

IMSA5000-E(Dell)透明模式部署配置方法

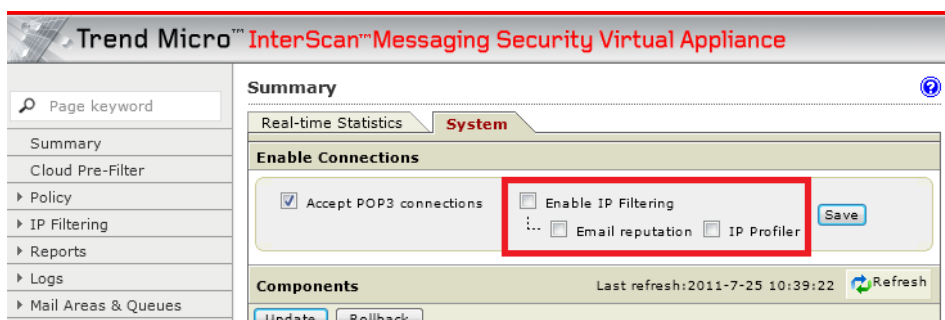
由于 IMSA 使用 postfix 来进行邮件的 Relay，IMSA 并不支持传递 SMTP 身份认证。在某些用户的环境中，必须要支持 SMTP 身份认证，在这种环境下，IMSA 需要配置成透明模式才能支持传递 SMTP 身份认证。以下是 IMSA5000-E(Dell)设置为透明模式的方法。

注：

1. 非不得已，趋势科技不建议取消 postfix。
2. IMSA 工作在透明模式下时，不能使用 IP Filtering 模块(Email reputation 和 ip profiler)。

操作步骤：(在以下操作过程中，勿同时在 IMSA Web 界面上进行任何设置修改)

1. 关闭 IMSA 的 NRS 和 IP Filtering 功能。



2. 取消 postfix 监听 25 端口。

- a) 停止 postfix.

```
#postfix stop
```

- b) 备份 master.cf 文件。

```
#cp /opt/trend/imss/postfix/etc/postfix/master.cf  
/opt/trend/imss/postfix/etc/postfix/master.cf.backup
```

- c) 修改 master.cf 文件

```
#vi /opt/trend/imss/postfix/etc/postfix/master.cf
```

保证以下两行都是注释掉的：

```
#smtp inet n - n - - smtpd  
#2500 inet n - n - 200 smtpd
```

```
#smtp inet n - n - - smtpd  
#smtp inet n - n - 200 smtpd  
#submission inet n - n - - smtpd  
#  
-o smtpd etrn_restrictions=reject
```

- d) 启动 postfix

```
#postfix start
```

- e) 验证修改是否成功。

```
#netstat -ant | grep :25
```

在关闭 postfix 25 端口之前，看到的输出应如下：

```
[root@imsva8 ~]# netstat -ant | grep :25
tcp        0      0 0.0.0.0:25          0.0.0.0:*          LISTEN
[root@imsva8 ~]#
```

在关闭 postfix 25 端口之后，看到的输出应如下：

```
[root@imsva8 ~]# netstat -ant | grep :25
[root@imsva8 ~]#
```

3. 修改 IMSA 的配置文件。

a) 备份 imsa 的配置文件。

```
#cp /opt/trend/imss/config/imss.ini /opt/trend/imss/config/imss.ini.backup
```

b) 编辑 imsa 配置文件。

```
vi /opt/trend/imss/config/imss.ini
```

c) 找到并修改如下参数：

enable_postfix_ui=yes 修改为 enable_postfix_ui=no

```
enable_postfix_ui=no
```

#downstream_smtp_server_addr=127.0.0.1 修改为

downstream_smtp_server_addr=smtp 服务器的 IP,并取消注释符

#downstream_smtp_server_port=10026 修改为

downstream_smtp_server_port=25 取消注释符

```
# 8.1
# Downstream or back end MTA server IP address or hostname.
# The IP is recommended to avoid security issues that arise
# from resolving the host.
downstream_smtp_server_addr=10.28.132.102

# 8.2
# Downstream or back end MTA server listening port.
downstream_smtp_server_port=25
```

#proxy_smtp_server_ip=127.0.0.1 修改为 proxy_smtp_server_ip=0.0.0.0,并取消注释符。

```
# 10.1
# The IP address the proxy service will bind to on a machine with
# multiple NIC cards.
# If not specified, the proxy service sets it to the first IP address
# that it successfully binds to.
# If not specified or specified as "all" or 0.0.0.0,
# then proxy service binds to INADDR_ALL.
proxy_smtp_server_ip= 0.0.0.0
#proxy_pop3_server_ip= 0.0.0.0
```

[socket_1]

```
#proxy_service=SMTP_SERVICE
```

```
#proxy_port=10025
```

修改为

```
[socket_1]
```

```
proxy_service=SMTP_SERVICE
```

```
proxy_port=25
```

并取消注释符。

```
[socket_1]
proxy_service=SMTP_SERVICE
proxy_port=25
```

open_to_all_connections = no 修改为 open_to_all_connections = yes，并取消注释符。

```
# 8.8
# Accept SMTP client connections.
# If "no" (default), the IMSS daemon only accept SMTP client connections
# from localhost (and IP address required in smtp_allow_client_ip).
# If "yes", then all connections allowed.
open_to_all_connections = yes
```

enable_postset_thd=yes 修改为 enable_postset_thd=no

```
enable_soap_server=
enable_postset_thd=no
detach_key_postfix=
```

smtp_greeting_msg=TrendMicro IMSS SMTP proxy 修改为

smtp_greeting_msg= 并取消注释符。

```
# 8.3
# The upstream MTA receives the following message (in addition to the greeting
# from the downstream MTA).
smtp_greeting_msg=
```

在[smtp]下添加如下内容：

```
supported_esmtp_cmds=PIPELINING,SIZE,VERFY,ETRN,XVERP,8BITMIME,AUTH
,ONEX,XUSR,HELP,AUTH=LOGIN
```

```
#####
[smtp]
#####
supported_esmtp_cmds=PIPELINING,SIZE,VERFY,ETRN,XVERP,8BITMIME,AUTH,ONEX,XUSR,HELP,AUTH=LOGIN
```

- d) 保存文件。
- e) 重新启动 S99IMSS 服务。
#/opt/trend/imss/script/S99IMSS restart
- f) 验证修改是否成功。（**请务必确认进行以下测试前，IMSA 可以访问到后端邮件服务器的 25 端口**）

如果在修改 imss.ini 的时候 IMSA 无法访问后端邮件服务器，请确认 IMSA 现在可以访问后端邮件服务器，并执行#/opt/trend/imss/script/S99IMSS restart。

执行 `netstat -ant | grep :25`,应看到如下信息:

```
[root@imsva8 ~]# netstat -ant | grep :25
tcp        0      0 0.0.0.0:25          0.0.0.0:*          LISTEN
[root@imsva8 ~]#
```

执行 `telnet 127.0.0.1 25`, 应看到后端邮件服务器的欢迎信息。

```
[root@imsva8 ~]# telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
220 cn-soiphon-temi.soiphon-windows.org Microsoft ESMTPL MAIL Service, Version: 6
.0.3790.3959 ready at Tue, 14 Feb 2012 14:51:36 +0800

```

执行 `telnet IMSA_IP 25`, 应看到后端邮件服务器的欢迎信息。

```
[root@imsva8 ~]# telnet 172.16.4.218 25
Trying 172.16.4.218...
Connected to 172.16.4.218.
Escape character is '^'.
220 cn-soiphon-temi.soiphon-windows.org Microsoft ESMTPL MAIL Service, Version: 6.0.3790.3959 ready
at Tue, 14 Feb 2012 15:03:23 +0800

```

如果 IMSA 无法访问到后端邮件服务器的 25 端口,很可能会看到如下错误提示:

```
[root@imsva8 ~]# telnet 172.16.4.218 25
Trying 172.16.4.218...
Connected to 172.16.4.218.
Escape character is '^'.
421 Internal configuration error
Connection closed by foreign host.

```

4. 如果 IMSA 的版本为 8.0 或者 8.2 的版本, 请执行以下操作 (如果是 7.0 版本, 请跳过该操作)。

a) 备份 `MsgTracing.conf` 文件。

```
#cp /opt/trend/imss/config/MsgTracing.conf
/opt/trend/imss/config/MsgTracing.conf.backup
```

b) 修改 `MsgTracing.conf`。

```
vi /opt/trend/imss/config/MsgTracing.conf
```

将 `SessionGroupExpiredInterval=1200` 修改 `SessionGroupExpiredInterval=120`。

```
# in SessionGroup longer till the interval expiring.
SessionGroupExpiredInterval=120
```

c) 保存修改。

d) 重新启动服务。

```
#!/opt/trend/imss/script/S99MSGTRACING restart
```

此步操作的目的是: 当 IMSA 为透明模式时, 如果该参数未进行修改, 邮件经过 IMSA 后, 在 Message Tracking 里需要等待 20 分钟后才能查到该日志。进行如上修改后, 邮件在 Message Tracking 里 2-3 分钟后就能查到相关日志。