



Content filtering strategies



Index

1. Filtering in mail servers	03
2. Filter characteristics	04
3. Items to filter	06
4. Malformed MIME headers	12
5. Content filtering characteristics and features in Panda Software antivirus software	13
:: Filter options	
:: Monitor	
:: Report	
:: Warnings	
:: Vulnerabilities	
7. Content filtering characteristics and features in Panda Antivirus Appliance	19

Filtering in mail servers

Latest figures indicate that some 90 percent of viruses that infect companies enter via e-mail. This exceptionally high figure is due, above all, to the widespread use of this means of communication by users who are not only exchanging messages but in many cases, are exchanging attached files such as documents, presentations etc.

If the use of e-mail were limited to just legitimate business purposes, there would probably be little need to worry about the threat of viruses when receiving e-mails. But the reality is that mail users don't just exchange work related messages. Jokes, leg-pulls and all sorts of executable files are just some of the things employees exchange with others both inside and outside the company.

Because of this, receiving an e-mail with an unusual subject title or an executable file unrelated to work is as commonplace as receiving a genuine internal work-related message.

Leaving aside issues concerning the legality of companies monitoring these kinds of messages, the subject of debate in many countries, what is essential is to avoid mail servers becoming hosts to files that could represent a security threat for the whole company.

Any executable code entering a company could be susceptible to containing viruses. Just because a specific type of virus has yet to be written for a particular system doesn't mean that the network is safe. From the obvious files with an EXE or COM extension, to the unheard of such as some Shockwave Flash versions, all files represent a varying degree of risk of containing malicious code. For this reason, filtering of items attached to e-mails should be constantly enabled.

Filter characteristics

Content filtering should work at two levels: corporate e-mail servers and Internet gateways.

Content filtering at just one of these levels is inadequate:

- If used exclusively in internal mail servers, the use of e-mail with tools other than the company's would produce a 'hole' in the filtering system. For example, all post Windows 98 versions of this operating system have Outlook Express as the default e-mail client. Using this application, it is easy to by pass the corporate server, although not the firewall.
- If filtering is only applied in the external mail server, e-mails that don't pass through the firewall will go unchecked. This means that any virus or hoax, any inappropriate message or just those that are considered unnecessary might not leave the company but will circulate throughout the company and go uncontrolled across the entire internal network.

Content filtering should be integrated with other systems.

Filtering should be based on three parameters:

- By e-mail subject. Thus drastically reducing SPAM and other unwanted advertising or hoaxes.
- By attached files. This allows files to be blocked by name, extension or both.
- By certain characteristics of the information. A corrupt or encrypted message can contain an item that may be a threat to the company.

Administrators can use the filter to take action on dangerous files without having to stop the mail server or the firewall and have a tight control over inbound and outbound messages without interfering directly with them.

Filter characteristics

The options available will be applicable to both nested messages and compressed files: :

Ignore: When the filter detects a file or message that meets filter criteria, the corresponding report will be generated, but no action will be taken on the object. This is the default option and allows administrators to monitor messages without users being aware.

Delete attachment: When a file meets filter criteria, by name or extension, or when it cannot be opened for some reason, the file will be deleted..

Move attachment: When a file meets filter criteria, by name or extension, the file will be moved to a folder as stipulated in the registry.

A warning will appear in the message. This can be customized by an entry in the registry.

Block message: Can apply to both subject and attachment filtering (in the latter case, the whole message will be deleted when a file meeting filter criteria is found). A warning message will be sent in plain text.

Items to filter

The following items should be filtered in servers to avoid immediate danger.

These recommendations aside, it is still possible that an item not in this list could pose a threat. Take BMP files for example. In theory, this file format cannot possibly contain malicious code, so it would seem safe to assume that it poses no threat.

However, just because the file is not dangerous doesn't automatically mean that the application isn't. If the application used to view these files has flaws, it may be possible that even a BMP file could prompt a program error, by exploiting a buffer overflow for example, or any other problem caused by malformed files or programming errors in a reader for a certain format.

The danger can only therefore be eliminated to a certain degree. Higher levels of protection involve closer study of the latest published vulnerabilities.

File extensions which must be filtered include:

***.{*}**. CLSID code. These are class identifiers. These codes, which are stored in the Windows registry, are used to register system components, ActiveX controls, etc. The danger is evident as registering an item without first having checked it represents a serious security risk. So for example, an attacker could offer, in a HTML e-mail or a web page, the file `testhta.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}` but Windows Explorer and Internet Explorer won't show the CLSID `{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}` so users would only see the apparently innocuous `.txt` extension when it is really `.hta` which can be executed and could contain malicious code.

ASD. Advanced Streaming Format Description file for Windows Media. Contains descriptions for Audio decoders for Windows Media.

ASF. Active Streaming File. Due to an error affecting 6.4, 7, 7.1 and XP versions of Windows Media Player related to ASF (Advanced Streaming Format). If a specially created `.ASF` file is created, it is possible to exploit a vulnerability in Media Player, because of an unchecked buffer in the processor.

Although it is not possible to exploit this vulnerability via web pages or HTML mail, the problem is serious as it allows attackers to run arbitrary code on a vulnerable machine if the program runs a malicious ASF file.

Items to filter

ASX. Windows Media Active Stream Redirector File. There are vulnerabilities in versions 6.4 and 7.0 of Windows Media Player. The Microsoft bulletin MS01-029 deals with this problem.

BAS. Visual Basic® module. These are executable code, and can be used to introduce almost any malicious code in the system.

BAT. MS-DOS batch processing file. In this programming system, although it is limited, there are viruses that can delete the content of the hard drive.

CHM. Compiled HTML file. This is the format of Windows help files. If a user receives a file and this is open, the HTML code will be run. This contains a script automatically enabled by Windows.

The problem lies in a vulnerability in Microsoft Internet Explorer 5.0 and 5.01 and Outlook 5.0 and 5.01 known as "Microsoft IFrame vulnerability", that allows malicious code to be run simply on opening an infected e-mail (Windows 95, 98 and NT). The root problem is in the creation of files in the Windows TEMP directory, with a known name and random content which allows a .CHM file to be downloaded to this directory and can then be executed. This vulnerability has been corrected in Internet Explorer 5.5 and in Outlook 5.5.

CMD. Windows NT and OS/2 Command files. These are similar to MS-DOS BAT files and can harbor malicious code.

COM. MS-DOS executable (Command). This was the first kind of MS-DOS executables, which was followed by EXE format. These files can occupy up to 64KB.

CPL. Control Panel Library. Although these are files with .CPL extensions, they are really DLL files with Control Panel functions, in Windows PE format. As these are executable, they can contain malicious code. In fact, many viruses infect CPL as well as the 'classic' executables.

CRT. Security certificate. Although these are designed to guarantee security, they can in fact validate unsafe elements or websites.

DLL. Dynamic Link Library. These are sections of code that can be run from any application. An infected DLL will be activated every time it is called from another program.

Items to filter

DOC, DOT, MCW. These are MS Word and Word for Macintosh documents or templates. They can contain macro viruses.

EXE. Executable applications. An extension generally used to store code that can be run directly by the user. This is real virus breeding ground..

HLP. Windows Help files. These files can also contain code that could infect the system.

HTA. HTML Application. HTA (Content-Type: application/hta), these are executed by Microsoft HTML Application host (MSHTA.EXE). Apart from the numerous viruses that exploit this extension (from the famous BubbleBoy to other really dangerous viruses), this type of extension still leaves Microsoft Internet Explorer 6 vulnerable, even if the patch released by Microsoft is installed.

HTO. Hierarchical Tagged Objects. A data description language that can be run on multiple platforms.

INF. Configuration information file.

INS. Internet Settings. Establishes the parameters to configure the Internet connection. Numerous INS files modify Internet connections to redirect them to premium rate numbers.

ISP. Internet Service Provider configuration.

JS. Java Script code file. It has been shown that there are a lot of possibilities for running malicious code, even breaching Java Virtual Machine security.

JSE. Java Script Encoded file. See JS.

LNK. Windows shortcut (Link). These allow programs to be run directly from a different location to the one where the program is. If the call is to items that could damage the system it could pose a serious threat.

MDB. Microsoft Data Base file. Access files contain a lot of data which could include certain macros that could contain viruses.

MDE. Microsoft Database Encoded.

Items to filter

MSC. Microsoft Console document. This is used to manage COM+ objects. There are two ways of implementing and managing COM+ applications, by using the Component Services administration tool (a Microsoft Management Console) or by writing command sequences for implementing and managing COM+ applications automatically, using code that uses administration objects supplied through the COMAdmin DLL.

MSI. Microsoft Installer. The code to be installed could contain dangerous objects.

MSP. Microsoft Patch. These are patches that are added to an existing installation file. They allow a program to be kept updated without needing to carry out the installation process again.

MST. Visual Test Source File.

OCX. Ole Control Extension. OLE controls in Windows can run code on the system and call internal functions without the user knowing what is being done and how.

PCD. Visual Basic file. As these files can contain executable code, there is a high risk that when they are run by users, computers will be damaged.

PIF. Program Information File. Used to pass parameters and set run conditions in DOS programs running under Windows. They can also be used to call programs installed in the system with certain parameters.

REG. Text file containing registry entries. By double-clicking on this file, the Registry entries it contains can be modified, changing the system functioning.

SCT. Windows Script file. Used for automating tasks in Windows, it can run and launch all types of programs and carry out other dangerous tasks.

SCR. Windows Screensaver. This file can contain potentially dangerous executable code.

SH. Shell script. Contains instructions that can be executed by Windows, which could be dangerous.

SHB. Embedded Shortcut. See .LNK.

Items to filter

SHS. Shell Scrap file. Information cut from an application and pasted as an independent file in another application. This information could be executable code, Scripts, etc.

URL. Uniform Resource Locator. This is a link to a Web address. It could point to an address that contains a virus or code that could damage the system.

VB. Visual Basic Script. Executable code that could contain a virus.

VBE. Visual Basic Encoded. See VB.

VBS. Visual Basic Script. See VB.

VCS. VCalendar file (Netscape, Works, Outlook). File for exchanging calendar data in HTML format which could contain malicious code.

WMS. Windows Messaging System. Mail file that could include attachments or other dangerous objects.

WMD. Windows Media Download. Certain vulnerabilities in Windows Media Player can be exploited using a JavaScript file embedded in a Windows Media download file (.wmd).

WMZ. Windows Media Player skins. JAVA code could be added to skins and run any local program, without the user knowing.

WSC. Windows Script Component. Can include many codes ranging from Visual Basic to Java, which could be malicious.

WSF. Windows Script File. See VB.

WSH. Windows Script Host. This is Microsoft's response to the need for a system programming language, similar to DOS BAT files.

XLS, XLT, XLA. Excel spreadsheet, template or Add-in file. Like Office documents, they could contain dangerous macros or code..

Items to filter

CORRUPT FILES. A file that seems to be corrupt could be a good hiding place for malicious code. Many programs incorporate options for restoring corrupt files so that the information can be recovered. If a virus were hidden in a corrupt file, an incorrectly configured filtering system would not identify the file as dangerous and would let the malicious code through.

ENCRYPTED FILES. The use of encryption to prevent information from being intercepted by a third-party is becoming more widely used. However, this function also prevents antivirus programs from opening the file and scanning it. Therefore, malicious code could reach a workstation without being detected by the protection system.

Malformed MIME headers

There is a constant increase in the amount of e-mails with malformed MIME headers, which can lead to serious security problems.

E-mail messages adhere to a standard for transmission over the Internet. Programs emitting and receiving emails interpret a series of instructions to ensure transmission and reception is performed correctly. These specifications, established in a document called RFC 822, define the message headers, which includes data such as recipient, subject etc.

However, specification RFC 822 did not broach any e-mail elements that went beyond plain text, and so an extra set of specifications were established called MIME, Multipurpose Internet Mail Extensions. These standards redefine message formats to allow texts coded other than by ASCII. MIME actually redefines the format of messages to allow for multi-part message bodies, for non-textual message bodies and textual header information in character sets other than US-ASCII.

These extensions can be malformed and thus compromise system security. Basically, there are two problems:

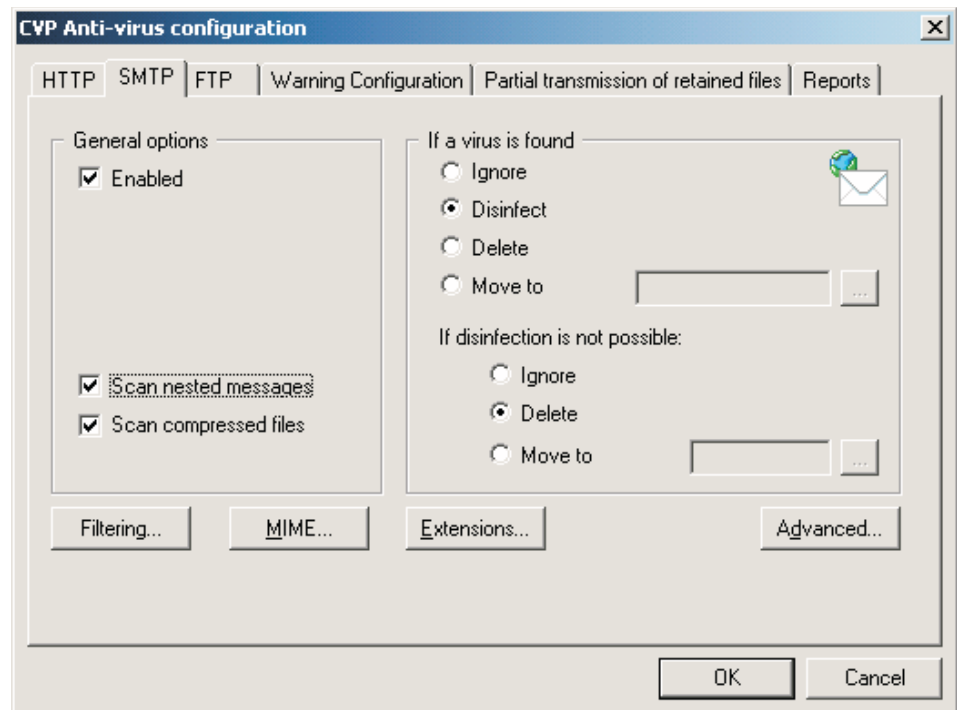
1. Opening an attachment to an e-mail without the user having expressly requested it. This is due to a vulnerability in Microsoft Internet Explorer 5.5 SP1, 5.01 SP1 or previous versions.
2. The impossibility for an antivirus program to scan the content of a message as the message header is malformed.

Content filtering characteristics and features in Panda Software antivirus software

The filter works under the antivirus developed for Firewalls, Exchange Server 5.5 and Exchange 2000.

It allows message filtering integrated with the antivirus, and can be configured from Panda Administrator. In Firewall it is configured through the SMTP scan options screen and in Exchange it is configured through the advanced configuration.

Administrators can use the filter to take action on dangerous files without having to stop the mail server or the firewall and have a tight control over inbound and outbound messages without interfering directly with them.



Content filtering characteristics and features in Panda Software antivirus software

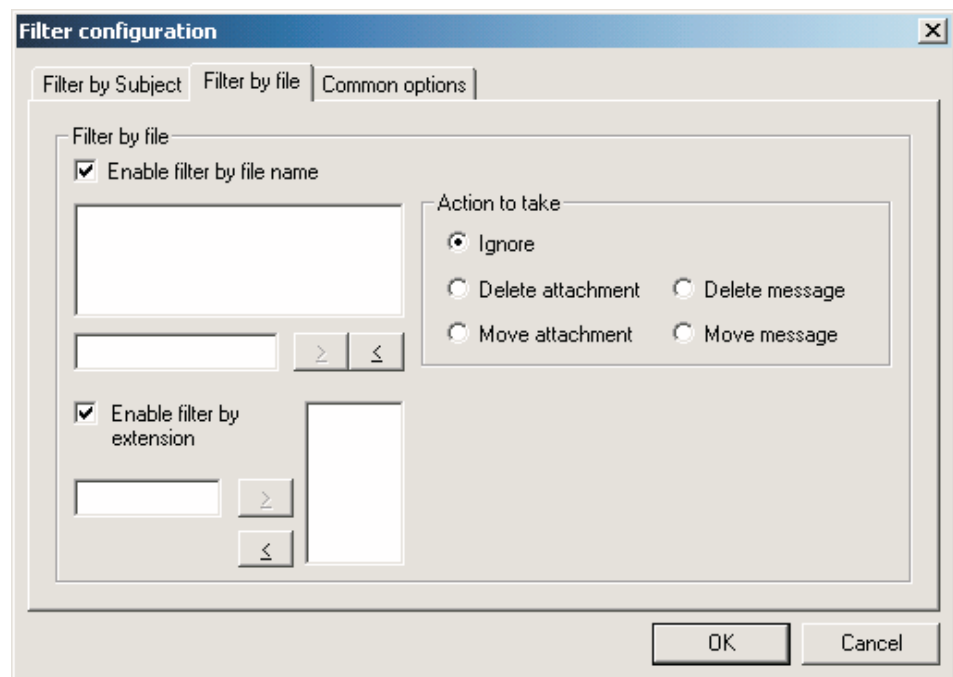
There are 2 types of filtering:

By subject: The subject field of the message is filtered by comparing it with a list of words. All messages with subject fields containing these words are filtered.

The following operators can be selected, || operators (if any word in the list is found, the message is filtered) and && (all of the words in the exclusions list must appear in the subject for the message to be filtered). These two options are exclusive.

By file: Messages can be filtered by both file name and extension. If both options are selected, the message is filtered if it fulfils one of the two conditions.

Filtering by file name allows file names and their extension to be entered, in order to filter specific files.



All of the filtering operations can be configured, regardless of the type of filtering.

1. Filter options

Ignore: When the filter detects a file or message that meets filter criteria, the corresponding report will be generated, but no action will be taken on the object.

This option is set by default and allows administrators to monitor messages without users being aware.

Delete attachment: When a file meets filter criteria, by name or extension, it will be deleted.

Move attachment: When a file meets filter criteria, by name or extension, it will be moved to a folder as stipulated in the registry.

A warning will appear in the message. This can be customized by an entry in the registry.

Block message: Can apply to both subject and attachment filtering (in the latter case, the whole message will be deleted when a file meeting filter criteria is found). A warning message will be sent in plain text, provided that the corresponding checkbox is enabled.

The options available will be applicable to both nested messages and compressed files.

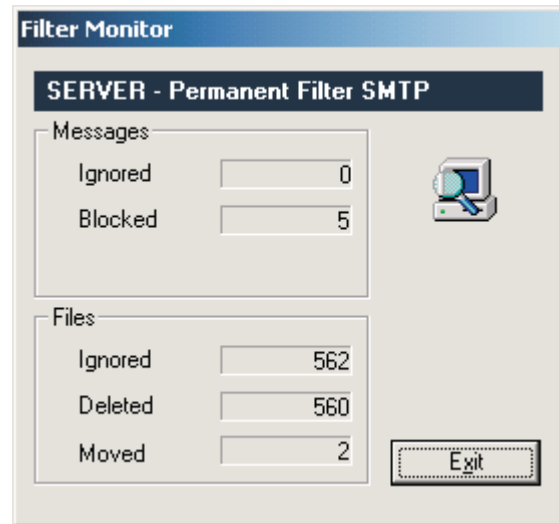
In the case of nested messages, it acts on the message with the filtered subject, regardless of its level of nesting, without modifying the 'parents' of this message.

In the case of compressed files, it acts inside these files in the same way as the antivirus, as long as they can be modified.

Content filtering characteristics and features in Panda Software antivirus software

2. Monitor

The number of files deleted, moved, ignored and blocked are monitored in a screen in Panda Administrator, independent of the antivirus monitor.



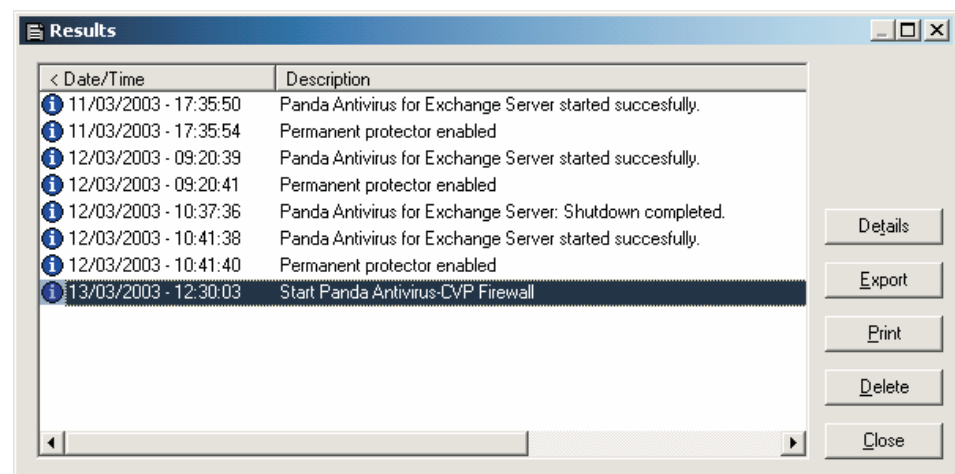
3. Report

The report option has the same characteristics as the antivirus report. It specifies the message that has been filtered, the actions carried out on the message or its files and the reasons why this action has been performed.

When it tries to carry out an action on an object and fails, the action reported is ignored.

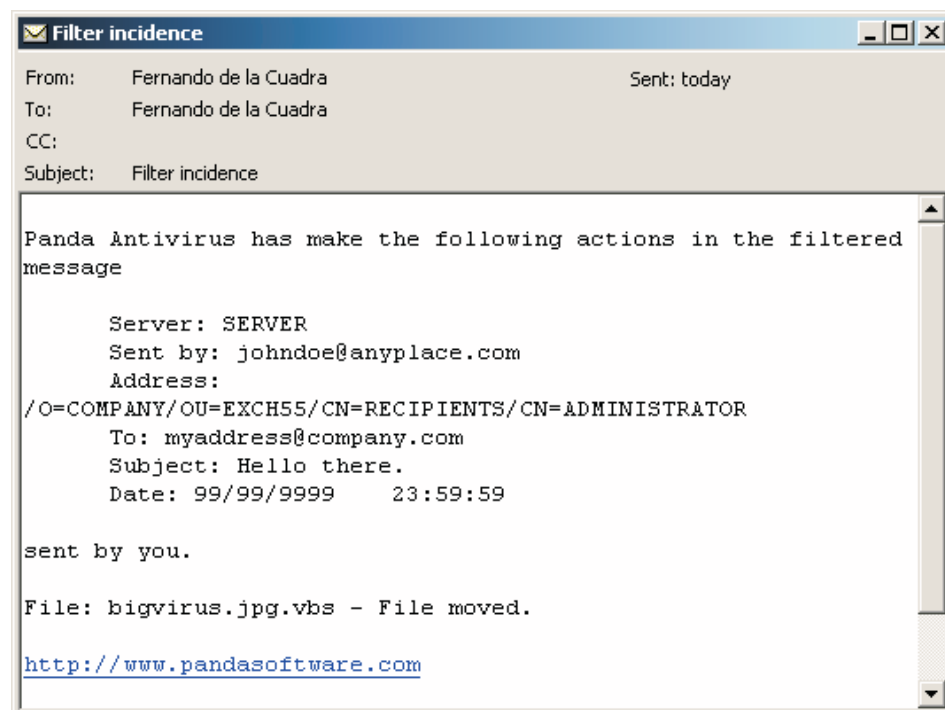
The report can be disabled independently from the antivirus report.

Content filtering STRATEGIES



4. Warnings

The configuration and functioning of the filter warnings work in the same way as in the antivirus. Both warnings are sent to the same recipients, but the content varies, specifying whether it is a virus warning or a filter warning.

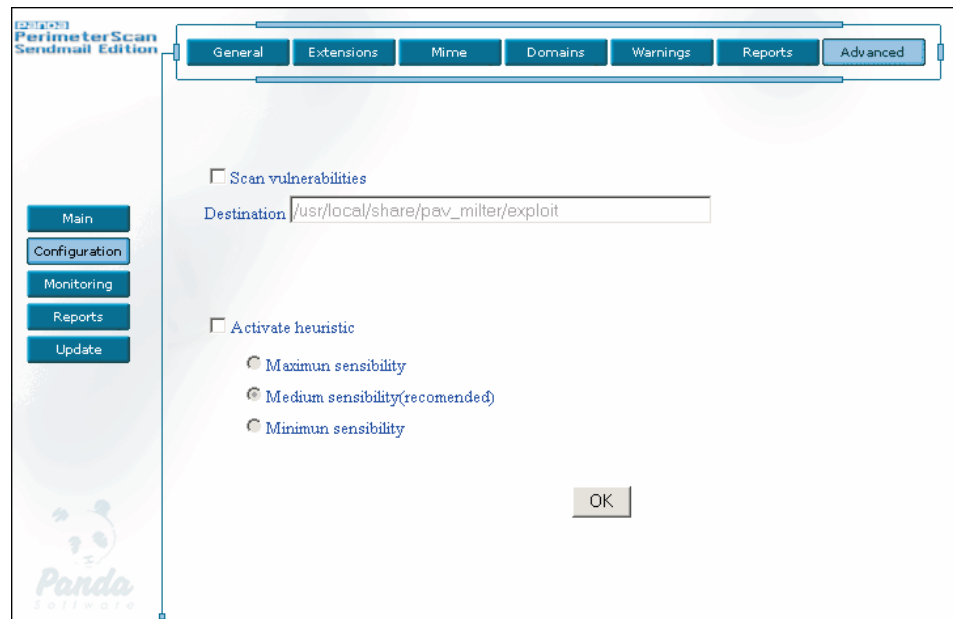


5. Vulnerabilities

To avoid the problems with malformed MIME headers, Panda Software has developed a system that blocks messages with malformed headers in the mail server, before they reach the recipients.

This feature is included in Panda Antivirus for Exchange Server, Panda Antivirus for Lotus Notes / Domino, Panda Antivirus for Firewalls, Panda Antivirus for ISA Server, Panda Antivirus PerimeterScan Sendmail Edition and Panda Antivirus PerimeterScan Qmail Edition.

Content filtering characteristics and features in Panda Software antivirus software



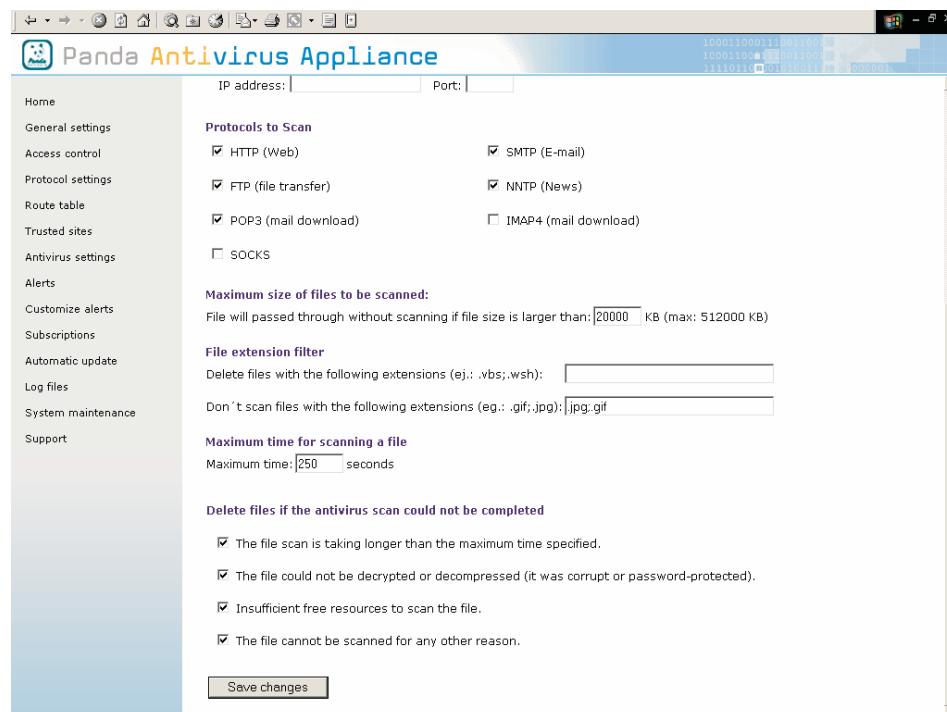
Content filtering characteristics and features in Panda Antivirus Appliance

Content filtering prevents unknown computer viruses and worms from entering a corporate network. This system avoids using network resources and bandwidth by stopping potentially dangerous content from crossing the network threshold.

The protection and filtering system is designed to be easily implemented in any corporate network, without needing to change any settings or redirect traffic. From the moment it is installed, Panda Antivirus Appliance will start to scan all network and Internet traffic, both inbound and outbound.

The filtering system easily and efficiently covers all the protection needs of the network against Internet-borne threats through its scan of the most commonly used protocols: SMTP, HTTP, POP3, FTP, NNTP, IMAP4 and SOCKS.

It can be managed remotely and securely through a simple and intuitive web console, offering the administrator the flexibility to access it from any computer. Through the web page you can configure:



Content filtering characteristics and features in Panda Antivirus Appliance

Protocols to Scan. In this section the protocols scanned by Panda Antivirus Appliance are enabled and disabled.

Maximum size of files to be scanned. The value entered in this box specifies the maximum size, in Kilobytes (KB), that a single file must occupy in order to be scanned for viruses.

File extension filter. The file extensions filter consists of two parts:

- Delete the files which have the extensions specified in the box. For example, if you do not want any executable files to enter the network, add the extension EXE to this box.
- Omit certain extensions from the scan. For example, you can leave files with a JPG or GIF out of the scan.

Maximum time for scanning a file. Panda Antivirus Appliance can be configured to stop scanning a certain file after a certain number of seconds. If for any reason the scan is not complete by the specified time, the options set in the section below will be applied.

Delete files if the antivirus scan could not be completed. When the scan of a certain file cannot be completed, for whatever reason, the file will be deleted according to the options selected:

- If “The file scan is taking longer than the maximum time specified” checkbox is enabled, the file will be deleted if the maximum time (in seconds) set in the previous section is exceeded.
- If the “The file could not be decrypted or decompressed (it was corrupt or password-protected)” checkbox is enabled, compressed, encrypted or corrupt files will be automatically deleted. These include files with the following extensions ZIP, ARJ, ARK, LHA, MSCOMP, CAB, LZEXE, PKLite, TAR, GZIP, Diet, LZW, Z, AMG, BINHEX, UUEncode, Base64, MIME, etc.

Content filtering characteristics and features in Panda Antivirus Appliance

- If the “Insufficient free resources to scan the file” checkbox is enabled, the files that the Appliance tries to scan when there are not enough free resources will be deleted.
- If “The file cannot be scanned for any other reason” checkbox is enabled and the file cannot be scanned for any other reason than those covered in the options described above, it will be immediately deleted. This is obviously the most drastic option and also that which offers the highest level of protection to files that cannot be scanned.