Users manual UCEPROTECT V2.4

1. System requirements

UCEPROTECT was made for i386 and compatible hardware. Other architectures can possible be used, however this will impair the efficiency of the system and therefore it cannot be supported. Multi-processor environments are also not supported at present. UCEPROTECT may run on those systems, but only make use of the first CPU.

2. Minimum requirements

Prozessor : minimum Pentium II 400 Mhz optimal: Pentium IV 2,6 GHz
Ram: minimum 128 MB RAM optimal: 512 MB DDR-RAM
Harddisk : minimum 500 MB free optimal : Some Gigs :-)

3 Supported Operating Systems

UCEPROTECT is available as a binary distribution for following Operating Systems:

1. OpenBSD – UCEPROTECT´s Development platform- therefore the best choice for you.
2. FreeBSD – is supported.
3. NetBSD – is supported.
4. Linux – is supported.

4. Before you install

The installation described in this manual assumes you are using OpenBSD. On other systems deviations can occur. In this case read the documentation of your operating system.

4.1 Install Operating System

Start your Computer using the OpenBSD-CD and install the operating system according to your desires. You find assistance for the installation of OpenBSD also online at
http://www.openbsd.org

4.2 Needed Packages

Download following Packages from the OpenBSD Portstree: PCRE, GLIBC2, POSTFIX and install them. To get assistance on installing Packages under OpenBSD type in following on the command prompt: man pkg_add

4.3 Install UCEPROTECT-Files

Create following Directorys using the mkdir command:
/usr/local/uceprotect
/usr/local/uceprotect/etc
/usr/local/uceprotect/bin
/usr/local/uceprotect/lib
/usr/local/uceprotect/sbin
/usr/local/uceprotect/var

Mount the UCEPROTECT-CD (z.B. mount /dev/cd0a /mnt) and copy all Files to the Directorys you just created on your Harddisk.
Set all Attributes to 755 under /usr/local/uceprotect/ and set User und GroupID to your desires...
Example : chown –R postfix:postdrop /usr/local/uceprotect/

4.4 Install the patched Postfix Daemon

OVERWRITE the Postfix Version from the Portstree with the Postfix you got from us ...

To do this simply decompress our postfix to /tmp and give following commands:

```
cd /tmp/postfix*
make distclean
make tidy
make
make install
```

It is a good idea to follow and simply confirm the suggested values which Postfix does on installaion.

4.5 Modify Postfix - Configuration

Edit the file /etc/postfix/main.cf so they will fit your needs and do additional following Lines at the end:

```
message_size_limit = 20480000
batch2user_destination_recipient_limit = 1
default_destination_concurrency_limit = 1
local_destination_concurrency_limit = 1
transport_destination_recipient_limit = 1
maximal_queue_lifetime = 7d
address_verify_map = hash:/tmp/verify
unverified_sender_reject_code = 550
address_verify_poll_count = 3
address_verify_poll_delay = 3s
address_verify_positive_expire_time = 31d
address_verify_positive_refresh_time = 7d
address_verify_negative_cache = yes
address_verify_negative_expire_time = 3d
address_verify_negative_refresh_time = 2h
smtpd_helo_required = yes
smtpd_helo_restictions = reject_unauth_pipelining
smtpd_sender_restrictions = reject_unknown_sender_domain
disable_vrfy_command = yes
smtpd_recipient_restrictions =
permit_sasl_authenticated,check_uceprotect,reject_multi_recipient_bounce,permit_mynetworks,reject
_unverified_sender, reject_unauth_destination
```

4.6 Adapt the UCEPROTECT Example Ruleset

Edit all Files below:
/usr/local/uceprotect/etc so they will fit your personal needs.
The Files are self-describing, because we did heavy comments – Please be shure you did also read Chapter 5 to understand the syntax.

If your UCEPROTECT-Server runs on a different Host than your MTA, you have at leaset to copy following File to the MTA-Box: /usr/local/uceprotect/etc/uceprotect.config

4.7 Test UCEPROTECT-Integration to Postfix

Start the Postfix-Daemon /usr/local/sbin/postfix start
and do following Test :

```
telnet 127.0.0.1 25
```

Your MTA welcomes you

type in helo anything

MTA should say 250 OK to this

type in: mail from: root@localhost

MTA should say 250 OK

type in: rcpt to: root@localhost

MTA should tell you after a short delay (about 120 seconds):

451 UCEPROTECT Policy Server could not be reached

This means:
Integration of UCEPROTECT into your MTA was successfull.

4.8 Start UCEPROTECT-DAEMON

Do this with following command:

/usr/local/uceprotect/sbin/uceprotect

UCEPROTECT compiles your Ruleset and puts it into your RAM.....
If you see something like ::
Done loading. UCEPROTECT V.xx ready to handle .....

all went fine ...

Your Spam-Protection system should now be up and running....

To force a Ruleset-RELOAD (necessary if you did manual changes to a running UCEROTECT) type:

/usr/local/uceprotect/bin/uceprotectctl reload

If you get strange ERRORS while loading the Daemon, please contact our technical Hotline at: + 49 – 1805 – 444894208 during the usual Business-Hours in Germany.

4.9 Test complete Installation

Repeat the Test from 4.7 . This time you should get a 250 Ok after the RCPT TO. This means, UCEPROTECT did its first Decision on your System.
You should also find something in your logfile at /usr/local/uceprotect/var/uceprotect.log

5. Syntax of UCEPROTECT-Rules

5.1 The Logic behind UCEPROTECT Rules

Normal Rules are always made of 6 Parameters, which are to write in following way:

= ip-or-hostname-of opposide senders@email recipients@email 250 OK

1 = How to interpret this Rule
2 = IP-Address or if available Hostname of the Client
3 = Claimed E-Mailaddresse of the Sender
4 = E-Mailaddress of the Reciepient
5 = SMTP-CODE / UCEPROTECT-COMMANDCODE
6 = Textmessage for Logfile and Client

Colors are here for better understanding, they do not matter to UCEPROTECT.

5.2 The Parameters at all:

Within the first 5 Parameters SPACES are interpreted as END of the actual Parameter,
within the 6. PARAMETER they are interpreted as PLAIN TEXT.

Parameter 1:
This is how to interpret the rule, actually 3 kinds of interpretation are possible:

= means FINAL CHOICE if Rules is hit and matches.
+ means NOT FINAL POSITIVE CHOICE, if it matches it becomes FINAL, if not a better matching – Rule follows.
- means NOT FINAL NEGATIVE CHOICE, if it matches it becomes FINAL if, no better matching + Rule follows.

While following Rules are not even processed on FINAL RULES, UCEPROTECT will check the complete Ruleset on NON FINAL RULES, and this way the last matching Rule wins.

You can do very powerfull Policys combining FINAL nad NOT FINAL Rules.

Parameter 2:
IPs and Hostnames of Opposides (Clients) can be given complete or in Parts, also Sublists and REGEX is possible.
Example :
1.2.3.4 means a single IP, 1.2.3.0/24 means the Net 1.2.3.0/24, but 1.2.3.* means a /24 Netz or a HOSTNAME beginning with 1.2.3.
admins.ws means a Hostnamen while for e.G *.ws stands for the TLD (COUTRYCODE).
Wildcards as * are always possible within Hostnames or IPs, you can do so interesting things as blocking all ADSL User of a Provider by doing something like following:
.adsl.provider.com would for e.G match on 1-2-3-4.adsl-standort-blabla.provider.com
* without anything else means no matter which IP oder Hostname the Client has
:local:true means Client must be Part of our local Net
:local:false means Client is not a Part of our local Net
:dns:timeout means a Timeout on DNS
:dns:false means a BOGUS DNS for the Client
:rbl:true means Client is known to the DNS-BLACKLIST (configured in unceprotect.config).
unknown means missing or wrong PTR Record
:sublist:filename means Result of Sublist filename will match (be a +)
not: can be used to negate the Result

Parameter 3:
Claimed E-Mailaddress of the Sender, Part of the E-Mail Address, Sublist or REGEX
Example:
user@abc.de for a single E-mailaddress
*@abc.de means all Addresses at Domain abc.de
any:abc.de means all Addresses at Domain abc.de and also on its Subdomains
* means E-Mailaddress does not matter
:local:true means LOCAL E-MAILADDRESS
:local:false means NOT LOCAL E-MAILADDRESS
:sublist:filename means Result of Sublist filename is Positive (+)

Parameter 4:
E-Mailaddress of the Recipient, Part of the E-MailAddress, Subliste or Regex.
Syntax identical to Parameter 3

Parameter 5:
200 means Dunno :-) Postfix has to do more Test for e.G VERIFY the Email ....
250 means Mail will become accepted
451 means Mail can temporary not be allowed (will stay at the Clients Sytsem for now ..)
550 means REJECT Mail
888 means Mail is accepted and Recipient will be added to the automatic Whitelist.
990 means Mail will be rejected and IP of the Client in combination with the Senders-Email will be blocked (automatic SOFT-BLACKLIST)
999 means Mail will be rejected and the IP of the CLIENT will become blocked (Automatic HARD BLACKLIST)

Parameter 6:
This is the Errormessage for your Logfile and also transmitted as a Plain-Text Reason to the Opposide to tell them why you did or not like their Mail :-).
Parameter 6 may contain multiple Words and Spaces, Variables or Marcos but must not be longer than 1024 SIGNS.

5.3 Examples:

Records of good Domains to your manual WHITELIST:
(File: uceprotect.250)

= * *@domain.com :local:true 250 OK

our 6 Parameter are:
= Final Choice* IP or Hostname of the Opposide does not matter
*@domain.com Each User at domain.com
:local:true Mail has to be addressed to a LOCAL E-Mail
250 ACCEPT Mail
OK CLEAR TEXT to the Opposide

Records of BANNED Domains in your manual Blacklist:
(File: uceprotect.550)

= * *@domain.com * 550 We do´nt like your Spam ...

our 6 Parameter are :
= FINAL Choice
* IP or Hostname of the Opposide does not matter
*@domain.com Each User at domain.com
* No matter to what Recipient
550 REJECT Mail
We don´t like your Spam ... CLEAT TEXT to the Opposide

Automatic Blacklisting of IPs which send Spam to your Traps:
(Spammer IPs will be added to File: uceprotect.999)

= * * sonderlocke@admins.ws 999 Game OVER :-) ...

our 6 Parameter are:
= FINAL CHOICE
* IP or Hostname of the Opposide does not matter
* Claimed E-Mail of the Sender does not matter
sonderlocke@admins.ws One of our Traps :-)
999 REJECT Mail and add the IP of the Opposide to your automatic Blacklist :-)
Game over.... CLEAR TEXT to the Opposide

Automatic Whitelisting of external RECIPIENTS:
(Your Contacts will be added to File: uceprotect.888)

= :local:true * :local:false 888 User on Whitelist

our 6 Parameters are :
= FINAL Choice
:local:true Sender is part of our local Network
* It does not matter which Emailadress we are using to send the Mail
:local:false Recipient has no LOCAL E-Mailaddress or DOMAIN
888 ACCEPT Mail and add the RECIPIENT to the automatic Whitelist
User on Whitelist CLEAR TEXT
If your MTA handles E-Mail für some hundrets or thousand Users, we suggest you do not automatic whitelist EVERY Recipient. It makes only sense to offer a Webformular, where the less users having Problems can whitelist their Emailadress.

5.4 What you should know about Sublists

In Sublists (and only there) are 4 Parameters written instead of the normal 6.
You should also not use = Rules where possible use + and – Rules only in Sublists.
+ means Result of the Sublist is a MATCH if there is no better matching – following within that Sublist.
- means Result of the Sublist is NOT MATCH if there is no better matching + following in that Sublist.
You can compare the Function of Sublists with a GUSUB in Basic :-)
If a Sublist is TRUE (Results in a +) the Commandocode (Parameter 5) and the Plain Text (Parameter 6) of this Rule will be used, which did call the Sublist.

Please note that we actually distribute following Sublists on RSYNC:

uceprotect.dialups (Defines what will be detected as DIALUP)
uceprotect.neverblacklist (List of Providers which did sign up our Anti-Abuse Contract)
uceprotect.spamdomains (List with Hardcore-Spammern Domains)
uceprotect.spamserver (List with PTRs of Hardcore-Spammer)
uceprotect.suspect (List with typical Spamwords within PTR of Clients)
uceprotect.unlogic (Defines unlogic Combinations of E-Mailadresses and Clients)

Please do not modify these Files, otherwise your Modifications would be lost with the next Update.
If you have a need to have for e.G a individual Neverblacklist, give it a unique Name for e.G. local.neverblacklist and modify your Ruleset so that it will be used.

If you have the ISP-Version of UCEPROTECT, the System uses a Sublist called : uceprotect.customers to list your automatic whitelisted Recipients.
This File should therefore contain all Domains, which your System accepts or relays Mail for.
If you have the HOME or COMPANY Version, your Domainname is hardcoded in UCEPROTECT, so the File uceprotect.customers does not even exist.

Distributed Sublist you got with your Distribution contain the Content of the Release-DATE. If there are changes for actual reasons, you can get those Modifications by RSYNC, if and ONLY IF you have a Service-Agreement with us.

5.5 Automatic Update (only with Service-Agreement)

Customers with Serviceagreement can get Modifications and Updates on a regular basis to keep your System up to date.
Actually following syncs are possible:
UCEPROTECT-Blacklists Level 1, 2 and 3 and also the UCEPROTECT-Sublists.

To do automatic Updates, your IP has to be allowed on the UCEPROTECT-Rsync Server. If you have a Service-Contract, you can request to be enabled at our Firewall at no extra charge. To do this call or mail our Hotline.

After your System is enabled install RSYNC.
You will find the newest Release at http://rsync.samba.org

Write a Cronjob at a Minute of your Choice which startes a script like like this one:

```
#/bin/sh
# UCEPROTECT-Blacklist Level 1 (Single-IPs)
rsync -avz blacklist.uceprotect.net::UCE-1 /usr/local/uceprotect/etc/
# UCEPROTECT-Blacklist Level 2 (/24 Nets)
rsync -avz blacklist.uceprotect.net::UCE-2 /usr/local/uceprotect/etc/
# UCEPROTECT-Blacklist Level 3 (Virus-Spreaders)
rsync -avz blacklist.uceprotect.net::UCE-3 /usr/local/uceprotect/etc/
# UCEPROTECT-Sublists (all)
rsync -avz blacklist.uceprotect.net::UCE-SUBLISTS /usr/local/uceprotect/etc/
# Ruleset reload
/usr/local/uceprotect/bin/uceprotectctl reload
```

5.6 Macros, Variables and Order of Rules

UCEPROTECT has some predefined Variables, which can be used within Rules in Parameter 6 or in Macros:
{ipaddress} translates to the IP-Address of the Client
{hostname} translates to the Hostname of the Client
{helo} translates to the HELO of the Client
{mailfrom} translates to Senders claimed E-Mailaddress
{rcptto} translates to Reciepients E-Mailaddress

Macros makes writing of Rules very easy, because you can use them for Text which you need in more than a single Rule. In Parameter 6 Macros and Variables and also Text can be combined. The complet Lenght of the so build Parameter 6 MAY NEVER BE LONGER than 1024 Signs. If you write BOOKS there all following Signs will be ignored. :-)
One Example Macro used by the global Blacklists of UCEPROTECT-Network is {$website}
{$website} To make an exception for your Address {mailfrom} visit http:// .....
Macros are always using the DOLLAR-SIGN, Variables DO NEVER. You have to define all the macros you need at the Beginning of the File uceprotect.rules.

After the MACROS you must tell UCEPROTECT which Rulefiles to use in which ORDER.

Lines beginning with # are interpreted as Comments and Ignored by the RULE-COMPILER.
You can use as much Rulefiles as you want, but you have to tell the Programm that they should be used by setting INCLUDER FILENAME in uceprotect.rules, but NOT Sublists. Sublists should always be called from real RULES ...

6.Tuning UCEPROTECT

If you run a „HIGH-TRAFFIC“ Mailserver with more than 200 Mails per Minute it is important, that you prevent Errors which might result in a massive Performance-Loss.

If your PC has a Attitude called „HYPERTHREADING“ in BIOS, please disable it.
Same thing for Energy Star or Energy-Save – Mode.
Prevent to use REGEX in your Rules wherever this is Possible.
One single FAST CPU is better than 2 or 4 slower ones ...(remember we only use the first one)
DO NOT SAVE MONEY ON RAM. Ram is the most important thing to UCEPROTECT, because it COMPILES YOUR RULES and LOADS THEM THERE so it is able to make very fast Decisions on Requests. Having to less, the cheapes (or worst fault-tolerant Simms in your PC) UCEPROTECT will start swapping the compiled Rules to your Harddisk, which will end up in poor Performance or cause your System to hang or become unstable.

If you use Rulesets with 100000 Lines (we are shure you will on using our distributed Blacklists :-) note that you must have lots of HIGH-QUALITY RAMs in your System.
Prevent to use automatic whitelisting to everyone you or your customers are sending mail to ...USE automatic Whitelisting for People only which would otherwise have noch chance to pass your rulesets. If you ignore this Warning you might have problems with a in Whitelist containing 20 Million Rules and a System which can handle a maximum of 4 GB Ram where you would need the double ;-).
If possible use OpenBSD as Operating System, some others have up to 10 % Performance loss.
Always use the newest UCEPROTECT-Version, so your System can always benefit from all features and goodies done to the Program.

On correct dimensioned Quality Hardware UCEPROTECT should not exceed following Values:
CPU-Last < 30 %, RAM < 30 % Cache should be between 80 and 100 %.
Test CPU and RAM on OpenBSD with Command : top
Test UCEPROTECT Cacheusage : /usr/local/uceprotect/bin/uceprotectctl stats

7. Technical Support for UCEPROTECT

7.1 Customers with Service-Agreement:

Germany : Tel. 01805 / 444 894 208
Other Countrys: Tel. +49 1805 / 444 894 208

7.2 Customers without Service-Agreement:

Germany: Tel. 0190 / 862 394 033
Austria: Tel. 0900 / 545 382 099

Other Countrys: You will be billed by PAPAL (accepts all major Credit-Cards).

Please open a Trouble-Ticket using the Contact-Form on our Website http://www.admins.ws