Protecting the AXIGEN Messaging Solution with NOD32

GECAD Technologies

10A Dimitrie Pompei Blvd., BUCHAREST 2, ROMANIA

Tel.: +40 21 303 20 80

+40 21 303 20 81

http://www.axigen.com

Last modified: 1/29/2007

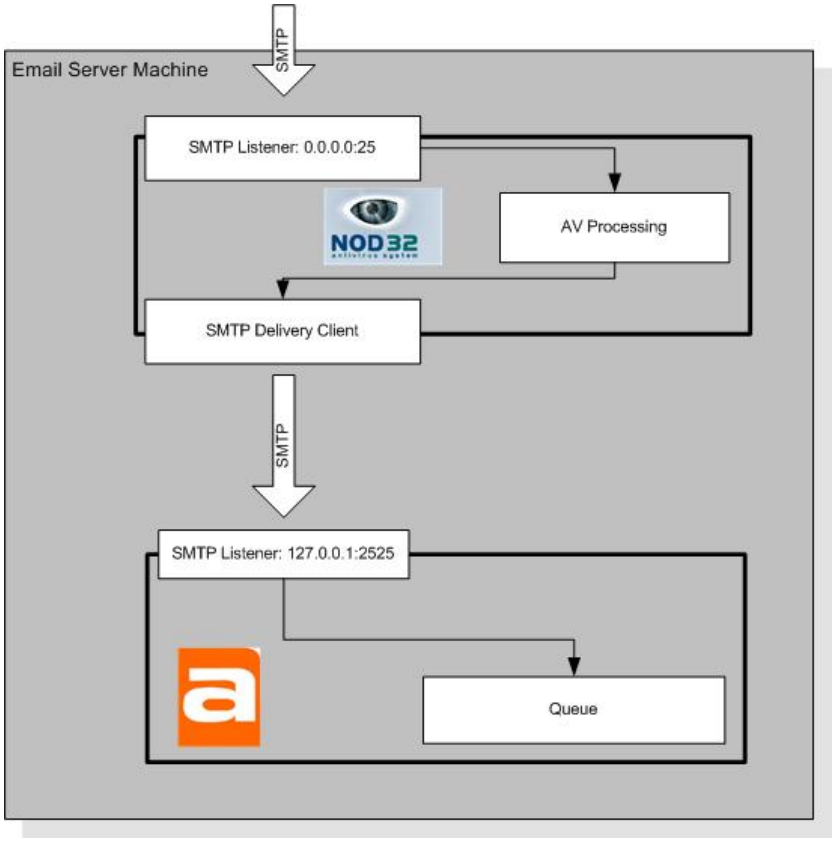
Introduction

This article focuses on the integration of the AXIGEN Mail Server with ESET's NOD32 antivirus for the purpose of obtaining virus-safe email traffic.

Overview

The integration of AXIGEN with NOD32 is performed by replacing the AXIGEN listener on port 25 with NOD32's SMTP service. NOD32 delivers the email, after processing it, to AXIGEN's SMTP listener on a different port (in our example, tcp/2525).

The figure below depicts the flow of the messages through NOD32 and AXIGEN.



Email messages pass from SMTP through NOD32's antivirus engine for detection before being delivered to the AXIGEN Mail Server.

Prerequisites

Software & Licenses:

- AXIGEN Mail Server (v 1.2) license - for the number of mailboxes you would like to host;
- NOD 32 for Linux Mail Server (LMS) v 2.51 license – for the number of mailboxes you would like to protect; it should be the same number of mailboxes as defined in AXIGEN.

- Common available platforms: Linux, the following distributions:
  - Fedora Core 1, 2, 3, 4, 5
  - Mandrake 10.2
  - Mandriva 2006.2
  - SuSE 9.0, 9.3, 10.0, 10.1
  - Debian 3.1
  - Ubuntu 5.04, Server 5.10, Server 6.06

Installation

The AXIGEN mail server must be installed on the machine and configured as per your needs. If you need information on performing a normal AXIGEN installation, please see the product manual.

Follow the procedure from the manual for installing the NOD32 antivirus. Remember to copy your license file to the '/etc/opt/eset/nod32/license/' directory *before* actually installing the NOD32 rpm. **Please note that if you do not copy the license before installing the rpm, *'nod32d'* will not be automatically started by the installer.**

After the installation the 'nod32d' service is automatically started but the 'nod32smtp' is not. Start it with the following command:

```
# /etc/init.d/nod32smtp start
```

In order to verify that NOD32 was successfully installed, run a telnet on port 2526 (the default SMTP port for NOD32). The connection should be established and then be closed immediately (due to the fact that NOD32 cannot yet connect to the mail server).

```
[root@localhost ~]# telnet localhost 2526
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
421 nod32smtp: server connect error, closing connection
Connection closed by foreign host.
```

If the connection is rejected before being established or a different error is reported, please consult the troubleshooting section of the NOD32 manual.

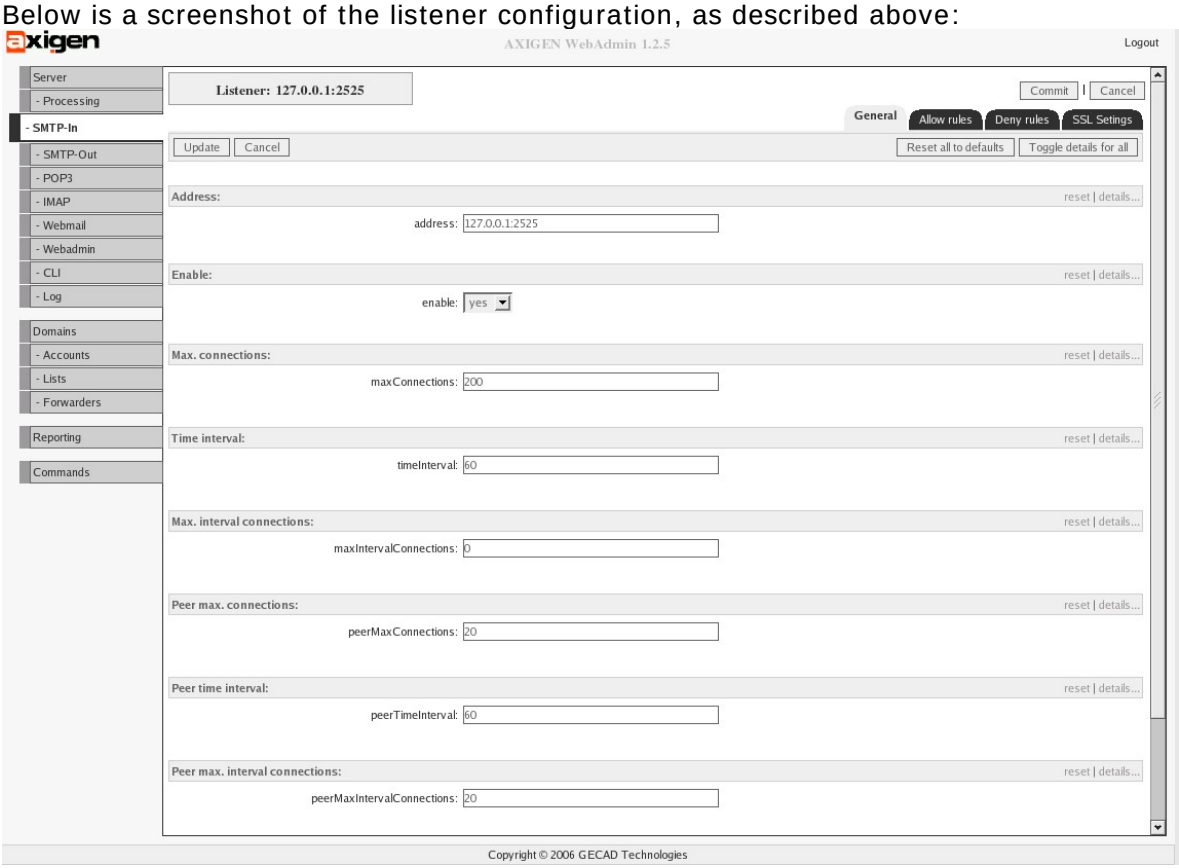
Interconnecting AXIGEN and NOD32

Now that both AXIGEN and NOD32 are installed, some configuration steps must be taken to ensure the appropriate email flow.

1. **Reconfigure AXIGEN's SMTP listener.**
   - Login to the web administration interface (typically located at http://localhost:9000, if you're running the browser from the same machine);
   - Go to the 'SMTP-In' section;
   - Click on the 'Listeners' property tab;
   - Configure one listener with '*address*': "127.0.0.1:2525". Make sure no other listeners exist;
   - Set the '*enable*' option to 'yes';
   - Set the '*maxIntervalConnections*' parameter to '0' (Unlimited);
   - Set the '*peerMaxConnections*' parameter to '200';

- Set the '*peerMaxIntervalConnections*' parameter to '0' (Unlimited);
- Click 'Update', the 'Commit';
- Make sure you save the configuration by going to the 'Commands' administration section and, when located there, clicking 'Save Config'.

Below is a screenshot of the listener configuration, as described above:



2. Reconfigure NOD32's SMTP service

- Using a text editor, open the '/etc/opt/eset/nod32/nod32.cfg' file
- In the '[smtp]' section, modify the 'listen_addr' option from 'localhost' to '0.0.0.0'. This will configure NOD32 to bind on all network addresses.
- In the same section, modify the 'listen_port' option from '2526' to '25'. This way, NOD32 receives all incoming SMTP traffic.
- Restart the NOD32 services by running:

```
# /etc/init.d/nod32d restart
# /etc/init.d/nod32smtp restart
```

3. Verify the connection

- Run a telnet, on the local machine, on port 25. The connection should be established, and the AXIGEN SMTP banner should appear:

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 localhost.localdomain AXIGEN SMTP ready
```

- Enter the 'quit' command in order to close the connection.

4. **Send a mail through**

- Using an SMTP email client (Outlook, Mozilla) already configured to use the AXIGEN mail server, send an email to a valid recipient;
- The email must reach the destination mailbox and it must contain the NOD32 header: 'X-Virus-Scanner'.

Configuring the NOD32 Behavior

This section describes the behavior of your newly configured solution when a virus/spam is detected. At this point the AXIGEN integration with NOD32 is operational.

Default settings:

By default, NOD32 will attempt to disinfect the attachments and deliver them. If disinfection fails, NOD32 will remove the attachment from the message and add a footnote to it informing the recipient. Furthermore, if an attachment cannot be scanned, it will be removed from the message.

Changing the default settings:

The behavior of NOD32 can be altered by modifying the configuration file ('/etc/opt/eset/nod32/nod32.cfg'), mainly through the following configuration options:

- action_on_infected
- action_on_uncleanable
- action_on_notscanned
- quarantine

For information on how to configure NOD32 to obtain the desired functionality, please consult the product's manual.

Tweaking

1. **By default, NOD32 advertises all the ESMTP extensions AXIGEN supports. However, some of them are not supported and must be disabled; otherwise, in some cases, mail delivery may fail.**

- Login to the AXIGEN web administration interface (typically http://localhost:9000);
- Go to the 'SMTP-in' section, then to the 'Clients' tab;
- Add a new client with priority '501';
- Set the '*patternIn*' and '*patternOut*' options to '*' in order for this client to replace the default;
- Set to 'no' the following options:
  - allowStartTLS
  - allowBinaryData
- Make sure the other options ('*maxRCPTCount*', '*maxDataSize*,'etc) are set correctly according to your desired configuration, since this will be the default client;
- Save the configuration;

Note: if you have previously added a client thus replacing the default functionality, modify the settings of that client, without adding a new one. **Make sure the '*allowStartTLS*' and '*allowBinaryData*' options are set to 'no' for all the 'clients' defined in your SMTP-in module configuration**.

2. **Normally, since outside SMTP clients no longer connect directly to AXIGEN, connections cannot be directly managed. However, the NOD32 SMTP connection manager immediately closes the connection if AXIGEN does so. This way, one can *manage the maximum number of simultaneous connections and the connection rate* directly from AXIGEN.**

- Login to the AXIGEN web administration interface (typically http://localhost:9000);
- Go to the 'SMTP-in' section, then to the 'Listeners' tab;
- Edit the listener;
- Configure, as desired, the following parameters:
  - '*maxConnections*'
  - '*maxIntervalConnections*'
  - '*timeInterval*'
- Do not modify the peer-related options since they no longer make sense in this set-up.

3. **Optimize the number of parallel threads**
   By default, NOD32 limits the number of parallel scanning threads. It is recommended to increase this value, depending on your traffic level. A typical setting – suitable for most users – would be 10 threads. A good 'rule of thumb' would be to have the number of threads parameter set to half the peak number of simultaneous SMTP connections you expect. (e.g. if you expect to have a peak of 20 parallel SMTP connections, set the number of threads to 10).

- Using a text editor, open the '/etc/opt/eset/nod32/nod32.cfg' file;
- In the '[*global*]' section, change the '*num_thrd*' option from '2' to '10'. This will configure NOD32 to use 10 parallel threads for email scanning. Remember to remove the comment mark semicolon (;) from the beginning of the line;
- Restart the NOD32 services by running:

```
# /etc/init.d/nod32d restart
# /etc/init.d/nod32smtp restart
```

Caveats

Although the configuration guidelines provided in this article cover the needs of most users, there are some aspects that one must keep in mind when using the Axige/NOD32 combination:

1. NOD32 does not support TLS. AXIGEN must not advertise TLS in the EHLO phase (see the 'Tweaking' section) – otherwise, **any attempt to establish a TLS session will fail and messages will not be delivered**.
2. Emails going into the AXIGEN mail server through channels other than SMTP (e.g. webmail) will not pass through NOD32 thus will not be scanned for antivirus or antispam.

3. Since all SMTP connections AXIGEN receives are from NOD32, hence originate from the 127.0.0.1 IP, configuring IP-based rules in the 'Clients' section of the SMTP-In module no longer makes sense.
4. As previously said, all the SMTP connections received by AXIGEN originate from the 127.0.0.1 IP. When running the AXIGEN Configuration Wizard, the following code will be added in the SMTP Policy File, in the onEhlo event definition:

```
if (…iprange (remoteSmtpIp, "127.0.0.0/255.0.0.0")…) {
    set(remoteDelivery, "all");
}
```

   This means that all connections from 127.0.0.1 will allow open relaying which is a crucial security flaw. To correct it, you should remove the specified code lines.
5. For the same reason as described above, setting the 'peerMaxIntervalConnections' parameter for the SMTP-in listener to a value different than 0 is of no use. Use the 'maxIntervalConnections' parameter instead.
6. NOD32 does not support the BINARYMIME ESMTP extension, therefore if it is not disabled from AXIGEN (see the 'Tweaking' section), emails sent with the BINARYMIME extensions **will not be scanned**.