NethServer 6 - Enhancement #3295
Log smtp traffic rejection

10/27/2015 11:58 AM - Filippo Carletti

Status:	CLOSED	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	nethserver-mail-filter		
Target version:	v6.7		
Resolution:		**NEEDINFO:**	No

Description

If the mail server is installed, outbound traffic to port 25 (smtp) is rejected without traces in the firewall.log.
I'd prefer to have rejected client-originated smtp sessions logged, to potentially identify "infected" machines and/or internal system that need to directly deliver mail outside.

Related issues:

Related to NethServer 6 - Enhancement # 2894: Mail filter: block port 25 from...	**CLOSED**

Associated revisions

Revision 14015779 - 10/23/2015 06:35 PM - Filippo Carletti

shorewall/rules: log rejects for outbound SMTP. Refs #3295

History

#1 - 10/27/2015 11:58 AM - Filippo Carletti

- Related to Enhancement #2894: Mail filter: block port 25 from LAN to external network added

#2 - 10/27/2015 11:58 AM - Filippo Carletti

- Status changed from NEW to TRIAGED

- Assignee set to Filippo Carletti

- % Done changed from 0 to 20

#3 - 10/27/2015 12:00 PM - Filippo Carletti

- Status changed from TRIAGED to ON_DEV

- % Done changed from 20 to 30

#4 - 10/27/2015 12:15 PM - Filippo Carletti

- Status changed from ON_DEV to MODIFIED

- Assignee deleted (Filippo Carletti)

- % Done changed from 30 to 60

#5 - 10/27/2015 12:25 PM - Filippo Carletti

- Status changed from MODIFIED to ON_QA

- % Done changed from 60 to 70

In nethserver-testing:

nethserver-mail-filter-1.3.3-1.2.g1401577.ns6.noarch.rpm

Test case

NethServer should be the lan gateway and have the mail server installed.
Traffic from a client behind NethServer to port 25 (SMTP) will be rejected but not logged to /var/log/firewall.log.
From a client pc:

```
telnet gmail-smtp-in.l.google.com. 25
Trying 74.125.206.27...
telnet: connect to address 74.125.206.27: Connection refused
```

After update, try again and look at /var/log/firewall.log. You'd see something like:

```
Oct 27 17:20:40 nethsecurity kernel: Shorewall:loc2net:REJECT:IN=eth0 OUT=eth4 SRC=192.168.5.5 DST=74.125.206.27 LEN=60
TOS=0x00 PRE
C=0x00 TTL=63 ID=26084 DF PROTO=TCP SPT=34104 DPT=25 WINDOW=29200 RES=0x00 SYN URGP=0
```

#6 - 11/10/2015 05:31 AM - Giacomo Sanchietti

- Assignee set to Giacomo Sanchietti

#7 - 11/10/2015 06:21 AM - Giacomo Sanchietti

- Status changed from ON_QA to VERIFIED
- Assignee deleted (Giacomo Sanchietti)
- % Done changed from 70 to 90

System and Package Version installed
VM VirtualBox - Clean install of Nethserver 6.7 fully updated
Package Installed: nethserver-mail-filter-1.3.3-1.3.gcb1395c.ns6.noarch
Other Package installed: Email

Test Original Problem
Enchantment

Install Updated Package

```
yum --enablerepo=nethserver-testing install nethserver-mail-filter
```

Test Results after update
Test case:

```
[root@localhost ~]# grep 25 /etc/shorewall/rules
ACCEPT    loc    $FW    tcp    25
ACCEPT    net    $FW    tcp    25
?COMMENT block port 25 from green
REJECT:info loc     net     tcp     25
```

After trying to access port 25 from a LAN client, extract from firewall.log:

Nov 10 11:19:07 localhost kernel: Shorewall:loc2net:REJECT:IN=eth0 OUT=eth1 SRC=192.168.5.22 DST=64.233.184.27 LEN=60 TOS=0x10 PREC=0x00 TTL=63 ID=44705 DF PROTO=TCP SPT=40472 DPT=25 WINDOW=29200 RES=0x00 SYN URGP=0

The rule is generated also for blue networks:

```
[root@localhost ~]# grep 25 /etc/shorewall/rules
ACCEPT    loc    $FW    tcp    25
ACCEPT    net    $FW    tcp    25
?COMMENT block port 25 from green
REJECT:info loc     net     tcp     25
?COMMENT block port 25 from blue
REJECT:info blue    net     tcp     25
```

Verified or Reopen
Verified

Note

#8 - 11/10/2015 06:35 AM - Giacomo Sanchietti

- Status changed from VERIFIED to CLOSED

- % Done changed from 90 to 100

Released in nethserver-updates:

- nethserver-mail-filter-1.3.4-1.ns6.noarch.rpm