

```

*****
* Email Security Virtual Appliance (ESVA)
* v 1.7.1.5 (Lyford) - Final
*
* http://www.global-dominion.org/
*****

Kernel 2.6.17-1.2142_FC4 on an i686

mail-gw login: _

```

Console screen

```

top - 01:54:43 up 6:36, 0 users, load average: 0.00, 0.03, 0.00
Tasks: 71 total, 1 running, 70 sleeping, 0 stopped, 0 zombie
Cpus(s): 0.0% uz, 0.7% sy, 0.0% ni, 99.0% id, 0.0% wa, 0.3% hi, 0.0% si
Mem: 51596k total, 45849k used, 5780k free, 2194k buffers
Swap: 52428k total, 0k used, 52428k free, 78688k cached

  PID USER   PR  NI  VIRT  RES  SHR  S %CPU  %MEM    TIME+  COMMAND
 1898 root    16   0 2024 1012  804  R  0.3   0.2   0:01.07 top
   1 root    16   0 1744  500  500  S  0.1   0.0   0:00.62 init
   2 root    34  19   0   0   0  S  0.0   0.0   0:00.00 ksoftirqd/0
   3 root    RT   0   0   0   0  S  0.0   0.0   0:00.00 watchdog/0
   4 root    10  -5   0   0   0  S  0.0   0.0   0:00.03 events/0
   5 root    20  -5   0   0   0  S  0.0   0.0   0:00.00 khelper
   6 root    11  -5   0   0   0  S  0.0   0.0   0:00.00 kthread
   8 root    10  -5   0   0   0  S  0.0   0.0   0:00.06 kblockd/0
   9 root    20  -5   0   0   0  S  0.0   0.0   0:00.00 kacpid
  66 root    20  -5   0   0   0  S  0.0   0.0   0:00.00 khubd
  68 root    11  -5   0   0   0  S  0.0   0.0   0:00.00 kserfd
 125 root    20  0   0   0   0  S  0.0   0.0   0:00.00 pdflush
 126 root    15  0   0   0   0  S  0.0   0.0   0:00.10 pdflush
 127 root    15  0   0   0   0  S  0.0   0.0   0:00.05 kswapd0
 128 root    20  -5   0   0   0  S  0.0   0.0   0:00.00 aiod
 283 root    11  -5   0   0   0  S  0.0   0.0   0:00.00 kpsmouse
 239 root    11  -5   0   0   0  S  0.0   0.0   0:00.00 scs1_eh_0
 319 root    11  -5   0   0   0  S  0.0   0.0   0:00.00 kxirqd

```

```

May 20 01:48:34 mail-gw MailScanner[11006]: Read 764 hostnames from the phishing
whitelist
May 20 01:48:34 mail-gw MailScanner[11006]: Config: calling custom init function
SQLBlacklist
May 20 01:48:34 mail-gw MailScanner[11006]: Starting up SQL Blacklist
May 20 01:48:34 mail-gw MailScanner[11006]: Read 0 blacklist entries
May 20 01:48:34 mail-gw MailScanner[11006]: Config: calling custom init function
MailWatchLogging
May 20 01:48:34 mail-gw MailScanner[11006]: Started SQL Logging child
May 20 01:48:34 mail-gw MailScanner[11006]: Config: calling custom init function
SQLWhitelist
May 20 01:48:34 mail-gw MailScanner[11006]: Starting up SQL Whitelist
May 20 01:48:34 mail-gw MailScanner[11006]: Read 1 whitelist entries
May 20 01:48:34 mail-gw MailScanner[11006]: Using SpamAssassin results cache
May 20 01:48:34 mail-gw MailScanner[11006]: Connected to SpamAssassin cache data
base
May 20 01:48:34 mail-gw MailScanner[11006]: Enabling SpamAssassin auto-whitelist
functionality
May 20 01:48:35 mail-gw postfix/smtp[11005]: C9BFZ99A6: to=<[redacted]@data.hkr
.se>, relay=mx1.hkr.se[194.47.25.23], delay=5, status=deferred (Host mx1.hkr.se[
194.47.25.23] said: 450 <[redacted]@data.hkr.se>: Recipient address rejected: Gr
aylisted, see http://[redacted].ch/tools/postgrey/help/data.hkr.se.html (in rep
ly to RCPT TO command))
May 20 01:48:38 mail-gw MailScanner[11006]: Using locktype = flock

```

The screenshot shows the ESVA web interface. At the top, there are three summary boxes: 'Color Counts' (Bad Content/Infected: 0, Spam: 0, High Spam: 0, MCP: 0, High MCP: 0, Whitelisted: 0, Blacklisted: 0, Clean: 0), 'Status' (MailScanner: YES 5 children, Postfix: YES 1 proc(s), Load Average: 0.03 0.04 0.00), and 'Today's Totals' (Processed: 4 12.9kb, Clean: 4 100.0%, Viruses: 0 0.0%, Top Virus: None, Blocked files: 0 0.0%, Others: 0 0.0%, Spam: 0 0.0%, High Scoring Spam: 0 0.0%, MCP: 0 0.0%, High Scoring MCP: 0 0.0%). Below these is a 'Recent Messages' table with columns for Date/Time, From, To, Subject, Size, SA Score, and Status. The table lists several messages, including one from 'andymac@global-dominion.org' with a subject 'ESVA 1.7.1.5 - ready to go!' and a status of 'Spam'.

New colour scheme

The screenshot shows the ESVA web interface with a new color scheme. It features a 'Status' box (MailScanner: YES 5 children, Postfix: YES 1 proc(s), Load Average: 0.01 0.03 0.00), a 'Mail Queues' box (Inbound: 0, Outbound: 0, Greylisted: 0), and a 'Today's Totals' box (Processed: 4 12.9kb, Clean: 4 100.0%, Viruses: 0 0.0%, Top Virus: None, Blocked files: 0 0.0%, Others: 0 0.0%, Spam: 0 0.0%, High Scoring Spam: 0 0.0%, MCP: 0 0.0%, High Scoring MCP: 0 0.0%). Below these is a 'Recent Messages' table with a 'Quarantine' tab selected, showing a list of messages with a date selector on the left.

New quarantine selection screen

This message was scanned by ESVA and is believed to be clean. Click here to report this message as spam. <http://mail-gw.global-dominion.org/cgi-bin/learn-msg.cgi?id=7841327F59.03199>

Easily report messages as spam via a link in the footer

The screenshot shows the ESVA web interface with a new color scheme. It features a 'Status' box (MailScanner: YES 5 children, Postfix: YES 1 proc(s), Load Average: 0.01 0.03 0.00), a 'Mail Queues' box (Inbound: 0, Outbound: 0, Greylisted: 0), and a 'Today's Totals' box (Processed: 4 12.9kb, Clean: 4 100.0%, Viruses: 0 0.0%, Top Virus: None, Blocked files: 0 0.0%, Others: 0 0.0%, Spam: 0 0.0%, High Scoring Spam: 0 0.0%, MCP: 0 0.0%, High Scoring MCP: 0 0.0%). Below these is a 'Recent Messages' table with a 'Quarantine' tab selected, showing a list of messages with a date selector on the left.

Summary information in the information bar at the top of most screens

The screenshot shows the ESVA web interface with a new color scheme. It features a 'Status' box (MailScanner: YES 5 children, Postfix: YES 1 proc(s), Load Average: 0.01 0.03 0.00), a 'Mail Queues' box (Inbound: 0, Outbound: 0, Greylisted: 0), and a 'Today's Totals' box (Processed: 4 12.9kb, Clean: 4 100.0%, Viruses: 0 0.0%, Top Virus: None, Blocked files: 0 0.0%, Others: 0 0.0%, Spam: 0 0.0%, High Scoring Spam: 0 0.0%, MCP: 0 0.0%, High Scoring MCP: 0 0.0%). Below these is a 'Recent Messages' table with a 'Quarantine' tab selected, showing a list of messages with a date selector on the left.

Audit log

The screenshot shows the ESVA web interface with a new color scheme. It features a 'Status' box (MailScanner: YES 5 children, Postfix: YES 1 proc(s), Load Average: 0.01 0.03 0.00), a 'Mail Queues' box (Inbound: 0, Outbound: 0, Greylisted: 0), and a 'Today's Totals' box (Processed: 4 12.9kb, Clean: 4 100.0%, Viruses: 0 0.0%, Top Virus: None, Blocked files: 0 0.0%, Others: 0 0.0%, Spam: 0 0.0%, High Scoring Spam: 0 0.0%, MCP: 0 0.0%, High Scoring MCP: 0 0.0%). Below these is a 'Recent Messages' table with a 'Quarantine' tab selected, showing a list of messages with a date selector on the left.

Controllable, smart Greylist functionality

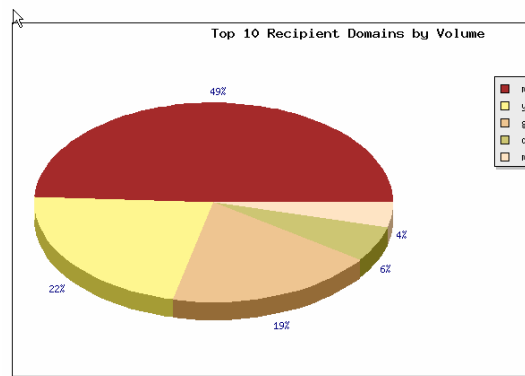
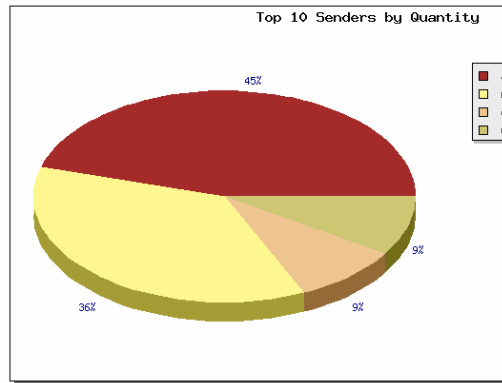
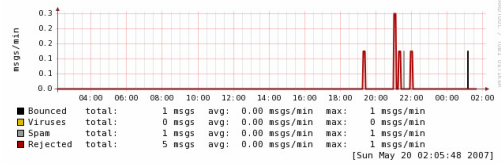
The screenshot shows the ESVA web interface with a new color scheme. It features a 'Status' box (MailScanner: YES 5 children, Postfix: YES 1 proc(s), Load Average: 0.01 0.03 0.00), a 'Mail Queues' box (Inbound: 0, Outbound: 0, Greylisted: 0), and a 'Today's Totals' box (Processed: 4 12.9kb, Clean: 4 100.0%, Viruses: 0 0.0%, Top Virus: None, Blocked files: 0 0.0%, Others: 0 0.0%, Spam: 0 0.0%, High Scoring Spam: 0 0.0%, MCP: 0 0.0%, High Scoring MCP: 0 0.0%). Below these is a 'Recent Messages' table with a 'Quarantine' tab selected, showing a list of messages with a date selector on the left.

Active user community & online support forum

Mail statistics for mail-gw.global-domination.org

Last Day | Last Week | Last Month | Last Year

Last Day



Rule	Description	Total	Ham %	Spam %
required		7	685.7	114.3
autolearn=not		5	5100	0
HTML_MESSAGE	HTML included in message	2	150	150
AWL	From: address is in the auto white-list	2	2100	0
RAZOR2_CHECK	Listed in Razor2 (http://razor.sf.net/)	1	0	1100
RAZOR2_CF_RANGE_S1_100	Razor2 gives confidence level above 50%	1	0	1100
RAZOR2_CF_RANGE_E8_S1_100	Razor2 gives engine 8 confidence level above 50%	1	0	1100
HTML_IMAGE_ONLY_32	HTML: images with 2800-3200 bytes of words	1	0	1100
NO_REAL_NAME	From: does not include a real name	1	1100	0
EXTRA_PART_TYPE	Header has extraneous Content-type: type entry	1	0	1100
HELO_DYNAMIC_DHCP	Relay HELO'd using suspicious hostname (DHCP)	1	0	1100

Graphical reports