CIA MTA 2. Lab 7

Ali Abdulmadzhidov

28 September 2016

1 MTA loop

1.1 Step by step

1. Add alias to /etc/mail/aliases, where st15.os3.su is neighboor whom i send mail in triangle loop

```
loop: loop@st15.os3.su
```

2. Generate aliases.db

```
cd /etc/mail
newaliases
```

3. Restart sendmail

```
service sendmail restart
```

1.2 Answers

1. It'll go through all computers and it'll be reciverd to sender with error that maximum hops was made. For my sendmail is max is 25 hops, on 26'th it'll stop.
2. On my sendmail i can change max hops count by adding line to config file and recompile it

```
define(‘confMAX_HOP’,hops)
```

```
From MAILER-DAEMON  Tue Sep 27 15:06:03 2016
Return-Path: <MAILER-DAEMON>
Received: from st15.os3.su (mail.st15.os3.su [188.130.155.48])
    by mail.st9.os3.su (8.15.2/8.15.2) with ESMTP id u8RC63il026117
    for <root@mail.st9.os3.su>; Tue, 27 Sep 2016 15:06:03 +0300
Received: by st15.os3.su (Postfix)
    id E4FEE202113D; Tue, 27 Sep 2016 15:06:02 +0300 (MSK)
Date: Tue, 27 Sep 2016 15:06:02 +0300 (MSK)
From: MAILER-DAEMON@st15.os3.su (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
To: root@mail.st9.os3.su
Auto-Submitted: auto-replied
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
    boundary="D054620210E4.1474977962/st15.os3.su"
```

```
Message-Id: <20160927120602.E4FEE202113D@st15.os3.su>
Status: RO
Content-Length: 3277
Lines: 80

This is a MIME-encapsulated message.

--D054620210E4.1474977962/st15.os3.su
Content-Description: Notification
Content-Type: text/plain; charset=us-ascii

This is the mail system at host st15.os3.su.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                   The mail system

<loop@st15.os3.su>: mail forwarding loop for loop@st15.os3.su

--D054620210E4.1474977962/st15.os3.su
Content-Description: Delivery report
Content-Type: message/delivery-status

Reporting-MTA: dns; st15.os3.su
X-Postfix-Queue-ID: D054620210E4
X-Postfix-Sender: rfc822; root@mail.st9.os3.su
Arrival-Date: Tue, 27 Sep 2016 15:06:02 +0300 (MSK)

Final-Recipient: rfc822; loop@st15.os3.su
Original-Recipient: rfc822;loop@st15.os3.su
Action: failed
Status: 5.4.6
Diagnostic-Code: X-Postfix; mail forwarding loop for loop@st15.os3.su

--D054620210E4.1474977962/st15.os3.su
Content-Description: Undelivered Message
Content-Type: message/rfc822

Return-Path: <root@mail.st9.os3.su>
Received: from mail.st9.os3.su (mail.st9.os3.su [188.130.155.42])
    by st15.os3.su (Postfix) with ESMTP id D054620210E4
    for <loop@st15.os3.su>; Tue, 27 Sep 2016 15:06:02 +0300 (MSK)
Received: from st12.os3.su (mail.st12.os3.su [188.130.155.45])
    by mail.st9.os3.su (8.15.2/8.15.2) with ESMTP id u8RC6220026090
    for <loop@mail.st9.os3.su>; Tue, 27 Sep 2016 15:06:02 +0300
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
    d=mail.st12.os3.su; s=default; h=Message-Id:From:Date:Sender:Reply-To:Subject
    :To:Cc:MIME-Version:Content-Type:Content-Transfer-Encoding:Content-ID:
    Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc
    :Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:
    List-Subscribe:List-Post:List-Owner:List-Archive;
    bh=P8YA7gvhetesGWSlzyOnF+1ig1eETsGbkPXTUcY5VQM=; b=b/aeKQA4Xu5n4I0AlY5uP2nlvf
    eh6n3SngHUbtU6TO+CVFB1v6rtqiFDIUk9/cKty12YGdhkJUU46cOi1TZXmgRcRnHtjgwrVSi2VGp
    sTaBBxr9JMR0oOmgl2Debp0sc4jVgCnKXYPQDBeg0JuSXt13E/ok8rXlKSnoH4G66Toc=;
```

```
Received: from mail.st15.os3.su ([188.130.155.48] helo=st15.os3.su)
    by st12.os3.su with esmtp (Exim 4.87_167-ff5929e)
    (envelope-from <root@mail.st9.os3.su>)
    id 1bor97-0000OG-P6
    for loop@mail.st12.os3.su; Tue, 27 Sep 2016 15:06:01 +0300
Received: by st15.os3.su (Postfix)
    id CEB63202113D; Tue, 27 Sep 2016 15:06:00 +0300 (MSK)
Delivered-To: loop@st15.os3.su
Received: from mail.st9.os3.su (mail.st9.os3.su [188.130.155.42])
    by st15.os3.su (Postfix) with ESMTP id BE0A420210E4
    for <loop@st15.os3.su>; Tue, 27 Sep 2016 15:06:00 +0300 (MSK)
Received: from mail.st9.os3.su (localhost [127.0.0.1])
    by mail.st9.os3.su (8.15.2/8.15.2) with ESMTP id u8RC60U6026085
    for <loop@st15.os3.su>; Tue, 27 Sep 2016 15:06:00 +0300
Received: (from root@localhost)
    by mail.st9.os3.su (8.15.2/8.15.2/Submit) id u8RC5VNm026071
    for loop@st15.os3.su; Tue, 27 Sep 2016 15:05:31 +0300
Date: Tue, 27 Sep 2016 15:05:31 +0300
From: root <root@mail.st9.os3.su>
Message-Id: <201609271205.u8RC5VNm026071@mail.st9.os3.su>

aaa
/

--D054620210E4.1474977962/st15.os3.su--
0
```

2 Virtual domains

2.1 Step by step

1. (b) Add feature to /etc/mail/sendmail.mc

   ```
   FEATURE(virtusertable, ‘hash -o /etc/mail/virtusertable’)
   ```

2. (a) Add MX RR to our zone file

   ```
   altmail          IN      MX      0      mail.st9.os3.su.
   ```

3. Restart nsd

   ```
   nsd-contron restart
   ```

4. Add virtuser’s to new domain in virtusertable

   ```
   ali@altmail.st9.os3.su  a.abdulmadzhidov
   ```

5. Compile all configs and make virtusertable.db

   ```
   cd /etc/mail
   make all
   ```

6. Restart sendmail

```
service sendmail restart
```

Tested by sending mail with sendmail ali@altmail.st9.os3.su ¡ mess.txt

```
From mrzizik@mail.st9.os3.su  Wed Sep 28 14:14:59 2016
Return-Path: <mrzizik@mail.st9.os3.su>
Received: from mail.st9.os3.su (localhost [127.0.0.1])
    by mail.st9.os3.su (8.15.2/8.15.2) with ESMTP id u8SBEwei011414
    for <ali@altmail.st9.os3.su>; Wed, 28 Sep 2016 14:14:59 +0300
Received: (from mrzizik@localhost)
    by mail.st9.os3.su (8.15.2/8.15.2/Submit) id u8SBEp9r011411
    for ali@altmail.st9.os3.su; Wed, 28 Sep 2016 14:14:51 +0300
Date: Wed, 28 Sep 2016 14:14:51 +0300
From: mrzizik <mrzizik@mail.st9.os3.su>
Message-Id: <201609281114.u8SBEp9r011411@mail.st9.os3.su>

testing
```

Output of mails form altmail was tested by telnet.

```
root@SNE09:~# telnet 188.130.155.42 25
Trying 188.130.155.42...
Connected to 188.130.155.42.
Escape character is '^]'.
220 mail.st9.os3.su ESMTP Sendmail 8.15.2/8.15.2; Wed, 28 Sep 2016 14:23:46 +0300
ehlo altmail.st9.os3.su
250-mail.st9.os3.su Hello mail.st9.os3.su [188.130.155.42] (may be forged), pleased to mee
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
mail from: ali@altmail.st9.os3.su
250 2.1.0 ali@altmail.st9.os3.su... Sender ok
rcpt to: root@mail.st9.os3.su
250 2.1.5 root@mail.st9.os3.su... Recipient ok
data
354 Enter mail, end with "." on a line by itself
this is mail for ali at altmail
.
250 2.0.0 u8SBNkPh011824 Message accepted for delivery
```

The mail

```
From ali@altmail.st9.os3.su  Wed Sep 28 14:24:35 2016
Return-Path: <ali@altmail.st9.os3.su>
Received: from altmail.st9.os3.su (mail.st9.os3.su [188.130.155.42] (may be forged))
    by mail.st9.os3.su (8.15.2/8.15.2) with ESMTP id u8SBNkPh011824
    for root@mail.st9.os3.su; Wed, 28 Sep 2016 14:24:22 +0300
Date: Wed, 28 Sep 2016 14:23:46 +0300
From: ali@altmail.st9.os3.su
Message-Id: <201609281124.u8SBNkPh011824@mail.st9.os3.su>

this is mail for ali at altmail
```

3 Spam and Security

3.1 SPF and DKIM

3.1.1 SPF

SPF verifies sender by SPF or TXT record in DNS and filters it by that compare. It's weakness is dns spoofing, cause in that situation it would be useless.

3.1.2 DKIM

DKIM uses cryptography for verifiyng sender of mail. In headers of email it sends signature of mail. When message comes to recepient, it gets public key from dns and checks dkim-signature. After that it decides what to do with email. Problem of this way is resources that we spend to sign and verify every message and also not strong to dns spoof.

(b) I chose SPF, cause i also implemented DNSSEC and dnsspoof isn't scaring me anymore. Also SPF a bit easier to implement.

3.1.3 Installation

1. Installing spf-milter-python and libspf2 from repo's

```
apt install spf-milter python libspf2-2
```

2. Looking to spf's configs to find where it stores socket

```
> cat /etc/spf-milter-python/spfmilter.cfg
...
socketname = /var/run/spf-milter-python/spfmiltersock
...
```

   Also there we can change the networks mail from whom wouln't be checked

3. Setting up sendmail config for using spf-milter. We need to add one line to sendmail.mc

```
> nano /etc/mail/sendmail.mc
...
INPUT_MAIL_FILTER(‘spfmilter’,‘S=unix:/var/run/spf-milter-python/spfmiltersock
...
```

4. Recompiling config files and restarting sendmail

```
service sendmail restart
```

5. Adding TXT RR to our zone on NSD domnain server.

```
mail        IN  TXT "v=spf1 ip4:188.130.155.42 +mx ~all
```

6. Resigning our zone and restarting dns

SPF inbox pass

```
From mboldyrev@mail.st12.os3.su  Thu Sep 29 13:27:59 2016
Return-Path: <mboldyrev@mail.st12.os3.su>
Received-SPF: Pass (mail.st9.os3.su: domain of mail.st12.os3.su designates 188.130.155.45 a
Received: from st12.os3.su (mail.st12.os3.su [188.130.155.45])
    by mail.st9.os3.su (8.15.2/8.15.2) with ESMTP id u8TARxV7005879
    for <root@mail.st9.os3.su>; Thu, 29 Sep 2016 13:27:59 +0300
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
    d=mail.st12.os3.su; s=default; h=Date:From:Message-Id:Sender:Reply-To:Subject
    :To:Cc:MIME-Version:Content-Type:Content-Transfer-Encoding:Content-ID:
    Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc
    :Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:
    List-Subscribe:List-Post:List-Owner:List-Archive;
    bh=a+WK1yvGvIXnnB6UKyVEidaky0FPifEFBKk53/i4JBU=; b=hYKT80UtVIRX0YF+SS2PYXsCTL
    UddZRwMvdLLPhbIOZ1R1mYhPP9ZR86dw57boR5mGUZXPvNxhr55lHGwM1UWqinI/N9K5viaRIYT6u
    Ul9Gs0kdcZhuAvG8OBuEqcubSk4EBIZhIhLPYyiqVyr1DkxILooYd3Nai3RIP/3r5MK8=;
Received: from mail.st9.os3.su ([188.130.155.42] helo=mail.st12.os3.su)
    by st12.os3.su with esmtp (Exim 4.87_167-ff5929e)
    (envelope-from <mboldyrev@mail.st12.os3.su>)
    id 1bpYZD-0002Ky-GK
    for root@mail.st9.os3.su; Thu, 29 Sep 2016 13:27:55 +0300
Message-Id: <E1bpYZD-0002Ky-GK@st12.os3.su>
From: mboldyrev@mail.st12.os3.su
Date: Thu, 29 Sep 2016 13:27:55 +0300

testSPFtest
```

SPF inbox filtered

```
From sne8@st8.os3.su  Thu Sep 29 13:34:35 2016
Return-Path: <sne8@st8.os3.su>
X-Hello-SPF: pass
Received-SPF: None (mail.st9.os3.su: 188.130.155.41 is neither permitted nor denied by dom
Received: from mail.st8.os3.su (mail.st8.os3.su [188.130.155.41])
    by mail.st9.os3.su (8.15.2/8.15.2) with ESMTP id u8TAYUF1006112
    for <root@mail.st9.os3.su>; Thu, 29 Sep 2016 13:34:35 +0300
Received: by mail.st8.os3.su (Postfix, from userid 1000)
    id 9B8A5BE06BA; Thu, 29 Sep 2016 13:34:24 +0300 (MSK)
DKIM-Filter: OpenDKIM Filter v2.10.3 mail.st8.os3.su 9B8A5BE06BA
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=st8.os3.su; s=mail;
    t=1475145264; bh=vRaZkUWuKXoyya0tqJOUtXWOf8urpnxdoAk0zwJRYcw=;
    h=Date:From:From;
    b=gAojl0WuxWnwNPxjiHOok7V2gOOqzPY7vElcOIo6D5/sp2+jhv4pv8YCWM2CF250p
     O0fdrBAzV1PTKyQh1tAMR2TfwRz8AZ69K5W9odqrpXlqYCFRtjSHKU0KdsJt0yD+Oq
     U4wEsd6uulIoFsYjplc6XLQsMHHIBoSQiP0F2yfg=
Message-Id: <20160929103424.9B8A5BE06BA@mail.st8.os3.su>
Date: Thu, 29 Sep 2016 13:34:19 +0300 (MSK)
From: sne8@st8.os3.su (sne8)

0134
```

Output SPF is checked by online service. Debug screenshots are attached.

3.2 Generic anti-spam solutions

From the various spam solutions i chose spamassassin

3.2.1 Installation

1. Installing spamassassin and spamass-milter from repo

```
apt install spamassassin spamass-milter
```

2. Lookin to spamassassing configs to change configurations if needed

```
> nano /etc/spamassassin/local.cf
...
trusted_networks 188.130.155/24
...
```

3. Setting sendmail to work with spamass-milter

```
> nano /etc/mail/sendmail.mc
...
INPUT_MAIL_FILTER(‘spamassassin’, ‘S=local:/var/run/spamass/spamass.sock, F=T, T=C
...
```

4. Recompiling config files and restarting sendmail

```
service sendmail restart
```

3.3 Authentication

3.3.1 Installation

1. Install openssl and sasl

```
apt install openssl sasl
```

2. Create certificates for openssl

```
mkdir -p /etc/mail/certs
cd /etc/mail/certs
openssl req -new -x509 -keyout cakey.pem -out cacert.pem -days 365
openssl req -nodes -new -x509 -keyout sendmail.pem -out sendmail.pem -days 365
openssl x509 -noout -text -in sendmail.pem
chmod 600 ./sendmail.pem
```

3. Change sendmail config and recompile

```
define(‘confAUTH_MECHANISMS’, ‘LOGIN PLAIN DIGEST-MD5 CRAM-MD5’)dnl
TRUST_AUTH_MECH(‘LOGIN PLAIN DIGEST-MD5 CRAM-MD5’)dnl

dnl ### do STARTTLS
define(‘confCACERT_PATH’, ‘/etc/mail/certs’)dnl
define(‘confCACERT’, ‘/etc/mail/certs/cacert.pem’)dnl
define(‘confSERVER_CERT’, ‘/etc/mail/certs/sendmail.pem’)dnl
define(‘confSERVER_KEY’, ‘/etc/mail/certs/sendmail.pem’)dnl
define(‘confCLIENT_CERT’, ‘/etc/mail/certs/sendmail.pem’)dnl
define(‘confCLIENT_KEY’, ‘/etc/mail/certs/sendmail.pem’)dnl
DAEMON_OPTIONS(‘Family=inet, Port=585, Name=MTA-SSL, M=s’)dnl
```