
Download configure file
https://drive.google.com/drive/folders/0B8kTAu8SZaHwcks5TWdoTW1ENG8?usp=sharing
---
sa-update
freshclam -v
systemctl daemon-reload
systemctl restart spamassassin
systemctl restart clamd@amavisd
systemctl restart amavisd.service
systemctl restart dovecot
systemctl restart postfix
systemctl status amavisd.service

yum -y update amavisd-new* spamassassin clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd

useradd -m -p VCX97jg6iZebc -s /bin/false virusalert
useradd -m -p VCX97jg6iZebc -s /bin/false spamalert
useradd -m -p VCX97jg6iZebc -s /bin/false spam.police
useradd -m -p VCX97jg6iZebc -s /bin/false junkmail

 # vi /etc/postfix/aliases
virusalert: root,junkmail
spam.police: root,junkmail
spamalert: root,junkmail

RELEASING A MESSAGE FROM A QUARANTINE WITH AMAVISD-RELASE

[root@mail ~]# **amavisd-release spam-1lvc624m6MVB.gz**
[root@mail ~]# **cd /var/spool/amavisd/quarantine** [virus Location]
du -h --max-depth=1

Postfix with amavisd, spamassassin, and clamav

yum install -y epel-release

yum install -y amavisd*

yum --enablerepo=epel -y install amavisd-new* spamassassin clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd unzip bzip2 perl-DBD-mysql

yum install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd

vi /etc/freshclam.conf

Comment or remove the line below.

#Example

DatabaseDirectory /var/lib/clamav

 # ls /var/lib/clamav/

daily.cvd main.cvd

vi /etc/sysconfig/freshclam

FRESHCLAM_DELAY=disabled-warn # REMOVE ME

#Manually run antivirus Signature update

 # freshclam

 # ls /var/lib/clamav/

bytecode.cvd daily.cld main.cvd main.cvd.broken mirrors.dat

Clamv signature update control

 # vi /etc/cron.d/clamav-update

Adjust this line...
MAILTO=root

It is ok to execute it as root; freshclam drops privileges and becomes
user 'clamupdate' as soon as possible
0 */3 * * * root /usr/share/clamav/freshclam-sleep

~

---

cp /etc/clamd.d/scan.conf /etc/clamd.conf

 # vi /etc/clamd.conf

Comment or remove the line below.

#Example

DatabaseDirectory /var/lib/clamav

#LocalSocket /var/run/clamd.scan/clamd.socket

LocalSocket "/var/run/clamd.amavisd/clamd.sock"

#User **clamscan**

User **amavis**

ScanMail yes

- ----------

clamd.amavisd

```
[root@mail ~]# cp /usr/share/doc/clamav-server*/clamd.sysconfig /etc/sysconfig/clamd.amavisd

[root@mail ~]# vi /etc/sysconfig/clamd.amavisd

# line 1, 2: uncomment and change

CLAMD_CONFIGFILE=/etc/clamd.d/amavisd.conf

CLAMD_SOCKET=/var/run/clamd.amavisd/clamd.sock


[root@mail ~]# vi /etc/tmpfiles.d/clamd.amavisd.conf

# create new

d /var/run/clamd.amavisd 0755 amavis amavis -


[root@mail ~]# vi /usr/lib/systemd/system/clamd@.service

# add to the end

[Install]

WantedBy=multi-user.target
```

systemctl start clamd@amavisd
systemctl enable clamd@amavisd

systemctl restart clamd@amavisd

====clamd configuration check=======

clamconf

Checking configuration files in /etc

Config file: clamd.conf

LogFile disabled

StatsHostID disabled

StatsEnabled disabled

StatsPEDisabled disabled

StatsTimeout disabled

LogFileUnlock disabled

LogFileMaxSize = "1048576"

LogTime disabled

LogClean disabled

LogSyslog = "yes"

LogFacility = "LOG_LOCAL6"

LogVerbose disabled

LogRotate disabled

ExtendedDetectionInfo disabled

PidFile disabled

TemporaryDirectory disabled

DatabaseDirectory = "/var/lib/clamav"

OfficialDatabaseOnly disabled

LocalSocket = "/var/run/clamd.amavisd/clamd.sock"

LocalSocketGroup disabled

LocalSocketMode disabled

FixStaleSocket = "yes"

TCPSocket disabled

TCPAddr disabled

MaxConnectionQueueLength = "200"

StreamMaxLength = "26214400"

StreamMinPort = "1024"

StreamMaxPort = "2048"

MaxThreads = "10"

ReadTimeout = "120"

CommandReadTimeout = "5"

SendBufTimeout = "500"

MaxQueue = "100"

IdleTimeout = "30"

ExcludePath disabled

MaxDirectoryRecursion = "15"

FollowDirectorySymlinks disabled

FollowFileSymlinks disabled

CrossFilesystems = "yes"

SelfCheck = "600"

DisableCache disabled

VirusEvent disabled

ExitOnOOM disabled

AllowAllMatchScan = "yes"

Foreground disabled

Debug disabled

LeaveTemporaryFiles disabled

User = "amavis"

AllowSupplementaryGroups = "yes"

Bytecode = "yes"

BytecodeSecurity = "TrustSigned"

BytecodeTimeout = "5000"

BytecodeUnsigned disabled

BytecodeMode = "ForceInterpreter"

DetectPUA disabled

ExcludePUA disabled

IncludePUA disabled

AlgorithmicDetection = "yes"

ScanPE = "yes"

ScanELF = "yes"

DetectBrokenExecutables disabled

ScanMail = "yes"

ScanPartialMessages disabled

PhishingSignatures = "yes"

PhishingScanURLs = "yes"

PhishingAlwaysBlockCloak disabled

PhishingAlwaysBlockSSLMismatch disabled

PartitionIntersection disabled

HeuristicScanPrecedence disabled

StructuredDataDetection disabled

StructuredMinCreditCardCount = "3"

StructuredMinSSNCount = "3"

StructuredSSNFormatNormal = "yes"

StructuredSSNFormatStripped disabled

ScanHTML = "yes"

ScanOLE2 = "yes"

OLE2BlockMacros disabled

ScanPDF = "yes"

ScanSWF = "yes"

ScanXMLDOCS = "yes"

ScanHWP3 = "yes"

ScanArchive = "yes"

ArchiveBlockEncrypted disabled

ForceToDisk disabled

MaxScanSize = "104857600"

MaxFileSize = "26214400"

MaxRecursion = "16"

MaxFiles = "10000"

MaxEmbeddedPE = "10485760"

MaxHTMLNormalize = "10485760"

MaxHTMLNoTags = "2097152"

MaxScriptNormalize = "5242880"

MaxZipTypeRcg = "1048576"

MaxPartitions = "50"

MaxIconsPE = "100"

MaxRecHWP3 = "16"

PCREMatchLimit = "10000"

PCRERecMatchLimit = "5000"

PCREMaxFileSize = "26214400"

ScanOnAccess disabled

OnAccessMountPath disabled

OnAccessIncludePath disabled

OnAccessExcludePath disabled

OnAccessExcludeUID disabled

OnAccessMaxFileSize = "5242880"

OnAccessDisableDDD disabled

OnAccessPrevention disabled

OnAccessExtraScanning disabled

DevACOnly disabled

DevACDepth disabled

DevPerformance disabled

DevLiblog disabled

DisableCertCheck disabled

Config file: freshclam.conf

StatsHostID disabled

StatsEnabled disabled

StatsTimeout disabled

LogFileMaxSize = "1048576"

LogTime disabled

LogSyslog = "yes"

LogFacility = "LOG_LOCAL6"

LogVerbose disabled

LogRotate disabled

PidFile disabled

DatabaseDirectory = "/var/lib/clamav"

Foreground disabled

Debug disabled

AllowSupplementaryGroups disabled

UpdateLogFile disabled

DatabaseOwner = "clamupdate"

Checks = "12"

DNSDatabaseInfo = "current.cvd.clamav.net"

DatabaseMirror = "database.clamav.net"

PrivateMirror disabled

MaxAttempts = "3"

ScriptedUpdates = "yes"

TestDatabases = "yes"

CompressLocalDatabase disabled

ExtraDatabase disabled

DatabaseCustomURL disabled

HTTPProxyServer disabled

HTTPProxyPort disabled

HTTPProxyUsername disabled

HTTPProxyPassword disabled

HTTPUserAgent disabled

NotifyClamd = "/etc/clamd.conf"

OnUpdateExecute disabled

OnErrorExecute disabled

OnOutdatedExecute disabled

LocalIPAddress disabled

ConnectTimeout = "30"

ReceiveTimeout = "30"

SubmitDetectionStats disabled

DetectionStatsCountry disabled

DetectionStatsHostID disabled

SafeBrowsing disabled

Bytecode = "yes"

clamav-milter.conf not found

Software settings

Version: 0.99.1

Optional features supported: MEMPOOL IPv6 AUTOIT_EA06 BZIP2 LIBXML2 PCRE ICONV JIT

Database information

Database directory: /var/lib/clamav

daily.cld: version 21539, sigs: 141475, built on Fri May 13 09:56:52 2016

bytecode.cvd: version 277, sigs: 47, built on Fri Apr 15 11:57:09 2016

main.cvd: version 57, sigs: 4218790, built on Wed Mar 16 16:17:06 2016

Total number of signatures: 4360312

Platform information

---

uname: Linux 3.10.0-327.13.1.el7.x86_64 #1 SMP Thu Mar 31 16:04:38 UTC 2016 x86_64

OS: linux-gnu, ARCH: x86_64, CPU: x86_64

zlib version: 1.2.7 (1.2.7), compile flags: a9

Triple: x86_64-redhat-linux-gnu

CPU: i686, Little-endian

platform id: 0x0a21525208040805030408 05

Build information

GNU C: 4.8.5 20150623 (Red Hat 4.8.5-4) (4.8.5)

GNU C++: 4.8.5 20150623 (Red Hat 4.8.5-4) (4.8.5)

CPPFLAGS:

CFLAGS: -O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic -Wall -W -Wmissing-prototypes -Wmissing-declarations -std=gnu99 -fno-strict-aliasing -D_LARGEFILE_SOURCE -D_LARGEFILE64_SOURCE

CXXFLAGS: -O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic -std=gnu++98

LDFLAGS: -Wl,-z,relro -specs=/usr/lib/rpm/redhat/redhat-hardened-ld -Wl,--as-needed

Configure: '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--program-prefix=' '--disable-dependency-tracking' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--disable-static' '--disable-rpath' '--disable-silent-rules' '--disable-clamav' '--with-user=clamupdate' '--with-group=clamupdate' '--with-libcurl=/usr' '--with-dbdir=/var/lib/clamav' '--enable-milter' '--enable-clamdtop' '--disable-unrar' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic -Wall -W -Wmissing-prototypes -Wmissing-declarations -std=gnu99' 'LDFLAGS=-Wl,-z,relro -specs=/usr/lib/rpm/redhat/redhat-hardened-ld -Wl,--as-needed' 'PKG_CONFIG_PATH=:/usr/lib64/pkgconfig:/usr/share/pkgconfig' --enable-ltdl-convenience

sizeof(void*) = 8

Engine flevel: 82, dconf: 82

======Database directory in both clamd.conf and freshclam.conf must point to the same location======

Confirm the clamav signature update by clamconf

Database information

Database directory: /var/lib/clamav

daily.cld: version 21543, sigs: 142010, built on Sat May 14 01:57:02 2016

bytecode.cvd: version 277, sigs: 47, built on Fri Apr 15 11:57:09 2016

main.cvd: version 57, sigs: 4218790, built on Wed Mar 16 16:17:06 2016

Total number of signatures: 4360847

Database information

Database directory: /var/lib/clamav

daily.cld: version 21552, sigs: 143202, built on Sun May 15 13:57:39 2016

bytecode.cvd: version 277, sigs: 47, built on Fri Apr 15 11:57:09 2016

main.cvd: version 57, sigs: 4218790, built on Wed Mar 16 16:17:06 2016

Total number of signatures: 4362039

===good===

---

amavisd ===>Reference

When amavisd-new is installed, the user:amavis is created. The amavisd-new will run as amavis. The clamd.conf is set to run as amavis, too. Both processes must run under the same user.

 # cat /etc/group | grep amavis

amavis:x:983:

 # cat /etc/passwd | grep amavis

amavis:x:988:983:User for amavisd-new:/var/spool/amavisd:/sbin/nologin

 # ls /var/spool/amavisd/

db quarantine tmp

The directory of /var/run/clamd.amavisd exists.

====***====

$ (dollar character)
indicates a scalar variable (a string, a number, a reference)
@ (at sign)
indicates an array variable (a list)

 # cp /etc/amavisd/amavisd.conf /etc/amavisd/amavisd.conf.ORG

vi /etc/amavisd/amavisd.conf

```
# To disable virus or spam checks, uncomment the following:
# to enable virus or spam checks, leave the commented out
# @bypass_virus_checks_maps = (1);  # controls running of anti-virus code
# @bypass_spam_checks_maps  = (1);  # controls running of anti-spam code
# $bypass_decode_parts = 1;         # controls running of decoders & dearchivers
#don't change the following lines
$max_servers = 2;                 # num of pre-forked children (2..30 is common), -m
$daemon_user  = "amavis";          # (no default;  customary: vscan or amavis), -u
$daemon_group = "amavis";          # (no default;  customary: vscan or amavis), -g
$helpers_home = "$MYHOME/var";             # Uncomment: working directory for SpamAssassin, -S
$myhostname = 'mail.1ask2.com';
$mydomain = '1ask2.com';
$MYHOME = '/var/spool/amavisd';
$inet_socket_port = 10024;         # listen on this local TCP port(s)
$notify_method  = 'smtp:[127.0.0.1]:10025';
$forward_method = 'smtp:[127.0.0.1]:10025';  # set to undef with milter!
#SpamAssassin settings which override the default SpamAssassin settings:
$sa_tag_level_deflt  = 2.0;               # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.2;               # add 'spam detected' headers at that level
$sa_kill_level_deflt = 6.9;               # triggers spam evasive actions (e.g. blocks mail)
$sa_dsn_cutoff_level = 10;                # spam level beyond which a DSN is not sent
# $sa_quarantine_cutoff_level = 25;       # spam level beyond which quarantine is off
$penpals_bonus_score = 8;                 # (no effect without a @storage_sql_dsn database)
$penpals_threshold_high = $sa_kill_level_deflt;         # don't waste time on hi spam
$bounce_killer_score = 100;               # spam score points to add for joe-jobbed bounces
$sa_mail_body_size_limit = 400*1024;      # don't waste time on SA if mail is larger
```

```
$sa_local_tests_only = 0;               # only tests which do not require internet access?
##uncomment the section for ClamAV-clamd  #    ### http://www.clamav.net/
 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamd.amavisd/clamd.sock"],
   qr/\bOK$/m, qr/\bFOUND$/m,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
 # NOTE: run clamd under the same user as amavisd - or run it under its own
 #   uid such as clamav, add user clamav to the amavis group, and then add
 #   AllowSupplementaryGroups to clamd.conf;
 # NOTE: match socket name (LocalSocket) in clamd.conf to the socket name in
 #   this entry; when running chrooted one may prefer a socket under $MYHOME.

$unix_socketname = "/var/run/amavisd/amavisd.sock"; #amavisd-release. Need to confirm???

#The clamd runs in LocalSocket /var/run/clamd.amavisd/clamd.sock. The amavisd-new will access this socket.

#Many other antivirus scanners are included but commentted out.

====***====

The amavisd-new links both spamassasin and clamav.

===***====

nano /etc/postfix/master.cf

copy & paste the configuration from https://wiki.centos.org/HowTos/Amavisd

amavisfeed unix  -       -       n       -       2       lmtp
   -o lmtp_data_done_timeout=1200
   -o lmtp_send_xforward_command=yes
   -o disable_dns_lookups=yes
   -o max_use=20
127.0.0.1:10025 inet n  -       n       -       -       smtpd
   -o content_filter=
   -o smtpd_delay_reject=no
   -o smtpd_client_restrictions=permit_mynetworks,reject
   -o smtpd_helo_restrictions=
   -o smtpd_sender_restrictions=
   -o smtpd_recipient_restrictions=permit_mynetworks,reject
   -o smtpd_data_restrictions=reject_unauth_pipelining
   -o smtpd_end_of_data_restrictions=
   -o smtpd_restriction_classes=
   -o mynetworks=127.0.0.0/8
   -o smtpd_error_sleep_time=0
   -o smtpd_soft_error_limit=1001
   -o smtpd_hard_error_limit=1000
   -o smtpd_client_connection_count_limit=0
   -o smtpd_client_connection_rate_limit=0
   -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters,no_address_mappings
   -o local_header_rewrite_clients=
   -o smtpd_milters=
   -o local_recipient_maps=
   -o relay_recipient_maps=
```

----------OR----------

```
smtp-amavis unix        -       -       n       -       2 smtp
    -o lmtp_data_done_timeout=1200
    -o lmtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20
127.0.0.1:10025 inet n  -       n       -       -       smtpd
    -o content_filter=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
    -o smtpd_end_of_data_restrictions=
    -o smtpd_restriction_classes=
    -o mynetworks=127.0.0.0/8
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters,no_address_mappings
    -o local_header_rewrite_clients=
    -o smtpd_milters=
    -o local_recipient_maps=
    -o relay_recipient_maps=


#########
$ amavisfeed unix –             –       n       –       2       lmtp
-o lmtp_data_done_timeout=1200
-o lmtp_send_xforward_command=yes
# define a service to inject mail back into Postfix
127.0.0.1:10025 inet n          –       n       –       –       smtpd
-o content_filter=
-o smtpd_delay_reject=no
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o smtpd_data_restrictions=reject_unauth_pipelining
-o smtpd_end_of_data_restrictions=
-o smtpd_restriction_classes=
-o mynetworks=127.0.0.0/8
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o smtpd_client_connection_count_limit=0
-o smtpd_client_connection_rate_limit=0
```

-o receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters,no_address_mappings
-o local_header_rewrite_clients=
-o smtpd_milters=
-o local_recipient_maps=
-o relay_recipient_maps=

 # vi /etc/postfix/main.cf

```
content_filter=amavisfeed:[127.0.0.1]:10024
```

----------OR----------

```
content_filter=smtp-amavis:[127.0.0.1]:10024
#receive_override_options = no_address_mappings
enable_original_recipient = no
```

systemctl restart postfix
systemctl enable amavisd.service
systemctl start amavisd.service
systemctl status amavisd.service

 # netstat -lptn

When amavisd.service starts, it starts the clamd daemon.

 # ps aux | grep clamd

```
root      6226  0.0  0.0 112644   956 pts/1    S+   13:39   0:00 grep --color=auto clamd
amavis   30715  0.4  1.6 858796 548988 ?       Ssl  12:33   0:17 /usr/sbin/clamd -c /etc/clamd.d/amavisd.conf --foreground=yes
```

The daemon clamd is using the configuration file /etc/clamd.d/amavisd.conf.

 # vi /etc/clamd.d/amavisd.conf

```
 # Use system logger.
LogSyslog yes

# Specify the type of syslog messages - please refer to 'man syslog'
# for facility names.
LogFacility LOG_MAIL

# This option allows you to save a process identifier of the listening
# daemon (main thread).
PidFile /var/run/clamd.amavisd/clamd.pid

# Remove stale socket after unclean shutdown.
```

```
# Default: disabled
FixStaleSocket yes

# Run as a selected user (clamd must be started by root).
User amavis

# Path to a local socket file the daemon will listen on.
LocalSocket /var/run/clamd.amavisd/clamd.sock
```

 # vi /usr/lib/systemd/system/amavisd.service

```
[Unit]
Description=Amavisd-new is an interface between MTA and content checkers.
Documentation=http://www.ijs.si/software/amavisd/#doc
After=network.target
Wants=clamd@amavisd.service
Wants=postfix.service

[Service]
Type=forking
User=amavis
Group=amavis
PIDFile=/var/run/amavisd/amavisd.pid
ExecStart=/usr/sbin/amavisd -c /etc/amavisd/amavisd.conf
ExecReload=/usr/sbin/amavisd -c /etc/amavisd/amavisd.conf reload
Restart=on-failure
PrivateTmp=true
NoNewPrivileges=true

[Install]
WantedBy=multi-user.target
```

To check the clamav configuration with clamconf

clamconf #Search for configuration files clamd.conf and freshclam.conf in /etc/

clamconf -c /etc/clamd.d/ # Search for configuration files clamd.conf and freshclam.conf in /etc/clamd.d/

with /usr/sbin/amavisd -c /etc/clamd.conf.

=== **# clamconf -c /etc/clamd.d/**

Checking configuration files in /etc/clamd.d/

clamd.conf not found

freshclam.conf not found

clamav-milter.conf not found

To use the clamconf command, better to modify amavisd.service

vi /usr/lib/systemd/system/clamd@.service

[Unit]
Description = clamd scanner (%i) daemon
After = syslog.target nss-lookup.target network.target

[Service]
Type = simple
ExecStart = /usr/sbin/clamd -c /etc/clamd.d/%i.conf --foreground=yes
Restart = on-failure
PrivateTmp = true

[Install]
WantedBy=multi-user.target

-------XXXXXX---------

[Unit]

Description = clamd scanner (%i) daemon

After = syslog.target nss-lookup.target network.target

[Service]

Type = simple

ExecStart = /usr/sbin/clamd -c /etc/clamd.conf --nofork=yes

#ExecStart = /usr/sbin/clamd -c /etc/clamd.d/%i.conf --nofork=yes

Restart = on-failure

PrivateTmp = true

=====

freshclam

ClamAV update process started at Wed May 18 08:25:45 2016

WARNING: Your ClamAV installation is OUTDATED!

WARNING: Local version: 0.99.1 Recommended version: 0.99.2

DON'T PANIC! Read http://www.clamav.net/documents/upgrading-clamav

main.cvd is up to date (version: 57, sigs: 4218790, f-level: 60, builder: amishhammer)

daily.cld is up to date (version: 21567, sigs: 151662, f-level: 63, builder: neo)

bytecode.cvd is up to date (version: 277, sigs: 47, f-level: 63, builder: neo)

clamconf

Database information

Database directory: /var/lib/clamav

bytecode.cvd: version 277, sigs: 47, built on Fri Apr 15 11:57:09 2016

main.cvd: version 57, sigs: 4218790, built on Wed Mar 16 16:17:06 2016

daily.cld: version 21567, sigs: 151662, built on Wed May 18 06:01:22 2016

Total number of signatures: 4370499

Why does the /var/log/maillog records "clamd[20396]: Loaded 4365110 signatures."?

After I kill the clamd process and manually start clamd, "clamd[20454]: Not loading PUA signatures." is logged.

 # vi /etc/clamd.conf

Detect Possibly Unwanted Applications.

Default: no

DetectPUA yes

When "DetectPUA yes", clamd will load 4370499 signatures.

---

reboot

========

ps aux | grep "amavis*"

amavis 3141 0.4 0.3 381492 119968 ? S 13:14 0:09 /usr/sbin/amavisd (ch10-avail)
amavis 3435 0.3 0.3 378652 117540 ? S 13:19 0:06 /usr/sbin/amavisd (ch7-avail)
postfix 6643 0.0 0.0 91528 4296 ? S 13:44 0:00 smtp -n smtp-amavis -t unix -u -o lmtp_data_done_timeout=1200 -o lmtp_send_xforward_command=yes -o disable_dns_lookups=yes -o max_use=20
root 6702 0.0 0.0 112648 964 pts/1 S+ 13:45 0:00 grep --color=auto amavis*
amavis 30715 0.4 1.6 858796 548988 ? Ssl 12:33 0:17 /usr/sbin/clamd -c /etc/clamd.d/amavisd.conf --foreground=yes
amavis 30920 0.0 0.3 367976 108088 ? Ss 12:33 0:01 /usr/sbin/amavisd (master)

---

test for spam

hotmail to 1ask2.com with body:

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

/var/log/maillog
amavis[3069]: (03069-04) Blocked SPAM {DiscardedInbound,Quarantined}, [65.55.111.147]:64821 <kmliao@hotmail.com> -> <sam@1ask2.com>

test for virus

urbanselect.com to 1ask2.com with a virus attachment.

/var/log/maillog
mavis[3069]: (03069-06) Blocked INFECTED (Clamav.Test.File-6) {DiscardedInbound,Quarantined}, [184.68.29.198]:54809 [184.68.29.198] <administrator@urbanselect.com> -> <sam@1ask2.com>,

---

Spamassassin update

 # vi /etc/cron.d/sa-update

========

Spamassassin Conf

Block email that has Chinese language

vi /etc/mail/spamassassin/v310.pre

AWL - do auto-whitelist checks

#

loadplugin Mail::SpamAssassin::Plugin::AWL

TextCat - language guesser

#

loadplugin Mail::SpamAssassin::Plugin::TextCat

vi /etc/mail/spamassassin/local.cf

required_hits 5

report_safe 0

rewrite_header Subject [SPAM]

ok_languages en

score UNWANTED_LANGUAGE_BODY 8.0

=====send an email with enough Chinese letters===

Blocked SPAM {DiscardedInbound,Quarantined}

sa-update -D

Update spamassassin rules

sa-update --nogpg

Restart postfix - spamassassin

systemctl enable spamassassin

systemctl start spamassassin

systemctl restart spamassassin

systemctl restart postfix

Check if spamassassin is listening

ss -tnlp | grep spamd

---------don't know what the spam score is?====

vi /etc/amavisd/amvisd.conf

vi /etc/amavisd/amavisd.conf

Update spamassassin rules

sa-update --nogpg

Restart postfix - spamassassin

systemctl enable spamassassin

systemctl start spamassassin

systemctl restart spamassassin

systemctl restart postfix

Check if spamassassin is listening

ss -tnlp | grep spamd

#$sa_kill_level_deflt = 6.9; # triggers spam evasive actions (e.g. blocks mail)

systemctl restart amavisd

email with English and Chinese

X-Virus-Scanned: amavisd-new at 1ask2.com

X-Spam-Flag: NO

X-Spam-Score: 4.919

X-Spam-Level: ****

X-Spam-Status: No, score=4.919 tagged_above=2 required=6.2 tests=[AWL=2.250,

BODY_8BITS=1.5, DNS_FROM_AHBL_RHSBL=2.438, FREEMAIL_FROM=0.001,

HTML_MESSAGE=0.001, RCVD_IN_DNSWL_LOW=-0.7, RCVD_IN_MSPIKE_H3=-0.01,

RCVD_IN_MSPIKE_WL=-0.01, RP_MATCHES_RCVD=-0.55, SPF_PASS=-0.001]

autolearn=no autolearn_force=no

email with Chinese only

X-Virus-Scanned: amavisd-new at 1ask2.com

X-Spam-Flag: YES

X-Spam-Score: 8.178

X-Spam-Level: ********

X-Spam-Status: Yes, score=8.178 tagged_above=2 required=6.2 tests=[AWL=-2.510,

BODY_8BITS=1.5, DNS_FROM_AHBL_RHSBL=2.438, FREEMAIL_FROM=0.001,

HTML_MESSAGE=0.001, RCVD_IN_DNSWL_LOW=-0.7, RCVD_IN_MSPIKE_H2=-0.001,

RP_MATCHES_RCVD=-0.55, SPF_PASS=-0.001, UNWANTED_LANGUAGE_BODY=8]

autolearn=no autolearn_force=no

==========Stop 125.71.228.113---backscatterer==

vi /etc/postfix/clientaccess

125.71.228.113 REJECT

postmap /etc/postfix/clientaccess

/var/log/maillog

May 16 15:02:04 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:02:04 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:02:14 c1 postfix/smtpd[5629]: connect from unknown[193.189.117.149]

May 16 15:02:14 c1 postfix/smtpd[5629]: lost connection after AUTH from unknown[193.189.117.149]

May 16 15:02:14 c1 postfix/smtpd[5629]: disconnect from unknown[193.189.117.149]

May 16 15:02:34 c1 postfix/smtpd[5549]: timeout after END-OF-MESSAGE from localhost[127.0.0.1]

May 16 15:02:34 c1 postfix/smtpd[5549]: disconnect from localhost[127.0.0.1]

May 16 15:03:12 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:03:12 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:03:13 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:04:23 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:04:23 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:04:24 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:05:34 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:05:37 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:05:37 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:06:57 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:06:57 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:06:57 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:08:02 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:08:03 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:08:03 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:09:05 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:09:06 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:09:06 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:09:11 c1 postfix/anvil[4993]: statistics: max connection rate 1/60s for (smtp:65.55.111.161) at May 16 15:00:23

May 16 15:09:11 c1 postfix/anvil[4993]: statistics: max connection count 1 for (smtp:65.55.111.161) at May 16 15:00:23

May 16 15:09:11 c1 postfix/anvil[4993]: statistics: max cache size 7 at May 16 15:02:14

125.71.228.113May 16 15:10:10 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:10:11 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:10:11 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:10:25 c1 clamd[1464]: SelfCheck: Database status OK.

May 16 15:11:16 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:11:17 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:11:17 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:12:35 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:12:35 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:12:36 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:13:39 c1 postfix/smtpd[5586]: connect from unknown[125.71.228.113]

May 16 15:13:39 c1 postfix/smtpd[5586]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [125.71.228.113]; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:13:39 c1 postfix/smtpd[5586]: disconnect from unknown[125.71.228.113]

May 16 15:14:45 c1 postfix/smtpd[5586]: table hash:/etc/postfix/clientaccess has changed -- restarting

May 16 15:14:45 c1 postfix/smtpd[5765]: connect from unknown[125.71.228.113]

May 16 15:14:45 c1 postfix/smtpd[5765]: NOQUEUE: reject: RCPT from unknown[125.71.228.113]: 554 5.7.1 <unknown[125.71.228.113]>: Client host rejected: Access denied; from=<> to=<bn@orienttechs.com> proto=ESMTP helo=<MS-SM-CH0.std.uestc.edu.cn>

May 16 15:14:45 c1 postfix/smtpd[5765]: disconnect from unknown[125.71.228.113]

May 16 15:18:06 c1 postfix/anvil[4993]: statistics: max connection rate 1/60s for (smtp:125.71.228.113) at May 16 15:10:10

May 16 15:18:06 c1 postfix/anvil[4993]: statistics: max connection count 1 for (smtp:125.71.228.113) at May 16 15:10:10

May 16 15:18:06 c1 postfix/anvil[4993]: statistics: max cache size 1 at May 16 15:10:10

--------from198.57.136.73 ----

telnet 127.0.0.1 25

mail from:kmliao@hotmail.com

250 OK

rcpt to:sam@1ask2.com

250 Accepted

data

354 Enter message, ending with "." on a line by itself

Subject:Security Alert

Hostgator

.

250 OK id=1b2gsQ-0003os-Pd

------#######-------

/var/log/maillog

amavis[14256]: (14256-01) Blocked BAD-HEADER-0 {BouncedInbound,Quarantined}, [198.57.136.73]

===The telnet method is the best way to compose an email with different fields, though!===

To make the telnet work,

nano /etc/amavisd/amavisd.conf

@bypass_header_checks_maps =([qw(sam@1ask2.com)]);

#@bypass_header_checks_maps is relevant to rcpt to field.

---message header---

Received: from c1.1ask2.com (191.121.6.30) by spam.1ask2.com (191.121.6.20)

with Microsoft SMTP Server id 14.3.294.0; Wed, 18 May 2016 09:39:13 -0700

Received: from localhost (localhost [127.0.0.1]) by c1.1ask2.com (Postfix)

with ESMTP id 0DD8CC3CC4CA for <sam@1ask2.com>; Wed, 18 May 2016 09:41:25

-0700 (PDT)

X-Virus-Scanned: amavisd-new at 1ask2.com

X-Spam-Flag: NO

X-Spam-Score: 5.99

X-Spam-Level: *****

X-Spam-Status: No, score=5.99 tagged_above=2 required=6.2

tests=[FREEMAIL_FROM=0.001, MISSING_DATE=1.396, MISSING_FROM=1,

MISSING_HEADERS=1.207, MISSING_MID=0.14, RDNS_NONE=1.274,

SPF_SOFTFAIL=0.972] autolearn=no autolearn_force=no

Received: from c1.1ask2.com ([127.0.0.1]) by localhost (mail.1ask2.com

[127.0.0.1]) (amavisd-new, port 10024) with LMTP id TFQwEJKCDUrd for

<sam@1ask2.com>; Wed, 18 May 2016 09:41:19 -0700 (PDT)

Received-SPF: softfail (hotmail.com: Sender is not authorized by default to use 'kmliao@hotmail.com' in 'mfrom' identity, however domain is not currently prepared for false failures (mechanism '~all' matched)) receiver=c1.1ask2.com; identity=mailfrom; envelope-from="kmliao@hotmail.com"; helo=van.vanarts.com; client-ip=198.57.136.73

Received: from van.vanarts.com (unknown [198.57.136.73]) by c1.1ask2.com

(Postfix) with ESMTP id AF85FC3CC4BA for <sam@1ask2.com>; Wed, 18 May 2016

09:41:18 -0700 (PDT)

Received: from [127.0.0.1] (port=39658 helo=hotmail.com) by van.vanarts.com

with esmtp (Exim 4.87) (envelope-from <kmliao@hotmail.com>) id

1b34Y2-00011V-KB for sam@1ask2.com; Wed, 18 May 2016 11:42:29 -0500

Subject: Ten Dollar

X-AntiAbuse: This header was added to track abuse, please include it with any abuse report

X-AntiAbuse: Primary Hostname - van.vanarts.com

X-AntiAbuse: Original Domain - 1ask2.com

X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]

X-AntiAbuse: Sender Address Domain - hotmail.com

X-Get-Message-Sender-Via: van.vanarts.com: acl_c_authenticated_local_user: root

X-Authenticated-Sender: van.vanarts.com: root

MIME-Version: 1.0

Content-Type: text/plain

Message-ID: <3ab5a205-a254-4a37-a4d9-f88e854fb417@spam.1ask2.com>

From: <kmliao@hotmail.com>

To: Undisclosed recipients:;

Return-Path: kmliao@hotmail.com

Date: Wed, 18 May 2016 09:39:13 -0700

X-MS-Exchange-Organization-AuthSource: spam.1ask2.com

X-MS-Exchange-Organization-AuthAs: Anonymous

===SMTP Commands===

helo

mail from

rcpt to

data

reset

vrfy

noop

quit

ehlo

auth

starttls

size

help

==========No bad-header error===

Telnet 127.0.0.1 25

ehlo hotmail.com

250-van.vanarts.com Hello hotmail.com [127.0.0.1]

250-SIZE 52428800

250-8BITMIME

250-PIPELINING

250-AUTH PLAIN LOGIN

250-STARTTLS

250 HELP

mail from:kmliao@hotmail.com

250 OK

rcpt to:sam@1ask2.com

250 Accepted

data

354 Enter message, ending with "." on a line by itself

Subject:Donald Trump

From:kmliao@hotmail.com

To:sam@1ask2.com

This is a test

What is going on?

.

250 OK id=1b34q4-00014d-1P

====message header===

Received: from c1.1ask2.com (191.121.6.30) by spam.1ask2.com (191.121.6.20)

with Microsoft SMTP Server id 14.3.294.0; Wed, 18 May 2016 10:01:56 -0700

Received: from localhost (localhost [127.0.0.1]) by c1.1ask2.com (Postfix)

with ESMTP id EABC3C396B8A for <sam@1ask2.com>; Wed, 18 May 2016 10:04:07

-0700 (PDT)

X-Virus-Scanned: amavisd-new at 1ask2.com

X-Spam-Flag: NO

X-Spam-Score: 4.666

X-Spam-Level: ****

X-Spam-Status: No, score=4.666 tagged_above=2 required=6.2 tests=[AWL=0.883,

FREEMAIL_FROM=0.001, MISSING_DATE=1.396, MISSING_MID=0.14,

RDNS_NONE=1.274, SPF_SOFTFAIL=0.972] autolearn=no autolearn_force=no

Received: from c1.1ask2.com ([127.0.0.1]) by localhost (mail.1ask2.com

[127.0.0.1]) (amavisd-new, port 10024) with LMTP id 0WvotPXfFVas for

<sam@1ask2.com>; Wed, 18 May 2016 10:04:02 -0700 (PDT)

Received-SPF: softfail (hotmail.com: Sender is not authorized by default to use 'kmliao@hotmail.com' in 'mfrom' identity, however domain is not currently prepared for false failures (mechanism '~all' matched)) receiver=c1.1ask2.com; identity=mailfrom; envelope-from="kmliao@hotmail.com"; helo=van.vanarts.com; client-ip=198.57.136.73

Received: from van.vanarts.com (unknown [198.57.136.73]) by c1.1ask2.com

(Postfix) with ESMTP id 9897BC396B82 for <sam@1ask2.com>; Wed, 18 May 2016

10:04:01 -0700 (PDT)

Received: from [127.0.0.1] (port=56702 helo=hotmail.com) by van.vanarts.com

with esmtp (Exim 4.87) (envelope-from <kmliao@hotmail.com>) id

1b34td-00015S-BT for sam@1ask2.com; Wed, 18 May 2016 12:05:13 -0500

From: <kmliao@hotmail.com>

To: <sam@1ask2.com>

Subject: test email from telnet

X-AntiAbuse: This header was added to track abuse, please include it with any abuse report

X-AntiAbuse: Primary Hostname - van.vanarts.com

X-AntiAbuse: Original Domain - 1ask2.com

X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]

X-AntiAbuse: Sender Address Domain - hotmail.com

X-Get-Message-Sender-Via: van.vanarts.com: acl_c_authenticated_local_user: root

X-Authenticated-Sender: van.vanarts.com: root

MIME-Version: 1.0

Content-Type: text/plain

Message-ID: <3a63f5a5-4193-4ded-864d-cc308f18fcf9@spam.1ask2.com>

Return-Path: kmliao@hotmail.com

Date: Wed, 18 May 2016 10:01:56 -0700

X-MS-Exchange-Organization-AuthSource: spam.1ask2.com

X-MS-Exchange-Organization-AuthAs: Anonymous

----MISSING_DATE----

ehlo hotmail.com

250-van.vanarts.com Hello hotmail.com [127.0.0.1]

250-SIZE 52428800

250-8BITMIME

250-PIPELINING

250-AUTH PLAIN LOGIN

250-STARTTLS

250 HELP

mail from:kmliao@hotmail.com

250 OK

rcpt to:sam@1ask2.com

250 Accepted

data

354 Enter message, ending with "." on a line by itself

From:"King Moon" <kmliao@hotmail.com>

To:"Sam Simpson" <sam@1ask2.com>

Date: Wednesday, May 18, 2016 10:10:45

Subject:Daylight Time

Hello Sam:

This is a test message.

KM

.

===message header will have INVALID_DATE=0.432,MISSING_MID=0.14====

ehlo hotmail.com

mail from:kmliao@hotmail.com

rcpt to:sam@1ask2.com

data

from:"King Morrison" <kmliao@hotmail.com>

to:"Sam Lang" <sam@1ask2.com>

Message-ID: <B365E3DADC4F9741AAFC72FC7A2370D92FF6896C@c1.vanarts.com>

date: Wed, 18 May 2016 10:39:26 -0700

subject: outgoing message

Hello Sam:

How are you doing?

your friend,

King

.

quit

==message header==="INVALID_DATE" and "MISSING-MID" are gone.

ehlo hotmail.com

mail from:kmliao@hotmail.com

rcpt to:Administrator@1ask2.com

data

from:"King Morrison" <kmliao@hotmail.com>

to:"Administrator Lang" <administrator@1ask2.com>

Message-ID: <B365E3DADC4F9741AAFC72FC7A2370D92FF6896D@c1.vanarts.com>

date: Wed, 18 May 2016 10:39:27 -0700

subject: outgoing message

Hello Sam:

How are you doing?

your friend,

King

.

quit

====

Administrator@1ask2.com receives the email even though it is not included in @bypass_header_checks_maps =([qw(sam@1ask2.com)]);

====

ehlo hotmail.com

mail from:kmliao@hotmail.com

rcpt to:kaiming@orienttechs.com

data

from:"King Morrison" <kmliao@hotmail.com>

to:"Administrator Cicino" <kaiming@orienttechs.com>

Message-ID: <B365E3DADC4F9741AAFC72FC7A2370D92FF6896E@c1.vanarts.com>

date: Wed, 18 May 2016 10:39:36 -0700

subject: outgoing message

Hello Sam:

How are you doing?

your friend,

King

.

quit

----message delivered to kaiming@orienttechs.com---amavis[21042]: (21042-07) Passed CLEAN {RelayedInbound},

---

/etc/amavisd/amavisd.conf

$mydomain=1ask2.com;

@local_domains_maps = ([".$mydomain",".orienttechs.com",".pony.com"]); # list of all local domains

systemctl restart amavisd

If the orienttechs.com and pony.com are not included in @local_domains_maps , email goes in or out the Postfix server will not have Spam and Virus check.

=====Block::::::::rudimentary===

banned filename###Blocked Anywhere

Even though, you configure "bypass_virus_checks_maps ==> [1],", the attachment with the banned extensions will be blocked.

/etc/amavisd/amavisd.conf

When "qr'^\.zip$'," is active, email with zip attachment will be blocked. The log will have the amavis[5152]: (05152-01) Blocked BANNED

=====Block====

When a zip file is allowed, its archive (e.g. 00541010.zip) may contain a file 00541010.doc.js, with qr'.\.js$', the attachment is blocked.

amavis[5491]: (05491-01) Blocked BANNED (.asc,00541010.doc.js)

===Decoders===

amavis[3970]: Found decoder for .F at /usr/bin/unfreeze

amavis[3970]: Found decoder for .Z at /usr/bin/uncompress

amavis[3970]: Found decoder for .gz at /usr/bin/gzip -d

amavis[3970]: Found decoder for .bz2 at /usr/bin/bzip2 -d

amavis[3970]: Found decoder for .xz at /usr/bin/xzdec

amavis[3970]: Found decoder for .lzma at /usr/bin/xz -dc --format=lzma

amavis[3970]: Found decoder for .lrz at /usr/bin/lrzip -q -k -d -o -

amavis[3970]: Found decoder for .lzo at /usr/bin/lzop -d

amavis[3970]: No ext program for .lz4, tried: lz4c -d

amavis[3970]: Found decoder for .rpm at /usr/bin/rpm2cpio

amavis[3970]: Found decoder for .cpio at /usr/bin/pax

amavis[3970]: Found decoder for .tar at /usr/bin/pax

amavis[3970]: Found decoder for .deb at /usr/bin/ar

amavis[3970]: No ext program for .rar, tried: unrar, rar

amavis[3970]: Found decoder for .arj at /usr/bin/unarj

amavis[3970]: Found decoder for .arc at /usr/bin/nomarch

amavis[3970]: Found decoder for .zoo at /usr/bin/unzoo

amavis[3970]: Found decoder for .cab at /usr/bin/cabextract

amavis[3970]: Internal decoder for .tnef

amavis[3970]: Found decoder for .zip at /usr/bin/7za

amavis[3970]: Found decoder for .kmz at /usr/bin/7za

amavis[3970]: Found decoder for .7z at /usr/bin/7za

amavis[3970]: Found decoder for .jar at /usr/bin/7z

amavis[3970]: Found decoder for .rar at /usr/bin/7z

amavis[3970]: Found decoder for .swf at /usr/bin/7z

amavis[3970]: Found decoder for .lha at /usr/bin/7z

amavis[3970]: Found decoder for .iso at /usr/bin/7z

amavis[3970]: Found decoder for .exe at /usr/bin/unarj

amavis[3970]: No decoder for .lz4

amavis[3970]: Using primary internal av scanner code for ClamAV-clamd

===Decoders====

Don't do virus and spam checks for outgoing email

=====Block====

Download a virus file

wget https://secure.eicar.org/eicar.com.txt

compress it as eiscar.zip

The urbanselect.com sends the attachment to 1ask2.com.

/var/log/maillog:

Blocked INFECTED (Eicar-Test-Signature)

The 1ask2.com sends the attachment to hotmail.com.

Blocked INFECTED (Eicar-Test-Signature)

=====Block====

/etc/amavisd/amavisd.conf

@mynetworks =qw (127.0.0.0/8 **191.121.0.0/17**) ;

@local_domains_maps = ([".$mydomain",".orienttechs.com","pony.com"]);

$policy_bank{'MYNETS'} = { # mail originating from @mynetworks

originating => 1, # is true in MYNETS by default, but let's make it explicit

os_fingerprint_method => undef, # don't query p0f for internal clients

don't perform spam/virus/header check.

bypass_spam_checks_maps => [1],

bypass_virus_checks_maps => [1],

bypass_header_checks_maps => [1],

};

#####

systemctl restart amavisd

1ask2.com sends a spam test

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

./var/log/maillog

amavis[10131]: (10131-01) Passed CLEAN {RelayedOutbound}, MYNETS LOCAL [191.121.6.20]:50025 [191.121.6.20] <sam@1ask2.com> -> <kmliao@hotmail.com>

#######

1ask2.com sends a virus attachment.

Passed CLEAN {RelayedOutbound}, MYNETS LOCAL [191.121.6.20]:50043 [191.121.6.20] <sam@1ask2.com> -> <kmliao@hotmail.com>,

========Block====

more permissive banning rules for MYNETS

/etc/amavisd/amavisd.conf

```
%banned_rules = (
 'MYNETS-DEFAULT' => new_RE(   # permissive set of rules for internal hosts
   [ qr'^\.(rpm|cpio|tar)$' => 0 ],  # allow any name/type in Unix archives
   qr'.\.(vbs|pif|scr)$'i,     # banned extension - rudimentary
 ),
 'DEFAULT' => $banned_filename_re,
);

$policy_bank{'MYNETS'} = {   # mail originating from @mynetworks
 originating => 1,  # is true in MYNETS by default, but let's make it explicit
 os_fingerprint_method => undef,  # don't query p0f for internal clients
 # don't perform spam/virus/header check.
  bypass_spam_checks_maps => [1],
  bypass_virus_checks_maps => [1],
  bypass_header_checks_maps => [1],
  banned_filename_maps => ['MYNETS-DEFAULT'],
};

  # it is up to MTA to re-route mail from authenticated roaming users or
   # from internal hosts to a dedicated TCP port (such as 10026) for filtering
   #$interface_policy{'10026'} = 'ORIGINATING';
   $interface_policy{'10024'} = 'ORIGINATING';
$policy_bank{'ORIGINATING'} = {  # mail supposedly originating from our users
   originating => 1,  # declare that mail was submitted by our smtp client
   allow_disclaimers => 1,  # enables disclaimer insertion if available
   # notify administrator of locally originating malware
   virus_admin_maps => ["virusalert\@$mydomain"],
   spam_admin_maps  => ["virusalert\@$mydomain"],
   warnbadhsender   => 1,
   # forward to a smtpd service providing DKIM signing service
   forward_method => 'smtp:[127.0.0.1]:10027',
   # force MTA conversion to 7-bit (e.g. before DKIM signing)
   smtpd_discard_ehlo_keywords => ['8BITMIME'],
   bypass_banned_checks_maps => [1],  # allow sending any file names and types
   terminate_dsn_on_notify_success => 0,  # don't remove NOTIFY=SUCCESS option
  banned_filename_maps => ['DEFAULT'],
   };
```

======######=====

Sam@1ask2.com can send out an attachment with 7z extension.

====

X-MS-Exchange-Organization-SCL: 9

Using X-Spam-Flag:YES, to set X-MS-Exchange-Organization-SCL: 9

New-TransportRule -Name 'X-Spam-flag' -Comments '' -Priority '0' -Enabled $true -HeaderMatchesMessageHeader 'X-Spam-Flag' -HeaderMatchesPatterns 'YES' -SetSCL '9'

===

Send a spam message:

X-Virus-Scanned: amavisd-new at 1ask2.com

X-Spam-Flag: YES

X-Spam-Score: 1000.825

X-Spam-Level: **********

X-Spam-Status: Yes, score=1000.825 tagged_above=2 required=6.2

tests=[AWL=2.970, FREEMAIL_FROM=0.001, GTUBE=1000, HTML_MESSAGE=0.001,

RCVD_IN_DNSWL_LOW=-0.7, RCVD_IN_MSPIKE_H3=-0.01,

RCVD_IN_MSPIKE_WL=-0.01, RP_MATCHES_RCVD=-1.426, SPF_PASS=-0.001]

autolearn=no autolearn_force=no

X-MS-Exchange-Organization-AuthSource: spam.1ask2.com

X-MS-Exchange-Organization-AuthAs: Anonymous

X-MS-Exchange-Organization-SCL: 9

===

The message is in Junk E-Mail Folder.

===Block email that are in Chinese===

/etc/mail/spamassassin/local.cf

ok_lanaguages en

score UNWANTED_LANGUAGE_BODY 10.0

=====

When "score UNWANTED_LANGUAGE_BODY 8.0" is used, the score is 5.377 for an email body with a paragraph of Chinese

X-Spam-Status: No, score=5.377 tagged_above=2 required=6.2 tests=[AWL=-1.978,

BODY_8BITS=1.5, FREEMAIL_FROM=0.001, HTML_MESSAGE=0.001,

RCVD_IN_DNSWL_LOW=-0.7, RCVD_IN_MSPIKE_H3=-0.01,

RCVD_IN_MSPIKE_WL=-0.01, RP_MATCHES_RCVD=-1.426, SPF_PASS=-0.001,

UNWANTED_LANGUAGE_BODY=8] autolearn=no autolearn_force=no

====

When "score UNWANTED_LANGUAGE_BODY 10.0" is used, the score is 6.804 for an email body of a paragraph of Chinese and a paragraph of English.

X-Spam-Status: Yes, score=6.804 tagged_above=2 required=6.2 tests=[AWL=-2.551,

BODY_8BITS=1.5, FREEMAIL_FROM=0.001, HTML_MESSAGE=0.001,

RCVD_IN_DNSWL_LOW=-0.7, RCVD_IN_MSPIKE_H3=-0.01,

RCVD_IN_MSPIKE_WL=-0.01, RP_MATCHES_RCVD=-1.426, SPF_PASS=-0.001,

UNWANTED_LANGUAGE_BODY=10] autolearn=no autolearn_force=no

=========

$sa_tag_level_deflt is the level at which Amavisd-new will write spam info headers such as X-Spam-Flag, X-Spam-Score and X-Spam-Status. If you would always like header info to be written to all messages, set this value to -999.

$sa_tag2_level_deflt sets the level at which spam is tagged in the subject line of the message.

$sa_kill_level_deflt sets the level at which Amavisd-new will block the message and quarantine it. This is useful as SpamAssassin doesn't do this by default.

$sa_dsn_cutoff_level is the level at which delivery failure notices are no longer sent to the sender. As most spam sender addresses are forged anyway, it makes sense not to send failure notices in response to obvious spam as you're only contributing to the problem of backscatter.

$sa_quarantine_cutoff_level is the level at which spam isn't even quarantined. By default it is commented out meaning all spam will be quarantined.

DSN (delivery status notification)

Reference

$sa_tag_level_deflt = 2.0; # add spam info headers if at, or above that level

$sa_tag2_level_deflt = 5.2; # add 'spam detected' headers at that level

$sa_kill_level_deflt = 5.9; # triggers spam evasive actions (e.g. blocks mail)

$sa_dsn_cutoff_level = 10; # spam level beyond which a DSN is not sent

$final_virus_destiny = D_DISCARD;

$final_banned_destiny = D_BOUNCE;

$final_spam_destiny = D_DISCARD;

$final_bad_header_destiny = D_BOUNCE;

/var/log/maillog

Blocked SPAM {DiscardedInbound,Quarantined}

But the directory /var/spool/amavisd/quarantine is empty.

$final_spam_destiny = D_DISCARD;
#the default value of $QUARANTINEDIR is undef, meaning no quarantine
$QUARANTINEDIR= undef;

How about?
$final_spam_destiny = D_DISCARD;
#Enable quarantine by specifying a directory
$QUARANTINEDIR= '/var/spool/amavisd/quarantine'; ###good

systemctl restart amavisd

The emails with SPAM and Virus attachments are quarantined in /var/spool/amavisd/quarantine directory.

=== forward the quarantined spam & virus to a mailbox=====

vi /etc/amavisd/amavisd.conf

$QUARANTINEDIR =undef;

#$QUARANTINEDIR = '/var/spool/amavisd/quarantine';

@banned_filename_re = new_RE(

BLOCKED ANYWHERE

qr'^UNDECIPHERABLE$', # is or contains any undecipherable components

qr'^\.(exe-ms|dll)$', # banned file(1) types, rudimentary

qr'^\.(exe|lha|cab|dll)$', # banned file(1) types

BLOCK THE FOLLOWING, EXCEPT WITHIN UNIX ARCHIVES:

[qr'^\.(gz|bz2)$' => 0], # allow any in gzip or bzip2

[qr'^\.(rpm|cpio|tar)$' => 0], # allow any in Unix-type archives

qr'.\.(pif|scr)$'i, # banned extensions - rudimentary

qr'^\.zip$', # block zip type

qr'^\.js$',

qr'^\.zip$', # block zip type

qr'^\.js$',

);

$spam_quarantine_to = "spam\@$mydomain";

#$virus_quarantine_to = "spam\@$mydomain";

$banned_quarantine_to ="spam\@$mydomain";

#$bad_header_quarantine_to ="spam\@$mydomain";

The mailbox spam@1ask2.com will get the spam emails and the email with banned attachment types.

It may create looping!!!

If the banned_filename_re includes .7z with ($banned_quarantine_to ="spam\@$mydomain";), it is looping!!!

The following lines will solve the looping problem.

@bypass_spam_checks_maps =([qw(spam@1ask2.com)]);

@bypass_banned_checks_maps =([qw(spam@1ask2.com)]);

#@bypass_virus_checks_maps =([qw(spam@1ask2.com)]);

#@bypass_bad_header_checks_maps =([qw(spam@1ask2.com)]);

=======IN & OUT of POSTFIX are same with above configuration====

==outgoing of POSTFIX will bypass banned_filename check====

$policy_bank{'MYNETS'} = { # mail originating from @mynetworks

originating => 1, # is true in MYNETS by default, but let's make it explicit

os_fingerprint_method => undef, # don't query p0f for internal clients

don't perform spam/virus/header check.

bypass_spam_checks_maps => [1],

bypass_virus_checks_maps => [1],

bypass_header_checks_maps => [1],

banned_filename_maps => ['MYNETS-DEFAULT'],

bypass_banned_checks_maps => [1],

};

download config

Spamassassin update schedule

/etc/cron.d/sa-update

##

ps aux | grep clamd
ps aux | grep "amavis*"

systemctl daemon-reload
systemctl enable clamd@amavisd
systemctl enable amavisd.service
systemctl enable spamassassin
systemctl restart spamassassin
systemctl restart clamd@amavisd
systemctl restart amavisd.service
systemctl restart postfix
systemctl status amavisd.service

 # vi /etc/postfix/aliases
[ADD this]

virusalert: junkmail
spam.police: junkmail
spamalert: junkmail