



# TerminET

## Personal Firewall

User Guide



# Contents

<b>1</b>	<b>INTRODUCTION</b>	<b>3</b>
1.1	ABOUT TERMINET	3
1.2	KEY TECHNICAL FEATURES	3
<b>2</b>	<b>GETTING STARTED</b>	<b>4</b>
2.1	INSTALLING TERMINET	4
2.2	GETTING STARTED WITH TERMINET	4
2.2.1	<i>Windows 98/ME</i>	4
2.2.2	<i>Windows NT/2000/XP</i>	4
2.2.3	<i>Administrator Mode</i>	4
2.3	THE TERMINET INTERFACE	5
<b>3</b>	<b>USERS AND GROUPS; MANAGING USERS AND GROUPS</b>	<b>9</b>
3.1	ADDING USERS (WINDOWS 98/ME)	9
3.2	CREATING GROUPS	9
<b>4</b>	<b>PROTECTION MODE CHANGE</b>	<b>10</b>
<b>5</b>	<b>TRAFFIC RULES</b>	<b>11</b>
5.1	CREATING RULES	11
<b>6</b>	<b>TRAFFIC REGISTRATION LOG</b>	<b>15</b>
<b>7</b>	<b>SCHEDULE</b>	<b>16</b>
7.1	DAILY SCHEDULE SETTINGS	17
7.2	WEEKLY SCHEDULE SETTINGS	18
<b>8</b>	<b>WEB LISTS</b>	<b>19</b>
8.1	BLACK LISTS	19
8.2	WHITE LISTS	19
8.3	GLOBAL AND LOCAL LISTS	19
<b>9</b>	<b>INTRUSION DETECTION SYSTEM (IDS) SETTINGS</b>	<b>20</b>
9.1	IDS EVENTS	20
<b>10</b>	<b>PROBLEMS WITH NETBIOS</b>	<b>22</b>

# 1 Introduction

## 1.1 About TermiNET

TermiNET is a Personal Firewall designed to protect a PC from outside attacks while connected to the Internet, browsing the web or accessing other Internet services. TermiNET can be initially installed in any one of the following protection modes:

1. **Closed Mode** by default blocks all traffic to and from the local machine. The administrator can then selectively open up access - for example, allow FTP only or allow FTP, Telnet and Web access. For parental control access can be limited to a specified set of pages only. The pages can be entered directly as specific rules or read from a URL "Whitelist".
2. **Open Mode** which imposes no initial blocking conditions. The administrator can then selectively close down specific access by application, port and protocol- (e.g.: block all Telnet and FTP, Block all incoming communication on port 25, block access to a specific set of web pages). Once more these can be entered as specific rules or read from a URL "Blacklist" or acceptable sites.
3. **Stealth Mode** allows all outgoing traffic but blocks all incoming connections unless initiated locally. In this mode the machine can be used to for Web browsing, FTP etc. as normal but is protected from attack while connected to the Internet.

TermiNET is an ideal security solution for SMEs and home users who wish to connect to the Internet securely but do not have the resources to support a large security infrastructure.

## 1.2 Key Technical Features

The key technical features of TermiNET include:

- Creating rules for blocking/allowing traffic: Simple checkbox facility to turn rules **on** or **off**.
- Blacklist/Whitelist facility provides the ability to deny access to specified undesirable sites, or to allow access only to known acceptable sites.
- Intrusion Detection System (IDS), included into the program, provides detecting and preventing hacker actions.
- Flexible access control allows rules to be specified by IP Address (or IP addresses range), URL, Port and / or Protocol.
- Time based rules can be configured to be active only on specified days.
- Schedule settings for access to Internet for each TermiNET.
- Simple to use "Windows Explorer" style interface makes configuring TermiNET simple and intuitive, even for the non-technical user.


## 2 Getting Started

### 2.1 Installing TermiNET

Insert the TermiNET CD into the CD drive on the PC. Setup should run automatically, if Autorun has been disabled click **Start**→ **Run** and type **D:\setup** where **D:** is the drive letter of the CD drive. Follow the on screen instructions to install the product.


When the installation routine is complete the PC **must** be rebooted in order to complete the installation.

### 2.2 Getting Started with TermiNET

Once you have restarted, you will see the TermiNET icon  in the system tray at the bottom right corner of your screen, near the clock. By default TermiNET has been installed in Advanced Stealth mode. This Advanced Stealth mode analyzes data from each link by a number of parameters (address, protocol, port). Therefore, virtually no attack against your computer is possible, even from the computer you connect. This means your PC is effectively invisible while browsing the web, and is protected from any malicious “hacking” activity.

Work of the TermiNET program depends on Operating System installed on your computer.

#### 2.2.1 Windows 98/ME

At system start up TermiNET starts with a default set of rules, as defined by the Administrator. If multiple TermiNET user profiles have been created, there are two ways to logon as one of the defined users, either double click on the TermiNET icon  in the system tray or alternatively right click on the TermiNET icon and select **Logon**. In either case the user will be presented with a logon screen asking for a user ID and a password. Entering the User ID and Password will enable the security profile for the specified user.

#### 2.2.2 Windows NT/2000/XP

Users are automatically logged onto TermiNET based on the NT Logon profile:

- Administrator for TermiNET must be member of Administrator group on system;
- User must logon to system at least one time so TermiNET will begin to function;
- It is impossible or extremely hard to look up for user changes when TermiNET is running, so TermiNET must be restarted to rescan such changes.
- User does not belong to group Guest in system.

#### 2.2.3 Administrator Mode

If you wish to take advantage of the advanced features of TermiNET, such as a blocking access to specific web sites or changing the default mode of operation, you should assign an Administrator password, which can then be used to enter Administrator mode and configure the advanced security features.

To assign the Administrator password double click on the TermiNET icon in the system tray. This will bring up a screen allowing you to enter a password of your choice; you must enter the password twice for confirmation purposes.

Once you have entered an Administrator password the TermiNET Administration interface will open and you will be able to configure the advanced security features. You can enter Administrator mode at any time while **TermiNET** is running by right clicking on the TermiNET system tray icon, selecting Administrator Mode, and entering your Administrator password.

To exit Administrator mode, simply close the configuration screen using the **File → Close Administrator** menu option.

If a user doesn't know Administrator password he can't close the program. If a user wants to exit the TermiNET program, it will ask to type administrator password.

### 2.3 The TermiNET Interface

The TermiNET Interface (Figure 1) is only accessible using the Administrator password. It is easy to use graphical tool for defining the security profiles for a computer.

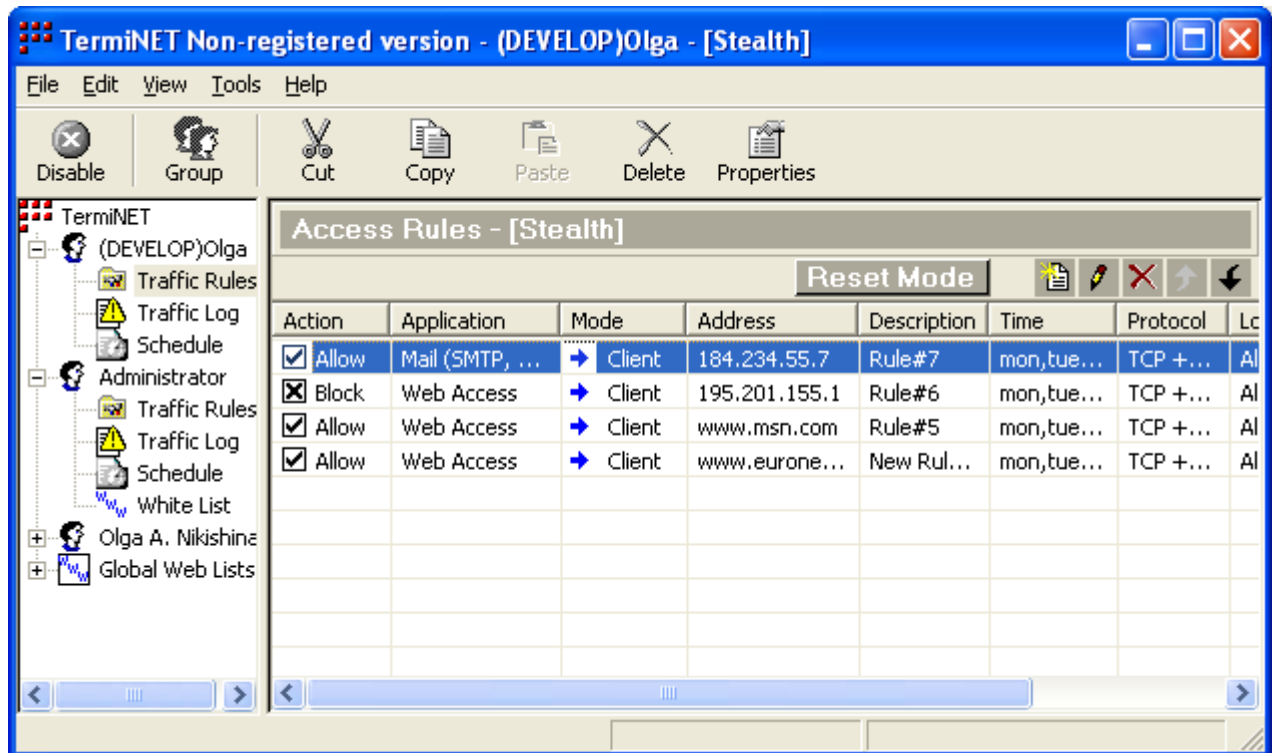


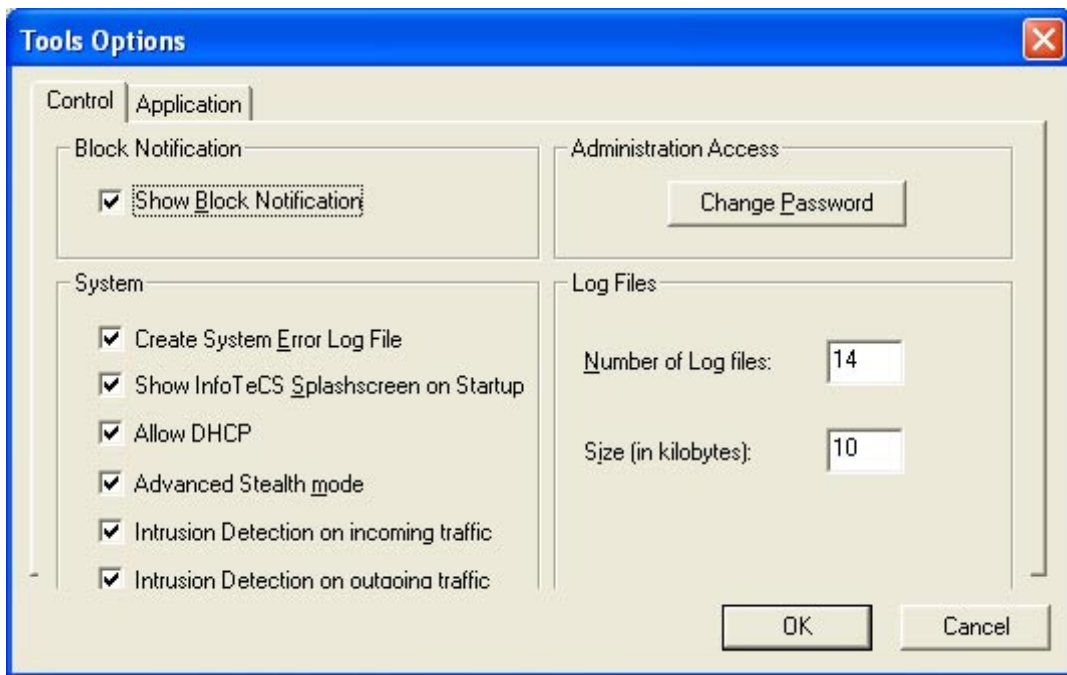
Figure 1

The interface is divided into two sections; the left hand section displays a tree view of the defined security system. The right hand section shows rules that have been created. Selecting a user in the left hand window causes the right hand windows to display the status of created rules.

There are **Reset Mode** button in the window. The button is designed to select security mode from three ones (see 4).

**Disable** button  allows disabling the TermiNET program (without unloading). Once you have disabled the program the button will turn to **Enable** button .

The **File**, **Edit** and **View** menus allow the interface to be customized according to the Administrators preferences. The **Tools → Options** menu allows system wide properties to be set.



**Figure 2**

The **Control** tab (Figure 2) gives access to the following options.

- **Show Block Notification:**When checked notification dialog will appear informing user that access attempt has been blocked.
- **Create System Error Log File** - When checked system errors will be written to the \Program Files\InfoTeCS\ TermiNET\Data\errorlog.txt file.
- **Show InfoTeCS Splashscreen on Startup** - Uncheck to prevent the Splashscreen appearing when TermiNET starts.
- **Allow DHCP** - If this option is on the program will support the Dynamic Host Configuration Protocol (DHCP).
- **Advanced Stealth Mode-** The option is selected by default. When the program is set in the Stealth mode and the option is selected the mode becomes more reliable. This Advanced Stealth mode analyzes data from each connection by a number of parameters (address, protocol, and port). Therefore, virtually no attack against your computer is possible, even from the computer you connect. If the option is unselected the program will be set in Soft Stealth mode. This Soft Stealth mode analyzes data from each connection by a number of parameters (address and protocol).
- **Intrusion Detection on Incoming Traffic** – The option is unselected by default. If the option is selected the program will check all incoming traffic of your computer on network attacks and at detecting such an attack the program will block it.
- **Intrusion Detection on Outgoing Traffic** – The option is unselected by default. If the option is selected the program will check all outgoing traffic from your computer on network attacks.
- **Change Password** - Allows the Administrator password to be changed.
- **Number of log files** - Sets the number of traffic log files which are recorded. Once the specified number of log files has been reached and the last file has reached its maximum size the first file is overwritten.
- **Size (in kilobytes)** - Sets the size in kilobytes to which a traffic log file will grow. Once this size is reached the file is saved and another file is recorded.

The **Application** tab (Figure 3) allows new standard applications to be created.

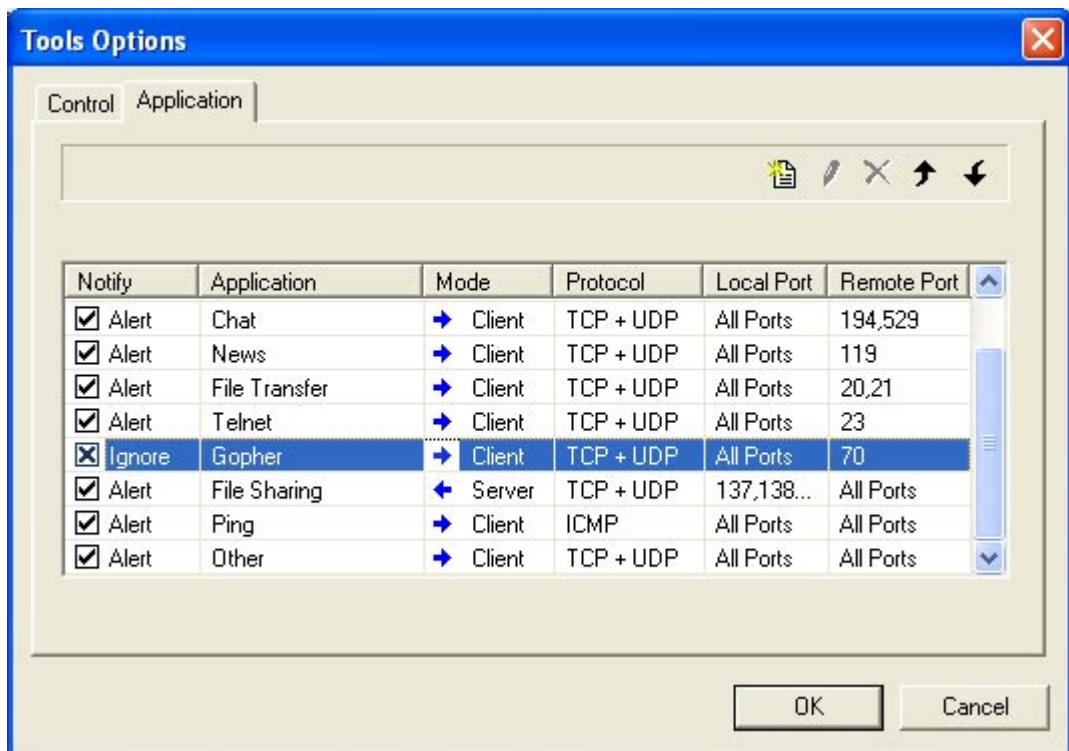


Figure 3

You can add application (📄), edit applications (✎) and delete them (✖) (Figure 3).

Click the **Add Application** button (📄) to bring up the **Custom Application** dialog box.

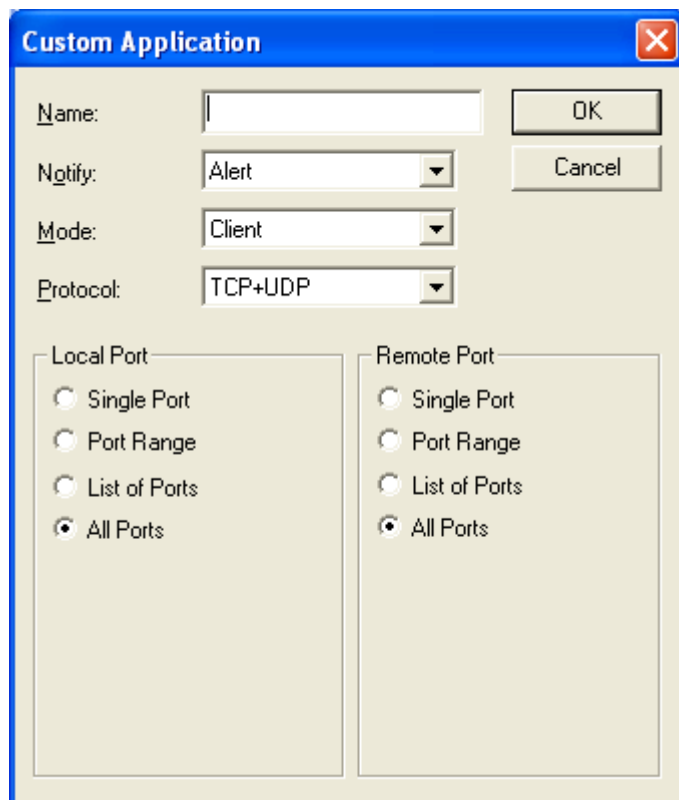


Figure 4

This window allows the following options to be set.

- **Name:** Specify the Name for the custom application.
- **Notify:** Select **Alert** or **Ignore** from the drop down list. If **Alert** is selected a notification will appear when traffic of this type is blocked.
- **Mode:** *Client* or *Server* mode of your computer.
- **Protocol:** Select the desired protocol for the application from the drop down list.
- **Local Port:** Specify the port settings applicable to the local machine for this application.
- **Remote Port:** Specify the port setting applicable to the remote machine for this application.

Press **OK** button to save changes you have made. Just created application will appear in the **Application** tab of the **Tools Options** window (Figure 3). Also you can select in **Notify** column the option (Alert, Ignore) by left clicking for any application.

### 3 Users and Groups; Managing Users and Groups

Adding users function will be available if Windows 98/Me is installed on your computer. If Windows NT/2000/XP is installed you can add users groups intended for organizational purposes (see below 3.2). Also you can change user properties. To change user properties right click on a user you want to change properties and select **User Properties** menu item. TermiNET User Properties window will open (Figure 5).

#### 3.1 Adding Users (Windows 98/Me)

To add a user profile, right click the highest level of the TermiNET tree view and select **Add User** from the shortcut menu, or click the User button on the toolbar. This displays the User Properties box (Figure 5)

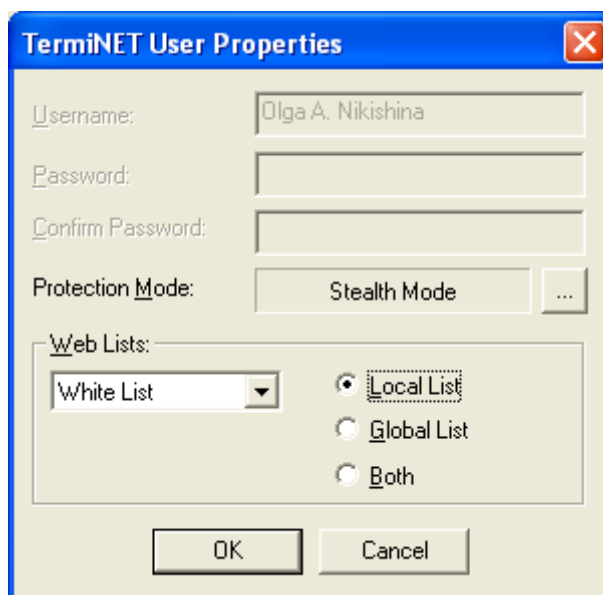


Figure 5

The following fields are available to add:

- **Username:** Used to enter the desired Username for the user.
- **Password:** Enter the required password for the user.
- **Confirm Password:** Enter the password a second time for confirmation purposes.
- **Protection Mode:** Select the default security Mode for this user.
- **Web Lists:** Determines if this user will use the Web Black or White Lists and whether the global list, local list or both will be used.

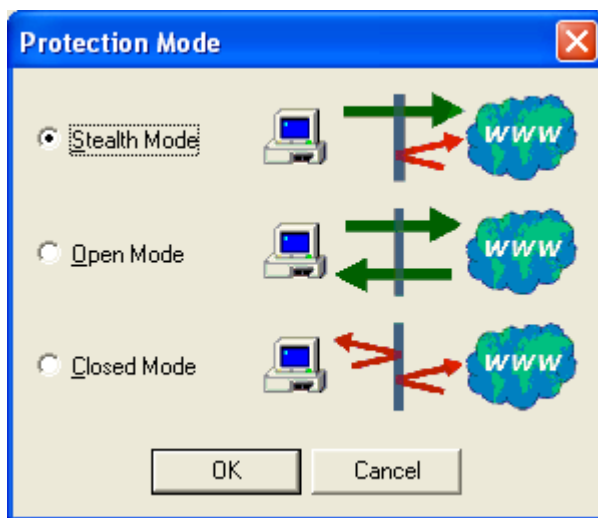
#### 3.2 Creating Groups

Groups can be used to organize lists of users within the TermiNET tree view. Create a new group by right clicking on the highest level of the tree and selecting “Add Group” from the shortcut menu and typing the desired name for the Group. Users can then be placed into groups by clicking the user name and dragging it into the desired group. A user can be created in an existing group by right clicking on the group in the tree view and selecting “Add User” from the shortcut menu.

**Note:** Groups are used for organizational purposes only. It is not possible to apply a specific set of rules to a group of user.

## 4 Protection Mode Change

To change protection mode select a user you want to change a mode and click **Reset mode** button in the **Access Rules** window. This clicking will bring **Protection Mode** window (Figure 6).



**Figure 6**

Set a mode (select a corresponding radio button) you want and press **OK** button.

You can set one of the three security modes of the TermiNET program. The most secure mode is Stealth Mode. This mode can be Advanced and Soft Stealth Mode. To set one of them use **Tools** → **Options** menu item and **Control** tab (Figure 2); then use **Advanced Stealth** option.


For more details about security modes see 1.1, About TermiNET.

## 5 Traffic Rules

Traffic rules (access rules) apply to a specific IP address or URL and are used to selectively allow or disallow access to sites and services.

Such rules are defined in all security modes.

### 5.1 Creating Rules

To add a new rule select a user to which the rule will apply, open his (her) **Access Rules** window (select **Traffic rules** item) and right click on table header. Then select **Add rule** from the shortcut menu (also you can click  icon in the **Access Rule** window) to bring up the **Enter New Rule** dialog box (Figure 7).

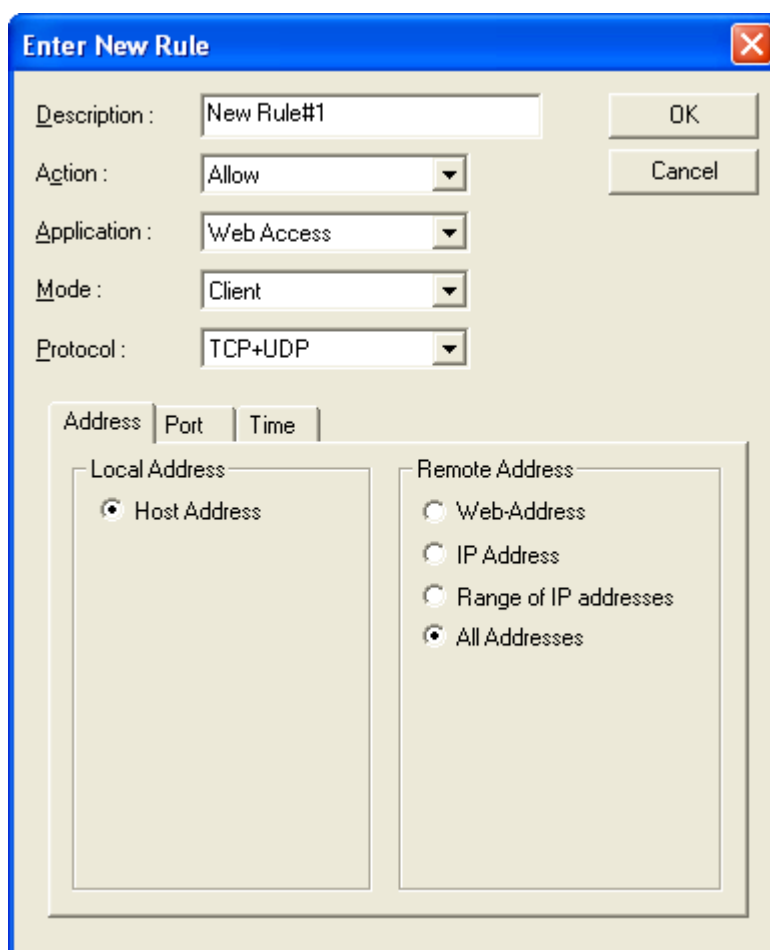


Figure 7

The following fields are available.

- **Description:** Type a description for the rule being created.
- **Action:** Select **Allow**, **Block**, or **Inactive** from the listbox.
- **Application:** Select from the offered listbox of applications.
- **Mode:** Specify whether the local machine will be a **client** or **server** for this rule. Specifying **client** means that the rule will be applied to outgoing traffic. Specifying server means that the rule will be applied to incoming traffic.
- **Protocol:** Select protocol from listbox.

The **Address** (Figure 8), **Port** (Figure 9) and **Time** (Figure 10) tabs are used to specify the advanced functions of the rule.

**Address:**

The screenshot shows a dialog box titled "Enter New Rule" with a close button in the top right corner. The dialog contains several configuration fields:

- Description:** New Rule#1
- Action:** Allow
- Application:** Web Access
- Mode:** Client
- Protocol:** TCP+UDP

Below these fields are three tabs: "Address", "Port", and "Time". The "Address" tab is selected and contains two main sections:

- Local Address:** A radio button is selected for "Host Address".
- Remote Address:** Four radio buttons are present: "Web-Address" (selected), "IP Address", "Range of IP addresses", and "All Addresses". Below these is a text field labeled "Web-Address:" containing the value "www.ghost.com".

"OK" and "Cancel" buttons are located in the top right corner of the dialog.

**Figure 8**

**Local Address** option defines your host address.

**Remote Address** option allows specifying URL, IP address, IP addresses range or all IP addresses to which the rule applies:

- Selecting **Web-Address** button allows typing this Web-Address into Web-Address entry field.
- Selecting **IP Address** button allows typing this IP Address into IP Address entry field.
- Selecting **Range of IP addresses** button allows typing this range (start and end address) into two entry fields correspondingly.
- Selecting **All Addresses** means the rule applies to all IP addresses.

**Port:**

The screenshot shows the 'Enter New Rule' dialog box with the 'Port' tab selected. The fields are as follows:

- Description: New Rule#1
- Action: Allow
- Application: Web Access
- Mode: Client
- Protocol: TCP+UDP

The 'Port' tab has three sub-tabs: 'Address', 'Port', and 'Time'. The 'Port' sub-tab is active, showing two sections: 'Local Port' and 'Remote Port'. Each section has four radio button options: 'Single Port', 'Port Range', 'List of Ports', and 'All Ports'. In the 'Local Port' section, 'All Ports' is selected. In the 'Remote Port' section, 'List of Ports' is selected. Below the 'Remote Port' section, there is a 'List of Ports' text box containing the numbers '80' and '443'. There are 'Add' and 'Remove' buttons below the text box.

**Figure 9**

The **Port** tab (Figure 9) is used to specify the port or port range to which the rule applies. Port settings must be configured for both the local and remote machines. The following options are available.

- **Single Port:** Allows the specification of a single port number for the rule.
- **Port Range:** Allows specification of a range of ports for the rule.
- **List of Ports:** Allows a list of ports to be specified for the rule.
- **All Ports:** Makes the rule apply to all ports.

In dependence on selected parameter you can specify a value of this parameter in the field located below.

**Time:**

The screenshot shows a dialog box titled "Enter New Rule" with a close button (X) in the top right corner. The dialog contains several fields and a tabbed section:

- Description:** Text box containing "New Rule#1".
- Action:** Dropdown menu set to "Allow".
- Application:** Dropdown menu set to "Web Access".
- Mode:** Dropdown menu set to "Client".
- Protocol:** Dropdown menu set to "TCP+UDP".
- Buttons:** "OK" and "Cancel" buttons are located to the right of the fields.
- Time Interval Section:** A tabbed section with "Address", "Port", and "Time" tabs. The "Time" tab is selected, showing a "Time Interval" section with a table of days and their status.

Day	Status
<input checked="" type="checkbox"/> Monday	On
<input checked="" type="checkbox"/> Tuesday	On
<input checked="" type="checkbox"/> Wednesday	On
<input checked="" type="checkbox"/> Thursday	On
<input checked="" type="checkbox"/> Friday	On
<input type="checkbox"/> Saturday	Off
<input checked="" type="checkbox"/> Sunday	On

**Figure 10**

The **Time** tab (Figure 10) allows the rule to be made active only in specific days.

## 6 Traffic Registration Log

Traffic Log is provided for each user (Figure 11). Such a log contains information about blocked and passed traffic, transmitting through computer of a user.

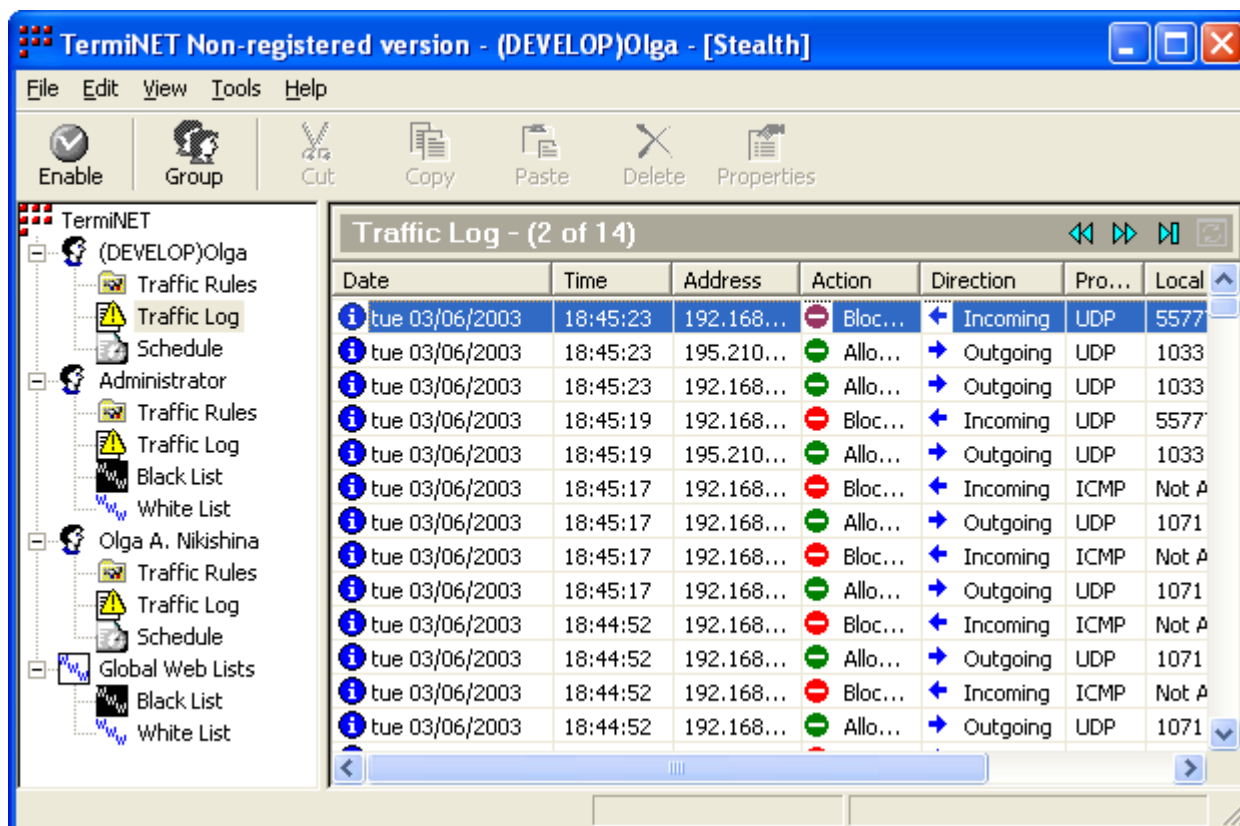


Figure 11

Number of logs is specified in **Tools** → **Options** menu item on **Control** tab (Figure 2, **Number of Logs** option). You can view logs using , and buttons (previous, next or back to current log).

Use button to refresh current log.



## 7.1 Daily Schedule Settings

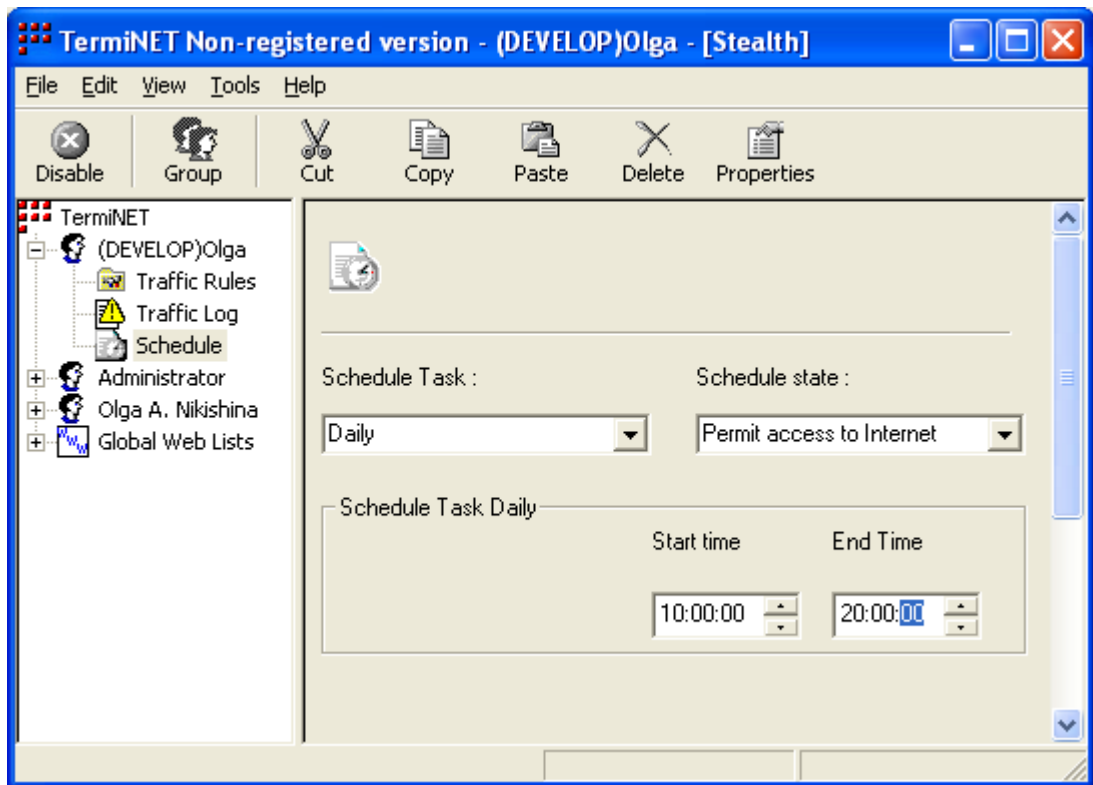


Figure 13

To set daily schedule select **Daily** under **Schedule task** option (Figure 13) and **Permit access to Internet** or **Deny access to Internet** under **Schedule State**.

Then set **Start time** and **End time** under **Schedule Task Daily**. By default **start** and **end** time is 00.00.00 that means selected **Schedule State** acts round the clock.

All settings go into effect immediately.

## 7.2 Weekly Schedule Settings

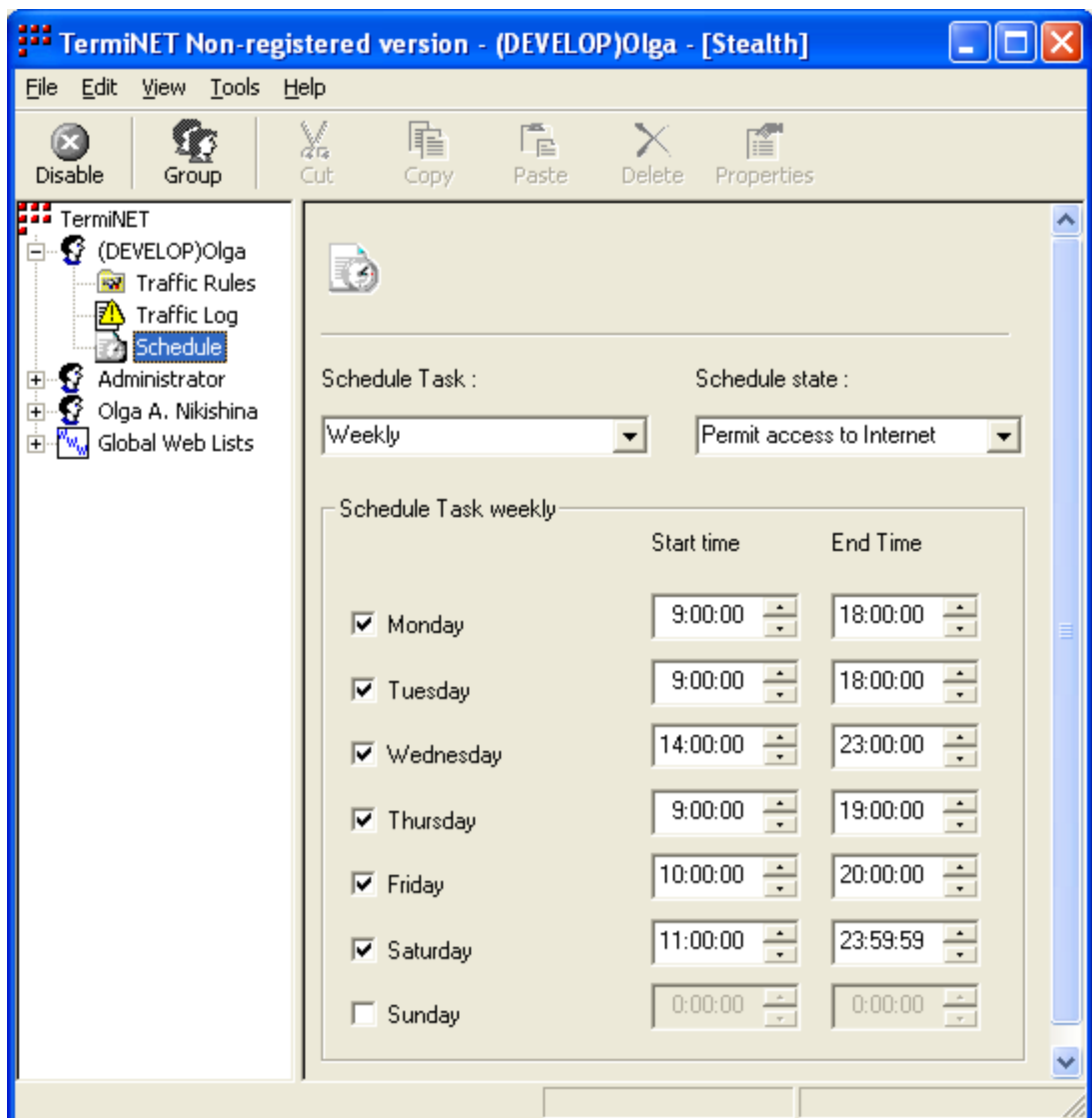


Figure 14

To set weekly schedule select **Weekly** under **Schedule task** option (Figure 14) and **Permit access to Internet** or **Deny access to Internet** under **Schedule State**.

Then set **Start time** and **End time** for every day of a week under **Schedule Task Weekly**. By default **start** and **end** time is 00.00.00 that means selected **Schedule State Weekly** acts round the clock. Also you can disable schedule for any day by unselecting the corresponding checkbox.

All settings go into effect immediately.

## 8 Web Lists

Web lists can be used to allow or block access to specific sites. URL lists can be either **Black** Lists or **White** Lists. The **Black** and **White** lists are mutually exclusive, i.e. a user who is configured to use a **Black** List can not be configured to use a white list and vice versa.


To add Web address to **Black** or **White** List select one of them from the left pane of the program window. Then press **Add new Address** button . Dialog box to add addresses will appear (Figure 15):



Figure 15

Type web address you want to add and press **Next** or **Finish**. As soon as you press one of these buttons typed web address will appear in the right pane table of the program window. Clicking **Next** allows you to add the next address. Clicking **Finish** will close the dialog box. The program will search added sites and set **Yes** or **No** in the **Exists** column of the right pane table.

Such lists can be deleted and edited.

### 8.1 Black Lists

**Black lists** are used to block access to sites that a rule may allow. For example a standard rule may be configured to allow all web access, but a specific site e.g. www.notallowed.com is listed in the Black list. Under these circumstances the user will be able to browse all web sites except www.notallowed.com.

### 8.2 White Lists

**White lists** are used to allow access to sites that a configured rule may block. For example a standard rule may block all web access but a specific site e.g. www.disney.com is listed in the white list so the user will not be able to browse any web sites except www.disney.com.

### 8.3 Global and Local Lists

There are two types of **Black** and **White** lists **Local** and **Global**. A **Global** list is created by the Administrator and can be applied to all users; entries in the global list will be applied to all users for whom the Administrator has specified use **Global** URL list. A **Local** list is created by the Administrator and can be applied to selected user. Entries in this list are applied only to the user for whom the list has been created. At first a **Local** list is created for selected user by right clicking on the user and selecting **Properties** option (properties dialog box will open and you can select list type, see Figure 5) or pressing the **Properties** button on the Toolbar. Then you can add sites to local lists as it was described above.

## 9 Intrusion Detection System (IDS) Settings

Due to working IDS system on network level the system has a number of advantages:

- Possibility to detect and block IP packets before processing them by TCP/IP stack, due to this the stack is protected against attacks (such as WinNuke attacks).
- Possibility to block attacks (at early stages), directed to overloading system, leading to denial of service (DoS) (for example, jolt2 (CAN-2000-0305)).
- Besides IDS system is capable to detect outgoing attacks (as though an intruder works at your computer). It is useful in case of your system compromising by any way (for example, by Trojan Horse programs), and after that your system is used by the intruder as attack to any third system.

To make IDS settings select **Tools** → **Options** menu item and **Control** tab. Then select **Intrusion Detection on Incoming Traffic** and **Intrusion Detection on Outgoing Traffic** options (see chapter 2.3, Figure 2).

If the program detects an IP packet, satisfying to any typical attack condition, the IP packet will be blocked. Log will show information about such a blocking.

Further you can find IDS events' description.

### 9.1 IDS events

There are attack types that can be detected by the IDS in TermiNET program:

#### **Attacks, based on IP protocol features**

<b>1001</b>	<b>Land attack</b>	An attacker is trying to slow down your computer. The attack uses TCP/IP stack vulnerability i.e. tries to transmit false TCP packet and by this way to make your computer connect with itself (by sending SYN packet with sender address, identical to attacked computer).
<b>1002</b>	<b>Zero length IP option</b>	An intruder has attempted to crash your firewall by sending a zero-length IP option.
<b>1003</b>	<b>Empty IP fragment</b>	An empty IP fragment was seen.
<b>1020</b>	<b>Jolt2</b>	Incorrect fragment offset in IP packet. A large number of such fragments sent in a short period of time can slow down your computer.

#### **Attacks, based on ICMP protocol features**

<b>1101</b>	<b>Possible Smurf attack initiated</b>	An ICMP echo frame has been sent to a subnet address (x.x.x.0 or x.x.x.255); this may cause a flurry of echo responses, which can overwhelm the network or the systems involved.
<b>1104</b>	<b>ICMP subnet mask request</b>	The value of the subnet mask has been requested - this may allow a hacker to gain knowledge about your network's configuration
<b>1106</b>	<b>ICMP header fragmentation</b>	An ICMP header has been split into multiple frames in an attempt to bypass firewalls or intrusion detection systems.

#### **Attacks, based on UDP protocol features**

<b>1203</b>	<b>UDP truncated header</b>	A frame containing a short UDP header has been seen
<b>1204</b>	<b>Possible Fraggle attack initiated</b>	A UDP packet destined for one of the "echoing" ports has been sent to a subnet address (x.x.x.0 or x.x.x.255); this may cause a flurry of responses, which can overwhelm the network or the systems involved.
<b>1205</b>	<b>UDP port loopback</b>	A UDP packet has been seen traveling between two "echoing" ports. Such packets can bounce an infinite number of times, using up network bandwidth and CPU
<b>1206</b>	<b>Snork attack</b>	Denial of Service overload attempt

***Attacks, based on TCP protocol features***

<b>1302</b>	<b>TCP header fragmentation</b>	A TCP header has been split into multiple frames in an attempt to bypass firewalls or intrusion detection systems.
<b>1303</b>	<b>TCP truncated header</b>	A frame containing a short TCP header has been seen.
<b>1304</b>	<b>TCP invalid Urgent offset</b>	Some TCP/IP implementations will hang when receiving many such frames
<b>1305</b>	<b>WinNuke attack</b>	This indicates a probable attempt to crash the system.
<b>1306</b>	<b>Zero length TCP option</b>	The intruder is trying to crash your firewall or your system by sending a zero-length TCP option
<b>1307</b>	<b>TCP XMAS scan</b>	A TCP frame has been seen with the FIN, URG, and PUSH bits all set. A hacker may be scanning your system by sending these specially formatted frames to see what services are available
<b>1308</b>	<b>TCP null scan</b>	A TCP frame has been seen with all control bits set to zero. A hacker may be scanning your system by sending these specially formatted frames to see what services are available

## 10 Problems with NetBIOS

Under certain circumstances you may experience problems accessing hosts using NetBIOS over TCP/IP when in Stealth Mode. The problem occurs when your machine uses broadcasts to determine the IP address of a host on the network. In Stealth Mode TermiNET will block the returned messages from the hosts preventing the establishment of communications. Under these circumstances it is necessary to make an entry in your "HOSTS" file relating the IP address of the required hosts to their NetBIOS names. "HOSTS" is a plain text file usually found in the C:\windows directory on Win'98 or the c:\system32\drivers\etc directory on Win NT and can be edited using any text editor. A sample file called hosts.sam in the directory gives details of the file structure. A typical host file will look something like this.

```
192.168.25.2    myserver.myorg.com
```

```
192.168.56.10  nt_server_1
```

If you wish to add a host named nt\_server\_2 with IP address 192.168.35.23 edit the file as follows.

```
192.168.25.2    myserver.myorg.com
```

```
192.168.55.10  nt_server_1
```

```
192.168.35.23  nt_server_2
```

This problem will not exist if your network has a WINS server configured.