AXIGEN Efficiently Fights Viruses and Spam

In a world where most communications are performed online, threats like viruses, Trojans, phishing or spam gain more importance when it comes to securing the transferred information. All these threats have one effect, losses. Be it time, money or data, the total value, given a financial expression, keeps growing. While the damage induced by viruses or phishing is easily comprehended by most, the impact of spam tends to be overlooked. It just takes time and too much space of our Inboxes at a fist glance. However, unsolicited emails are the preferred means of spreading viruses, worms and of enabling phishing attacks.

Spam is spreading fast all over the Internet and it gets harder and harder to avoid it. There are many methods that can be used to protect the users from these types of messages and other potential threats it can be the bearer of. Third party software, anti-virus and anti-spam bundles, authentication and validation to stop phishers, new protocols and server specific modifications and adaptations are all supporting the endeavor to eradicate spam messages. The AXIGEN Mail Server implements almost all of these into one package, enabling the system or network administrator to choose or combine the methods that he/she feels are appropriate to enforce the preferred security policy.

Summary

The AXIGEN Mail Server offers different ways to fight spam and viruses. Each of them is presented in a separate section, as follows:

- Anti-Malware and Direct Implementation
- Implementing Antivirus Applications with the Milter Extension
- Implementing Antivirus Applications with the AMAVIS Extension
- Sender Domain and IP Validation DomainKeys and SPF
- Message Rules (Outlook-like Rules and Server Side Message Filtering)
- Message Acceptance Policies (SMTP Firewall)
- Containing Internal Virus / Spam / Phishing Issues
- Routing Policies for Smart Delivery and Risk Hedging

Before explaining the best practices to reduce and prevent potential risks, one needs to properly define the threats these measures are directed against:

All the security tools and methods the AXIGEN Mail Server has to offer are presented below. These features guarantee secure reception, transit and delivery of emails and protection for your confidential data.

Spamming is the abuse of electronic messaging systems to send unsolicited, undesired bulk messages. E-mail spam is the most common form of internet spamming. It involves sending unsolicited commercial messages to many recipients. Unlike legitimate commercial e-mail, spam is generally sent without the explicit permission of the recipients, and frequently contains various tricks to bypass e-mail filtering.

Phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by

masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using unsolicited email messages to require sensitive information.

Malware or malicious software is software designed to infiltrate or damage a computer system without the owner's informed consent. Software is considered malware based on the perceived intent of the creator rather than any particular features. It includes computer viruses, worms, Trojan horses, spyware, adware, and other malicious and unwanted software.

Anti-Malware and Direct Implementations

The AXIGEN mail server includes even since installation a wide range of tools ready to deploy and use to protect your setup. Gateway products that act as scanning servers are very easy to integrate. The best example in this category is the NOD32 anti-virus scanning engine. Direct integration with open-source tools like SpamAssassin and ClamAV has also been offered by AXIGEN since the very start and are ready to use right after installation, also. Their popularity due to their reduced setup costs and great community support makes them a first choice for many of the industry's specialists. AXIGEN is able to communicate with these tools directly, reducing scanning time and increasing availability for the services provided.

Implementing Antivirus Applications with the Milter Extension

The AXIGEN mail server integrates with the most popular anti-virus/anti-spam third party software through the milter interface. This comes as a separate module, extending AXIGEN's ability to communicate with scanning software. It has great support for network scanning, distributing the work load of the mail server to other machines, increasing productivity and availability. For small load servers, the scanning engine can be set up on the same machine, thus reducing costs.

AntiVirus for Milter products = AntiVirus for Sendmail:

- **Kaspersky® Anti-Virus for Linux Mail Server**
- **avast! for Linux/Unix Servers**
- **Symantec Brightmail AntiSpam 6.0**
- **NOD32 for Linux & BSD Mail Servers**
- **BitDefender Mail Protection**
- **Avira AntiVir UNIX MailGate**

These are the most of the popular scan engines on the market that offer such a milter interface. This translates into a simpler setup, dedicated to your needs.
With the milter extension it's easy to deploy multiple scanning engines at the same time, adding to the security of your messages and redundancy in the event that one of the implementations fails.

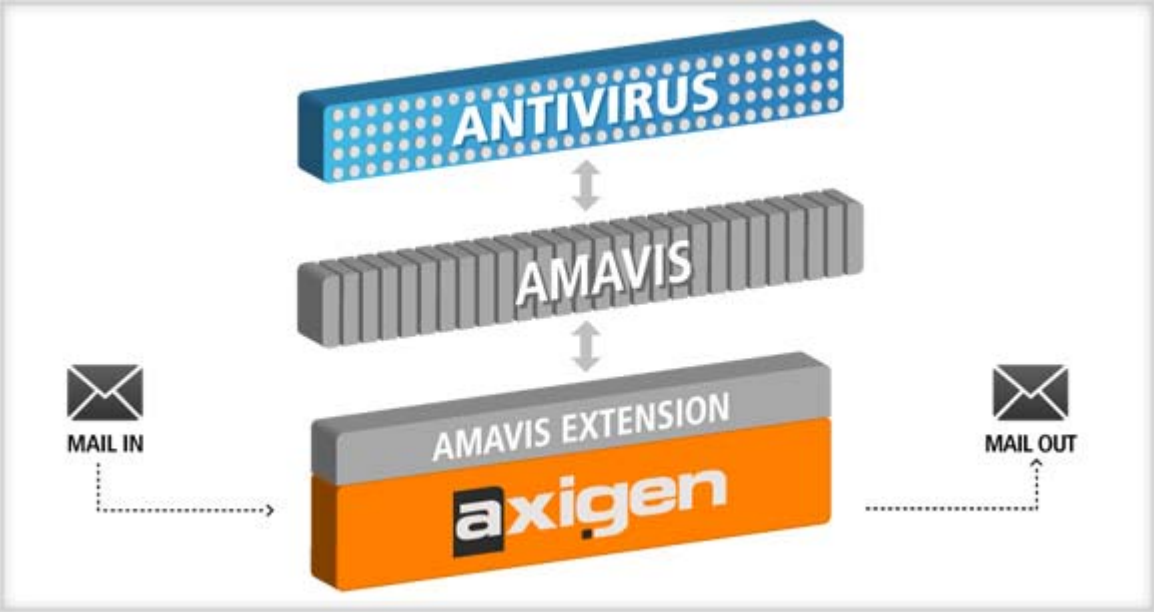
You can set a specific Filtering System and apply it to Server, Domain or User level. Within a Filtering system you can add and prioritize filters by assigning them different priorities. Based on the filter findings, you can add certain delivery decisions.

The most popular tools that use this deployment method are Symantec, Avast and Nod32. In the future, BitDefender and others will be supported along with the introduction of local

connections to support anti-viral applications that do not support network scanning through sockets.

Implementing Antivirus Applications with the Amavis Extension

This extension aims to complete and in some cases replace the milter. This extension, being very similar with the milter at its roots, has support for many scanning engines and also supports scanning with multiple engines at the same time.



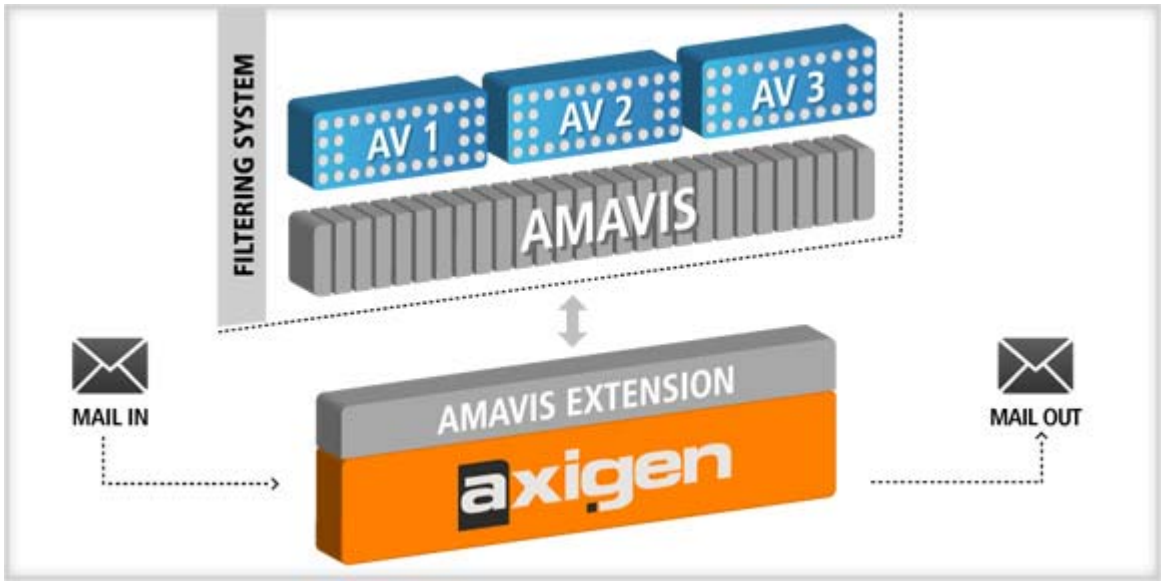
AMAVIS integration does not have, however, the speed and reliability of the Milter. Network scanning is also possible, although this process can be tedious to set up and is not always reliable. The Amavis extension excels only where the milter fails: that is, if your scanning engine does not have support for a milter implementation, there is a high chance that Amavis can be used instead.

Antivirus applications that integrate with AMAVIS are:

- **BitDefender,**
- **Kaspersky,**
- **F-Prot,**
- **McAfee.**
- **Sophos**
- **DrWeb**
- **Symantec**
- **F-Secure**
- **Avast**
- **eTrust**
- **Norman**
- **Panda**

However, we recommend to use Milter integration if the AV you have purchased supports it (such applications are specified in the AV for Milter product list)

Due to lack of speed, we do not recommend applying multiple filters on the mail flow. However, this is technically possible as follows:



Sender Domain and IP Validation (DomainKeys and SPF)

Great efforts have been made to create a safe working environment while using AXIGEN as a mail server. New technologies are also part of the product. Such innovations include Domain Keys message validation and the Sender Policy Framework. These are two of the youngest and most powerful tools against phishing and SPAM attacks. They can be used to secure and further increase the server's ability to hamper unsolicited e-mail propagation. Domain Keys comes as a separate package, while SPF is bundled into the SMTP policies of AXIGEN.

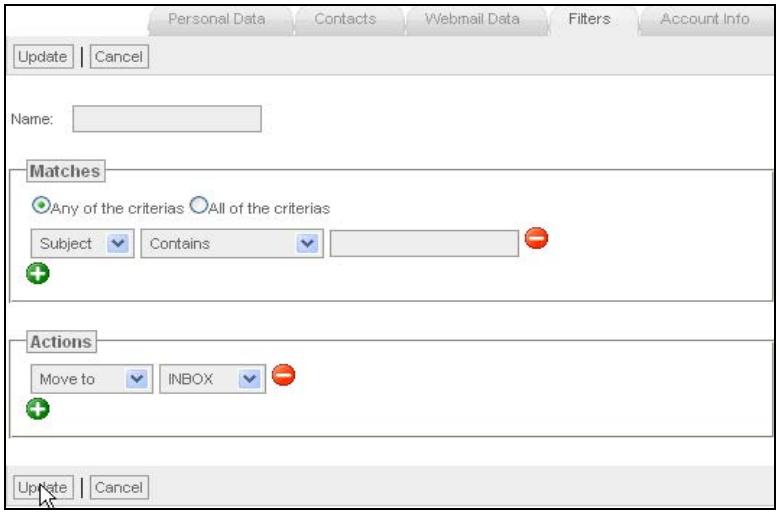
Domain Keys Integration:

SPF (Sender Policy Framework) Integration:

Message Rules (Outlook-like Rules and Server Side Content Filtering)

With AXIGEN, every user accessing the WebMail interface can define his/her own rules to deal with SPAM, based on his/her individual needs. Administrators can define rules that apply server-wide to all mail system users, thus extending the automated implementations of SPAM detection with a conscious human decision. This enables further and complete control over what gets delivered and what doesn't, increasing the filtering abilities of the product to the maximum.

Examples
Server side rules:
-Move all messages marked as spam to a certain folder;
-Relay all emails that do not have a valid user on the server to a catch-all account;
-Delete all emails containing a certain word or group of words in the subject line.
User defined rules:
-Move all emails from x@y to a certain folder;
-Delete all emails exceeding a certain size;
-Respond to all incoming emails with out-of-office reply.



Message Acceptance Policies (SMTP Firewall)

This new concept aims to give the system administrators a very low level control over the communications between the many elements involved in the mail sending process. Based on custom defined policies within SMTP modules, it is the perfect addition to security. Acting as an email firewall, the SMTP Firewall is able to decide the fate of an e-mail, based on certain properties, sometimes blocking it all together even before it reaches the server. An experienced system administrator, with this scripting tool at his/her disposal can literally create wonders for their mail server security policy and can optimize the mail flow.

Incoming connections established via SMTP and the message flow can be easily managed using the established policies. Moreover, they allow adding headers, changing addresses and other such actions.

Examples of message acceptance rules:

- allow incoming messages from a specific domain
- deny incoming messages with attachments exceeding 3 MB
- allow authenticated users only
- accept secured connections only
- deny looping emails (when the number of Received headers exceeds 20)

The events are predefined blocks within the script that will be executed at specific moments by the server. For each event, the server calls certain methods which can have a configurable or predefined behavior. The available events at SMTP Incoming level are:

- onConnect
- onEhlo
- onMailFrom
- onRcptTo
- onDataReceived

Containing Internal Virus / Spam / Impersonating Issues

Internal threats are at times as powerful as outside threats. A certain user making a habit of sending spam messages can get an entire domain blacklisted. There are ways for system administrators to change such a situation. But most of the times, preventing them is easier. Thus, being able to control the user accounts the AXIGEN Mail Server manages is a key feature of a company's policy.

When users fail to comply with internal policies, there are several ways system administrators have to control their email messaging activity. As spam and virus spreading prevention methods, administrators can either limit the number of emails users are allowed to send in a certain time frame, or, for more severe cases, they can completely stop the outgoing mail flow through a simple click: disabling a user's SMTP Outgoing service. As anti-phishing method, the AXIGEN Mail Servers allows users to send emails

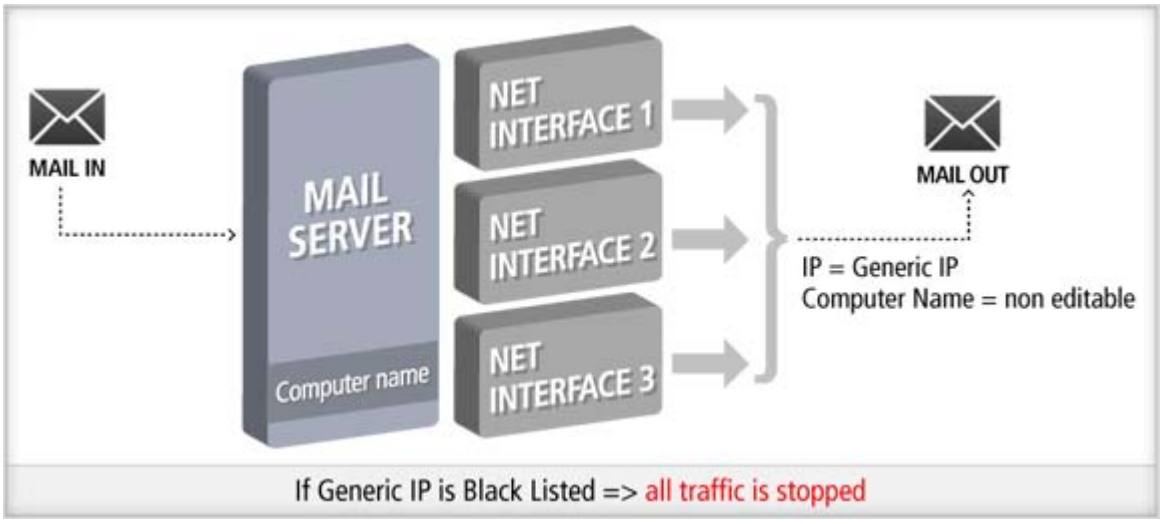
only from the email address they have used to authenticate. Therefore, identity theft is successfully prevented.

Routing Policies for Smart Delivery and Risk Hedging

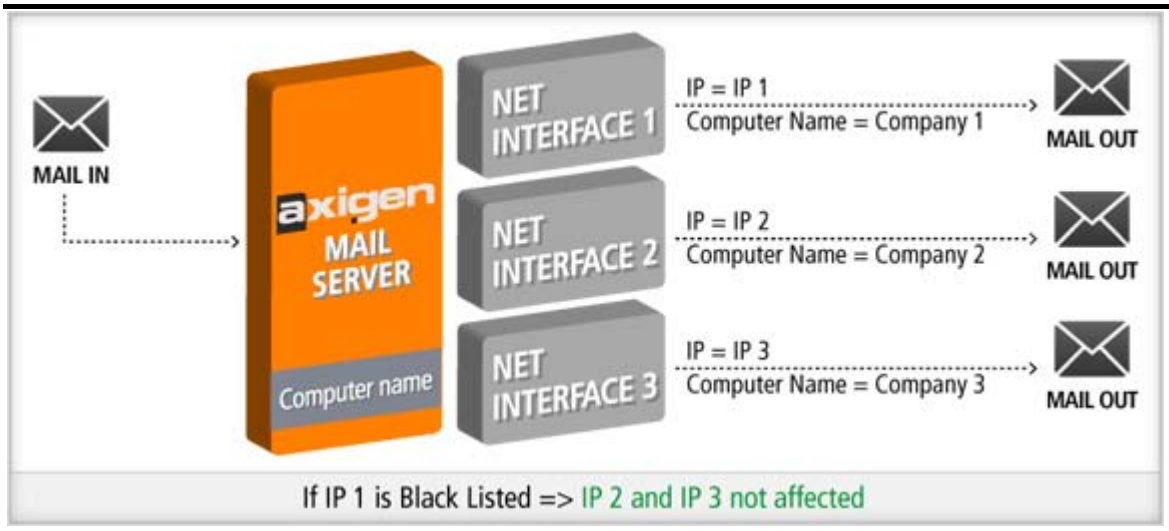
Routing policies enable administrators to define the NDR (Non-Delivery Receipt) text and the conditions when such a message is returned. As an example, NDR responses are sent when the specified recipient of an email message is invalid. They also allow system administrator to customize SMTP Outgoing actions for all or part of the relayed email communication. For example, they can

- establish a certain address where all emails from a certain domain are relayed;
- specify a username/password authentication before relaying emails to a certain address;
- requires AXIGEN to use a specific network interface when delivering an outgoing message

For most available mail servers, all emails sent from all the administered domains are sent via the same IP (the Generic IP in the below diagram). Moreover, there is no distinction between the internally used name assigned to a certain machine and the name it advertises outside the local network.



The AXIGEN Mail Server allows system administrators to assign different IP addresses to the domains our solution manages, as shown in the following diagram. If further enables them to assign more business relevant names to local machines, other than the internally used ones. The greatest advantage yielded by this unique feature is that if one of the company IPs is banned, the other domains will still be able to send emails.



Conclusion

Any of these methods can be used to protect you against current threats. AXIGEN provides system administrators with extended control over each step of the mail processing chain, allowing them a greater overall control. All of the above mentioned modules and extensions have been implemented in the product with security, availability and productivity in mind. One can use them in any combination to tailor the optimum setup, or all at once to ensure ultimate protection.

All the tools you will ever need to stop SPAM are here, where are you?

Article by Ciprian Negrila
Technical Support Engineer,
GeCAD Technologies, AXIGEN Division.
http://www.AXIGEN.com