

AVS4YOU Programs Help



AVS Firewall

www.avs4you.com

© Online Media Technologies, Ltd., UK. 2004 - 2010 All rights reserved

Contact Us

If you have any comments, suggestions or questions regarding **AVS4YOU** programs or if you have a new feature that you feel can be added to improve our product, please feel free to contact us.

When you register your product, you may be entitled to technical support.

General information:	info@avs4you.com
Technical support:	support@avs4you.com
Sales:	sales@avs4you.com
Help and other documentation:	help@avs4you.com


Technical Support

AVS4YOU programs do not require any professional knowledge. If you experience any problem or have a question, please refer to the **AVS4YOU Programs Help**. If you cannot find the solution, please contact our support staff.

 **Note:** only registered users receive technical support.

AVS4YOU staff provides several forms of automated customer support:

- **AVS4YOU Support System**
You can use the **Support Form** on our site to ask your questions.
- **E-mail Support**
You can also submit your technical questions and problems via e-mail to support@avs4you.com.

 **Note:** for more effective and quick resolving of the difficulties we will need the following information:

- Name and e-mail address used for registration
- System parameters (CPU, hard drive space available, etc.)
- Operating System
- The information about the capture, video or audio devices, disc drives connected to your computer (manufacturer and model)
- Detailed step by step describing of your action

Please do **NOT** attach any other files to your e-mail message unless specifically requested by AVS4YOU.com support staff.

Resources

Documentation for your AVS4YOU software is available in a variety of formats:

In-product (.chm-file) and Online Help

To reduce the size of the downloaded software installation files the in-product help was excluded from the installation although you can always download it from our web-site for your convenience. Please, visit AVS4YOU web-site at <http://www.avs4you.com/OnlineHelp/index.aspx> to download the latest available version of the help executable, run it and install into the AVS4YOU programs folder. After that you will be able to use it through the **Help** menu of the installed AVS4YOU software.

Online Help include all the content from the In-product help file and updates and links to additional instructional content available on the web. You can find the **Online Help** at our web-site -

<http://www.avs4you.com/OnlineHelp/index.aspx>. Please note, that the most complete and up-to-date version of AVS4YOU programs help is always on the web.

PDF Documentation

The offline help is also available as a pdf-file that is optimized for printing. All PDF help files are available for download at the programs pages at AVS4YOU web-site (both <http://www.avs4you.com/index.aspx> and <http://www.avs4you.com/OnlineHelp/index.aspx>). To be able to read and print AVS4YOU PDF help files you will need to have a PDF reading program installed.

User Guides

You have access to a wide variety of resources that help you make the most of your AVS4YOU software. The step-by-step user guides will be of help not only to the novice users but also to the users that face a certain task to be performed and look for a way to do it. Please, visit our **User Guides** section of AVS4YOU web-site at <http://www.avs4you.com/Guides/index.aspx> to read the detailed instructions for various software and tasks

Technical Support

Visit the **AVS4YOU Support** web-site at <http://support.avs4you.com> to ask your questions concerning AVS4YOU software installation, registration and use. Feel free to also use our e-mail address support@avs4you.com.

Downloads

Visit the **Downloads** section - <http://www.avs4you.com/downloads.aspx> - of our web-site to find free updates, tryouts, and other useful software. We constantly update the software, new versions of the most popular programs and new software are also frequently released.

Overview

AVS Firewall is an intuitive to use application aimed at:

- defending your computer against the hacker remote attacks and malicious software influence. Control the inbound connections from LAN or WAN and the outbound connection requests that the programs on your computer initiate by defining your rules. The port scanning attacks are discovered and blocked now. Intercept any attempt to modify the controlled registry key values;
- preventing you and your children from the undesirable or importunate web content and pages. Define the blocked URLs that refer to the ad-images, flash banners, pop-up windows, etc. Designate only the trusted sites, all others will be rejected;
- giving you the complete information on the network activity on your computer. Monitor all the established and maintained connections. Estimate the application traffic volume and the general incoming traffic size on protocols. Learn what events happened to the outbound connections.

AVS Firewall starts automatically after reboot that follows installation. If you happen to exit the program choose **AVS4YOU -> System Utilities -> AVS Firewall** from the **Programs** section of the **Start** menu or click twice on its desktop shortcut to load it again.

Introduction to Networking and Security

To use **AVS Firewall** efficiently we recommend to learn some basics on network components and addressing, computers understanding each other, what ports are for, what potential hacker's attacks can touch your system when you work with network and the way **AVS Firewall** provides security.

What is Computer Network?

To be what it's meant to be computer network should include the following components minimally:

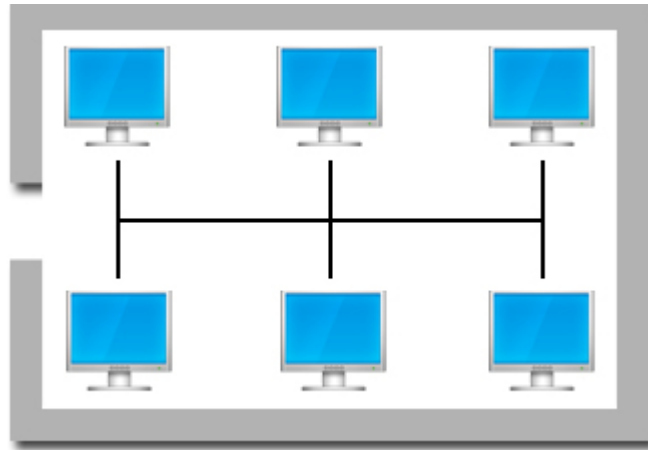
- At least two computers (supplied with network adapters) that have something to share;
- A cable or wireless pathway, called **transmission media**, for computers to signal each other;
- Rules, called **protocols**, so that computers can, figuratively, use the unified principle of data communication.

Today's computer networks include not only personal computers, but also other types of computers and a variety of communication devices as well.

Computer networks are often classified by size, distance covered, or structure. The following network classifications are commonly used:

- **Local area network (LAN)**

It is a combination of computer hardware and transmission media that is relatively small. Usually LANs do not exceed tens of kilometers in size and is contained within a building or set of a few adjacent buildings:



Today the most popular technologies of LAN organization are **Ethernet** (wireline LAN) and **WLAN** (wireless LAN).

- **Wide area network (WAN)**

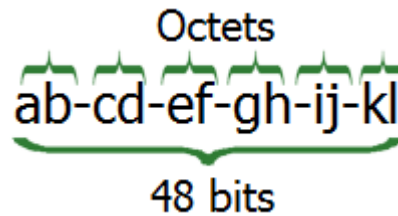
This type of networks interconnects LANs which may be at opposite sides of a country or located around the world:



How do Computers of Network Address Each Other?

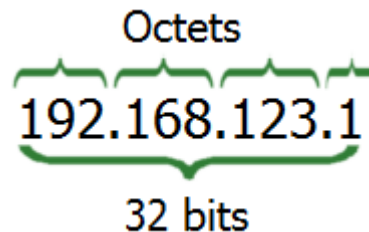
Each member of network must have:

- **Physical address** or **MAC-address** (which is unique and provided by a network adapter) so that to interact with other members of the same network. A MAC-address is a hexadecimal number of 6 octets with general size 48 bits i.e. 8 bits per an octet. 8 bits allow to store number in the range 00h - FFh (0-255 if it was decimal notation):



Where ab - kl are some hexadecimal numbers. You can find out your physical address by entering *getmac* in the command prompt of Windows operating system;

- **Logical network address** or **IP-address** assigned so that to distinguish the computer itself and make it possible to communicate with the members of other networks as well. An IP-address is a unique number of 4 octets, with general size 32 bits i.e. 8 bits per an octet. 8 bits allow to store number in the range 0 - 255:



An IP-address is always used together with the so-called **subnet mask** that helps to distinguish the destination subnetwork out of the IP-address.

Note 1: to assign the right IP-address and subnet mask for your computer, if necessary, consult an IT-specialist of your network service provider.

Note 2: the described IP-address format refers to IP-protocol ver.4. Because of the IP-addresses shortage, IP-protocol ver.4 security issues and overgrowth of the routing mechanism tables IP-addressing ver.6 is introduced progressively. It suggests the hexadecimal IP-address format with general size 128 bits, 16 bits per an octet. Instead of the subnet mask, IP-addressing ver.6 uses the subnet prefix length which means how many bits of the IP-address define the subnet.

What Protocols do Exist?

As it has already been mentioned protocols are a kind of rules for computers to understand and communicate to each other. All the protocols have names and are described by means of RFC (Request For Comment) documents. Let's put all the protocols into two groups for simplicity - **Low Level** and **Application Level**. The **Low Level** protocols are responsible for data to reach the right destination and, if necessary, - safely while the **Application level** protocols declare the operating system processes (services) by means of which an application-initiator receives the requested data of specific organization (the e-mail, web-page, shared folder etc.).

For instance, **Low Level** protocols are:

- **IP - Internet Protocol**. It performs addressing and selects a route so that the sent data reach the destination computer;
- **ARP - Address Resolution Protocol**. This protocol is used to translate a computer logical network address into a physical one so that a member of a certain network can interact with the members of others;
- **TCP - Transmission Control Protocol**. This protocol provides the transmission of data in the right order and controls traffic regulating the speed of data communication;
- **UDP - User Datagram Protocol**. Like TCP this protocol provides the transmission of data but no control is applied. It is used when the speed of transferring is more important than reliability.

What is Port?

Although the transmitted data reach the destination computer due to **MAC** and **IP addresses**, they are meant anyway for an application that uses network. So for data to reach up the application they are intended for, some identifier must be used. This identifier is called **port**. A port is a number in the range 0 - 65535. A computer that initiates connection is called **client** and the one the initiated connection is aimed at is called **server**. When the client applications send requests they are assigned the outbound ports - called **ephemeral** in the range from 49152 to 65535 in case of Windows Vista or higher and from 1025 to 5000 for earlier Windows versions. A server is supposed to have services running which perform different functions, for instance, sending back the web page that the client has required. Services are bound to the fixed ports called **well known** which are in the range from 0 to 1023 (e.g. HTTP web server uses TCP port 80) and are listening to requests or data incoming from the clients to these ports. Services, by-turn, provide the server applications with data that came from the client ones. When the required data is sent back to the client they come using the corresponding **ephemeral** ports and then reach up the client application. How does an application know what port a response should be sent to? As a matter of fact when requests or data are sent information of what port has been used to transfer them is added too.

A **port** can be either **TCP** or **UDP** because those are protocols to transmit data. So **TCP** and **UDP ports** are not the same. The **well known** ports are always associated with a certain service of the operating system (which is declared as the Application level protocol). Some more information on the **well known** ports:

Port	Description
TCP Port 20	is used to transfer files (FTP-protocol);
TCP Port 21	is used to transfer commands of protocol (FTP-protocol);
TCP Port 25	is used to send emails (SMTP-protocol);
TCP Port 80	is used to have the web site pages displayed (HTTP-protocol);
TCP Port 110	is used for users to receive emails from server (POP3-protocol);
UDP Port 137	is used for computers in network to resolve and register their names (SMB over Netbios-protocol);
UDP Port 138	is used to establish and break connection sessions between computers (SMB over Netbios-protocol);
TCP Port 139	is used to transfer data as sharing within a connection session (SMB over Netbios-protocol);
TCP Port 443	is used to have the web site pages displayed applying the strong encryption (HTTPS-protocol);
TCP Port 445	is used by SMB-protocol directly and provides the same opportunities as UDP Port 137, Port 138 and TCP Port 139.



Note: SMB over Netbios (also known as Netbios over TCP/IP) is an "old-fashioned" protocol to browse computers and share data within a network and has potential vulnerabilities. You'd better disable it at all if there is no necessity in its using. Consult an IT-specialist of your network service provider for details.

What Kinds of Network Attacks Can Be?

All the network attacks can be rated as **passive** and **active**.

- **Passive attacks**

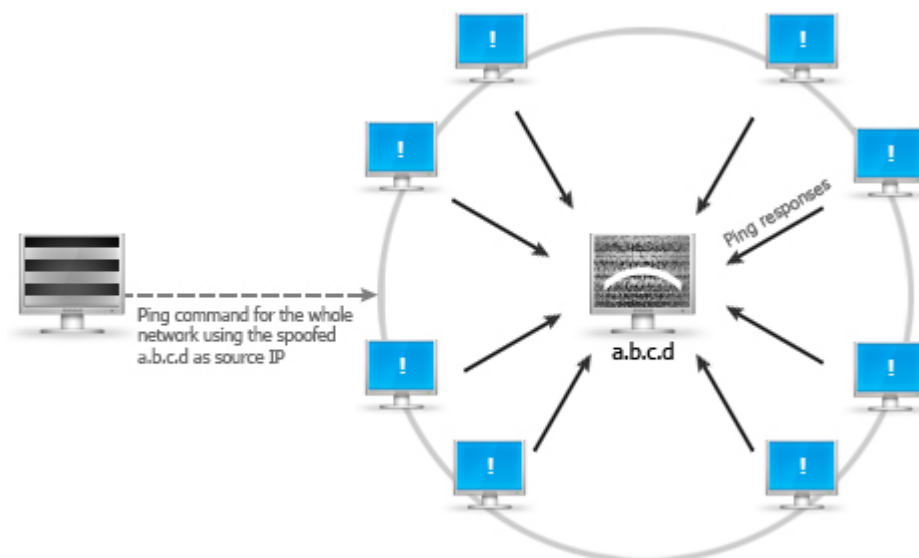
Such attacks are not aimed at corrupting any data or services on your computer. They are performed to get some information of your computer and estimate the possible ways of remote intrusion:

- **Sniffing.** The way of eavesdropping transmitted data. Usually it happens when data themselves are sent unencrypted and the networking equipment works in promiscuous mode i.e. when a network device discovers all the data packets passing through it no matter what source and destination computers are. Sniffing is executed by means of applications created for that.
- **Port and Operating System vulnerability scanning.** Generally the port scanning, the way of finding out which services of a remote computer operating system are active and ready to accept data and commands through the ports associated with them, is a reconnaissance before the vulnerability discovering. The operating system vulnerability scanning is aimed at finding out whether a service with its open port still has a known vulnerability to execute an exploit.

- **Active attacks**

These attacks are aimed at remote penetrating into your computer, stealing data or executing exploits so to disrupt the operating system normal functioning:

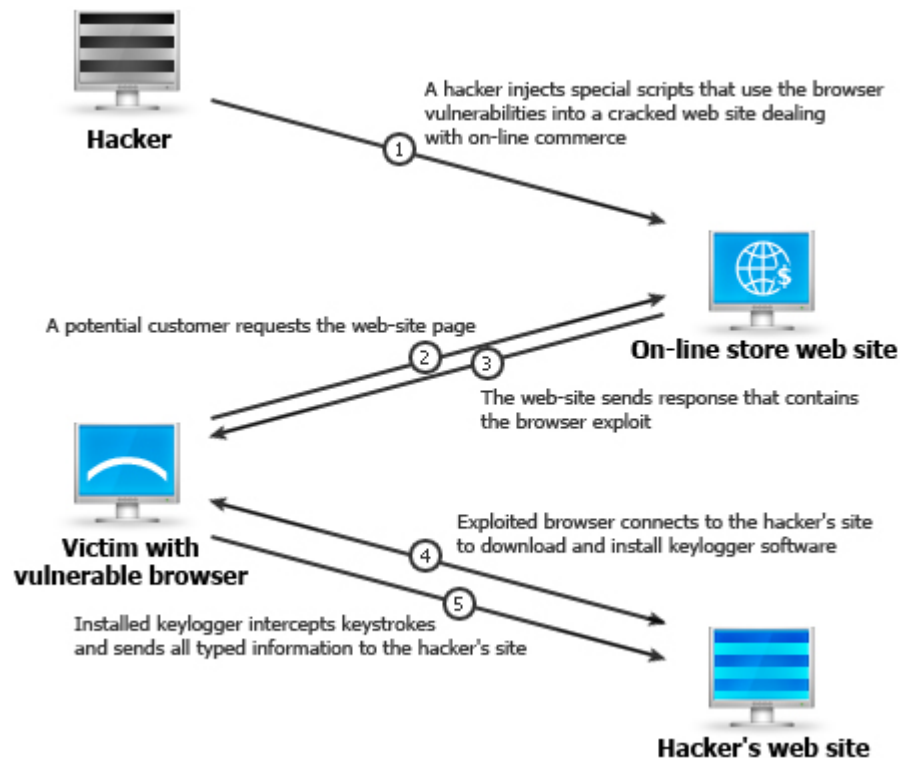
- **IP Address Spoofing.** That involves changing or disguising the IP address of a computer from which the attack is performed. It is especially dangerous in networks with authentication based on IP-address.
- **Denial of Service (DoS) attacks.** A massive flood against a concrete computer is performed so that to exhaust its resources and suck up network bandwidth that makes the computer inaccessible for other computers through network. One type of the DoS attack based on spoofing is shown at the pic below:



At that pic a hacker runs the ping command (that is used to check whether a destination network is available) specifying the a.b.c.d address, borrowed from other computer, as the IP-address that initiated the command (i.e the source IP). In response to the command all the computers of the destination network send back packets to the innocent computer with the a.b.c.d address so confirming their accessibility and at the same time overloading it that may cause its hanging.

- **Browsers attacks.** Browser vulnerabilities are discovered regularly. Browser holes let an attacker evade the security restrictions on active Web content and bypass cryptographic signature checks. For instance a

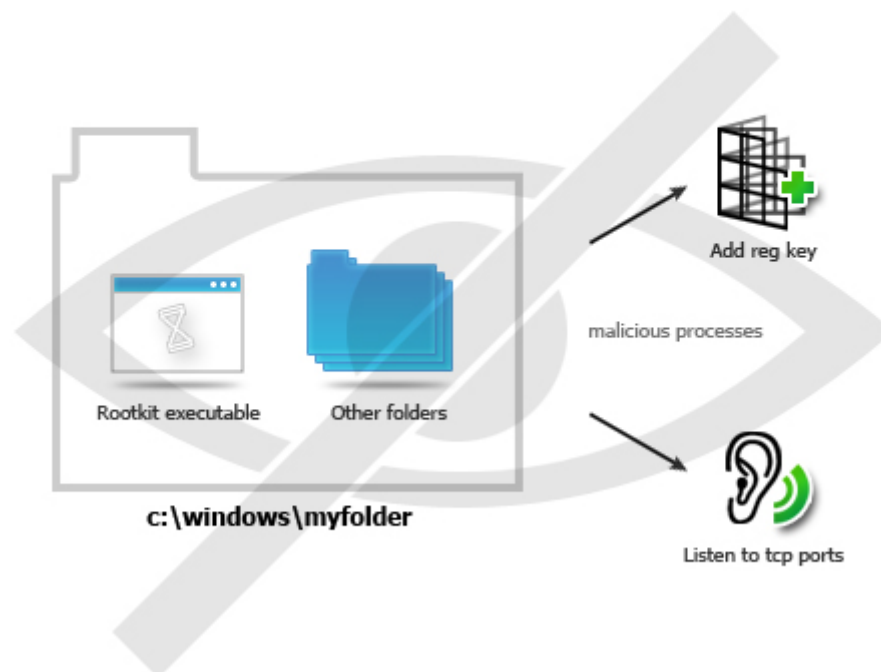
browser vulnerability may cause a keylogger installation by an attacker:



- **Backdoor attacks.** This allows an attacker to access a remote computer using an alternative entry methods. Usually users log in through front doors, such as login screens with user account names and passwords or token-based authentication (e.g. a smart card). Attackers use backdoors to bypass these system security controls that act as the front door. Commonly the very first time backdoor is preceded with penetrating into a computer using an undocumented feature or not yet announced operating system vulnerability and then when an attacker gains an access to the remote computer, he installs a backdoor software there so to penetrate into the remote computer over and over again but using his own entry since then and own, for instance, command prompt listening data on any ports and redirecting them wherever he wants.

- **Rootkit attacks.** These attacks are most dangerous and rather difficult to discover. Having penetrated into a computer an attacker replaces system files with the modified ones or directly modifies the heart of the operating system - kernel. So being hidden this way, they seem to be as the usual and native components of the operating system though they are not because subservient to the needs of the attacker. Look at the pic, that shows how a hacker using a rootkit executable in a folder hides it, all its contents and everything else that happens from this directory:

**User or Administrator runs taskmanager, netstat or other monitoring utilities
and can't see any processes**



How does AVS Firewall Defend the Computer?

AVS Firewall provides the solid defense of your system stability through:

Network protection. **AVS Firewall** works in both directions. That means the program intercepts the **outbound** connections initiated by applications on your computer and the ones which income to it i.e. the **inbound**. When a connection is intercepted **AVS Firewall** asks you whether to allow or forbid it, all your decisions can be saved as permanent rules so to prevent you from taking a decision on the same connection over and over again. In short you have the absolute power over connections, it is optimal because whatever network attack is it can do harm only in case if you allow a dangerous connection. Moreover **AVS Firewall** automatically beats off the port scanning attacks that both rids of an excess decision-taking on a permission and enhances the security.

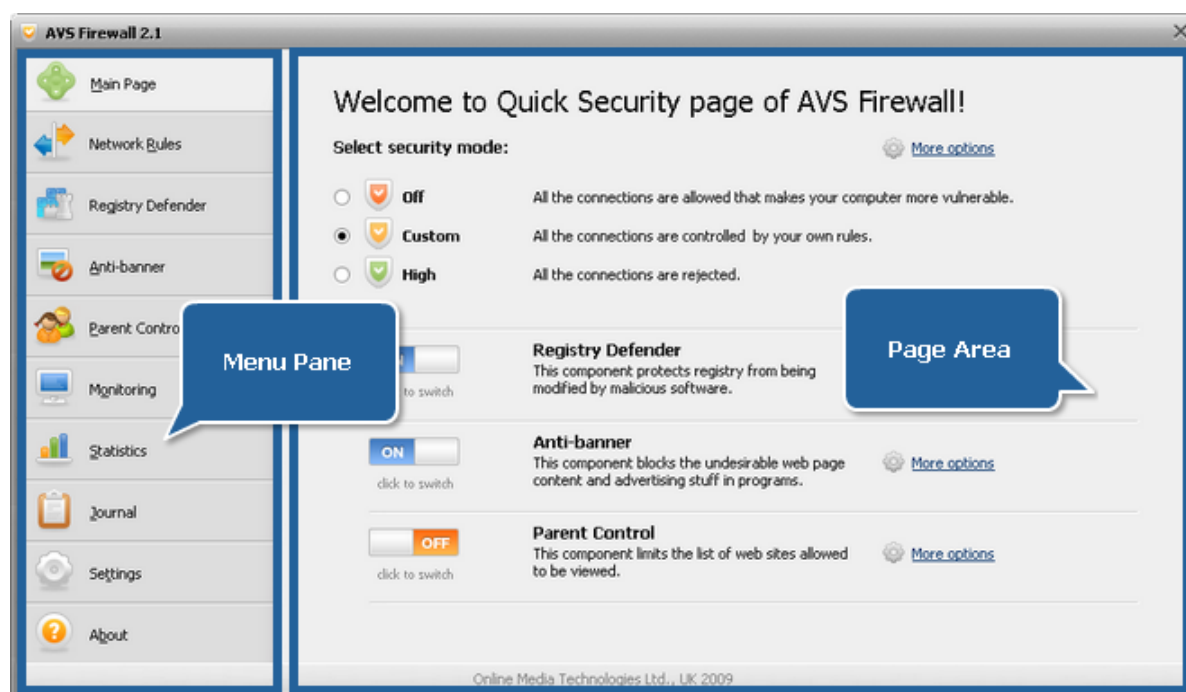
Registry protection. **AVS Firewall** includes the special component **Registry Defender** that controls any access to the the most critical registry key values initiated by applications on your computer. The component works from the principle of one-time permission. That means you should give a permission again as any attempt to modify the controlled registry key values occurs, no matter if the same attempt occurred earlier and what permission you gave it. In other words each new or newly initiated modification try awaits a permission given afresh:



The solid arrows show the inbound and outbounds connections or an attempt to modify the controlled registry key value and dashed ones simulate allowing or forbidding to establish connections or change the registry key value i.e a certain decision taken by the user.

Program Interface

The interface of **AVS Firewall** is designed to obtain the proper level of security with incredible ease and clarity - you just switch between the functional page tabs within the same window and manage your security, get different information on connections and events, adjust the program behaviour the way you like:



Menu Pane is the set of page tabs:

Page tab	Description
Main Page	Press the tab to set the security strategy and enable or disable the AVS Firewall components so that to obtain the desired defense scale quickly and instantly.
Network Rules	Press the tab to manage the outbound and inbound connection rules in the Custom mode.
Registry Defender	Press the tab to manage the controlled registry keys so that to protect your system from malicious software influence.
Anti-banner	Press the tab to manage and add your own blocked URLs which cause the undesired web content or advertising stuff in adware programs.
Parent Control	Press the tab to add the trusted sites only, so preventing your children from, for instance, visiting the X-rated web pages.
Monitoring	Press the tab to monitor all the initiated outbound and inbound connections.
Statistics	Press the tab to see persistently refreshed statistics on the application outgoing and incoming traffic volume. The chart is used to dynamically display the incoming traffic size on different protocols.
Journal	Press the tab to view the history of the occurred events on outbound connections.
Settings	Press the tab to adjust the AVS Firewall behaviour the way you like.
About	Press the tab to get information about the AVS Firewall version you are working with and read the end-user license agreement.

Page Area is the area where all the information and controls relating to a certain feature are placed. The view of this area differs depending upon the **Menu Pane** tab pressed.

If **AVS Firewall** is loaded the icon is shown in system tray, the way it looks depends upon the program mode:



Providing Security with AVS Firewall: Overview

AVS Firewall has all the necessary features to attain the proper security level on your computer:




- You can create the **Application rules** - to control outbound connections and the **External connections rules** - to regulate inbound requests;
- You are always in the know what connections are established and maintained including all the details by means of the real-time **Monitoring** feature;
- You get advanced information on incoming and outgoing traffic size and can estimate incoming traffic on different protocols through the graphic by means of the **Statistics** feature;
- You need not worry if you are not sure which event happened on a connection, just look through the **Journal**;
- Malicious software won't harm your system with the Registry Defender switched on that intercepts any attempt to modify the most critical registry key values;
- Get rid of importunate ad-images and flash banners while surfing through the Internet or using adware by means of the Anti-banner;
- You can prevent your children from visiting undesirable sites, specifying only trusted ones through the Parent Control;
- You will never fail to control a new connection or an attempt to modify registry with the **Alert Window** enabled.

Network Protection: Overview

The main idea of **AVS Firewall** consists in network protection so that to defend your computer from outer attacks. Usually network protection is based on a security mode. So the very first step you should take using **AVS Firewall** is to select the security mode.

Selecting the Security Mode: Overview

Depending on what requirements you lay to your computer network security, **AVS Firewall** can stick to one of three security modes:

-  **Off** - if you do not worry about your computer defense;
-  **Custom** - if you want to define behavior both for applications and incoming connections by yourself;
-  **High** - if your purpose is to forbid any outbound and inbound connections.

Off

Choosing this mode disables an opportunity to apply the restrictive rules to applications on and incoming connections to your computer, making it unguarded and vulnerable, although you still can monitor newly incipient connections, estimate traffic through **Statistics** and view the **Journal** which registers only allowed connections in this mode. You can switch into this mode, for instance, from the **Main Page**:

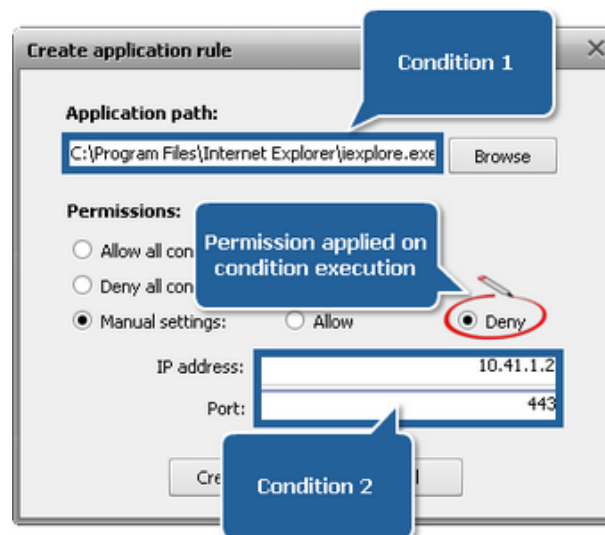


Custom: Overview

This mode lets you create your own rules for **applications** and **external connections**. Decide whether a connection should be permitted or declined. With due taken actions, the **Custom** mode provides the optimum security level.

Applying Rules: Overview

A rule is a **permission** applied in terms of a certain **condition** execution. Within the context of **AVS Firewall** the **condition** may be an **application** and **IP-address** with/without a specified **port**; **permissions** applied are either **allow** or **deny**. For instance, look at the snapshot below:



That rule can be put into words in the following way: "Forbid Internet Explorer to establish connection to port 443 of the remote computer with IP-address 10.41.1.12".

You can create two types of rules using **AVS Firewall**:

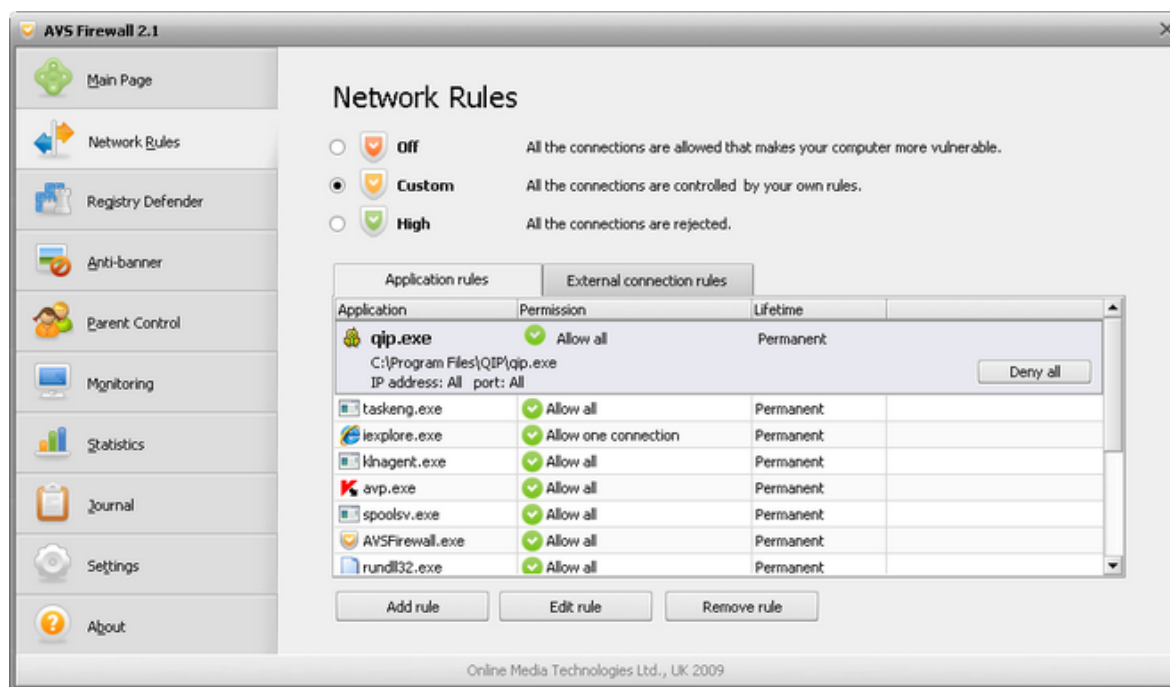
- **Application rules** - they regulate all the outbound connections **from** your computer **to** the outer environment;
- **External connection rules** - they regulate all the inbound connection **to** your computer **from** the outer environment.

Note: if there is no rule created for an application or inbound connection yet the **Alert Window** suggesting to make a decision on a permission will be shown by default.

Application Rules

Having created rules for applications you take them under your control and can be totally sure that they won't give you an unpleasant surprise one day. It is important to understand that application rules are aimed at outbound connections initiated by an application and can be created in **Custom** mode only.

To create a rule, click the **Network Rules** tab of **Menu Pane** then switch to the **Application rules** tab:

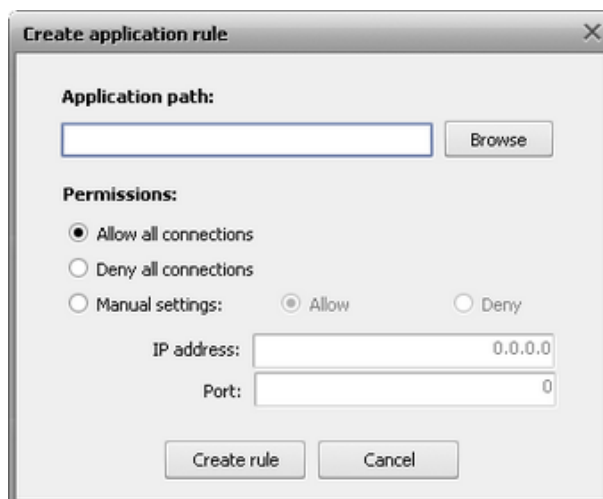


You will see the table of application rules that includes the following information fields:

Field	Description
Application	Shows the name of an application executable file a rule is applied to;
Permission	Shows the set permission for a rule: Allow all - an application has full access to the outer world; Allow one connection - an application is allowed to connect to a certain IP-address and port associated with it only; Deny all - an application is forbidden to initiate any connections; Deny one connection - an application is forbidden to connect to a certain IP-address and port associated with it only; Delayed decision - you put off taking a decision on assigning a permission having clicked the Ask me later button in the Alert Window. The temporary rule with the Allow all permission will be created;
Lifetime	Shows whether a rule is applied permanently or just until logging off.

Note: if you click on a certain row you will see extra information on a corresponding rule: full path to an application executable and which IP-address and port the rule is applied to. The same way you can change a rule permission to opposite - in case your rule has the **Allow all/Deny all** permission or choose between **Allow all** and **Deny all** - in case your rule has the **Allow one connection/Deny one connection** permission.

Then press the **Add rule** button at the bottom of the window, the **Create application rule** window will appear:

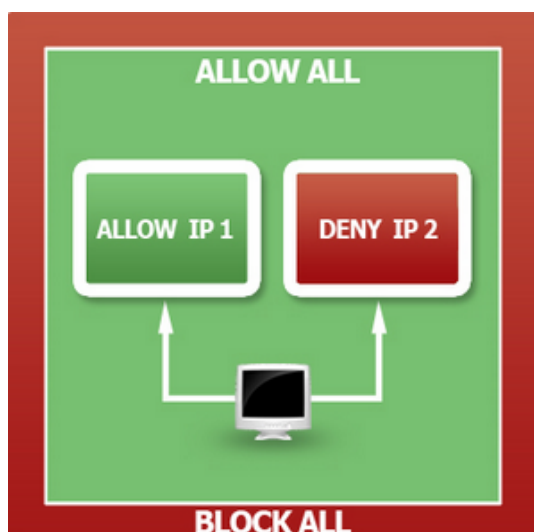


Press the **Browse** button to choose an application you want to create a rule for. And then set one of the permissions for it:

- **Allow all connections** - all outbound connections to any IP-address and port will be allowed;
- **Deny all connections** - all outbound connections to any IP-address and port will be forbidden;
- **Manual settings** - you allow or forbid connections to a certain IP-address and/or port only.

To change or delete a rule, select a row then press the **Edit rule** or **Remove rule** button correspondingly.

Rules for the same application may overlap each other - if they define different permissions. Have a look at the illustration:

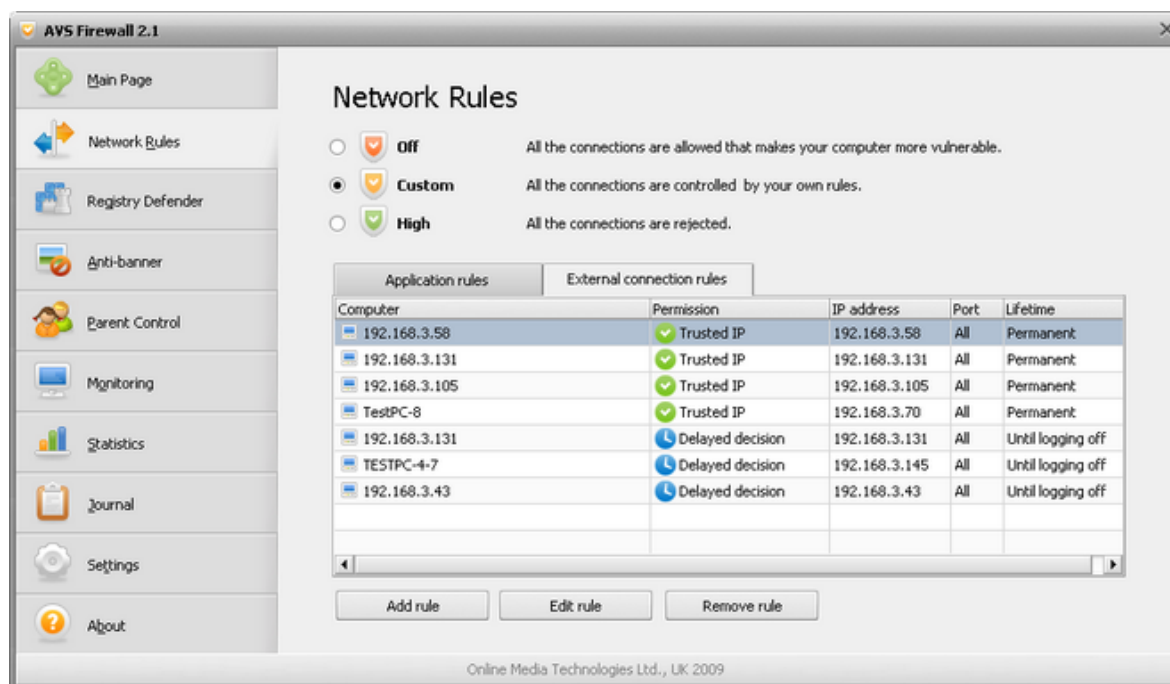


That shows the priority of permissions over each other if you define the different rules for the same application. For example, two rules, assigning contrary permissions for the outbound connection to different IPs don't overlap each other at all and work as two independent rules. If to create another rule, setting the permission **Allow all**, then the resulted permission is changed to **Allow all** overlapping two previously defined rules, which will disappear from the rule list being replaced with the new one. And if to add one more rule that assign the permission **Block (Deny) all** then it will overlap the previous **Allow all** rule, forbidding any outbound connections initiated by the application.

Note: if it came out to be so that you defined rules with absolutely equal conditions but different permissions, the following statement should be borne in mind: **Deny** overlaps **Allow**, **Allow all** overlaps both **Deny** and **Allow**, **Block (Deny) all** overlaps **Allow all**.

External Connection Rules

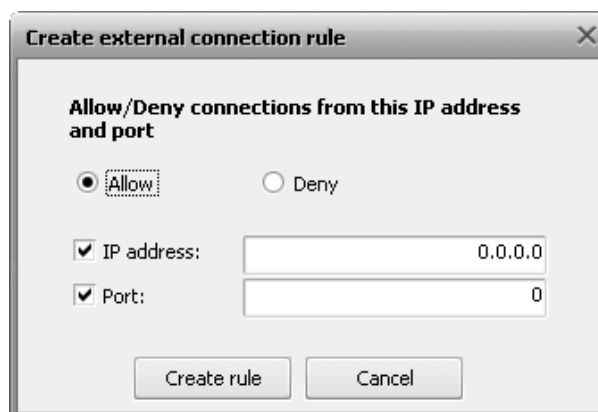
If you want to control all the inbound connection requests coming from the outer environment then you should create rules of this type. To add a rule, click the **Network Rules** tab of **Menu Pane** then switch to the **External connection rules** tab:



You will see the table of external connection rules that includes the following information fields:

Field	Description
Computer name	Shows, if possible, the Netbios or DNS name of a remote computer that initiated an inbound connection. If a rule has been created for a certain port only the field contains the Port rule text;
Permission	Shows the set permission including information what it is applied to: Trusted IP - the permissive rule for a certain IP-address and all ports associated with it; Opened port - the permissive rule for a certain port of all IP-addresses; Trusted IP and port - the permissive rule for a certain IP-address and port associated with it; Untrusted IP - the prohibitive rule for a certain IP-address and all ports associated with it; Closed port - the prohibitive rule for a certain port no matter what IP-address is; Blocked IP and port - the prohibitive rule for a certain IP-address and port associated with it; Delayed decision - you put off taking a decision on assigning a permission having clicked the Ask me later button in the Alert Window. The temporary rule with the Deny all permission will be created;
IP	Shows a remote computer IP-address;
Port	Shows a separate port number or the one associated with a certain IP-address;
Lifetime	Shows whether a rule is applied permanently or just until logging off.

Then press the **Add rule** button the **Create external connection rule** window will appear:



In that window input a remote IP and/or port and assign a permission - either **Allow** or **Deny**.

To change or delete a rule, select a row then press the **Edit rule** or **Remove rule** button correspondingly.

AVS Firewall automatically beats off the **port scanning** attacks. A certain quantity of inbound requests made in a certain time period and aimed at closed ports is detected as the **port scanning** attack. The prohibitive rule on an attacking computer IP-address is added in such a case. When the attack occurs, the right bottom corner notification window appears to inform you about that, you can click the **More info** link to move to the created rule as well:



Note: if a rule has been added for a network (by means of the **Alert Window**) that will be reflected in the table in the following way:

192.168.[0-7].[0-255]	Allow all	192.168.3.141	Permanent
-----------------------	-----------	---------------	-----------

where the rule for the network defines a default permission for all the computers that are included into it unless you add a specified rule for a computer that belongs the network manually:

192.168.[0-7].[0-255]	Allow all	192.168.3.141	Permanent
192.168.3.58	Untrusted IP	192.168.3.58	All Permanent

That means permissions specified for computers are stronger than a permission defined for a network they belong to.

High

Enabling this mode you break all the established connections and prohibit the subsequent ones. This mode is useful if you want to prevent sending data to and receiving them from the outer world just with a single mouse click. The **Journal** registers only denied connections and the **Monitoring** and **Statistics** are not performed at all in this mode.

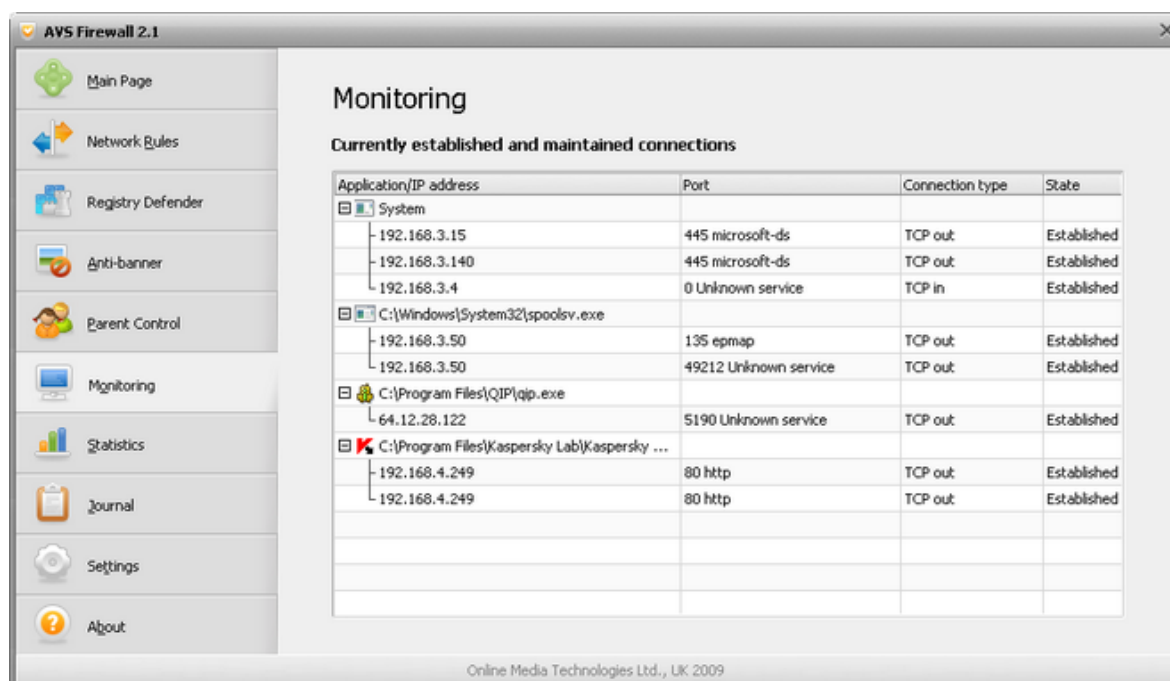
You can switch into this mode, for instance, from the **Main Page**:



Monitoring Network Activity

Monitoring is useful if you want to know which connections are established and ready to accept data at the moment including all the details.

To view the network activity, click the **Monitoring** tab of the **Menu Pane**:



The page has the table filled with the following information:

Field	Description
Application/IP-address	Shows the full path to an application including its executable name and an IP-address of a computer that has a connection associated with the application.
Port	Shows a port a connection is carried through.
Connection type	Shows a protocol that a connecton uses as well as direction: <ul style="list-style-type: none"> • TCP in - the TCP-protocol is used, the connection is inbound; • TCP out - the TCP-protocol is used, the connection is outbound; • UDP in - the UDP-protocol is used, the connection is inbound; • UDP out - the UDP-protocol is used, the connection is outbound.
State	Shows the current state of a connection: <ul style="list-style-type: none"> • Established - a connection is established; • Listening - a connection is ready to accept data.

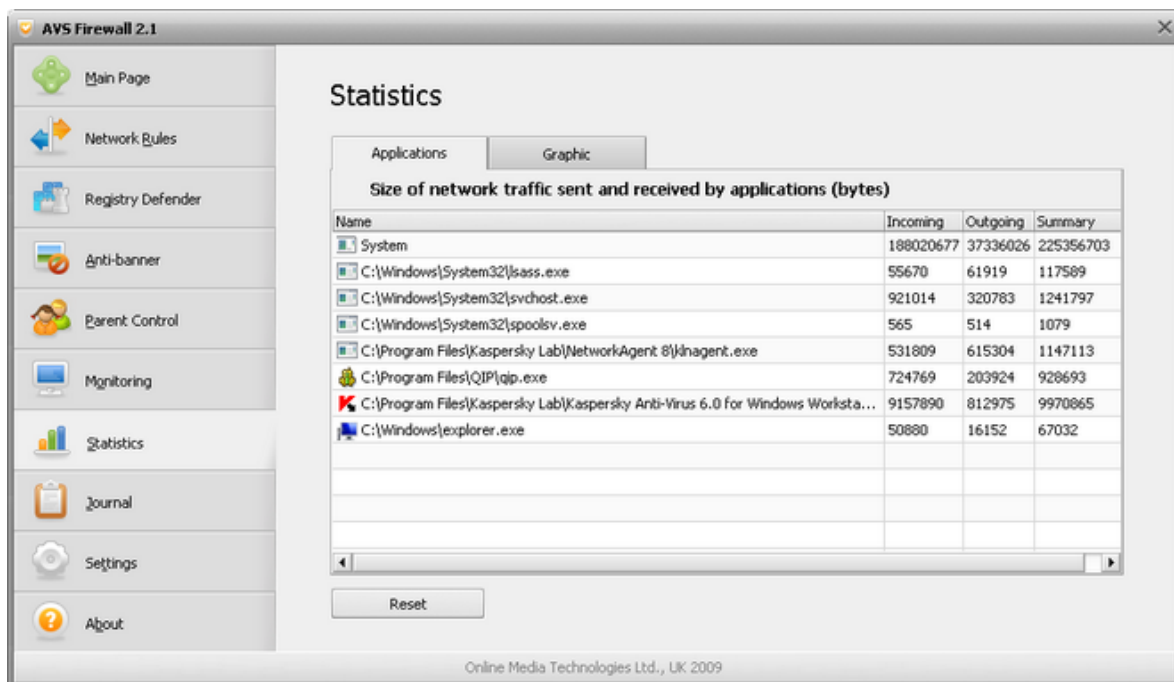


Note: when a new connection is just initiated its row is highlighted in bright green and when a connection is finished its row is highlighted in bright red.

Watching the Traffic Statistics

Traffic statistics lets you watch and estimate the incoming traffic received and outgoing one sent by applications on different protocols as well as general information on enabled connections of different types that you use to have an access to the outer environment.

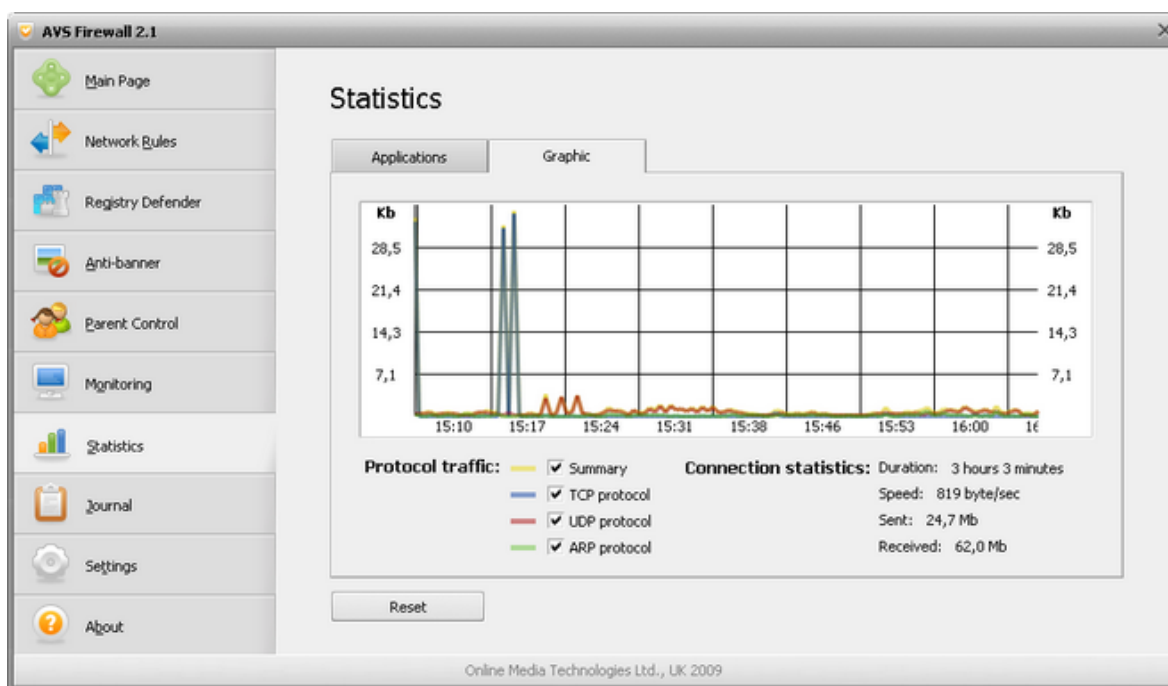
To watch the statistics, click the **Statistics** tab of the **Menu Pane**. The page area has two tabs:



Applications. This tab contains the table filled with detailed and refreshed in real time information on application connection traffic:

Field	Description
Name	Shows the full path to an application including its executable name.
Incoming	Shows the size of incoming traffic received by an application in bytes.
Outgoing	Shows the size of outgoing traffic sent by an application in bytes.
Summary	Shows the summarized size of traffic on an application in both directions.

Graphic. This tab contains the chart plotted on the incoming traffic data. Horizontal axis of the chart is used to designate time and vertical one shows the incoming traffic size in kilobytes per time units marked on the horizontal axis. Watching the chart you can track incoming traffic on TCP, UDP, ARP protocols both apart and summary - that's why you can see four curves of different colors. If you do not want to watch incoming traffic on all the criteria just uncheck unnecessary legends:



The **Connection statistics** section of the **Graphic** tab contains the following information on connection:

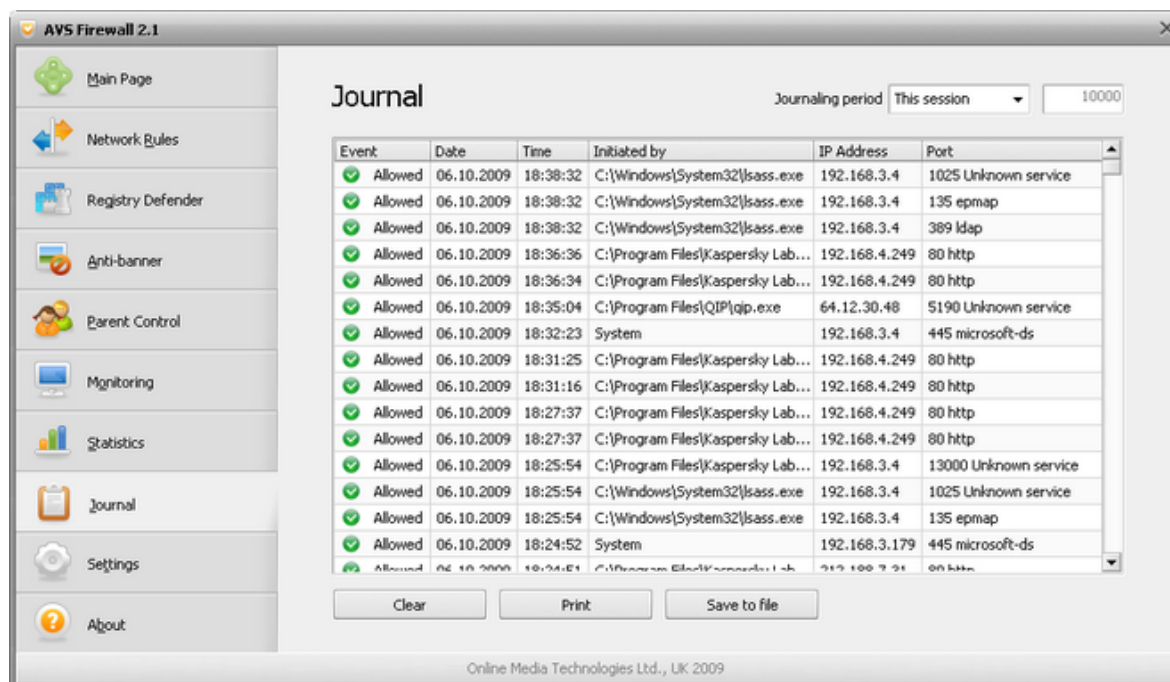
- **Duration** - time passed since **AVS Firewall** has been loaded;
- **Speed** - the current speed at which traffic is being received at the moment;
- **Sent** - the general size of outbound traffic sent during the current Windows session;
- **Received** - the general size of inbound traffic received during the current Windows session.

To clear and zeroize the shown statistics, click the **Reset** button.

Viewing the Journal of Occurred Events

Journal is useful if you want to track the history of initiated outbound connections and find out what happened to them - mainly whether they were allowed or denied although there are another two specific events as well.

To view the journal, click the **Journal** tab of the **Menu Pane**:



The page has the table filled with the following information:

Field	Description
Event	Shows an event happened: <ul style="list-style-type: none"> • Allowed - the event is provoked each time when a connection is allowed; • Denied - the event is provoked each time when a connection is denied; • Logged - the event is provoked when AVS Firewall working in the Custom mode is unloaded and a new outbound connection that does not have a rule is initiated. The new outbound connection is allowed until logging off in such a case; • Suspended - the event is provoked each time when the Alert Window for application appears.
Date	Shows the exact date when an event occurred.
Time	Shows the exact time when an event occurred.
Initiated by	Shows the full path to an application which provoked an event.
IP address	Shows a remote computer IP-address.
Port	Shows a specific port associated with IP-address.

You can select records to be shown by means of the **Journaling period** combo box:

- **This session** - all the records since the moment **AVS Firewall** has been launched are shown (default);
- **Day** - all the records during today are shown;
- **Month** - all the records during the current month are shown;
- **Custom count** - as many records are shown as you define. By default the value is set to 10000 records to be shown.

To delete all the records from the journal, click the **Clear** button.

To print all the records on events occurred, click the **Print** button. Make sure **Print range** is set to **All** then click the **Print** button in the **Print** window that appears.

The **Save to file** button is meant for saving all the records to a file with the *txt* extension so as to backup them in case when you are going to clear the journal, for instance.

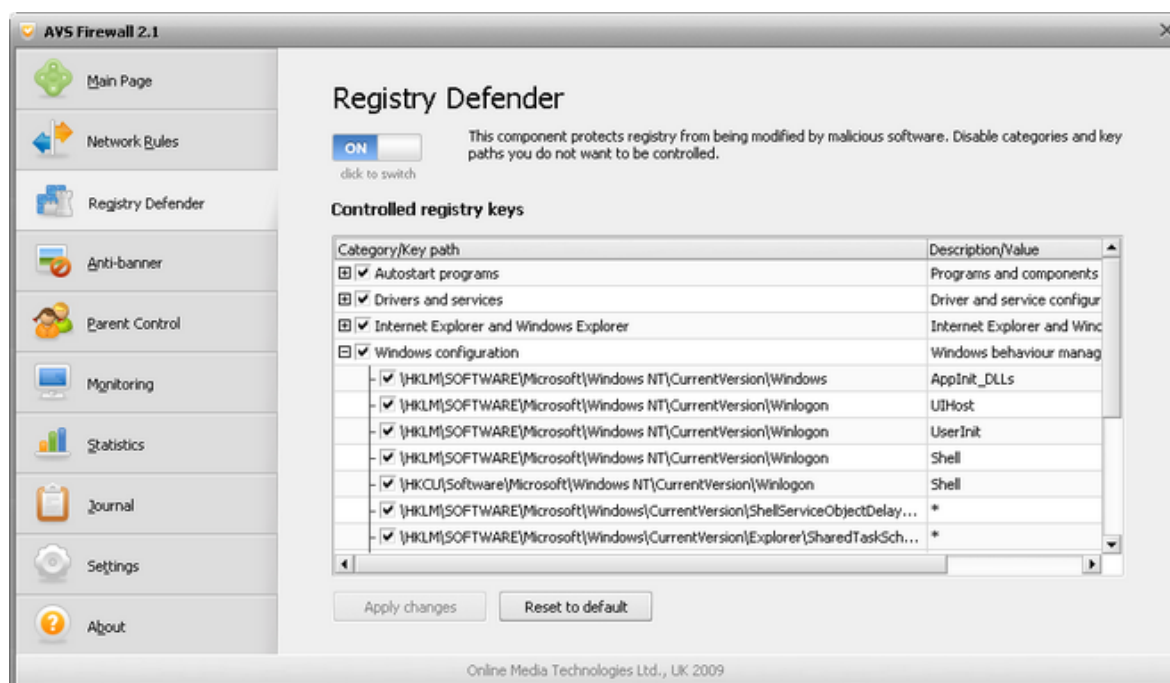
Note: you can perform all these actions through the contextual menu as well clicking the right mouse button on the table area.

Registry Defender

This component defends the most critical registry key values from modification by malicious programs. All the controlled keys are grouped into the built-in categories. **Registry Defender** is switched on by default.

To use **Registry Defender** make sure it is enabled first (set its switcher to **ON** from **Main Page**, for instance, if it is not so).

To manage the controlled keys, click the **Registry Defender** tab:



The page contains the table with predefined categories:

Field	Description
Category/ Key path	Shows the category name and key paths or key path masks it contains.
Description/Value	Shows the category description and values of the controlled key path. The * wildcard means all the values within a key path are controlled.

Note: you can see two types of key path mask. For instance:

- \HKLM\Software\Microsoft\Internet Explorer\Extensions* - only subkeys within the key path are taken;
- \HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\FindExtensions* - both the key path and its subkeys are taken.

To exclude a category or key path from the control, uncheck it then click the **Apply changes** button.

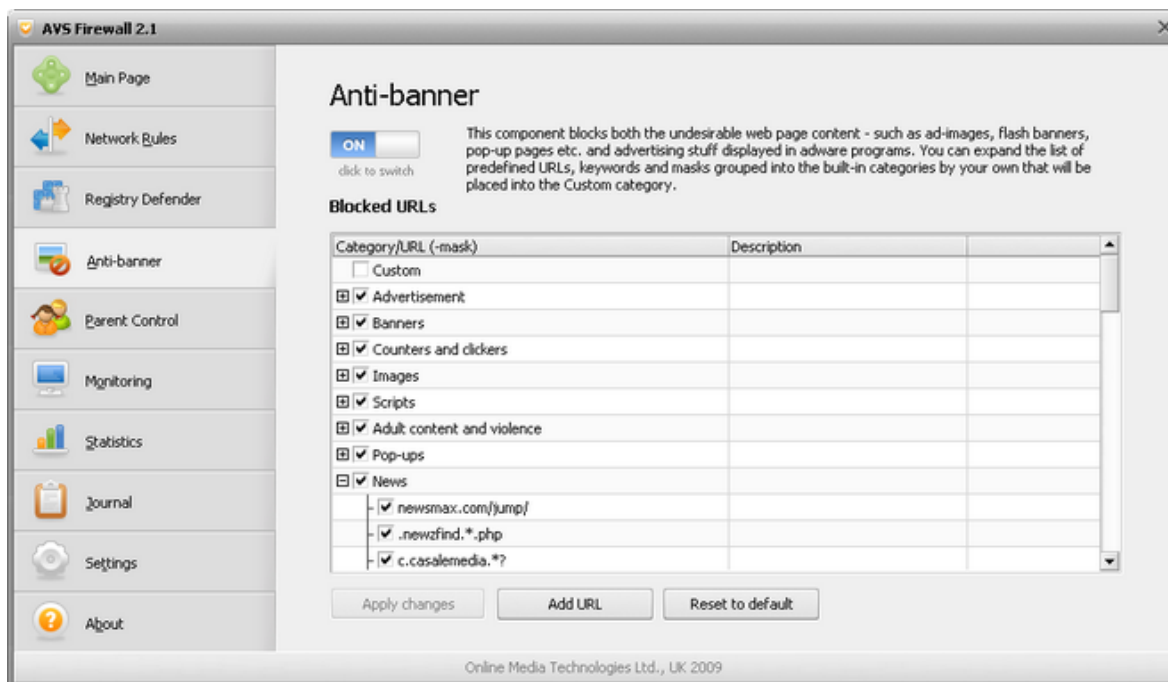
To return the default set of the controlled key paths, click the **Reset to default** button.

Anti-banner

This component blocks the undesired and importunate web content such as ad-images, flash banners, clickers, counters and pop-up pages and prevents the dangerous scripts from execution. More than that **Anti-banner** can block the advertising stuff that is displayed in adware programs. The predefined blocked URLs, keywords they may contain and URL masks are grouped into the built-in categories. **Anti-banner** is switched on by default.

To use **Anti-banner** make sure it is enabled first (set its switcher to **ON** from **Main Page**, for instance, if it is not so).

To manage or add the blocked URLs, click the **Anti-banner** tab:



The page contains the table with categories:

Field	Description
Category/URL (-mask)	Shows the category name and URLs, keywords, masks it contains.
Description	Shows a description you specified for a URL, keyword or mask added .

To add your own URLs, keywords they may contain or URL masks, click the **Add URL** button. They will be placed into the **Custom** category.

To exclude a category, URLs, keywords or masks from the control, just uncheck them then click the **Apply changes** button.

To return the default set of the blocked URLs, keywords and masks, click the **Reset to default** button.

Parent Control

This component limits the list of site allowed to be viewed. That is useful when you want to prevent your children from visiting sites with adult content, for instance. If **Parent Control** is on that means only sites added can be visited from your computer, all other sites will be blocked. The component is switched off by default.

To use **Parent Control** make sure it is enabled first (set its switcher to **ON** from **Main Page**, for instance, if it is not so).

To manage or add the trusted sites, click the **Parent Control** tab:



The page contains the table where you can add site names or URLs:

Field	Description
Site name/URL	Shows a site name or URL.
Description	Shows your description of a site name or URL added.

Note: if **Parent Control** is on and the table of trusted sites is empty, you will not be able to view sites through a browser at all.

To add a new site name or URL, click the **Add URL** button.

To edit a site name or URL, select the corresponding row then click the **Edit** button.

To disable a site name or URL, just uncheck it then click the **Apply changes** button.

To delete a site name or URL, select the corresponding row then click the **Delete** button.

To increase the **Parent Control** efficiency you should assign a password. Click the **Change password** button, input your password and its confirmation in the window that appears. Since that moment you will be asked to enter the password each time before start working with **Parent Control**.

Changing the Program Settings

To change settings, click the **Settings** tab:



The page contains the sections with settings:

Application

- **Start with Windows** - by default **AVS Firewall** starts together with Windows but you can disable that by unchecking this option.

Registry Defender

- **Automatically deny untrusted application attempts to modify registry** - if the option is checked then any attempt to modify registry by an application that does not have the digital signature will be rejected automatically. The right bottom corner notification window will appear to inform you about that.
- **Default permission for unhandled alerts** - choose what permission should be assigned for each new registry modification attempt by default - in case you close the Alert Window when it appears, its display time expires before you take a decision or if you do not use it at all (the **Show Alert Window** option is unchecked).

Network Protection

- **Automatically generate allowing rules for trusted applications** - if the option is checked the **Allow all** rule for an application that has the digital signature will be added automatically when it initiates a connection. The right bottom corner notification window will appear to inform you about that.
- **Always create a permanent rule** - if the option is enabled then the **Create a permanent rule** option of **Alert Window** will be always checked.
- **Default permission for unhandled alerts** - choose what permission should be assigned for each new connection by default - in case you close the Alert Window when it appears, its display time expires before you take a decision or do not use it at all (the **Show Alert Window** option is unchecked).

Alert

- **Show Alert Window** - if the option is checked the **Alert Window** will appear for each new connection or registry modification attempt.
- **Display time** - check the option and input a time value if you want to limit the **Alert Window** display duration.

To save the changes, click the **Save settings** button.



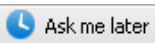
To restore the settings **AVS Firewall** had originally, click the **Reset to default** button.

Using Alert Window

Alert Window enabled appears each time if a connection is initiated the very first time (i.e. no rule has been created for it yet) or when an application tries to modify the controlled registry keys. The window suggests you to decide how to treat a connection or an attempt to modify registry further.

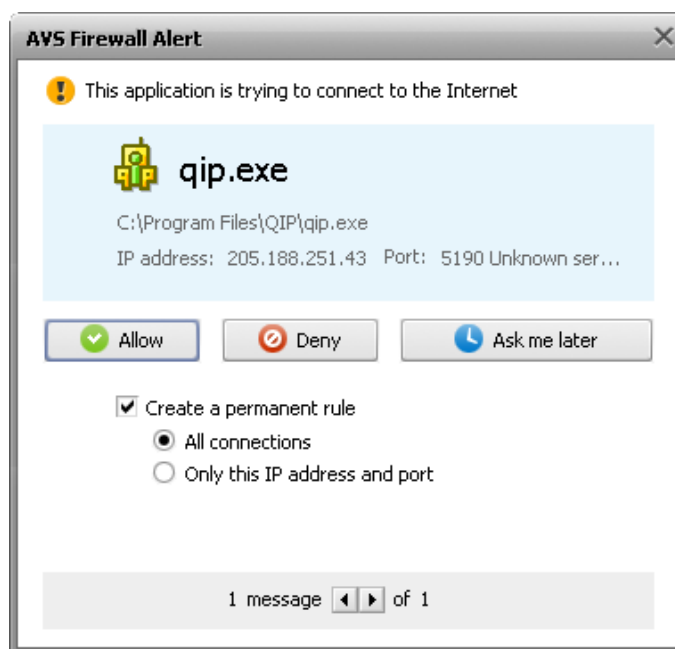
Network Protection Alert Window

The suggested permissions are the same both for the outbound and inbound connection **Alert Window**:

Button	Description
 Allow	You allow a connection.
 Deny	You reject a connection.
 Ask me later	You put off taking a decision. A temporary rule will be created.

- **Alert Window for application**

The window appears when a new application that does not have a rule created for initiates an outbound connection or if a rule for an application exists but its connection parameters are new and do not meet the rule permission conditions. The way it looks is shown below:



The name of an application that initiates an outbound connection is highlighted in bold. You can see information on **IP-address** and **Port** of a remote computer the connection is aimed at as well.

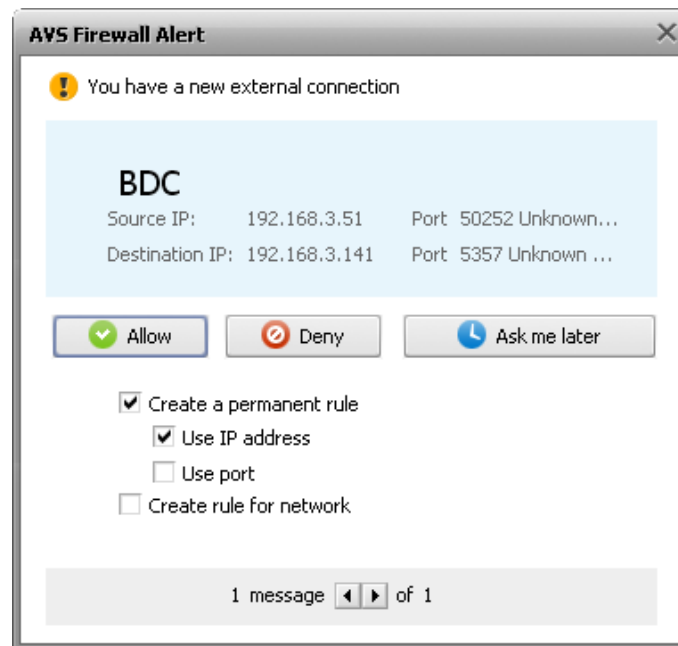
The **Create a permanent rule** option checked means you want a rule to be always applied and on a certain condition or

conditions:

- **All connections** - a permission will be assigned for all IP addresses and ports;
- **Only this IP address and port** - a permission will be applied only for the shown IP address and port.

● **Alert Window for external connection**

The window appears when a new remote computer that does not have a rule created for initiates an inbound connection or if a rule for a remote computer exists but its connection parameters are new and do not meet the rule permission conditions. The way it looks is shown below:



The name of a remote computer that initiates an inbound connection is highlighted in bold. You can see information on **Source IP** - an IP-address of a computer that initiated the connection; **Destination IP** - an IP-address of a computer the connection is aimed at, it is always the IP-address of the active connection interface you currently use for networking; **Ports** - ports associated with the **Source** and **Destination IPs**.

The **Create a permanent rule** option checked means you want a rule to be always applied and on a certain condition or conditions:



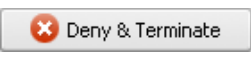
- **Use IP address** and **Use port**. When both options are checked a rule will be created only for the shown source IP-address and port, otherwise it will be applied either to all ports of a certain source IP-address (in case the **Use IP address** option is checked only) or to a certain port no matter what the source IP-address is;
- **Create rule for network**. If this option is checked then a rule will be applied to all the computers of a network the **Source IP** belongs to. Please, refer to the **External connection rules** page for details.



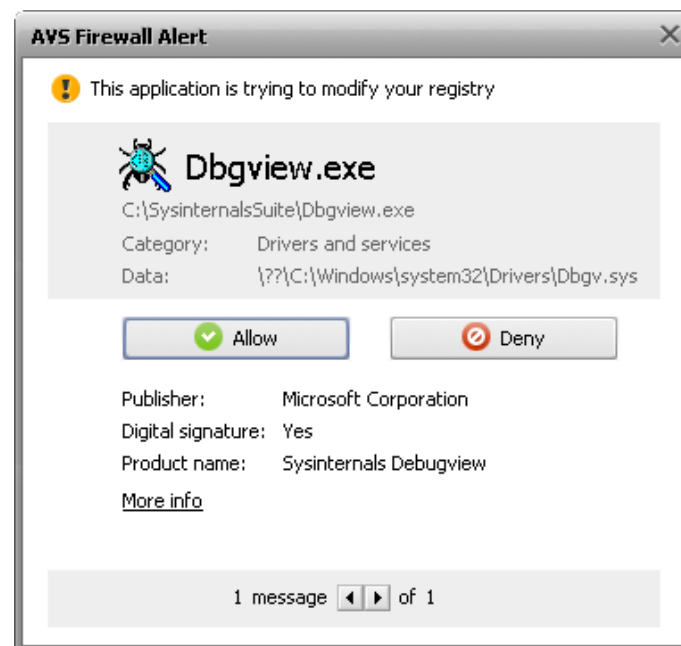
Note: if all three options are checked a rule for a network with the corresponding permission will be created including a rule for a computer (with the same permission) that belongs to that network and initiates a connection.

Registry Defender Alert Window

This **Alert Window** suggests the following permissions:

Button	Description
 Allow	You allow to modify a registry key value.
 Deny	You forbid to modify a registry key value.
 Deny & Terminate	When the same application tries to modify the same registry key value again after you defined a permission for the very first attempt this button becomes available. Pressing it you forbid the registry key value modification and kill the application process.

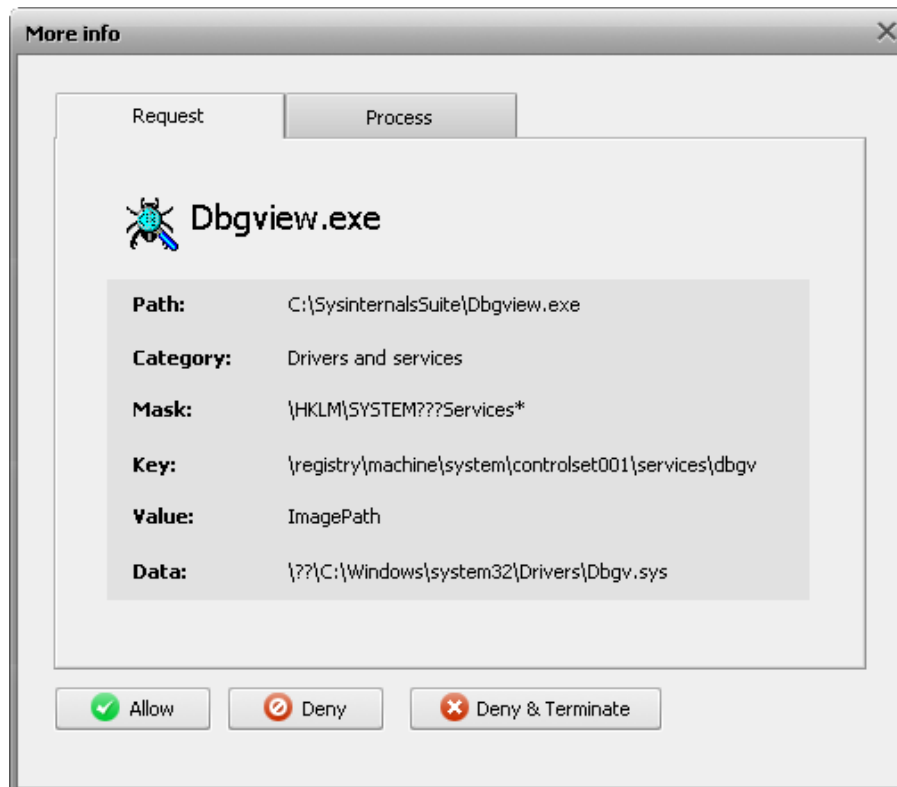
This **Alert Window** appears when an application tries to assign data to a value within the controlled registry key. The way it looks is shown below:



The name of an application that tries to modify a value data is highlighted in bold. You can see information on which **Category** a key value belongs to and what exact **Data** are added as well. At the bottom of the window the following information are shown:

- **Publisher** - the name of an application signer;
- **Digital signature** - shows whether an application has the right digital signature or not;
- **Product name** - the full and official name of an application as a software product.

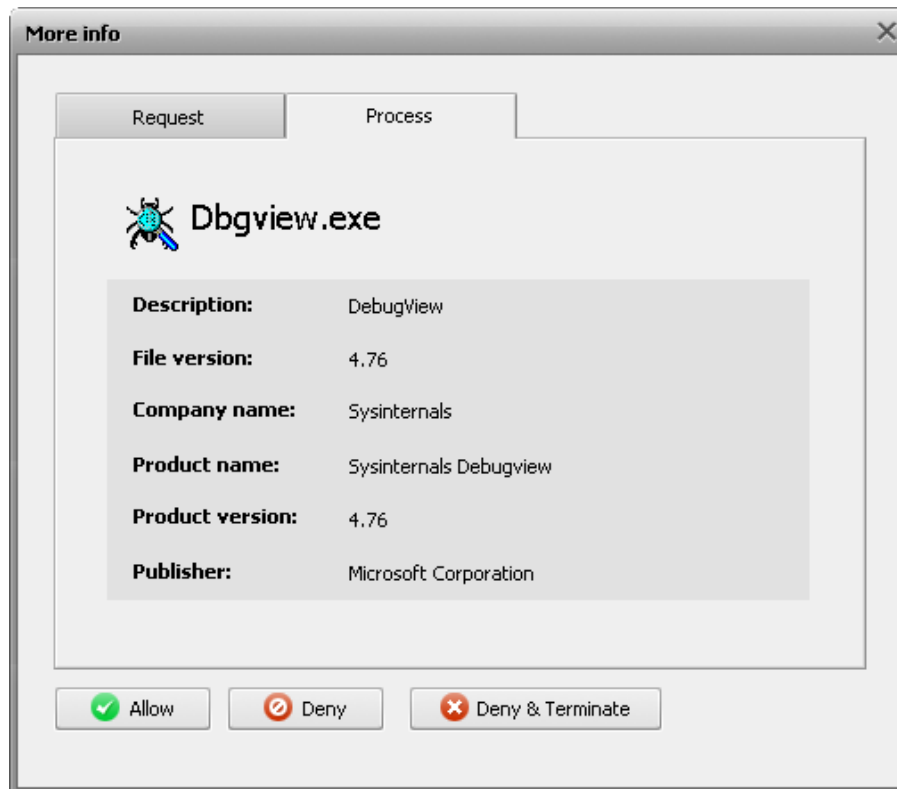
To learn even more details, click the **More info** link. The following window with two tabs will appear:



Request. This tab contains all the details about an attempt to modify the controlled registry key value:

- **Path** - the full path to an application that tries to modify a key value;
- **Category** - the name of the built-in category a key belongs to;
- **Mask** - the key path mask where modification is being aimed at;
- **Key** - the full path to a key where modification is being aimed at;
- **Value** - the name of a key value which is being modified;
- **Data** - data assigned to a key value.

Process. This tab contains the available details about a process file that tries to modify the controlled registry key value:



- **Description** - a process file description;
- **File version** - a process file version including the major, minor and build version;
- **Company name** - the name of a company that published a file;
- **Product name** - the full and official name of an application as a software product;
- **Product version** - the current version of an application as a software product;
- **Publisher** - the name of an application signer.