in order to be executed here.
“777-files” for example are not executed for security reasons.

MySQL database

In case you also like a mysql database, just ask using the request form on the homepage.
PHPMyAdmin is installed here: https://freeshell.de/phpmyadmin/

Tor and anonymous surfing

This project supports and promotes anonymous surfing. “Tor” is installed and running in the server.
It is accessible through the local privoxy-proxy service as well as with “tsocks”.
Set the proxy variables as follows:

```
$ export http_proxy=”http://127.0.0.1:8118”
$ export https_proxy=”http://127.0.0.1:8118”
```

Privoxy of course keeps no log files here!

Here is an example for simple "tsocks" usage on the shell:

```
$ tsocks ssh login@where_ever_remote_place.com
```

Support and help

In case of difficulties that are not covered by the manual please leave me a message through the request form on the homepage. In case the issue requires that: Write me an encrypted email.

Hint: Most login problems derive from **fail2ban** here. The server blocks any attempts to the system from your source ip when a attempted login fails 5 times in a row. The block lasts 1 hour. This slows down brute-force attacks and is in place to protect your account.

Link collection

Links to "freeshell.de" services provided here:

- HTML5 SSH-Client: https://gate.freeshell.de/
- SquirrelMail Webmail: https://freeshell.de/squirrelmail/
- Roundcube Webmail: https://freeshell.de/rc/
- PHPMyadmin: https://freeshell.de/phpmyadmin/
- Zarafa WebApp: https://secure.freeshell.de/
- Etherpad Text collaboration: https://pad.freeshell.de/

Additional useful external links:

- Mailserver crypto check: https://ssl-tools.net/mailservers
- Webserver crypto check: https://www.ssllabs.com/
- “Tails” privacy Live-Distro: https://tails.boum.org/
- DANE-SMTP Validator: https://dane.sys4.de/
- DNSSEC Zone-Analyzer: http://dnssec-debugger.verisignlabs.com/
- DNSSEC Browser-Plugin: https://www.dnssec-validator.cz/
- Secure E-Mail Test Tools: http://checktls.com/
- Meta-RBL-Check: http://multirbl.valli.org/
- Test-Mailaddress for various Checks: test@allaboutspam.com
- Test-Mailaddress for various Checks: check-auth@verifier.port25.com

Disclaimer / Misc.

The terms and conditions as well as the data protection statement are available through the homepage www.freeshell.de on menu item "Contact".

All documents are updated regularly. Please make sure you always use the most recent version.

Remember, this is a “shared system”. Over 2100 people from literally all over the world share the server. Please treat persons with respect and use the available resources wisely!

Date: 2016-05-15 - Version 1.3