



# Panda Antivirus for CVP Firewalls

Technical manual



## PART I: CHECKPOINT FIREWALL-1

↓		
➤	<b>1. Introduction .....</b>	<b>5</b>
➤	<b>2. Firewall .....</b>	<b>6</b>
	2.1. What does a firewall offer .....	6
➤	<b>3. Firewall-1 Components .....</b>	<b>8</b>
	3.1 Distributed client/server architecture .....	8
	3.2. Graphical User Interface .....	9
	3.3. Management Server .....	9
	3.4. FireWall-1 Firewall Module .....	9
	3.5. Authentication .....	9
➤	<b>4. Configuration of Firewall-1 .....</b>	<b>10</b>
	4.1. Setting a Security Policy .....	10
	4.2. Rule Base .....	10
	4.3. Properties .....	10
	4.4. Network Object .....	10
	4.5. Rule base wizard .....	11
	4.6. Log Viewer .....	11
	4.7. Authentication .....	12
	4.8. Authentication Methods .....	12
	4.9. Network Address Translation .....	12
	4.10. Virtual Private Networks .....	12
	4.11. Content Security .....	13
	4.12. High Availability .....	13
	4.13. Reports .....	13
	4.14. Single Server Protection .....	13
	4.15. Malicious Activity Detection .....	14
	4.16. Intrusion Detection .....	14
	4.17. Open Security Extension .....	14
➤	<b>5. Installation of Check Point FireWall-1 .....</b>	<b>15</b>

Document prepared by Panda  
Software International's Product  
Marketing Dept.

August 2001.



## PART II: PANDA ANTIVIRUS FOR CVP FIREWALLS

↓	
➤	<b>1. Introduction</b> .....19
	1.1. Panda Antivirus for CVP Firewall .....19
	1.2. Panda Administrator .....19
➤	<b>2. Installation of the Antivirus</b> .....20
	2.1. Setting up the Firewall for the antivirus .....20
	2.2. Installation requirements of the antivirus .....20
	2.3. Creation of CVP server .....21
➤	<b>3. Configuration of the firewall Antivirus</b> .....25
	3.1. Scan .....25
	3.2. Presentation of Firewall scan reports .....26
	3.3. Intelligent updates .....26
	3.4. Scan report configuration .....26
	3.5. Configuration of partial transmission of files .....27
	3.6. Configuration of Transmissions through HTTP .....27
	3.7. Configuration of SMTP transmissions .....27
	3.8. Configuration of internal mail domains .....28
	3.9. Configuration of transmissions through FTP .....28
	3.10. Configuration of security .....29
	3.11. Configuration of MIME format .....29
	3.12. Extensions configuration .....30
	3.13. Advanced configuration in Firewall (heuristic scan) .....30
	3.14. Alerts configuration .....31
➤	<b>4. Uninstallation of the Antivirus</b> .....32

## PART III: INSTALLATION STRATEGIES

↓	
➤	<b>1. Load sharing across multiple security servers with the CVP protocol</b> .....33
➤	<b>2. Steps for installing load sharing across multiple CVP servers</b> .....33
➤	<b>3. Partial transmission of retained files</b> .....38





## PART IV: FREQUENTLY ASKED QUESTIONS

- 1. Why does Panda Administrator return an incorrect Password error during installation? .....40
- 2. Why haven't I got a connection between Panda Administrator and the antivirus for firewall? .....40
- 3. What HTTP error codes does the firewall return? .....41
- 4. Why do I have problems viewing \*.PDF files through http? .....42
- 5. What log files are generated during updates? .....42
- 6. What log is generated when installing and uninstalling the antivirus? .....43
- 7. What data should I provide about an incident? .....43
- 8. How do I configure the antivirus to use authenticated connections with the firewall? .....43
- 9. Why is nothing that goes through the smtp rule scanned? .....45



## 1. Introduction

Internet technology is driving a genuine business revolution in which companies are redefining the way they communicate with customers, sell products, and form business relationships.

As companies embrace the Internet to forge new business models, Internet security has never been more important. Organizations need to provide access to critical applications, data, and other resources, while at the same time securing all elements of their enterprise network – networks, systems, applications, and users – across the Internet, intranets and extranets. This is the field that Firewall intends to cover.

## 2. Firewall

A firewall restricts external user access to the internal network and internal user access to external networks, which is only carried out through a carefully controlled point (something like a drawbridge). Therefore, it prevents attackers from reaching other internal defenses and information from being filtered from the inside, such as that caused by Trojans. For this reason, the firewall is installed at the point where the internal network connects to Internet.

Given that all of the traffic that enters from Internet or leaves the internal network does so through the firewall, the firewall can examine it and decide whether it is acceptable or not and whether it will be forwarded to the recipient. At this point it is important to define “acceptable”. In order to do this, a security policy is established (the firewall rules) in which it is clearly established what type of traffic is allowed, between which source and which destination, which services are enabled, what content is admitted, etc. Depending on each particular case, there may be highly restrictive policies in which almost everything is prohibited and others that are more permissive, in which almost no blocks are enabled. The key lies in reaching a compromise between security needs and convenience.

### 2.1. What does a firewall offer

- ❑ **Isolates from Internet.** The objective of a firewall is to isolate the internal network from Internet, by restricting access to certain services to and from the network, at the same time as analyzing all the traffic that goes through it.

When a company network connects directly to Internet, all of the computers can then access external addresses and similarly the internal network can be accessed from the outside, exposing it to all types of attacks, especially if the connection is uninterrupted. If any of the Intranet computers succumb to an attack, the rest of the local network will be at risk. The firewall acts as a screen, only allowing services that are considered secure (for example, only e-mail and browsing, or other services depending on the security policy), whilst superfluous or potentially dangerous services are prohibited.

- ❑ **Bottle neck.** The firewall can also constitute a bottleneck that keeps attackers and risks away from the network to be protected; it prohibits both incoming and outgoing services that are vulnerable to attacks and protects against some types of attacks based on packet routing. The firewall is a security focus point known as perimeter defense, in which the administration and monitoring of the network security is concentrated instead of trying to protect each network machine in-depth, an alternative known as in-depth defense. Of course, the best global protection strategy will make use of both focus points, which complement each other. As every connection attempt should go through it, a well-configured firewall can send alerts when suspicious activities are detected, they may correspond to attempts to enter the network or attempts to send information from it, such as those carried out by Trojans that have managed to get inside it. If intrusion attempts are made on computers that are isolated from the network and therefore without a firewall, it may be a long time before they send an alert or may even result in a successful attack before being discovered.
- ❑ **Audit and usage log.** The firewall is a good place for collecting information about network usage. As a single access point, it can register all of the activity between the external and internal network. Using this data the administrator can study the type of traffic, the times that the server has the highest load, bandwidth usage and of course all of the intrusion attempts or traces left behind by attackers.
- ❑ **Content security.** There are other threats such as viruses, etc., against which even the best firewalls offer limited protection. An antivirus inspection of the material transferred via services such as e-mail, Internet or FTP is a feature that is being incorporated into an increasing number of firewalls. However, the problem arises that a lot of resources are used, as certain files must be expanded (ZIP, MIME, etc.), scanned and a decision must be taken before they are transferred through the network. Added to the threat of viruses are those of Java programs ActiveX controls, JavaScript or VisualBasic Script, which are potentially very dangerous and could be included in an e-mail message or in a web page. Some firewalls also block this type of content when it is suspicious. However, antivirus software should also be installed and run frequently in all of the workstations as the firewall cannot offer 100% protection against these dangers.

- **Authentication.** Identifying people or entities that access a protected network is vital for the majority of environments. This authentication is traditionally carried out through user names and passwords. However, this is not considered a reliable technique by strict security policies. Therefore, some firewalls allow more sophisticated authentication techniques to be used: smart cards, single use passwords, hardware keys, etc.
  
- **NAT – Network Address Translation.** An additional function of the firewall is to conceal internal corporate addresses by translating the addresses. This way there is only one valid Internet address (or a reduced number of addresses) and a large number of private addresses for the internal computers, which are not routable in Internet. The internal addresses are hidden from the outside.

### 3. Firewall-1 components

FireWall-1's scalable, modular architecture enables an organization to define and implement a single, centrally managed Security Policy. The enterprise Security Policy is defined at a central management console and downloaded to multiple enforcement points throughout the network.

FireWall-1 consists of the following components:

- Graphic User Interface (GUI)
- Management Server
- FireWall-1 Firewall Module

#### 3.1. Distributed client/server deployment

FireWall-1 manages the enterprise Security Policy through a distributed Client/Server architecture that ensures high performance, scalability, and centralized control. FireWall-1 components can be installed on the same machine or in flexible Client/Server configurations across a broad range of platforms.

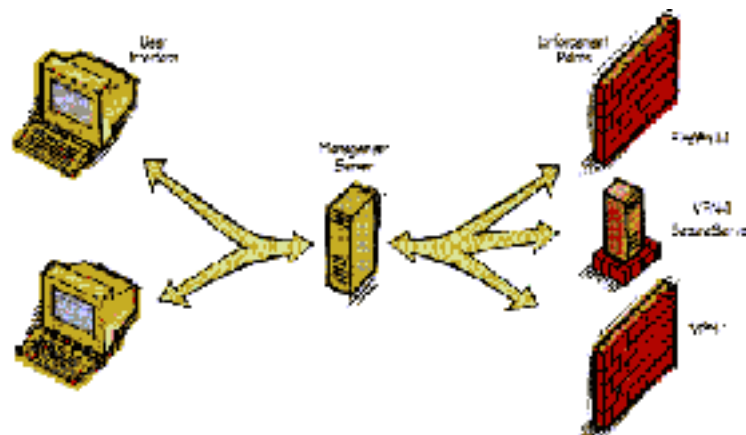


Figure I.1. Distributed Client/Server Configuration

In this configuration, the Security Administrator configures and monitors network activity for several sites from a single desktop machine.

The Security Policy is defined on the GUI Client, while the firewall database is maintained on the Management Server. The Security Policy is downloaded to three Firewall Modules, or enforcement points, that in turn protect three networks. The connections between the client, server, and multiple enforcement points are secured, enabling true remote management.

Although FireWall-1 is built in a distributed configuration, Security Policy enforcement is completely integrated. Any number of Firewall Modules can be set-up, monitored and controlled from a single workstation, but there is still only one enterprise-wide Security Policy that is defined and updated from a centralized management interface.

### 3.2. Graphical User Interface (GUI)

An enterprise-wide Security Policy is defined and managed using an intuitive graphical user interface. The Security Policy is defined in terms of network objects (for example, hosts, networks, gateways, etc.) and security rules. The FireWall-1 GUI also includes a Log Viewer and System Status Viewer.

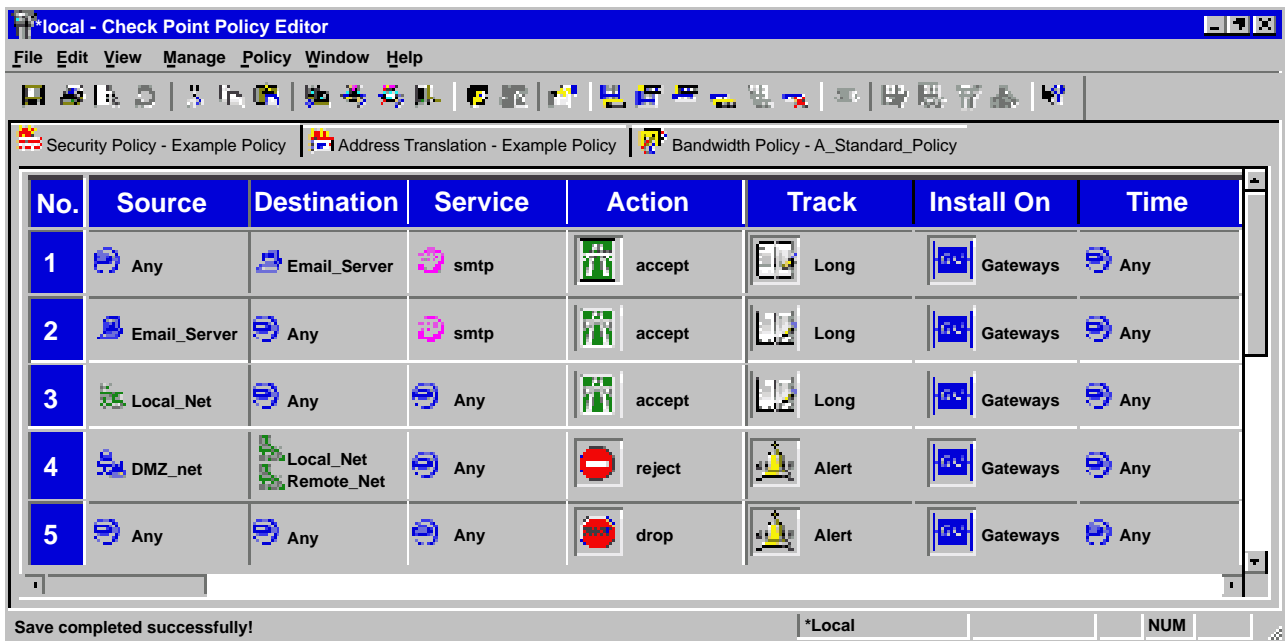


Figure I.2. Interfaz Gráfica de Usuario de FireWall-1

### 3.3. Management Server

The Security Policy is defined using the GUI and saved on the Management Server. The Management Server maintains the FireWall-1 databases, including network object definitions, user definitions, the Security Policy, and log files for any number of firewall enforcement points.

### 3.4. FireWall-1 Firewall Module

The FireWall-1 Firewall Module is deployed on Internet gateways and other network access points. The Management Server downloads the Security Policy to the Firewall Module, which protects the network.

Within the Firewall Module, a powerful FireWall-1 Inspection Module examines every packet passing through key locations in your network (Internet gateway, servers, workstations, routers, or switches), promptly blocking all unwanted communication attempts. Packets do not enter the network unless they comply with the enterprise Security Policy.

### 3.5. Authentication

The Security Servers provide authentication for users of FTP, HTTP, TELNET, and RLOGIN. If the Security Policy specifies authentication for any of these services, the Inspection Module diverts the connection to the appropriate Security Server. The Security Server performs the required authentication. If the authentication is successful, the connection proceeds to the specified destination.

## 4. Configuration of Firewall-1

### 4.1. Setting a Security Policy

The FireWall-1 GUI enables an enterprise to easily define a comprehensive Security Policy. A FireWall-1 Security Policy is defined in terms of a Rule Base and Properties.

### 4.2. Rule Base

A Rule Base is an ordered set of rules against which each communication is checked. Each rule specifies the source, destination, service, and action to be taken for each communication – for example, whether it is permitted or denied. A rule also specifies how a communication is tracked – for example, a specific event can be logged and then trigger an alert message.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	Email_Server	smtp	accept	Long	Gateways	Any
2	Email_Server	Any	smtp	accept	Long	Gateways	Any
3	Local_Net	Any	Any	accept	Long	Gateways	Any
4	DMZ_net	Local_Net Remote_Net	Any	reject	Alert	Gateways	Any
5	Any	Any	Any	drop	Alert	Gateways	Any

Figure I.3. Rule base

### 4.3. Properties

Properties specify general aspects of communication inspection, such as authentication session timeout periods, or how FireWall-1 handles established TCP connections. Properties are applied to all rules, so there is no need to specify repetitive details in the Security Policy.

### 4.4. Network Object

The Rule Base Editor enables administrators to define network resources in terms of simple objects (for example, gateways, networks, routers, or services) and their properties. Each object has a set of attributes, such as name or IP address. Objects are easily defined and updated. Network objects are defined and then used in the Rule Base.

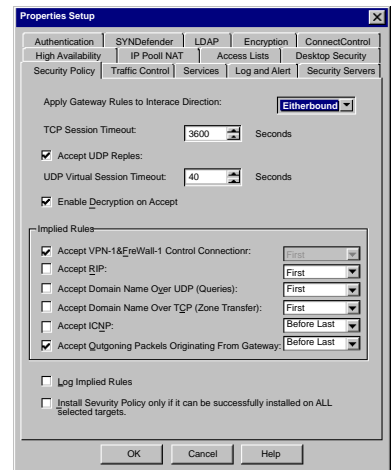


Figure I.4. Properties Setup Window

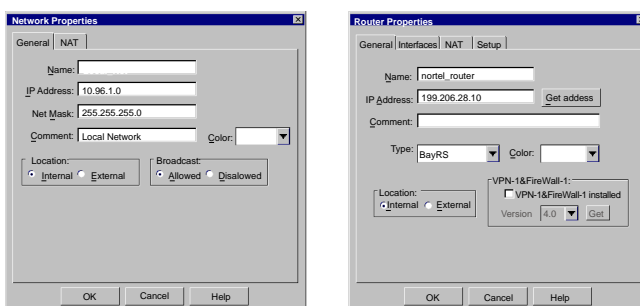


Figure I.5. Network and Router Object Definitions

### 4.5. Rule base wizard

FireWall-1 includes a Security Policy Wizard that automates security policy creation by walking the security manager through a series of security and network configuration questions. Security managers choose one of several network architectures and then answer a series of questions relating to security policy, NAT preferences, network object names, and IP addresses. From there, a rule base is automatically generated.

The Security Policy Wizard reduces the amount of time it takes to create a security policy and makes sure all the basic elements are in place for common network configurations. This makes initial FireWall-1 deployments faster and easier.

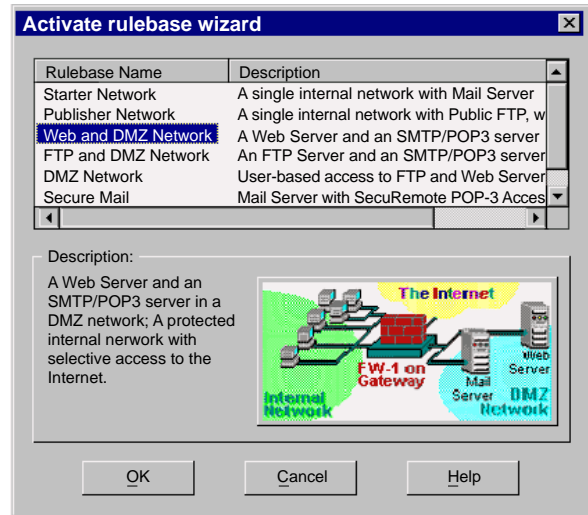


Figure I.6. Security Policy Wizard—Selecting a Network Architecture

### 4.6. Log Viewer: Visual Tracking and Accounting

FireWall-1’s graphical Log Viewer provides visual tracking, monitoring, and accounting information for all connections logged by FireWall-1 enforcement points. Online viewing features enable real-time monitoring of network activity. The Log Viewer provides control over the log file display, providing quick access to information. Administrators can customize the Log Viewer to display or hide specific fields or events. Logs and log records can be filtered and searched to quickly locate and track events of interest.

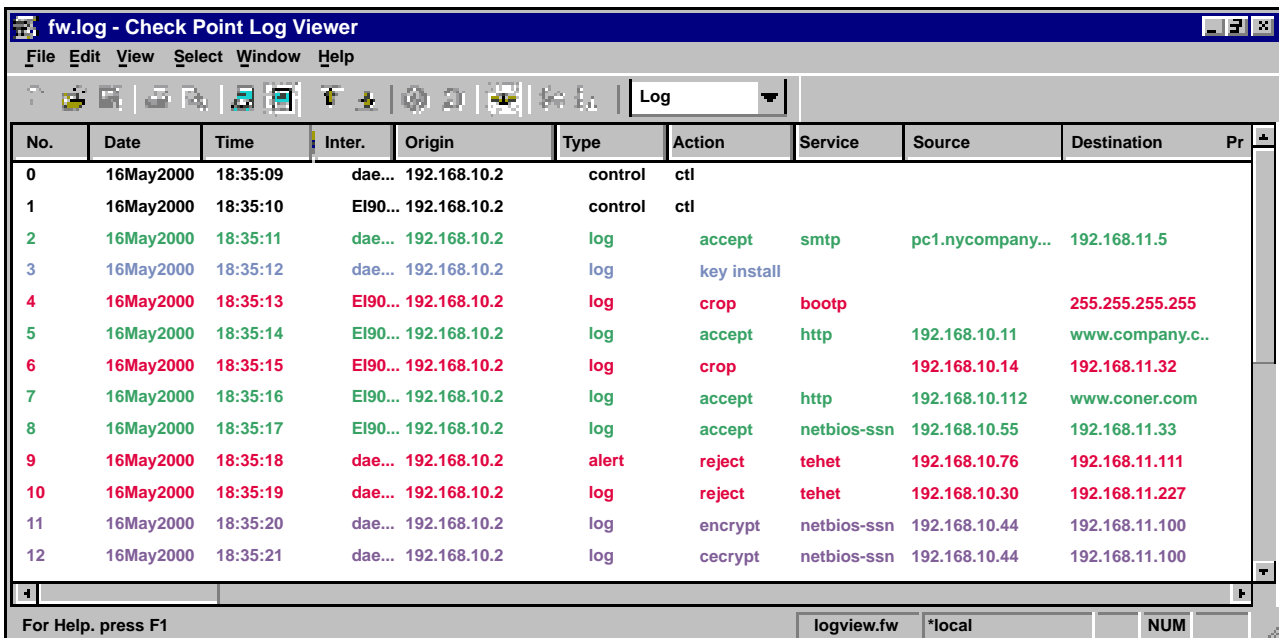


Figure I.7. Log Viewer

If administrators identify suspicious connections, the Log Viewer also allows them to terminate active and future connections based on specific IP addresses.

In addition to highly granular access control, FireWall-1 includes security and network management features that are fully integrated into the enterprise-wide Security Policy and managed through the graphical user interface. FireWall-1 and its add-on modules provide the following capabilities:

- Authentication
- Network Address Translation
- Virtual Private Networks
- Content Security
- High Availability
- Reporting
- Single Server Protection
- Visual Policy Editing
- LDAP-based User Management
- Malicious Activity Detection
- Intrusion Detection
- Third-party Device Management
- Server Load Balancing

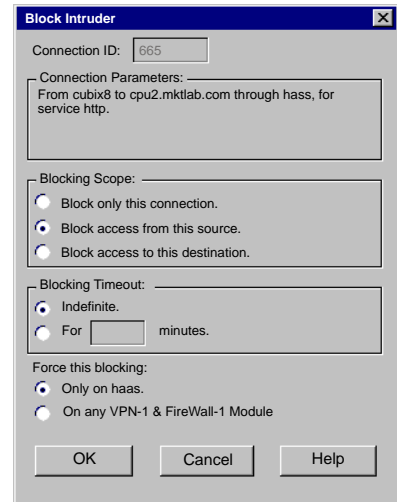


Figure I.8. Blocking Suspicious Connections.

#### 4.7. Authentication

FireWall-1 provides local and remote users secure, authenticated access to network resources. Flexible authentication methods provide access for users of any IP application or service. Administrators can determine how each individual is authenticated, which servers and applications are accessible and the times during which the user is granted access.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	All Users@Any	Public_FTP_Server	ftp	User Auth	Long	Gateways	Any

Figure I.9. User Authentication Rule.

#### 4.8. Authentication Methods

FireWall-1 provides the following authentication methods:

- User Authentication.** User Authentication provides access privileges on a per user basis for FTP, TELNET, HTTP, and RLOGIN, regardless of the user’s IP address.
- Client Authentication.** Client Authentication allows access from a specific IP address. The user working on a client performs the authentication by successfully meeting an authentication challenge, but it is the client machine that is granted access.
- Session Authentication.** Session Authentication can be used to transparently authenticate any service on a per-session basis.

#### 4.9. Network Address Translation

FireWall-1’s dynamic address translation hides internal addresses behind a single IP address, while static address translation maps each internal address to a corresponding valid address.

#### 4.10. Virtual Private Networks

The integration of FireWall-1 with Check Point’s optional VPN module forms VPN-1 Gateway, a tightly integrated software solution combining the security of FireWall-1 with VPN technologies.

#### 4.11. Content Security

FireWall-1 provides powerful Content Security for HTTP, SMTP and FTP connections, including anti-virus checking for transferred files, access control for specific network resources (for example, URLs, files, etc.) and SMTP commands.

#### 4.12. High Availability

The Check Point High Availability Module and high availability products deliver seamless fail-over for mission-critical FireWall-1 deployments by allowing customers to create clusters of redundant gateways. In the event that a primary gateway fails, all connections are re-directed to a designated backup.

The High Availability Module maintains all connections during a fail-over. If a primary gateway becomes unavailable, all sessions continue seamlessly without the need for users to re-connect and re-authenticate. Users will not even notice that an alternate gateway has taken over. In addition, high value business transactions and large file transfers continue intact without the need to restart.

#### 4.13. Reports

The optional CheckPoint Reporting Module is a log file analysis and reporting system that generates custom and pre-defined reports from FireWall-1 log data. The Reporting Module transforms FireWall-1's detailed log file data into useful management reports, presenting information in simple, intuitive tables and graphs.

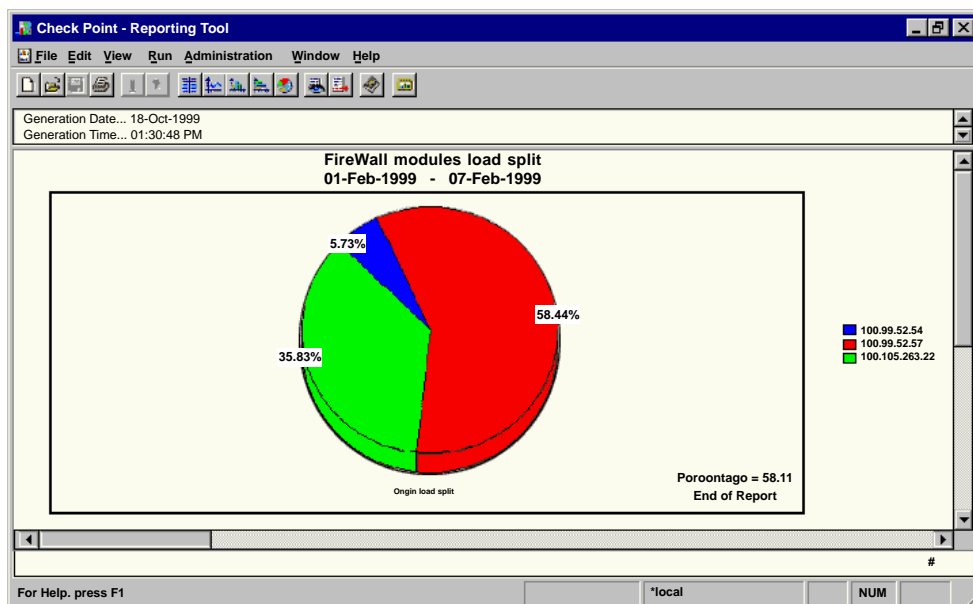


Figure I.10. Pie Chart Generated by the Reporting Module.

#### 4.14. Single Server Protection

VPN-1 SecureServer provides a cost-effective solution for protecting a single server running mission-critical applications.

#### 4.15. Malicious Activity Detection

FireWall-1's Malicious Activity Detection feature detects malicious or suspicious events and notifies the security administrator. Malicious Activity Detection analyzes log records to detect several well-known network attacks and suspicious activities, and generates alerts based on user defined thresholds when these activities are detected.

### 4.16. Intrusion Detection

Check Point RealSecure is a real time intrusion detection and response solution. When combined with FireWall-1, it provides the ultimate level of network security. Using RealSecure, administrators are dynamically able to detect network attacks and misuse based upon an extensive database of attack patterns that is regularly updated. Regardless of whether the attack originates externally or internally, it can be countered instantly in one of several ways depending upon the severity of the attack or misuse.

### 4.17. Open Security Extension

Check Point's Open Security Extension is an optional module that enables FireWall-1 to manage an enterprise-wide Security Policy for a variety of third-party network security devices, including products from Cisco, Nortel (Bay Networks), 3Com, and Microsoft.

## 5. Installation of Check Point FireWall-1

Installing Firewall is a very easy, though time-consuming, task, and, if you do not understand some concepts and have it clear which modules to install, it could become rather tedious. Follow these steps and you will complete the basic installation successfully.

After inserting the Firewall CD in the CD drive, the welcome screen will be displayed. This screen recommends you to close all programs you might have running, as well as giving you some information.

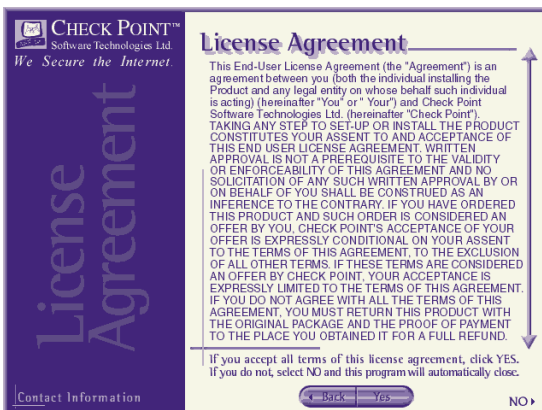
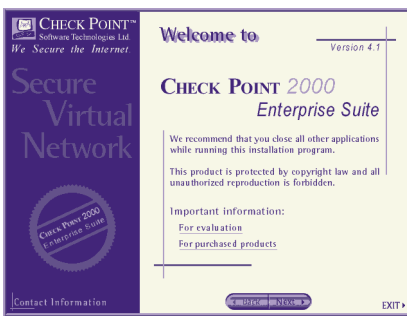


Figure I.11. After clicking on next “Next”, the license agreement appears.



Figure I.12. After accepting it, you will be asked which products you want to install. The first part, “Server/Gateway Components” allows you to install Firewall; the second, “Mobile/Desktop Components” is not strictly necessary unless you are going to install the VPN module or authentication sessions.

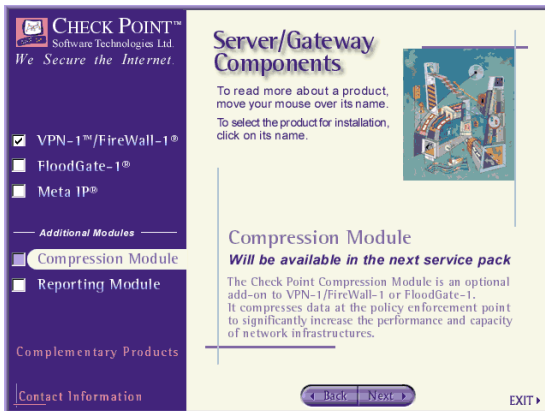


Figure I.13. The next screen gives you the option to install any Firewall module. For the basic installation, the “VPN-1/Firewall-1” module is enough.

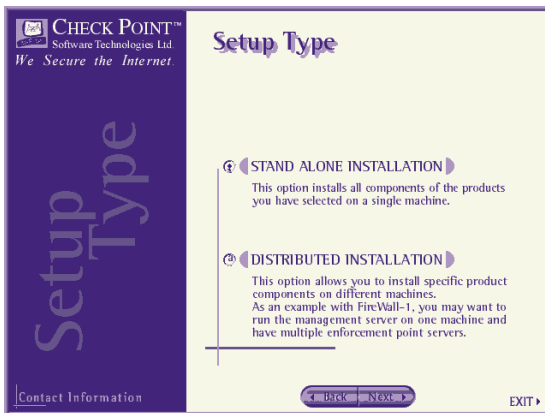


Figure I.14. The next screen gives you the option to install files on the system you are currently using or to perform a distributed installation. Select “Stand Alone Installation”.

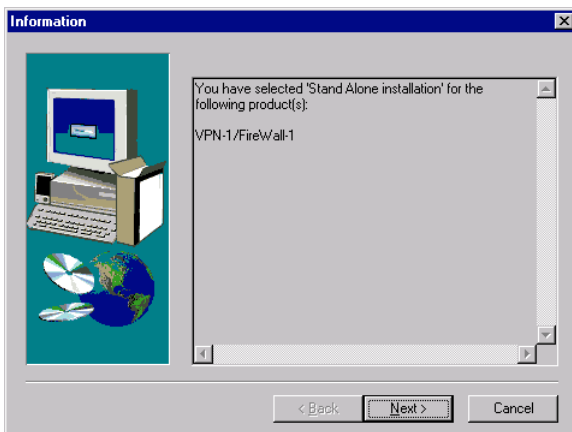
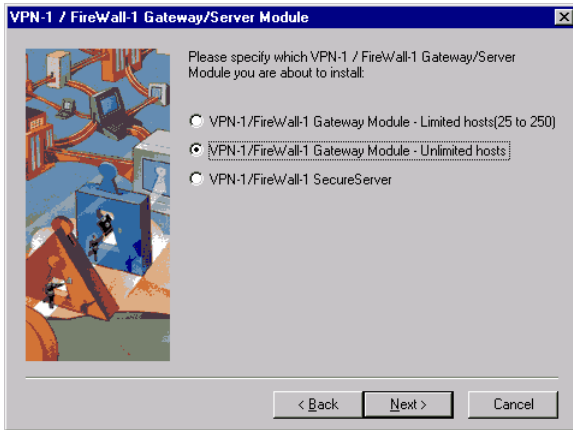
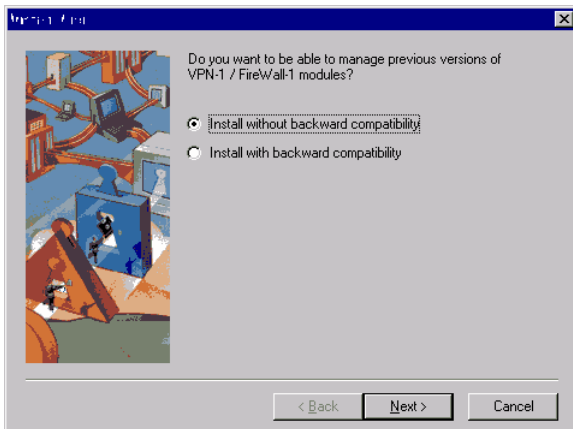


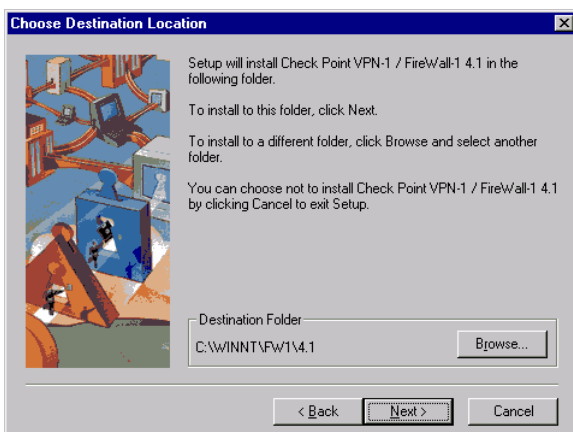
Figure I.15. You can now see a summary of the installation options chosen.



**Figure I.16.** The “real” installation begins now. You will be asked for the number of servers the Firewall is going to service in this network, depending on the number of licenses purchased.



**Figure I.17.** If you have an earlier version of Firewall already installed, you must choose whether you want the new version to be compatible with it or not. If you do not have an older version installed, you don't need to do anything.



**Figure I.18.** Next, the installation program asks you to choose the disk drive and folder where the necessary Firewall-1 files will be installed.

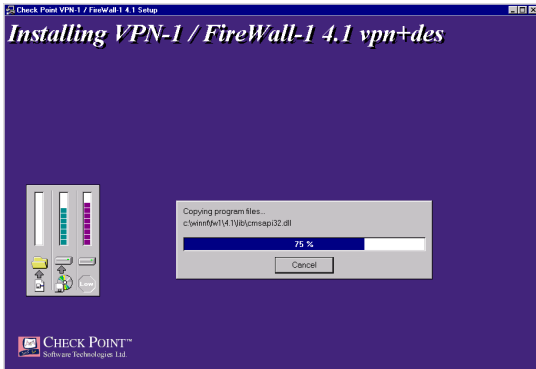


Figure I.19. After this, the copying of files begins.

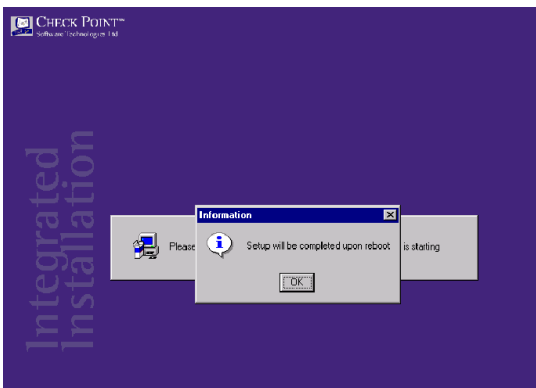


Figure I.20. Once the copying of files finishes, a message will be displayed telling you that installation will be completed the next time the computer is rebooted. **You don't need to reboot right now.**

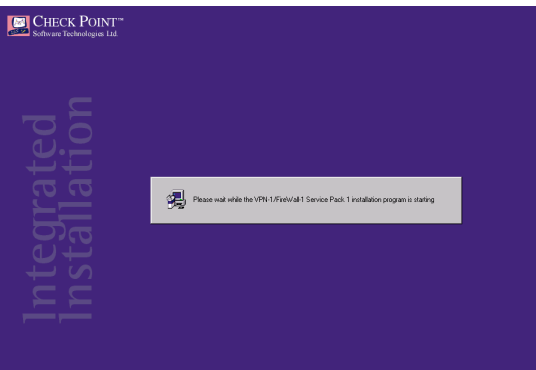


Figure I.21. Installation of Service Pack 2 for Check Point Firewall-1 begins. You only need to wait until all the files have been copied.

## 1. Introduction

### 1.1. Panda Antivirus for CVP Firewall

The objective of Panda Antivirus for Firewalls is to protect all of the information in files, which are sent to and from Internet, through the Firewall. Therefore it works like any other Firewall security component. The firewall controls access (to and from Internet), whilst the antivirus checks the information transferred and the elements that it contains (ActiveX Controls, Applets and scripts).

This means that it scans every transfer that is carried out from the protected network to Internet or vice-versa. Therefore the files that are sent or received through FTP, HTTP and SMTP protocols (a CVP server for all protocols or one for each protocol) will be protected by the network that contains the Firewall.

### 1.2. Panda Administrator

Panda Administrator is capable of managing antivirus protection for Checkpoint Firewall (CVP servers). To do this, certain conditions are necessary in the Firewall system: Check Point Firewall-1 v. 3.0b, or higher version and any operating system (Windows NT 4.0 Server SP5 or higher version, Unix, etc).

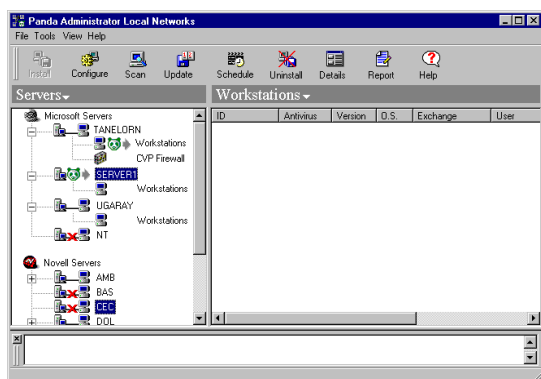


Figure II.1. Main window of Panda Administrator.

The main window of Panda Administrator shows the servers detected. Amongst these servers are the CVP servers in which the antivirus can be installed. The antivirus will scan all of the files transferred to the Firewall and will send it the appropriate information: file accepted (as it is virus-free) or file blocked until it has been disinfected. In summary, Panda Antivirus for Firewall acts as a security component that scans, controls and filters the files that go through the Firewall.

## 2. Installation of the Antivirus

When installing Panda Antivirus for Firewall certain conditions regarding the Firewall rules and certain requirements of the antivirus must be met. The Firewall rules must be modified so that it redirects the FTP, HTTP and SMTP protocol transmissions to the server with the antivirus installed (if there is one server for each protocol, the transmissions must be redirected to the corresponding server). To summarize, if the Firewall is not configured correctly, the corresponding scans will not be carried out from the CVP server.

### 2.1 Setting up the Firewall for the antivirus

- ❑ Check Point Firewall v. 3.0b, or later must be installed.
- ❑ Any operating system (Windows NT, Unix, etc).
- ❑ Consider the CVP servers (Content Vector Protocol) when configuring the Firewall. To do this follow the steps below:
  1. Create the CVP server.
  2. Select the redirection of FTP, HTTP and SMTP transmissions to the corresponding CVP server.
  3. Force all files to be redirected to the CVP server, for each protocol. This means modifying the Firewall security policy, indicating that the SMTP, FTP and HTTP should be FTP\_av, HTTP\_av and SMTP\_av, respectively.

These concepts are covered in detail in section 2.3 Creating CVP Servers on page 21.

### 2.2. Installation requirements of the antivirus

- ❑ Windows NT 4.0 Server SP3 or later version must be installed.
- ❑ Pentium processor II 300 MHz, or faster.
- ❑ 64 MB of RAM memory (recommended 128 MB).
- ❑ Minimum of 10 MB free space on the hard disk.

In order to carry out the installation a connection with administrator privileges must be opened with the server in which Panda Antivirus for Firewall is going to be installed.

Select the NT server in which the antivirus for Firewall is going to be installed. You should then expand the branch under it, right click on the branch and select "Show Antivirus for Firewall". The **CVP server** icon will be displayed in all computers with Windows NT 4.0 SP3 (or later), in which the antivirus can be installed. Select it and click on **Install**.

The version of the operating system installed will automatically be checked. If the antivirus can be installed in that server (as all of the requirements are met), the installation wizard will appear, which will guide you through the process step-by-step:

- ❑ **Administrator domain and account.** The following data must be entered: **Domain**, **Account** and **Password** of the computer in which the antivirus is being installed.

The field in which the administrator domain and account are entered should have the following format: **Domain\Account**. If it is being installed from the same computer as that in which **Panda Administrator** is running, the domain can be entered: **.Account**.

The early versions of the Firewall did not assign administrator accounts the "Start session as batch processing" and "Act as part of the operating system" privileges, as they had to have them beforehand. You should check if these privileges have been assigned.

- ❑ Then the installation process will begin, the appropriate directories will be created, the necessary files will be copied, the CVP server service will be created and started up, etc. When this has been done, the process will start up the service.

An icon will indicate that the antivirus is installed in the CVP server.

### 2.3. Creation of CVP server

#### □ Adding the physical server

This has usually been done. It involves giving the Firewall software some information about the computers in the network. If you have just finished the installation, follow these steps.

1. In the FireWall-1 configuration tab select **Manage |Network Objects...**
2. Select **New**, then **Workstation**.
3. In the **General** tab, enter the name of the computer where the antivirus is (or is going to be) installed in the **Name** field .
4. In the **IP Address** field, enter the IP address of the server or click on **Get address** so that FireWall-1 can automatically get it.
5. Fill out the rest of the page as necessary; e.g., **Type** (which must be Gateway) and **Location**.
6. In the **Interfaces** tab, fill out the fields for the network cards installed in the computer. Click on **Get** and the software will look for this data.
7. Click on **Close** when done.

**NOTE:**

If there is only one computer for the three antivirus services (SMTP, FTP and HTTP), you only need one network object. If you are going to share out the antivirus services or if you are going to use a shared load, you must repeat this process on every computer from where Firewall is going to send information to the antivirus program.

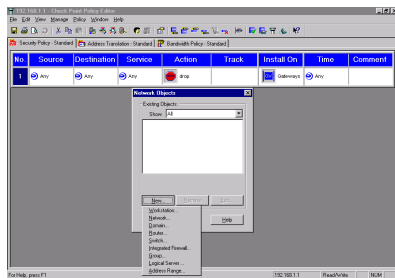


Figure II.2.

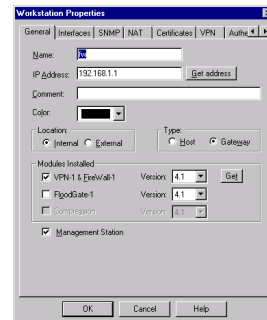


Figure II.3.

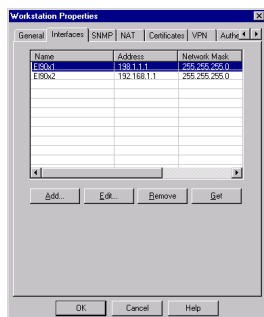


Figure II.4.

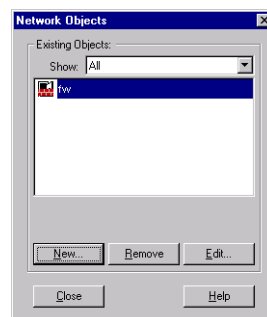


Figure II.5.

### □ Creation of the CVP server

1. In the FireWall-1 configuration tab, select **Manage | Servers...**
2. Select **New...**, then chose **CVP** from the menu.
3. Enter the name of the server in the **Name** field. You can give it any name you want, as long as you follow the naming rules given by CheckPoint (alphanumeric characters, no blank spaces, etc.).
4. Then, in the **Host** field, select the name of the network object(s) (previously created or created during the Firewall configuration) in which the antivirus program has been or is going to be installed.
5. Select the **FW1\_cvp** service.
6. Select **OK** and then **Close**. Repeat these steps for every computer with the antivirus installed (SMTP, HTTP, FTP).

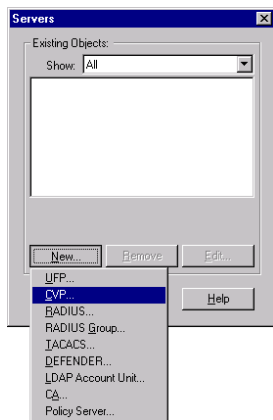


Figure II.6.

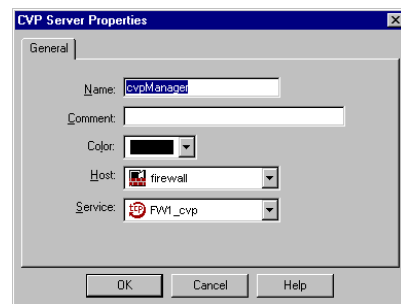


Figure II.7.

□ **Creation of the resource**

1. In the FireWall-1 configuration tab, select **Manage | Resources...**
2. Select **New...**, then select the appropriate protocol from the menu. To create a CVP server in charge of HTTP (or FTP) traffic:
  - ▶ Select URI (or FTP) from the menu.
  - ▶ In the **General** tab, enter the name of the resource in the **Name** field. This name will identify the CVP server. It does not have to be the same as the name of the server.
  - ▶ Select the **Match** tab and check the **HTTP** and **FTP** boxes. You should also include all methods of capturing files, as well as putting an asterisk in the **Other**, **Host**, **Path** and **Query** boxes.
  - ▶ Select the **Action** tab and, in the **Server** box, select the CVP server defined in the previous section "Creation of a CVP Server". You should also check the **Read/Write** box so the Antivirus program can disinfect.
3. To create a CVP server in charge of SMTP traffic, you need to create two different resources. One will be in charge of the internal mail and the other of external mail. So you will need to carry out the following steps twice, once for the internal mail and once for external.
  - ▶ Select SMTP from the resource creation menu.
  - ▶ In the **General** tab, enter the name of the resource in the **Name** field. This name will identify the CVP server. It does not have to be the same as the name of the server.
  - ▶ In the **General** tab, enter the name of the resource in the **Name** field. This name will identify the CVP server. It does not have to be the same as the name of the server.
  - ▶ In the **Match** tab, put an asterisk on both boxes.
  - ▶ In the **Action1** tab, you do not need to change anything. In the **Action2** tab, you need to select the resource defined in section 2 "Creating a CVP Server" and then check the **Read/Write** box.
  - ▶ When you click OK, a window will be displayed, asking you if MIME types should be stripped. You must choose no, otherwise viruses will not be detected.
4. Select **OK** and **Close**.



Figure II.8.

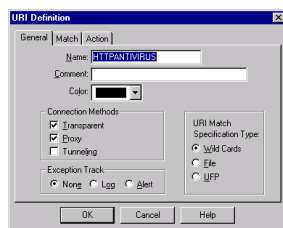


Figure II.9.

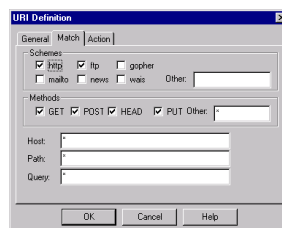


Figure II.10.

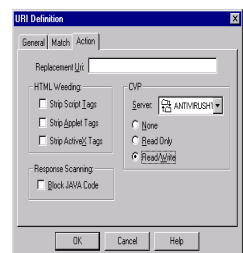


Figure II.11.

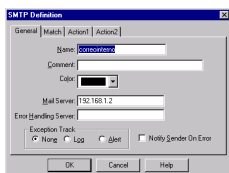


Figure II.12.

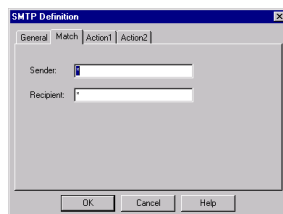


Figure II.13.

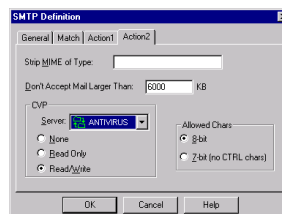


Figure II.14.



Figure II.15.

□ Configuration of the rules

1. In the FireWall-1 configuration tab, select **Edit | Add Rule | Top** to create a new rule.
2. Then, right click on the **Service** column of the rule and select **Add With Resource...**
3. From the service list that appears, select:
  - ▶ SMTP for e-mail and select the server with the antivirus installed that will be in charge of e-mail traffic.
  - ▶ HTTP for Internet traffic and select the server with the antivirus installed that will be in charge of Internet traffic.
  - ▶ FTP for file transfers and select the server with the antivirus installed that will be in charge of files.
4. Right click on the **Action** column and select **OK** from the menu.

No.	Source	Destination	Service	Action	Track
1	LocalNet	Any	http->http_viruswall_resource ftp->ftp_viruswall_resource	accept	Long
2	MailServer	Any	smtp->smtp_viruswall_resource	accept	Long
3	Any	MailServer	smtp->smtp_viruswall_resource	accept	Long
4	Any	Any	Any	reject	Long

Figure II.16.

**VERY IMPORTANT NOTE:**

FireWall-1 examines the rules sequentially, from top to bottom, until a rule matches the type of traffic being examined. We recommend placing antivirus rules before any others. In addition, after any change in the Firewall configuration or the rules (implicit or explicit), demand these rules (**Policy|Install**) to be installed again so they function normally.

### 3. Configuration of the firewall Antivirus

Panda Antivirus for Firewall allows users to configure the scans carried out in the CVP servers in which it is installed. Similarly, it is possible to configure the reports that the antivirus generates when certain events occur, the alerts messages that must be sent when a virus is detected, the partial transmission of files (in packets) through the server and the transfers carried out through the: HTTP, SMTP and FTP protocols.

To configure the antivirus, select the server in the Panda Administrator server tree and click on the **Configure** button. A dialog box will then appear with the following tabs:

- HTTP Transfer Configuration (Web Pages).
- SMTP Transfer Configuration (e-mail).
- FTP Transfer Configuration (File Transfer).
- Alerts Configuration.
- Configuration of Partial Transmission of Files.
- Reports Configuration.

#### 3.1 Scan

The scan carried out on the Firewall is based either on pre-established or default criteria. Any files sent or received will be scanned according to the following:

- Type of file (extensions).** The file may or may not be scanned, depending on its format. In other words, using the list of extensions to be scanned, it is possible to determine which files the antivirus should or should not scan. By default, the antivirus always scans EXE and COM files.
- MIME type or format (type/subtype).** In this case, files may or may not be scanned depending on its MIME type and subtype, (text/html, text/html, text/plain,). This is defined in the lists of Types Included and Types Excluded. You must have chosen not to strip MIME types in the Firewall, otherwise they will not be scanned. (See part 3. source on page 23, under section 2.3. Servers, on page 21).

With Panda Antivirus for Firewall it is possible to stop the permanent scan or protection. To access the permanent scan, select the CVP server in which it has been defined and click on the Scan button. In the dialog box a list of the scan jobs currently defined will be displayed:

This list is called the **Job Monitor** and presents information divided into columns which show the scan type (all permanent scans of SMTP, FTP or HTTP), the number of viruses that have been detected and the current status (if it is running or not). There will always be three scans in the central area. These scans corresponding to the continuous scanning of SMTP (e-mail), FTP (file transfer) and HTTP (Web pages). The only operations that can be carried out with the Firewall permanent scans are:

- Presentation of Firewall scan reports.
- Monitoring of Firewall scan jobs.
- Stop and abort a Firewall scan job.

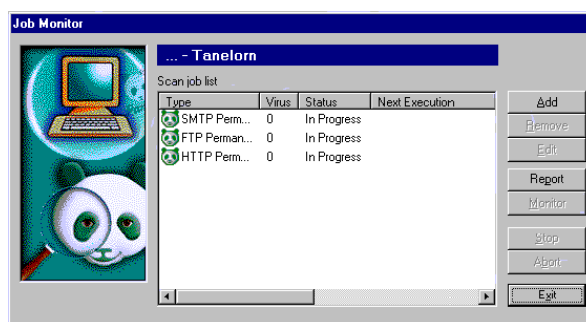


Figure II.17.

### 3.2. Presentation of Firewall scan reports

Panda Antivirus for Firewall offers you the possibility of creating a report file in which the activities of each scan performed are summarized. This report will be saved in a file that can be assigned a maximum size. This information is very useful, as it lets you see the job that has been carried out, the date and time the scan was performed and the results obtained.

The information shown is listed in columns. The first column details the date and time the detection was made and the second indicates the name of the virus detected. If you need a hard copy of this information, just click on the Print button. On the other hand, when you have finished viewing the information, you need only click the Seen button to close the window and return to the application. To delete the report, simply click on the Delete button. By doing this, you will delete the entire report containing all the scan activity data.

The information that appears in this report window is only a summary of the complete data available. By double clicking on any of the listed scans, the following additional information will be provided:

- ❑ **Date and time:** this shows the date and time that the detection occurred.
- ❑ **File:** this is the name of the infected file.
- ❑ **MIME Type:** indicates the MIME format of the infected file. This section gives details on the file type and subtype, in the following way: type/subtype (for example, application/msword).
- ❑ **Name of virus:** this field shows the name of the virus detected.
- ❑ **Host:** Indicates the name of the Internet server (its domain), from which the file that the antivirus considers to be infected has been transferred (downloaded).
- ❑ **URL:** indicates the path or address, as well as the how the virus has been detected. Information on how it was transferred will be presented (http://, for example), the name of the server and path or location of the infected file, as well as its name (this will appear at the end).
- ❑ **Result of the action:** presents the action carried out by the antivirus.
- ❑ **Date and time: this shows the date and** time that the detection occurred.
- ❑ **File:** this is the name of the infected file.
- ❑ **MIME Type:** indicates the MIME format of the infected file. This section gives details on the file type and subtype, in the following way: type/subtype (for example, application/msword).
- ❑ **Name of virus:** this field shows the name of the virus detected.
- ❑ **Host:** Indicates the name of the Internet server (its domain), from which the file that the antivirus considers to be infected has been transferred (downloaded).
- ❑ **URL:** indicates the path or address, as well as the how the virus has been detected. Information on how it was transferred will be presented (http://, for example), the name of the server and path or location of the infected file, as well as its name (this will appear at the end).
- ❑ **Result of the action:** presents the action carried out by the antivirus.

### 3.3. Intelligent updates

Panda Antivirus for Firewall can be updated manually as well as automatically. Intelligent updates apply to the virus signature file updates and the antivirus scan engine updates.

### 3.4. Scan report configuration

The information the antivirus generates when it performs certain operations can be saved in a file where all incidents are stored.

After accessing the antivirus for Firewall configuration, select the **Reports** tab. The following options will appear:

**Incidents to be logged in the report.** Using the checkboxes, the incidents that the antivirus must include in the report can be set.

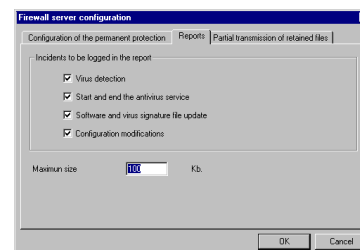


Figure II.18.

### 3.5. Configuration of partial transmission of files

The antivirus should scan all files sent or received through the Firewall. To do this, it needs to retain every one of these files in the server until the complete file has been received. Furthermore, the file cannot be retained in the server for longer than a certain amount of time, as the client that is receiving the file will terminate the connection.

When sending packets which are part of the file being transferred, the antivirus can scan each one without using up too much of the waiting time. If an infected file is being sent to a client through packets, the antivirus can disinfect it so that the recipient receives a disinfected file.

To set an ideal configuration for retained files, select the CVP server and click on the **Configure** button on the toolbar of Panda Administrator. In the dialog box which appears, select the tab; **Partial transmission of retained files**, the following options will appear:

- ❑ **Retain file until it has been scanned.** The antivirus will not send the complete file (from the CVP server to the client) until it has been fully scanned. This means that the client will not receive anything until this file has been fully scanned.
- ❑ **Send part of the file before it is scanned.** The user waiting for the file will receive it in packets. Each one will be scanned before it is sent. This means that the information arrives as sections of the file, which have already been scanned by the antivirus. This option is highly recommended. If it is selected, it is necessary to set a series of parameters, which guarantee the correct functioning of the system.

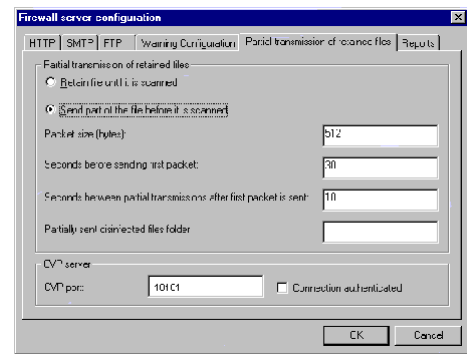


Figure II.19.

### 3.6. Configuration of Transmissions through HTTP (Web)

The configuration of transfers through the HTTP protocol allows you to determine the actions to carry out when an infected file transmitted through Web pages is detected (or when the Web page itself contains elements that might become infected). These actions are the following:

It is worth highlighting that the antivirus program scans Java Applets, i.e. it will scan CLASS files. If you chose to scan all extensions in the extensions list, CLASS files will not be included.

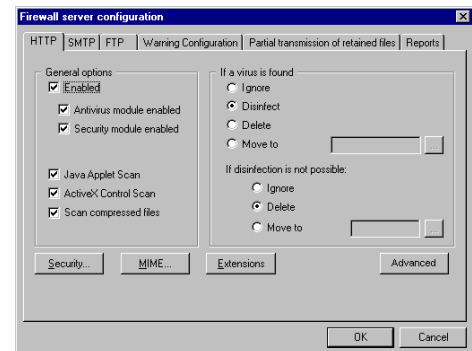


Figure II.20.

### 3.7. Configuration of SMTP transmissions

The configuration of file transfers through the SMTP protocol (e-mail) allows users to select the actions to carry out if an infected file is detected in e-mail messages. This type of scan is focused on e-mail messages, the files they might contain, nested files (included in other messages) and files contained in nested files.

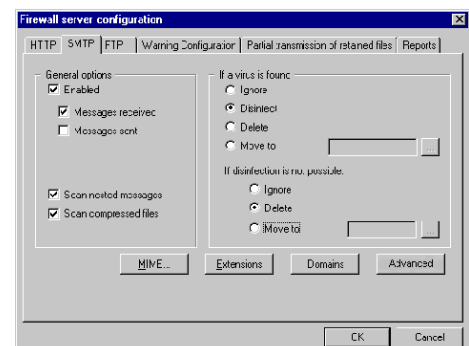


Figure II.21.

### 3.8. Configuration of internal mail domains

Internal mail domains must be defined very precisely, otherwise the antivirus will not scan anything. By configuring domains, it is possible to configure which are the internal domains (those which remain inside the network or networks used by the Firewall). From then on, it is easy to clarify the addresses of the messages (incoming/outgoing).

- ❑ **New domain:** allows you to enter the URL address of the server (domain) you want to include in the list of internal domains.
- ❑ **Add list:** includes the URL addresses entered in the section New domain to the list.
- ❑ **Delete list:** deletes the name selected from the list of domains.
- ❑ **Clear list:** deletes the entire list (all the domains which are included in the list).

Depending on the sender and the recipient of the message, a different transfer address for the message is considered. Therefore, it will only be scanned when necessary (when it must go through the Firewall):

- ❑ The sender of the message is included in the network or networks which are accessed with a Firewall CVP server, and the recipient is also included in it. In this case, the message is considered incoming (it must go through the server until it reaches the internal recipient/s) and it is scanned.
- ❑ The sender of the message is included in the network or networks which are accessed with a Firewall CVP server, and the recipient is not included in it. In this case, the message is considered outgoing (it must go through the server towards the external recipient/s) and it is scanned.
- ❑ The sender of the message is included in the network or networks which are accessed with a Firewall CVP server, and some of the recipients are also included in it (internal) but others are not (external). In this case, the message is considered incoming (it must go through the server towards the internal recipient/s) and outgoing (it must go through the server towards the external recipient/s). Therefore, the message will be scanned.
- ❑ The sender is outside the network or networks which are accessed with a Firewall CVP server, and the recipients are not (internal). In this case, the message is considered incoming (it must go through the server towards the internal recipient/s) and the message will be scanned.
- ❑ The sender is outside the network or networks which are accessed with a Firewall CVP server, and the recipient is also outside (external). It is irrelevant what happens with messages sent by an external sender to an external recipient. In this case, the message is neither inbound nor outbound (the message should not be delivered to any user in the network and should not go through the server). Therefore, the message will not be scanned.
- ❑ The sender is outside the network or networks which are accessed with a Firewall CVP server, and some of the recipients are also outside (external) but others are not (internal). In this case, the message is considered incoming (it must go through the server towards the internal recipient/s). Therefore, the message will be scanned.

### 3.9. Configuration of transmissions through FTP (File transfer)

The configuration of transfers through FTP protocol (File Transfer Protocol), allows you to set the actions and functions the antivirus must carry out, if it detects an infected file transmitted through FTP. The scan can be based on inspecting normal files or compressed files. The configuration options are as follows:

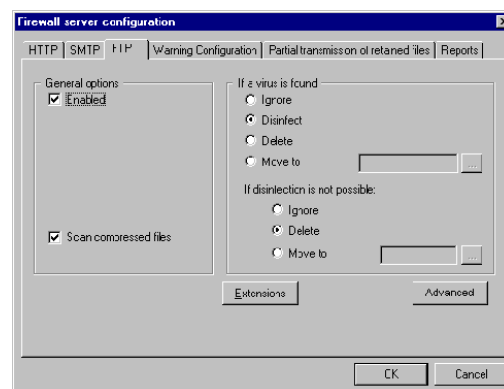


Figure II.22.

### 3.10. Configuration of security

This is a very important characteristic of the configuration of transfers via Firewall (SMTP, HTTP, FTP). It makes it possible to impede (in given circumstances and in certain conditions) computers which are connected to the Firewall CVP server, from receiving or accessing certain components: ActiveX controls, Applets, scripts, etc. By clicking on the Security... button in the configuration of transfers through HTTP, the following options will be displayed:

**Enable Security Module:** when this box is checked, the Firewall will take into account security restrictions that have been selected in this dialog box. It is also possible to enable or disable security conditions through the general options of the antivirus configuration.

The drop-down list, which is below the checkbox mentioned above, allows you to select the component for which you want to set security criteria. These components can be the following: **Java**, **Applets**, **ActiveX Controls** and **Scripts**. After selecting one of these components, each option that is marked will influence the security that the antivirus will apply to that component (and not to the others).

- ❑ **Ignore:** the antivirus for Firewall will not carry out any blocks or security controls on the component selected from the drop-down list.
- ❑ **Block all elements:** when this box is checked, the type of component that is selected in the drop-down menu will be blocked. This means that, if one of the three components (Java Applets, ActiveX Controls, or Scripts) is selected, all files containing these components which go through the Firewall will be blocked. Files, which contain the other two types of components, will not be blocked. If you want to block all of these components, select all the components in the list and check the box, (the configurations adopted in this section only apply to the component selected).
- ❑ **Block unreliable server elements:** blocks all types of components transferred through one of the servers in the unreliable servers list. The unreliable servers list affects all the types of components at the same time.
- ❑ **Block all server elements, except those from reliable servers:** blocks all the types of components from any server (those not included in either of the two lists, or unreliable servers). However, components coming from servers included in the list of reliable servers will not be blocked.
- ❑ **New reliable server:** allows you to enter a server URL address that the antivirus will consider reliable.
- ❑ **New unreliable server:** allows you to enter a server URL address that the antivirus will consider unreliable.

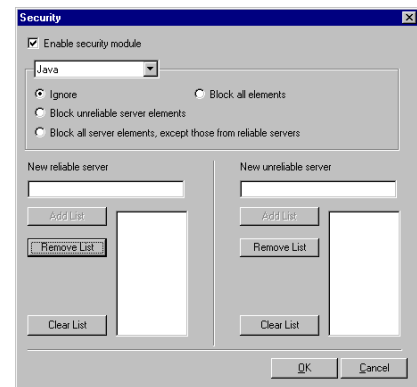


Figure II.23.

### 3.11. Configuration of MIME format

The format known as MIME is the format which appears in information (messages or files) transferred through HTTP. Certain information is given through a MIME type. Firstly, the TYPE of component and secondly, that known as SUBTYPE. The browser used to connect to Internet should interpret this information and display it depending on its features.

By clicking on the **MIME** button you can define or add new types, select what should be scanned, make exclusions, etc. It is "similar" to file extensions. Every group type/subtype, defines a "kind of information" or file format. Every kind can be included in or excluded from scanning. The file scan options, related to MIME character sets, work using two lists: the Type included list (on the left) and the Type excluded list (on the right):

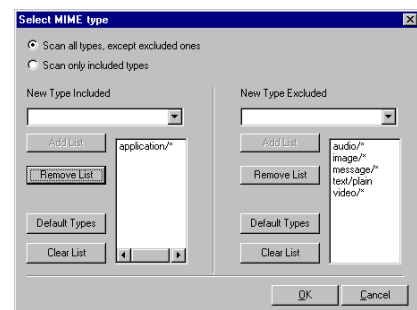


Figure II.24.

- ❑ **Scan all types, except excluded:** when this box is checked, all MIME type files and messages in the Included Types list, as well as other files and messages whose types are not in the Types included or the Types excluded list, will be scanned.
- ❑ **Scan only included types:** when this box is checked, only MIME type files and messages which are in the Types included list will be scanned.

In the Types Included list as well as in the Types Excluded list, it is possible to add or remove, add new or other types, remove them, etc. There are buttons for each operation.

When entering the name of a new type, always follow this format: Type/Subtype. The antivirus does not differentiate between upper and lowercase letters; therefore, it does not matter if you enter TYPE/SUBTYPE or type/subtype. The type should be entered in full and correctly. However, with subtypes an \* (asterisk) wildcard can be used. The asterisk refers to a particular type and can refer to any subtype available. For example, text/\* refers to all text subtypes: text/html, text/htm, text/plain... etc. In the Firewall, you must have chosen not to strip MIME types, otherwise they will not be scanned (see section 3. Creation of the Resource on page 23, under section 2.3 Creation of CVP Servers, on page 21).

### 3.12. Extensions configuration

By clicking on the Extensions button in the configuration dialog box, it is possible to select the extensions which must be scanned. Regardless of the selection of extensions you may make, EXE and COM files will always be scanned. Due to the fact that in the Types included by Default, the antivirus includes type/subtype application/\*. The extensions window options are as follows:

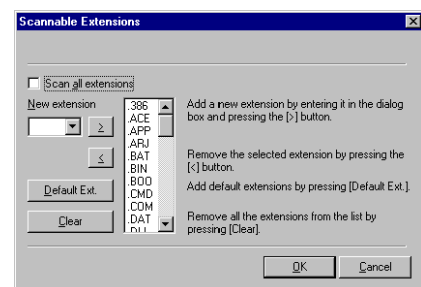


Figure II.25.

### 3.13. advanced configuration in Firewall (heuristic scan)

One of the interesting possibilities of the Antivirus for Firewalls is heuristic scans. This scan detects the vast majority of unknown viruses. It is possible to determine the level of sensitivity that the scan should have.

**Enabled:** when this box is checked, the scan must use heuristic techniques. This means that, not only will the scan search for known viruses but it will also be able to detect more recent unknown viruses.

#### Level of Sensitivity

- ❑ **Maximum sensitivity:** the scan will display alerts (as if it were detection) when there is the slightest sign that a file may be infected with a virus.
- ❑ **Medium sensitivity (recommended):** the scan will use heuristic techniques to scan any files with suspicious characteristics, but it will not spend too much time on this control.
- ❑ **Minimum sensibility:** the antivirus will only scan those files which could have a high probability of being infected by a virus.

### 3.14. Alerts configuration

In this section you can configure the alerts generated by the antivirus when a virus is detected. The options in this section are the following:

- ❑ **Replace an infected file with an alert when it is moved or deleted:** files which must be moved or deleted (as the antivirus has detected that they are infected with a virus), are substituted by an HTML page. This page includes the alert text, which has already been selected (using the **Text...** button), and the information that corresponds to this type of alert.
- ❑ **Send notification to the administrator:** when this option is selected, whenever a virus is detected, the administrator will be notified. In the **Administrator Address** section, the corresponding e-mail address must be entered. The content of this alert can be entered by clicking on the **Text** button. Also, by clicking on the **Select** button, the user can indicate what type of alert should be sent and configure the characteristics.

The following options are available for the configuration of every possible alert generated by the antivirus when a virus is detected:

**Type of alerts selected:** in this section you can choose the types of alerts to be generated. You can choose to generate Microsoft network alerts, send an e-mail message in SMTP, send a message through the Microsoft Exchange network or a Lotus Notes network.

- ❑ **Microsoft Network:** if you have chosen to send a message through the Microsoft network, you must indicate the domain to which you want the message to be sent and the message.
- ❑ **SMTP:** if you have chosen to send an electronic mail message, you will have to indicate the server through which the message is to be sent, the recipient's address and the message.
- ❑ **MS Exchange:** in this case, you should enter the e-mail address of the recipient, the address type and the profile with which the alert message should be sent.
- ❑ **Lotus Notes:** if you have chosen to send an electronic mail message via the Lotus Domino system, you will have to indicate the server through which the message is to be sent, the recipient's address and the message.

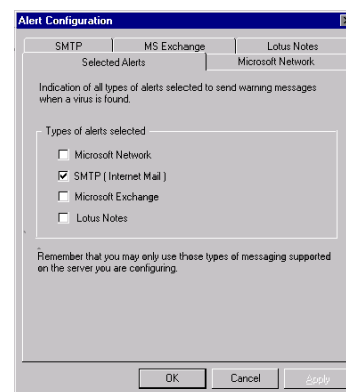


Figure II.26.

## 4. Uninstallation of the Antivirus

**IMPORTANT NOTE:**

*Before starting the uninstallation process of Panda Antivirus for Firewall, it is necessary to delete every security rule defined in the configuration of the Firewall which affect the CVP server in which you want to uninstall the antivirus.*

Once the security rules have been deleted and with a connection with administrator privileges is open, the antivirus can be uninstalled. Select the server click on the **Uninstall** button on the toolbar. An Uninstallation Wizard will appear.

The procedure is as follows:

1. If you accept the uninstallation, the process will begin and a window will be shown with a progress bar. The process only takes a few seconds.
2. When uninstallation is complete, the service corresponding to the Firewall will stop and restart (the server will not be restarted).

## 1. load sharing across multiple security servers with the CVP Protocol

With this method, when one of the CVP servers does not respond to the Firewall instead of retaining the data (as happens when load sharing does not exist), it is sent to another CVP.

In addition to this method is the load sharing functionality between the CVPs integrated in the CVP Manager load sharing group.

It has been observed that using this method the Spool that is created in the server when the CVP is installed not only grows less than when there is only a CVP without load sharing, but also the Firewall empties it more quickly.

It has also been observed that the Spool can be emptied more quickly by changing the following fields in the SMTP configuration of the Firewall: *MAIL RESEND PERIOD* (the default revision time of the spool is 600 sec.) set a lower value (E.g. 30 sec.) and in the Spool directory field (left blank by default) enter the Spool directory address of the Firewall directory *\$FWDIR\SPOOL*.

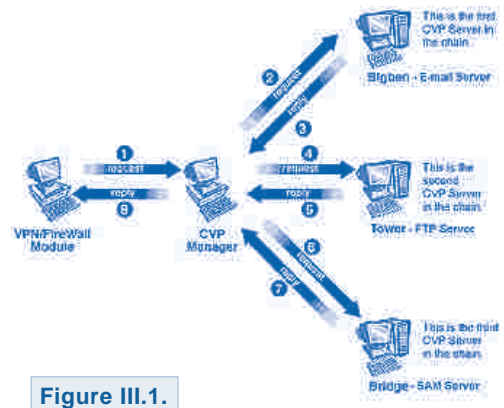


Figure III.1.

## 2. Steps for installing load sharing across multiple CVP servers

1. Install the CheckPoint CVP Manager option. This module is located on the Checkpoint Firewall-1 CD-ROM, in the directory \windows\CPcvpm-41. The executable file is called setup.exe

1.1. When this program is run, installation begins.



Figure III.2.

1.2. After accepting the license agreement...

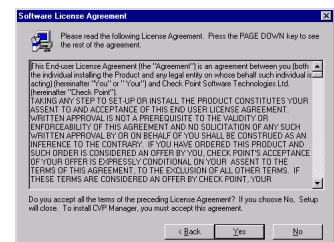


Figure III.3.

1.3. ...and selecting the installation directory...

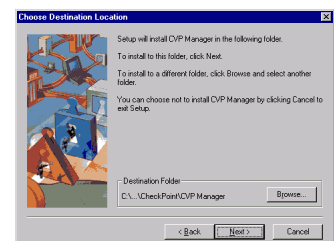


Figure III.4.

1.4. ...the files are copied.

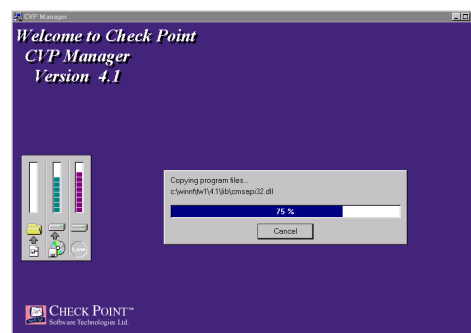


Figure III.5.

2. Install the antivirus in the machines to which the load will be distributed, checking that there is communication with the Firewall through port 18181 (Telnet from the Firewall to the machines in which the Av is installed and viceversa and check that is done correctly).
3. Modify the file **fwopsec.conf** that is in the Firewall directory **\$FWDIR\conf\fwopsec.conf**. Make sure that the file that is modified is in the active Firewall directory (there may be several copies of the file, 2 directories are created FW and FW1, FW1 is the active directory). The following lines must be included in the **fwopsec.conf** file:

- I. Line for enabling load sharing

```
use_load_share yes
```

- II. Line for setting the recovery time. (If the Firewall cannot connect to the CVP, it will try to reconnect after the time specified in this line).

```
Recovery_time <time in minutes>
```

- III. Line for specifying the CVP Manager server:

```
server <ip> <port> opsec
```

Where

**Ip:** Server address in the format xxx.xxx.xxx.xxx

**Port:** Server port number

- IV. Line for specifying the number of servers that will share the load:

```
<configured server> num_of_servers <num>
```

Where

**configured server:** Name of the server (not IP) that will distribute the load (CVP Manager).

**num:** Number of servers that will share the load.

- V. Line for selecting the load sharing method:

```
<configured server> method [random] [round_robin]
```

Where

**configured server:** Name of the server (not IP) that will distribute the load (CVP Manager)

**meted.** Specifies the load sharing method. There are two possibilities:

**a. random:** Tasks are assigned to the CVP or UFP servers at random.

**b. round\_robin:** The tasks are assigned to the CVP or UFP Server alternately.

#### VI. Lines for specifying the name and configuration of each server that shares the load:

```
<configured server> server 1 <server name 1>
<configured server> server 2 <server name 2>
...
<configured server> server n <server name n>

<server name 1> port <port of server 1>
<server name 1> ip <address of server 1>
<server name 2> port <port of server 2>
<server name 2> ip <address of server 2>
...
<server name n> port <port of server n>
<server name n> ip <address of server n>
```

#### Example: (the lines that are preceded by “#” are comments)

```
#Line for enabling load sharing
use_load_share yes

#Recovery time in minutes
Recovery_time 1

#CVP Manager Server
server 192.168.1.1 18181 opsec

#Load cvpmanager server
load_share 192.168.1.1 18181 server_cvp_manager

#Number of servers that will be used to share the load

server_cvp_manager num_of_servers 2

#Load sharing method
servidor_cvp_manager method random

#Name and configuration of the Servers
servidor_cvp_manager server1 cvp_distribuido_uno
servidor_cvp_manager server2 cvp_distribuido_dos
cvp_distribuido_uno port 18181
cvp_distribuido_uno ip 192.168.1.125
cvp_distribuido_dos port 18181
cvp_distribuido_dos ip 192.168.1.2
```

#### 4. Create a new server for the CVP Manager, assigning it as a CVP server.

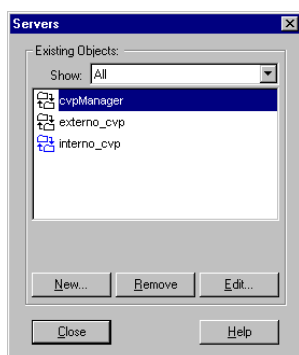


Figure III.6.

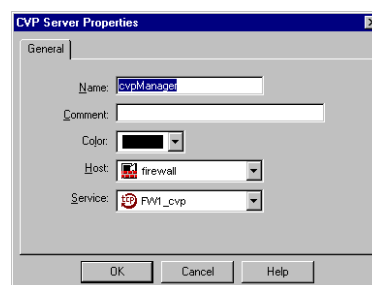


Figure III.7.

5. Create the servers (if they do not already exist) for the CVP servers that will share the load.

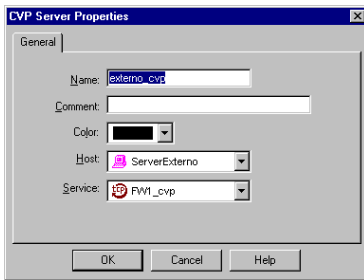


Figure III.8.

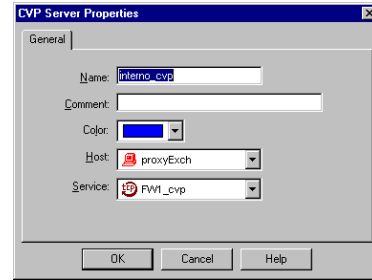


Figure III.9.

6. Create the resources for the protocols for which the load will be distributed

- SMTP

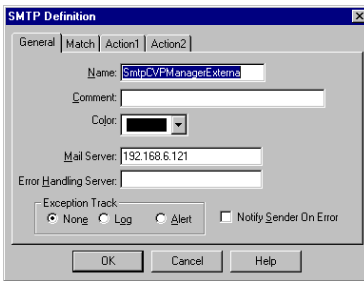


Figure III.10.

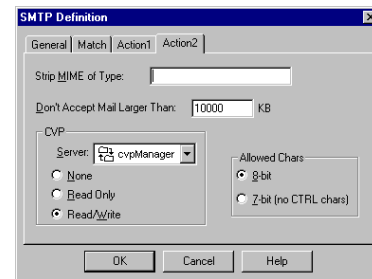


Figure III.11.

- HTTP

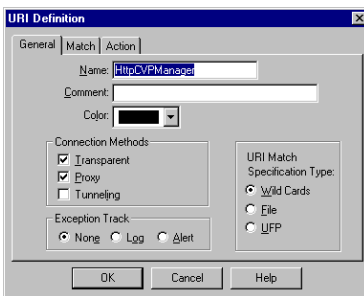


Figure III.12.

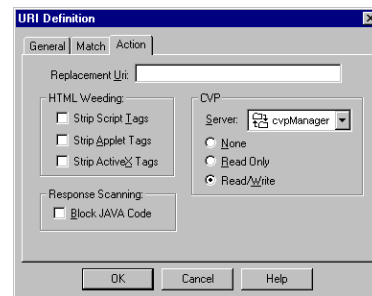


Figure III.13.

- FTP

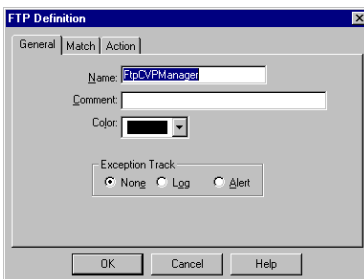


Figure III.14.

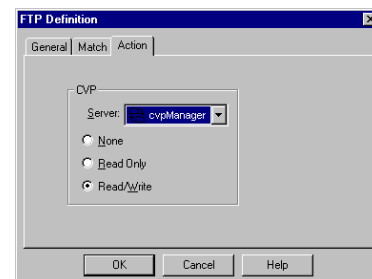


Figure III.15.

7. Create rules for the protocols for which the load will be distributed.

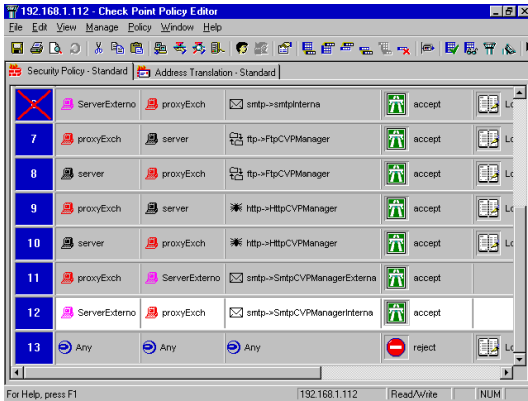


Figure III.16.

8. Stop and start the Firewall-1 and CVP manager services.

### 3. Partial transmission of retained files.

The antivirus should scan the content of all files received/sent through the Firewall CVP server. In order to do this, each file must be retained in the server until the complete file has been received. In addition, the file cannot be retained in the server for longer than a certain amount of time, as the client that is receiving the file will terminate the connection (when the waiting time is exceeded).

When sending packets that are part of the transferred file, the antivirus can scan each of them without using up too much of the waiting time. If the infected file is being sent to the client using packets, the antivirus can disinfect it so that the recipient receives a disinfected file.

In order to set the ideal configuration for retained files, select the Firewall CVP server and click on the Configure button on the Panda Administrator toolbar. In the dialog box that appears, select the tab Transmission of retained files. The following options will appear:

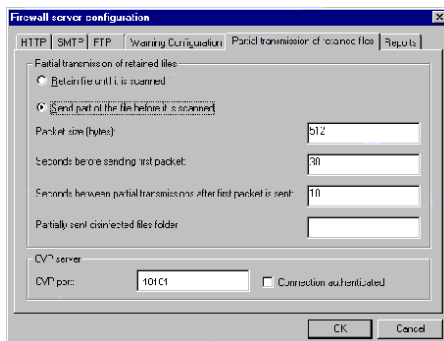


Figure III.17.

- ❑ **Retain file until it is scanned.** The antivirus will not send the complete file (from the Firewall CVP server to the client) until it has been fully scanned. The client will not receive anything until this file has been fully scanned.
- ❑ **Send parts of the file that have been scanned.** The user waiting for the file will receive it in packets. Each one will be scanned before it is sent. This means that the information reaches the recipient as sections of the file, which have already been scanned by the antivirus. This option is highly recommended. If it is selected, it is necessary to set a series of parameters, which guarantee the correct functioning of the system:
  - ❑ **Packet size (Bytes):** is the size of every packet of the information to be transferred. The file is sent from the Firewall CVP server divided into sections of this size, which the antivirus then scans. After they are scanned, they are sent to the client one at a time. It is ADVISABLE to maintain the size assigned by default, 512 Bytes.
  - ❑ **Seconds before sending first packet:** indicates the time from when the file is located in the server, until the first packet, is sent. It is ADVISABLE to maintain a time of 30 seconds.
  - ❑ **Seconds between partial transmissions after first packet is sent:** indicates the time that should pass between packet transmissions, from when the first packet is sent. It is ADVISABLE to maintain a time of 10 seconds.
  - ❑ **Partially sent disinfected files folder:** it is possible to specify the directory in which the antivirus should save all files which were infected when they were partially transmitted (in packets), and then disinfected.

If partial transmission of retained files is selected, whilst the antivirus is scanning the packets of the partially transmitted file, a virus may be detected after the recipient has already received some of the packets. In this case an action is carried out depending on the configuration established:

- ❑ **If the configuration indicates that an infected file must be removed or deleted.** In this case, the antivirus will not send any more information packets from the Firewall CVP server to the user. The waiting time will be exceeded and the connection will be terminated. The client will have received an incomplete file.
- ❑ **If the configuration indicates that an infected file must be moved.** The antivirus will not send any more information packets. The waiting time will be exceeded and the connection will be terminated.

If the configuration indicates that an infected file must be disinfected, there are two possible outcomes:

- ❑ **If the user has already received some of the packets of the infected file, which have been modified by the antivirus.** The file will be sent to a specific directory (the one selected in the section Partially transmitted disinfected files directory, in the configuration of partially transmitted files). After this, the user will not receive any more packets and the waiting time will be exceeded. Therefore, the connection with the server will be terminated.
- ❑ If the user has not received any packets of the infected file modified by the antivirus the user will receive the complete file once it has been disinfected.
- ❑ **CVP Server.** The antivirus carries out its scan through the communications port used between the Firewall and the CVP server. This section of the configuration of partial transmission of files allows you to select which port the antivirus must scan. When the antivirus is scanning or active, the modifications carried out in this section do not have any effect. In other words, for the antivirus to scan everything which passes through the port that you have just selected, the antivirus service must be stopped and restarted.
- ❑ **CVP Port:** allows you to enter the number of the port through which the antivirus must control transmissions between the CVP server and the Firewall. It must be the same as the port associated with the FW1\_cvp service (in the configuration of the Firewall). If this data is modified at any time, the antivirus must be stopped and restarted for the change to come into effect.
- ❑ **Authenticated Connection:** When this box is checked a connection can be established that uses authentication between the CVP server and the Firewall. This means that it is necessary to configure the CVP client (Firewall) and the CVP server (antivirus).

## 1. Why does Panda Administrator return an incorrect Password error during installation?

This error mainly occurs in Windows 2000 workstations when authenticating the user and password used during the installation of the product. In order to solve this problem, follow the steps below:

1. Copy the file ZNETBOX.EXE, available from the Technical Support department, in the root directory of Panda Administrator (by default \PAVLN).
2. Install the preferred product.

In certain systems an error could be returned, indicating that the password could not be checked. This message will not affect the installation of the product.

## 2. Why haven't I got a connection between Panda Administrator and the antivirus for firewall?

There may be a DCOM communication problem. In order to check the configuration of the DCOM, run START - RUN - DCOMCNFG in the machine in which Administrator is located.

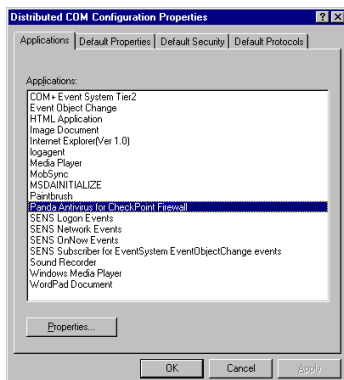


Figure IV.1.

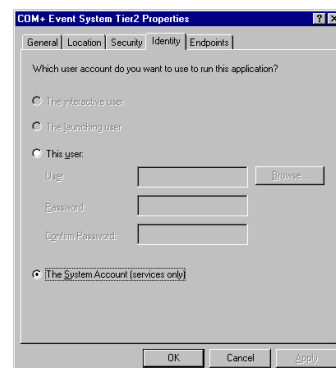


Figure IV.2.

If the machine in which the antivirus is going to be installed does not belong to any domain, simply enter: *Name\_Machine\Administrator* or *.Administrator* (although by default the installer will enter *Domain name\Administrator* or *.Administrator*)

### 3. What HTTP error codes does the firewall return?

Constant	Value	Description
HTTP_STATUS_CONTINUE	100	The request can be continued.
HTTP_STATUS_SWITCH_PROTOCOLS	101	The server has switched protocols in an upgrade header.
HTTP_STATUS_OK	200	The request completed successfully.
HTTP_STATUS_CREATED	201	The request has been fulfilled and resulted in the creation of a new resource.
HTTP_STATUS_ACCEPTED	202	The request has been accepted for processing, but the processing has not been completed.
HTTP_STATUS_PARTIAL	203	The returned meta information in the entity-header is not the definitive set available from the origin server.
HTTP_STATUS_NO_CONTENT	204	The server has fulfilled the request, but there is no new information to send back.
HTTP_STATUS_RESET_CONTENT	205	The request has been completed, and the client program should reset the document view that caused the request to be sent to allow the user to easily initiate another input action.
HTTP_STATUS_PARTIAL_CONTENT	206	The server has fulfilled the partial GET request for the resource.
HTTP_STATUS_AMBIGUOUS	300	The server couldn't decide what to return.
HTTP_STATUS_MOVED	301	The requested resource has been assigned to a new permanent URI (Uniform Resource Identifier), and any future references to this resource should be done using one of the returned URIs.
HTTP_STATUS_REDIRECT	302	The requested resource resides temporarily under a different URI (Uniform Resource Identifier).
HTTP_STATUS_REDIRECT_METHOD	303	The response to the request can be found under a different URI (Uniform Resource Identifier) and should be retrieved using a GET method on that resource.
HTTP_STATUS_NOT_MODIFIED	304	The requested resource has not been modified.
HTTP_STATUS_USE_PROXY	305	The requested resource must be accessed through the proxy given by the location field.
HTTP_STATUS_REDIRECT_KEEP_VERB	307	The redirected request keeps the same verb. HTTP/1.1 behavior.
HTTP_STATUS_BAD_REQUEST	400	The request could not be processed by the server due to invalid syntax.
HTTP_STATUS_DENIED	401	The requested resource requires user authentication.
HTTP_STATUS_PAYMENT_REQ	402	Not currently implemented in the HTTP protocol.
HTTP_STATUS_FORBIDDEN	403	The server understood the request, but is refusing to fulfill it.
HTTP_STATUS_NOT_FOUND	404	The server has not found anything matching the requested URI (Uniform Resource Identifier).
HTTP_STATUS_BAD_METHOD	405	The method used is not allowed.
HTTP_STATUS_NONE_ACCEPTABLE	406	No responses acceptable to the client were found.
HTTP_STATUS_PROXY_AUTH_REQ	407	Proxy authentication required.
HTTP_STATUS_REQUEST_TIMEOUT	408	The server timed out waiting for the request.
HTTP_STATUS_CONFLICT	409	The request could not be completed due to a conflict with the current state of the resource. The user should resubmit with more information.
HTTP_STATUS_GONE	410	The requested resource is no longer available at the server, and no forwarding address is known.
HTTP_STATUS_LENGTH_REQUIRED	411	The server refuses to accept the request without a defined content length.
HTTP_STATUS_PRECOND_FAILED	412	The precondition given in one or more of the request header fields evaluated to false when it was tested on the server.
HTTP_STATUS_REQUEST_TOO_LARGE	413	The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
HTTP_STATUS_URI_TOO_LONG	414	The server is refusing to service the request because the request URI (Uniform Resource Identifier) is longer than the server is willing to interpret.
HTTP_STATUS_UNSUPPORTED_MEDIA	415	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.
HTTP_STATUS_RETRY_WITH	449	The request should be retried after doing the appropriate action.
HTTP_STATUS_SERVER_ERROR	500	The server encountered an unexpected condition that prevented it from fulfilling the request.
HTTP_STATUS_NOT_SUPPORTED	501	The server does not support the functionality required to fulfill the request.
HTTP_STATUS_BAD_GATEWAY	502	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
HTTP_STATUS_SERVICE_UNAVAIL	503	The service is temporarily overloaded.
HTTP_STATUS_GATEWAY_TIMEOUT	504	The request was timed out waiting for a gateway.
HTTP_STATUS_VERSION_NOT_SUP	505	The server does not support, or refuses to support, the HTTP protocol version that was used in the request message.

#### 4. Why do i have problems viewing \*.PDF files through http?

It seems that the use of antivirus programs that use CVP protocol for communicating with FIREWALL-1 is causing problems when handling files with \*.PDF extensions.

What generally happens is that when an "internal" user (behind the FIREWALL) tries to access a \*.PDF file through HTTP (to which a resource is applied) in order to view it, the browser does not display it and blocks. However, this does not happen when a file is downloaded in order to be opened later.

In order to solve this problem modify the following in "PROPS" in *\$FWDIR/conf/objects.C*:

- :http\_allow\_ranges (true)
- :http\_cvp\_allow\_chunked (true)
- :http\_weeding\_allow\_chunked (true)
- :http\_force\_down\_to\_10 (true)
- :http\_block\_java\_allow\_chunked (true)

Then run a FWSTOP/FWSTART (Stop and restart the Firewall service)

#### 5. What log files are generated during updates?

The LOG files that are generated during updates are:

- EXCH.SRV (in the Panda Administrator part or the update server part).
- PAVCVPFW.

##### **PavacC.exe module**

Generates the file EXCH.SRV which includes:

- Server-client connection errors.
- Update errors depending on the server status (whilst an update is in progress another is launched).
- Errors on transferring files between the client-server.

In addition to these errors references are also included (OK or ERROR) for the 3 update stages: Start of update, Preparation of Update and File transfer

##### **PavacS.exe module**

- Generates the file PAVCVPFW which includes:
- The antivirus status (Prepared for the update, update in progress).
- Error creating the temporary directory for copies.
- Error transferring files.
- Result of the copying of files and the action to be carried out (Clean temporary files for Update OK and Undo changes for Update ERROR).
- Result of the process of copying the PAV.SIG and the action to be carried out.

## 6. What log is generated when installing and uninstalling the antivirus?

Panda Administrator generates a log file when installing and uninstalling the antivirus for Firewall. This file is located in the Panda Administrator directory and is called INSTALL\_LOG.TXT. It stores information during uninstallation as well as during installation. Its content is deleted when the antivirus for Firewall is installed or uninstalled in any machine from Panda Administrator; therefore, it will only store data on the last process carried out.

The objective of this file is to provide a record of an unsuccessful installation to be used by Technical Support or Development. It does not offer any information that is relevant to users, or at least, it does not give them any clues on how to solve the problem.

## 7. What data should i provide about an incident?

### FILES

- ❑ EXCH.SRV (in Winnt)
- ❑ VERSION.DAT (in the root directory of every platform in Admin)
- ❑ DRWTSN32.LOG (doctor watson log)
- ❑ EVENT.LOG
- ❑ CVP\_SERVER\_LOG\*.TXT (in the directory SystemRoot%\system32\PavCvpFw)
- ❑ CVP\_SERVER\_LOG.TXT
- ❑ CVP\_SERVER\_LOG\_COPIA\_1.TXT
- ❑ CVP\_SERVER\_LOG\_COPIA\_n.TXT
- ❑ PAV\_CVPFW\*.LOG (in the directory %SystemRoot%\system32\PavCvpFw)
- ❑ PAV\_CVPFW.LOG
- ❑ PAV\_CVPFW\_COPIA\_1.LOG
- ❑ PAV\_CVPFW\_COPIA\_n.LOG
- ❑ PAVCVPFW.CLT

### REGISTRY

- ❑ HKLM\Software\Panda Software\Updates

## 8. how do i configure the antivirus to use authenticated connections with the firewall?

In order to configure the antivirus to connect to the Firewall using authenticated connections, follow the steps explained below:

### In the Firewall side:

1. Edit the file: \$FWDIR\CONF\FWOPSEC.CONF, and change the line server 127.0.0.1 18181 auth\_Opsec to server <CVP ip> 18181 auth\_opsec

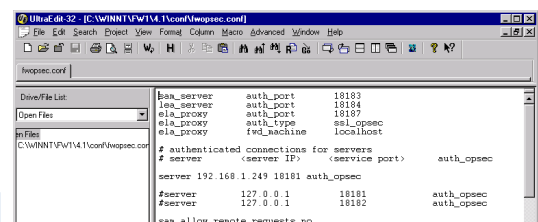


Figure IV.3.

- Save the file.
- It is necessary to generate an encryption key, therefore type the following in command line: `$FWDIR\bin\fw putkey -opsec -p <password (over 5 characters)> [host (CVP)]` . For example,

```
fw putkey -opsec -p pandapanda 192.168.1.2
```

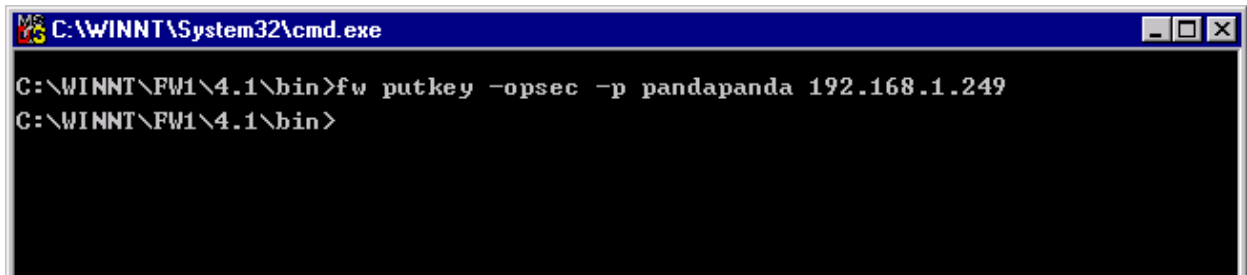


Figure IV.4.

- Stop and restart the Firewall service
- Temporarily disable the rules so that communication can be established without any problems.
- In the server in which the CVP is installed generate the same key by executing the command line: `C:\winnt\system32\PavCvpFw\Opsec_putkey -p <password (the same as that entered in the Firewall host)> [host (Firewall)]`

```
Opsec_putkey -p pandapanda 192.168.1.1
```

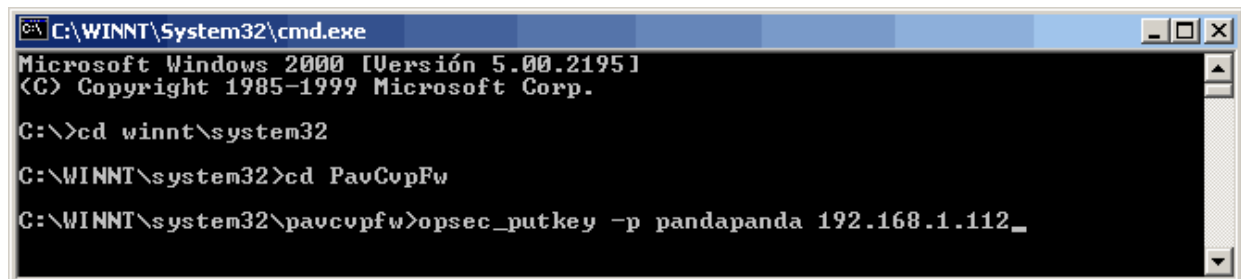


Figure IV.5.

- Check the box **Authenticated communication** in the configuration of Panda Administrator and click on **OK**.

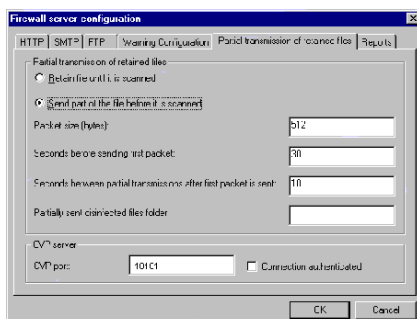


Figure IV.6.

- The antivirus service must be stopped and restarted for these changes to come into effect.

#### NOTE :

Check that the file `AUTHKEYS.C` is located in the antivirus installation directory (by default: `C:\WINNT\SYSTEM32\PAVCVPFW`), by doing this you can check that all of the steps have been carried out correctly and that the authenticated connection works correctly.

## 9. Why is nothing that goes through the SMTP rule scanned?

This error occurs when the domains of the SMTP rule that must be scanned by the Firewall antivirus have not been defined, in other words, the list of domains that must be scanned has been left blank. Therefore nothing will be scanned. In order to fix this problem, simply enter the domains that must be scanned.

In order to configure the domains of the SMTP rule of the antivirus for Firewall, follow the steps below:

- Select the antivirus that you want to manage and click on the **configure** button in order to open the server configuration, then select the **SMTP tab**:

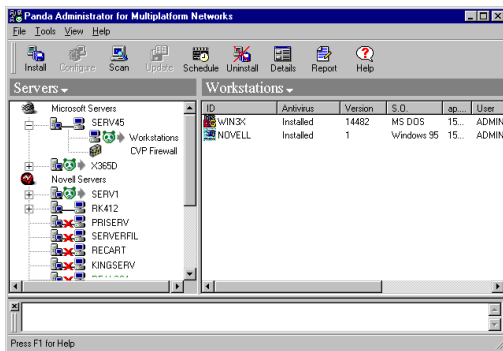


Figure IV.7.

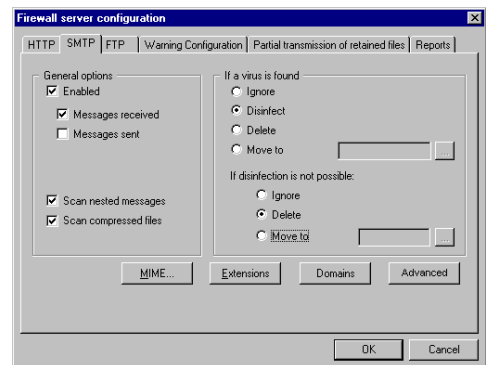


Figure IV.8.

By clicking on the Domains button the following screen will appear:

For the antivirus to be able to scan mail, the internal mail domain must be entered in the list, for example, if your mail is me@home.com, enter “home.com” in the list and click on add.

If there are other internal domains whose mail must be scanned, add them to the list in the same way as described above.

The internal domains must be entered in order to differentiate between incoming and outgoing mail, as the antivirus for FireWall offers the option of scanning incoming mail, outgoing mail or both.

The table below shows the different sender and recipient combinations possible and classifies each combination as incoming or outgoing:

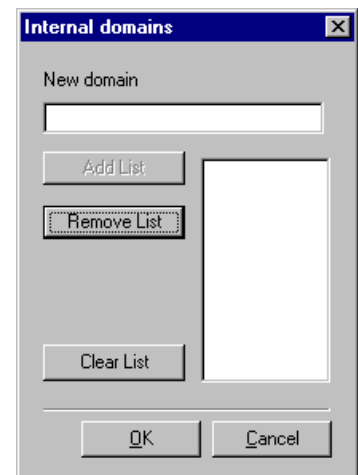


Figure IV.9.

Sender	Recipients	Direction
From Internal domain	To Internal domains	Incoming Mail
From Internal domain	To External domains	Outgoing Mail
From Internal domain	To Internal and external domains	Incoming and outgoing mail
From External domain	To Internal domains	Incoming mail
From External domain	To External domains	Neither incoming nor outgoing mail (not scanned)
From External domain	To Internal and external domains	Incoming mail