

Re: Anyone configured IMS 5.1 to work with Spamhaus?

# Re: Anyone configured IMS 5.1 to work with Spamhaus?

---

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.unix.solaris/2005-12/msg00626.html>

---

- *From:* Bruno Delbono <[bruno.s.delbono@xxxxxxx](mailto:bruno.s.delbono@xxxxxxx)>
  - *Date:* Sat, 10 Dec 2005 22:29:38 GMT
- 

govindo@xxxxxxxxxxx wrote:

Please send me the configuration.

See below. Also ensure that you've cn/ch built the configuration and refreshed dispatcher.

-----mappings-----

! MTA mappings file  
! for access control and other table lookups

PORT\_ACCESS

```
*|*|*|*|*  $C$|INTERNAL_IP;$3|$Y$E  
*  $YEXTERNAL
```

INTERNAL\_IP

```
$(10.10.33.245/24)  $Y  
127.0.0.1  $Y  
*.*.*.*  $C${TRUSTED|$0.0.0.0}$Y$E  
*.*.*.*  $C${TRUSTED|$0.$1.0.0}$Y$E  
*.*.*.*  $C${TRUSTED|$0.$1.$2.0}$Y$E  
*.*.*.*  $C${TRUSTED|$0.$1.$2.$3}$Y$E  
*  $N
```

! ORIG\_MAIL\_ACCESS  
!

Re: Anyone configured IMS 5.1 to work with Spamhaus?



## Re: Anyone configured IMS 5.1 to work with Spamhaus?

! it is valid. The dns\_verify routine will return a positive match if a  
! "server error" is returned, so some bad domain mail could slip through  
! which is probably a good thing.

! We need the ip\_addr back to pass to the throttle lib, thus  
! the \$0.\$1.\$2.\$3 notation on the result

### RATE\_LIMIT

```
*.*.*.*      $C${RATE|$0.0.0.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${RATE|$0.$1.0.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${RATE|$0.$1.$2.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${RATE|$0.$1.$2.$3}$Y$0.$1.$2.$3$E
```

### REJECT\_IP

```
*.*.*.*      $C${rip|$0.0.0.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${rip|$0.$1.0.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${rip|$0.$1.$2.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${rip|$0.$1.$2.$3}$Y$0.$1.$2.$3$E
```

### ALWAYS\_ACCEPT

```
*              $C${ALWAYS|$0}$Y
```

### ALWAYS\_ACCEPT\_IP

```
*.*.*.*      $C${ALWAYS_IP|$0.0.0.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${ALWAYS_IP|$0.$1.0.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${ALWAYS_IP|$0.$1.$2.0}$Y$0.$1.$2.$3$E
*.*.*.*      $C${ALWAYS_IP|$0.$1.$2.$3}$Y$0.$1.$2.$3$E
```

### ALWAYS\_ACCEPT\_SNDR

Re: Anyone configured IMS 5.1 to work with Spamhaus?

\*            \$C\${ALWAYS|\$0}\$Y

REJECT\_FROM\_USER\_DOMAIN

\*            \$C\${rfud|\$0}\$Y

REJECT\_VIRUS

\*            \$C\${virus|\$0}\$Y

REJECT\_FROM\_USER

\*            \$C\${rfu|\$0}\$Y

REJECT\_FROM\_DOMAIN

\*            \$C\${rfd|\$0}\$Y

REJECT\_TO\_USER

\*            \$C\${rtu|\$0}\$Y

REJECT\_TO\_USER\_DOMAIN

\*            \$C\${rtud|\$0}\$Y

Re: Anyone configured IMS 5.1 to work with Spamhaus?

DELAY\_FROM\_USER\_DOMAIN

\*           \$C\${DELAY\_FROM\_USER\_DOMAIN|\$0}\$Y

DELAY\_FROM\_USER

\*           \$C\${DELAY\_FROM\_USER|\$0}\$Y

DELAY\_TO\_USER

\*           \$C\${DELAY\_TO\_USER|\$0}\$Y

DELAY\_TO\_USER\_DOMAIN

\*           \$C\${DELAY\_TO\_USER\_DOMAIN|\$0}\$Y

DELAY\_IP

\*           \$C\${DELAY\_IP|\$0}\$Y

## Re: Anyone configured IMS 5.1 to work with Spamhaus?

```
!INTERNAL_IP
!
! $(10.10.33.245/32) $Y
! *.*.*.* $C${TRUSTED|$0.0.0.0}$Y$E
! *.*.*.* $C${TRUSTED|$0.$1.0.0}$Y$E
! *.*.*.* $C${TRUSTED|$0.$1.$2.0}$Y$E
! *.*.*.* $C${TRUSTED|$0.$1.$2.$3}$Y$E
! 127.0.0.1 $Y
! * $N

LIST_AUTH

*;*|* ${IMTA_LIBUTIL,imdlauth,$2+$1@$0}

!
! src-channel|from-address|dst-channel|to-address
!

ORIG_SEND_ACCESS

tcp_local|*|tcp_local|* $N$D30|Relaying$ not$ allowed
tcp_*|*|native|* $N
tcp_*|*|hold|* $N
tcp_*|*|pipe|* $N
tcp_*|*|ims-ms|* $N
!
! The following three lines stop mail from:<stop me now>
! being accepted, if the address is not qualified then
! go away, but accept NULLs, aka DSNs, we are required too
! plus it is just a very good idea.
!
tcp_*|*|*|* $Y$E
tcp_*||*|* $Y$E
tcp_*|*|*|* $N$D30Nice$ try,$ you'll$ to$ be$ more$ creative$ than$ $1,$
not$ accepted

!
! Block "external" submissions of explicitly source-routed "internal"
addresses
!
tcp_local|*|tcp_intranet|@*:*.* $N$D30|Explicit$ routing$ not$ allowed
```

Re: Anyone configured IMS 5.1 to work with Spamhaus?

tcp\_local|\*|tcp\_intranet|\$%\*@\$ \$N\$D30|Explicit\$ routing\$ not\$ allowed
tcp\_local|\*|tcp\_intranet|\*.\*!\*\$ \$N\$D30|Explicit\$ routing\$ not\$ allowed
tcp\_local|\*|tcp\_intranet|"\*@\*"@\$ \$N\$D30|Explicit\$ routing\$ not\$ allowed

SEND\_ACCESS

tcp\_\*|\*|\*@[127.\*] \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@localhost.\* \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@example.com \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@example.net \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@example.org \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@\*.test \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@\*.example \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@\*.invalid \$X5.1.2|\$NBad\$ destination\$ system
tcp\_\*|\*|\*@\*.localhost \$X5.1.2|\$NBad\$ destination\$ system

!\*\*\*\*\*
!
! Blacklist sites use different numbers to mean different things
! thus we want those reasons in the log files and thus a table
! for each site is needed.
!

! If the client address is found on one of the blacklist zones then
! this mapping needs to return \$Y so that the orig\_mail\_access mapping
! is positive and thus the desired action is taken.

BLACKLIST

\*.\*.\*.\*
\$C\$|SPAMHAUS\_TYPE;\$0.\$1.\$2.\$3.\$[IMTA\_LIB:dns\_verify.so,dns\_verify,\$3.\$2.\$1.\$0.sl
\*.\*.\*.\*
\$C\$|RBLPLUS\_TYPE;\$0.\$1.\$2.\$3.\$[IMTA\_LIB:dns\_verify.so,dns\_verify,\$3.\$2.\$1.\$0.rb
\*.\*.\*.\*
\$C\$|SPAMCOP\_TYPE;\$0.\$1.\$2.\$3.\$[IMTA\_LIB:dns\_verify.so,dns\_verify,\$3.\$2.\$1.\$0.bl
\*.\*.\*.\*
\$C\$|CBL\_TYPE;\$0.\$1.\$2.\$3.\$[IMTA\_LIB:dns\_verify.so,dns\_verify,\$3.\$2.\$1.\$0.cbl.ab
\*.\*.\*.\*
\$C\$|NJABL\_ORG\_TYPE;\$0.\$1.\$2.\$3.\$[IMTA\_LIB:dns\_verify.so,dns\_verify,\$3.\$2.\$1.\$0.
! \*.\*.\*.\*



Re: Anyone configured IMS 5.1 to work with Spamhaus?

\*.127.0.0.12 \$Y\$ Your\$ domain\$ requests\$ nomail\$ See\$  
<URL:<http://www.dnsbl.sorbs.net/>>

DNSBL\_SORBS\_TYPE

\*.127.0.0.2 \$Y\$ Open\$ HTTP\$ Proxy\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.3 \$Y\$ Open\$ Socks\$ Proxy\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.4 \$Y\$ Open\$ Proxy\$ Server\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.5 \$Y\$ Open\$ SMTP\$ Server\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.6 \$Y\$ UBE/UCE\$ Source\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.7 \$Y\$ Web\$ Server\$ has\$ vulnerabilities\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.8 \$Y\$ Refused\$ testing\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.9 \$Y\$ Hijacked\$ network\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>  
\*.127.0.0.10 \$Y\$ Dynamic\$ IP\$ Range\$ See\$  
<URL:[http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=\\$0](http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=$0)>

! I have not found a description of the type of entries found in SPAM  
COP's RBL.

! If you know of them, please let me know. Chad@xxxxxxxxxxxx

SPAMCOP\_TYPE

\*.127.0.0.2 \$Y\$ entry:\$ \$0\$ found\$ in\$ <URL:<http://spamcop.net/>>

CBL\_TYPE

\*.127.0.0.2 \$Y\$ entry:\$ \$0\$ found\$ in\$ <URL:<http://cbl.abuseat.org/>>

## Re: Anyone configured IMS 5.1 to work with Spamhaus?

SPAMHAUS\_TYPE

```
*.127.0.0.2 $Y$ Your$ IP$ Addr$ ($0)$ is$ listed$ in$  
<URL:http://www.spamhaus.org/SBL>
```

NJABL\_ORG\_TYPE

```
*.127.0.0.2 $Y$ Open$ Relay$ See$  
<URL:http://njabl.org/cgi-bin/lookup.cgi?query=\$0>  
*.127.0.0.3 $Y$ Dial$ Up$ or$ Dynamic$ IP$ Address$ See$  
<URL:http://njabl.org/cgi-bin/lookup.cgi?query=\$0>  
*.127.0.0.4 $Y$ UBE/UCE$ Source$ See$  
<URL:http://njabl.org/cgi-bin/lookup.cgi?query=\$0>  
*.127.0.0.5 $Y$ Multi-stage$ Open$ Relay$ See$  
<URL:http://njabl.org/cgi-bin/lookup.cgi?query=\$0>  
*.127.0.0.8 $Y$ CGI$ or$ similar$ problem$ See$  
<URL:http://njabl.org/cgi-bin/lookup.cgi?query=\$0>  
*.127.0.0.9 $Y$ Open$ Proxy$ server$ See$  
<URL:http://njabl.org/cgi-bin/lookup.cgi?query=\$0>
```

```
! The following table is derived from david20@xxxxxxxxxxxxxxxxxxxxxxxxxxxx  
! and Steve +1 608 278 7700 <Stephen.L.Arnold@xxxxxxxxxxxx> via the  
! info-pmdf mailing list.
```

RBLPLUS\_TYPE

```
! The left hand side of the RBL_PLUS_TYPE mapping is the client IP  
! address concatenated with the IP address returned from the RBL+ list.  
! It returns the error message to send to the client.  
*.127.1.0.1 $Y$ Blackholed:$ \  
See$ <URL:http://mail-abuse.org/cgi-bin/lookup?\$0>  
  
*.127.1.0.2 $Y$ Dial-up$ IP$ $0:$ \  
See$ <URL:http://mail-abuse.org/dul/>  
*.127.1.0.3 $Y$ Blackholed$ and$ Dial-up$ IP:$ \  
See$ <URL:http://mail-abuse.org/cgi-bin/lookup?\$0>  
  
*.127.1.0.4 $Y$ Open$ relay:$ \  
See$ <URL:http://work-rss.mail-abuse.org/cgi-bin/nph-rss?query=\$0>  
*.127.1.0.5 $Y$ Blackholed$ and$ Open$ relay:$ \  
See$ <URL:http://mail-abuse.org/cgi-bin/lookup?\$0>
```

Re: Anyone configured IMS 5.1 to work with Spamhaus?

Re: Anyone configured IMS 5.1 to work with Spamhaus?

```
*.127.1.0.6 $Y$ Dial-up$ IP$ and $Open Relay:$ \
See$ <URL:http://work-rss.mail-abuse.org/cgi-bin/nph-rss?query=\$0>
*.127.1.0.7 $Y$ Blackholde,$ Dial-up$ IP, $and$ Open$ relay:$ \
See$ <URL:http://mail-abuse.org/cgi-bin/lookup?\$0>
```

```
<IMTA_TABLE:mappings.locale
-----mappings-----
```

```
--
int main(){int O=0,s[]={0x84,0xe4,0xea,0xdc,0xde,0100,0xa6,'\\'
,0100,0x88,0xca,0xd8,0xc4,0xde,0xdc,0xde,0100,0xf8,0100,0170,0x\
c4,0xe4,0xea,0xdc,0xde,'\\',0xe6,'\\',0xc8,0xca,0xd8,0xc4,0xde,\
0xdc,0xde,0x80,0xda,0xc2,0xd2,0xd8,'\\',0xc2,0xc6,0174,0100,0xf\
8,0100,0xd0,0xe8,0xe8,0xe0,0164,0136,0136,0xee,0xee,0xee,'\\',0\
xda,0xc2,0xd2,0xd8,'\\',0xc2,0xc6,0x0};while(O<66){(s[O]==0)?pr\
intf("%c\n", (47<<2)>>2):printf("%c",s[O]>>1);++O;}return s[--O]\
;}
.
```