

INFORMATION SECURITY GATEWAY(ISG) USER MANUAL DFL-M510



NETWORK SECURITY SOLUTION http://www.dlink.com



Before You Begin

Before you begin using this manual, take a look at the copyright, trademark, and safety information in this section.

Copyright

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of D-Link.

Copyright 2006

Version 1.02

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Trademark Recognition

- MSN (⁴) is a registered trademark of Microsoft Corporation
- ICQ (⁵⁵⁸) is a registered trademark of ICQ Inc.
- Yahoo (1980) is a registered trademark of Yahoo! Inc.
- QQ (⁴⁵) is a registered trademark of TENCENT Inc.
- Skype (
) is a registered trademark of Skype Technologies.
- IRC (**m**) is a registered trademark of mIRC Co. Ltd.
- Odigo (is a registered trademark of Comverse Technology, Inc.
- Rediff (⁶) is a registered trademark of rediff.com India Limited.
- ezPeer (1997) is a registered trademark of Eastern Sky Ltd.
- Kuro () is a registered trademark of music.com.tw Int.

Gnutella	(💶)	is a registered tra	ademark of	OSMB,	LLC
----------	-------	---------------------	------------	-------	-----

0.000

Kazza (is a registered trademark of Sharman Networks

BitTorrent (is a registered trademark of BitTorrent, Inc.

DirectConnect () is a registered trademark of Neo Modus Inc.

PP365 (PP365.com Inc.

WinMX () is a registered trademark of Frontcode Technologies

GetRight (
) is a registered trademark of Headlight Software. Inc.

MS Media Player () is a registered trademark of Microsoft Corporation

iTunes (⁴) is a registered trademark of Apple Computer, Inc.

Winamp () is a registered trademark of Nullsoft Inc.

Player365 (100) is a registered trademark of Live365, Inc.

D-Link is a registered trademark of D-Link Systems, Inc.

Java is a trademarks or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

All other product names used in this manual are the properties of their respective owners and are acknowledged.

Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment onto an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interconnect cables and a shielded AC power cable must be employed with this equipment to ensure compliance with the pertinent RF emission limits governing this device. Changes or modifications not expressly approved by the system's manufacturer could void the user's authority to operate the equipment.

Declaration of Conformity

This device complies with part 15 of the FCC rules. Operation is subject to the following conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Safety Certifications

CE, C-Tick, TUV, UL

About this Manual

This manual provides information for setting up and configuring the DFL-M510. This manual is intended for network administrators.

Safety Information

READ THIS IMPORTANT SAFETY INFORMATION SECTION. RETAIN THIS MANUAL FOR REFERENCE. READ THIS SECTION BEFORE SERVICING.

CAUTION:

To reduce the risk of electric shock, this device should only be serviced by qualified service personnel.

- Follow all warnings and cautions in this manual and on the unit case.
- Do not place the unit on an unstable surface, cart, or stand.
- Avoid using the system near water, in direct sunlight, or near a heating device.
- Do not place heavy objects such as books or bags on the unit.
- Only use the supplied power cord.

Table of Contents

Chapter 1:	
Getting Started with the DFL-M510	1
Identifying Components	1
Front View	
Rear View	2
Configuring the DFL-M510	
Configuration Through the Command Line Interface	
Configuration Through a Web-based Interface	7
Running the Setup Wizard	9
Toolbar	10
Wizard	10
Setup Wizard	11
Policy Wizard	15
Tools	21
Backup	21
Reset	22
Upgrade	23
Debug	24
Status	24
System Status	
Logging Status	
Report for Network status	
Policy Status	
Pallem Status	

Chapter 2:

System	37
The System Screen	. 37
The Date & Time Screen	. 38
The Remote Management Screen	. 40
The Log Setting Screen	. 42

Chapter 3:

Interfaces	
The Interface Screen	
Network Setting Tab	
Interface Tab	
Parameter Tab	
VLAN Tab	

Chapter 4:

User Authentication		63
The Use Authentication	Screen	63
Accounts		.63

Chapter 5:

Obiects	66
The Objects Screen	
The Setup Hosts Tab	
Exporting a Host Database	70
The Setup Groups Tab	72
Assign Hosts to Groups	73

Chapter 6:

Policy	75
The Policy Setting Screen	76
The Template Setting Tab	80
The Assign Policy Tab	83
The Policy Viewer Tab	87
User Defined Pattern	88
Defining a Pattern by Protocol	89
Defining a Pattern by Server	91
The Schedule Screen	93
Message Setting	
Keyword Filter	
Pattern Update	97

Chapter 7:

Real Time Monitor	98
The Real Time Monitor Screen	
Monitoring Real Time Traffic	
Monitoring Real Time Application	
Common Network Protocol	
Health Checking	
EIM	103
Two Levels Top 10 Analysis	104

Chapter 8:

Traffic Shaping	111
Traffic Shaping Policy for Applications	112
Traffic Charling Policy for Lloss Crowne	
Traffic Shaping Policy for User Groups	

Appendix A:

The Command Line Interface	115
Terminal/SSH (Secure Shell) Connection	115
Getting Started	
CLI Command List	
Help Command	
Get Command	
Set Command	
"set system" command	
"set time" command	
"set state" command	
"set remote" command	
"set interface" command	129
History Command	
Exit Command	
Reboot Command	
Reset Command	
Ping Command	131
Appendix B: Glossary	132
Annondix C:	
Features and Specifications	137
Hardware Specification	
Features Specification	
LCM Module	
Other Specifications	
Mechanic & ID Design Front LED indicators	141
Physical Environment	142
Index	143

CHAPTER 1: GETTING STARTED WITH THE DFL-M510

The DFL-M5 10 is a transparent network device. To ensure there is no disruption to your network, it can be installed in In-Line mode with a hardware bypass function enabled. The hardware bypass ensures that if the DFL-M510 crashes, or experiences a power out or some other problem; your network is still up and running. This allows your network administrator to begin monitoring selected PCs, while checking for anything that may upset your current network environment. Refer to the Quick Installation Guide for instructions on connecting the DFL-M510 to your network. This section covers the following topics:

- "Identifying Components" on page 1
- "Configuring the DFL-M510" on page 3
- "Running the Setup Wizard" on page 9



Before using this manual, take a look at the copyright, trademark, and safety information section. See "**Before you Begin**" on page i.

IDENTIFYING COMPONENTS

The following illustrations show the front and rear of the DFL-M510.

FRONT VIEW



LCM BUTTON DESCRIPTION

The LCM buttons are described below.

Button Name	Description	
Up	Scroll Up	
Down	Scroll Down	
ESC	Go back to the previous screen	
Enter	Next screen	

STATUS LEDS

The following table describes the status LEDs on the front of the DFL-M510.

Function	Naming	Color	Status	LED Description
Power	Power	Green	Off	Power off
			On	Power
System	System	Green	Off	Power off (System not ready)
			On	System ready and running ok
Bypass	Bypass	Red	Off	Hardware bypass is not enabled
			On	Hardware bypass is enabled
Inbound (Left)	Inbound (LAN)	Green	Off	Ethernet link OK and the speed is 10Mbps
			On	Ethernet link OK and the speed is 100Mbps
Inbound		Green	Off	No packets sending/receiving
(Right)			On	Link
			Blinking	Activity, port is sending/receiving data
Outbound	Outbound	Green	Off	Ethernet link ok, and the speed is 10Mbps
(Left)	(WAN)		On	Ethernet link ok, and the speed is 100Mbps
Outbound		Green	Off	No packets sending/receiving
(Right)			On	Link
			Blinking	Activity, port is sending/receiving data

REAR VIEW



1	Power socket
2	Power switch



Detailed information on the LCM can be found in the Appendix. See "**Appendix A: The Command Line Interface**" on page 115.

CONFIGURING THE DFL-M510

Before managing the DFL-M510, it must be initialized. This procedure is accomplished through the DFL-M510 Command Line Interface. Access to the Command Line Interface can be made either through SSH or from a terminal connected directly to the DFL-M510.

You can use Hyper Terminal, SSH v2 or browser to set up the IP parameters of the DFL-M510. The following are the default settings:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
User name	admin
Password	admin

CONFIGURATION THROUGH THE COMMAND LINE INTERFACE

Configure the DFL-M510 using the following parameters.



The IP address shown below is only an example. Instead use the IP address for your network.

IP Address	192.168.9.231
Subnet Mask	255.255.255.0
Default Gateway	192.168.9.254

1. Connect one end of the RS-232 cable to the console port on the DFL-M510 and the other end to the COM1 or COM2 port on the PC. (The pin-out definitions are shown below.)

Terminal Emulation	VT-100, ANSI, or auto
Bit per Second	115200

Data Bits	8
Parity	None
Stop Bits	1
Flow Control	Nine

- 2. To open a connection in Windows 95/98/NT/2000/XP go to, Program Files Accessory \rightarrow Communications \rightarrow Super Terminal.
- 3. Once you access the Command Line Interface (CLI) with a terminal connection, press any key. The following prompt appears:

Welcome to D-Link DFL-M510 Console Environment Copyright (C) 2005 D-Link Corp. <www.dlink.com> DFL-M510 login:

4. Type in the username and password.

```
Welcome to D-Link DFL-M510 Console Environment
Copyright (C) 2005 D-Link Corp. <www.dlink.com>
DFL-M510 login: admin
Password:
>>> Welcome to the DFL-M510 Administration Console <<<</p>
    You can configure and manage your DFL-M510 system 
by making selections from the displayed menu.
                  - This message.
         help
                     Get system information.
                  -
         get
         set
                  -
                     Set system parameters.
         history -
                     Show all command history.
                  -
         exit
                     Log out.
                 - Reboot system.
- Reset system c
         reboot
         reset
                     Reset system configurations to manufacturing defaults.
                  - Ping utility
         ping
>> _
```

5. Use the **get system** command to get information on the DFL-M510.

```
Device name: DFL-M510
MAC Address: 00:0a:1b:12:12:88

DFL-M510 IP Address:192.168. 1. 1, netmask:255.255.255. 0,

gateway:192.168. 1.254

TCP cold start duration time: 30 seconds

VLAN function: off. VLAN ID: 0.
Detection parameters:
 Maximum ping packet size: 1000.
TCP state check bypass: on.
WAN port: policy check < on> Stealth <off> max ping
LAN port: policy check < on> Stealth <off> max ping
                                                                                                10000.
                                                                                                10000.
Remote access:
HTTP:
Access: all
1 - Client IP: all
2 - Client IP: 0.
3 - Client IP: 0.
                                                        Netmask: 255.255.255.
Netmask: 255.255.255.
                                                                                                  Ø
                              0. 0. 0. 0
                                                                                                  Ø
                                                        Netmask: 255.255.255.
                                                                                                  ø
                              0. 0. 0. 0
SSH:
Access: all
1 - Client IP: all
2 - Client IP: 0
                                                        Netmask: 255.255.255.
Netmask: 255.255.255.
                                                                                                  Ñ
                              0. 0. 0. 0
                                                                                                  Й
3 - Client IP:
                              0. 0. 0. 0 Netmask: 255.255.255.
                                                                                                  Ø
>>
```

6. Use the set system ip command to set the IP address.

```
Password:
>>> Welcome to the DFL-M510 Administration Console <<<
    You can configure and manage your DFL-M510 system
    by making selections from the displayed menu.
                 - This message.
        help
                 - Get system information.
         get
        set

    Set system parameters.

        history - Show all command history.
                 - Log out.
        exit
        reboot
                - Reboot system.
                 - Reset system configurations to manufacturing defaults.
        reset
                 - Ping utility
        ping
>> set system ip 192.168.62.100
Do you want to apply this setting immediately?
Your current ssh/http connection will be cut off. (y/n) y
Change device ip OK.
Device ip is changed, reboot now
Are you sure to reboot system? (y/n) y
```

After the system reboots, use set system gateway to set the default gateway.

```
Password:
>>> Welcome to the DFL-M510 Administration Console <<<</p>
     You can configure and manage your DFL-M510 system
     by making selections from the displayed menu.
                    - This message.
          help
                    - Get system information.
          get
                   - Set system parameters.
          set
          history - Show all command history.
          exit
                    - Log out.
                   - Reboot system.
          reboot
                    - Reset system configurations to manufacturing defaults.
          reset
                    - Ping utility
          ping
>> set system gateway 192.168.62.1
Do you want to apply this setting immediately?
Your current ssh/http connection will be cut off. (y/n) y
route: SIOCIADD|DEL]RT: No such process
Change device gateway OK.
>> _
```

 After setting the IP address, Mask and Gateway, use the get system command to get correct information. Use the web-based interface to configure other parameters. See "Configuration Through a Web-based Interface" on page 7.

```
Device name: DFL-M510
MAC Address: 00:0a:1b:12:12:88
DFL-M510 IP Address:192.168. 62.100, netmask:255.255.255. 0,
gateway:192.168. 62. 1
TCP cold start duration time: 30 seconds
VLAN function: off. VLAN ID: 0.
Detection parameters:
 Maximum ping packet size: 1000.
 TCP state check bypass: on.
WAN port: policy check < on> Stealth <off> max ping
                                                                                                    10000.
 LAN port: policy check < on> Stealth <off> max ping
                                                                                                     10000.
Remote access:
HTTP:
Access: all
1 - Client IP: all
                                                           Netmask: 255.255.255.
Netmask: 255.255.255.
Netmask: 255.255.255.
                                                                                                       0
2 - Client IP:
3 - Client IP:
                               0. 0. 0. 0
0. 0. 0. 0
                                                                                                       0
SSH:
Access: all
1 - Client IP: all
2 - Client IP: 0.
3 - Client IP: 0.
                                                           Netmask: 255.255.255.
Netmask: 255.255.255.
Netmask: 255.255.255.
                                                                                                       Й
                               0. 0. 0. 0
0. 0. 0. 0
                                                                                                       0
                                                                                                       Ō
>>
```

CONFIGURATION THROUGH A WEB-BASED INTERFACE

The DFL-M510 GUI is a Web-based application that allows you to manage the DFL-M510. The GUI is a Java[™] applet application. Before accessing the GUI from any PC, you must install Java Run Time Environment (J2RE V1.4.2 or above). Then you can log on to the DFL-M510 from any computer on the network via a Web browser. You can download J2RE from <u>www.java.com</u> or you can download it from the link within the DFL-M510 GUI.

The PC you log in from must have the following system requirements:

- Microsoft Windows XP professional operation systems
- Device with Internet connection
- CPU: Intel Pentium4 2.0G or 100% compatible
- Memory: 512MB RAM or above
- Java Run Time Environment (J2RE V1.4.2 or above)

Refer to the following to log on to the DFL-M510.

1. Open your Web browser and type the IP address into the Address Bar: <u>http://192.168.1.1</u>. The login screen appears.



2. Click on the link to download the Java Runtime Environment.

3. Click **Run** to start the installation. Follow the onscreen prompts to complete the installation. The following Security Warning appears.

Warning	- Security 🔀
	Do you want to trust the signed application distributed by "D-Link"?
<u> </u>	Publisher authenticity can not be verified.
	The security certificate was issued by a company that is not trusted.
	It is security certificate has not expired and is still valid.
	More Details
	Yes No Always

4. Click **Always** to continue and prevent this screen appearing again. The login screen appears.



The IP address shown above is only an example. Instead use the IP address for your network.

Authentication Required	8
Please enter your user name and password	
User name:	
Password:	
Language: English	'
Login	
Optimized for Internet Explore6, Firefox and Netscape8	

5. Type in the default account name **admin** and the default password **admin**, choose your preferred language and click **Login**.



Language support on the DFL-M510 includes English, Traditional Chinese and Simplified Chinese.



For security reasons, you should change the default password to a more secure password after you have completed the setup. See Chapter 4 "**User Authentication**" on page 63.

6. After two or three minutes, the GUI opens on the DFL-M510 main screen.



7. To log out click the **Close** button 2 at the top-right of the screen.

RUNNING THE SETUP WIZARD

The **Setup Wizard** helps you to quickly apply basic settings for the DFL-M510. You will need the following information for your network to complete the **Setup Wizard**:

- IP Address
- Subnet Mask
- Default Gateway



Regarding how to configure DFL-M510 via **Setup Wizard**, see the "**Wizard**" section on page 11 for more detail.



The first time you log on to the DFL-M510, the **Setup Wizard** starts automatically.

TOOLBAR

The **Toolbar** provides many handy and frequent-use functions for you. These functions are mainly divided into three categories: **Wizard**, **Tools** and **Status**, illustrated as below.



The **Wizard**, including **Setup Wizard** and **Policy Wizard**, guides you step-by-step to complete the entire procedure, helps you easily configure the essential system information and policy configuration for DFL-M510.

For system maintenance, several handy tools such as **Backup**, **Reset**, **Upgrade**, and **Debug**, are provided in the **Tools**, enable you to quickly maintain the system configuration.

The **Status** is the most fabulous function you may frequently utilize, for instance, **System** information, **Logging** information and **Report** for network status. The current status of the supported application DFL-M510 can monitor and manage is provided in the **Policy Status**. Also, you can obtain the information of pattern version in the **Pattern Status**.

WIZARD

The **Wizard** provides a handy ways for you to quickly apply system and policy settings for the DFL-M510. On DFL-M510, two wizards shown as below are provided - Setup Wizard and Policy Wizard.



SETUP WIZARD

When initializing the DFL-M510 first time, the Setup Wizard will launch automatically after you logon the device. The Setup Wizard will guide you step-by-step through the entire procedure. After the procedure is completed, the basic system information for DFL-M510 is configured.

To run the Setup Wizard:

1. Go to **Toolbar,** click **Wizard**, **Setup Wizard**. The **Setup Wizard** window appears. Click **Next** to continue.



2. You need to provide your IP Address, Subnet Mask, Default Gateway, and DNS Server address to enable the device to connect to your network. If the network was set by CLI, check the settings here. Type in the required information and click **Next**.

DFL-M510	Informatio	n Security Gateway	
D-Link Building Networks for People			DNETDEFEND Logged in as Administrator admin. 102.089 0, 103
Home Witzard Tools > Statu DFL-M510 Image: Statu Image: Statu Image: Statution Image: Statution Image: Statution Image: Statution Image: Statution Image: Statution	DFL-M510	Setup Wizard Network Setting	Logout ? Help
• Traffic Shaping	Setup 1.Network Setting 2.Application- Policy Setting	Enter the following Network Inform	nation for DFL-M510
	3.Real Time Montor	Subnet Mask 255.255.255.0	
		Default Geteway 192 168 DNS Server 168 95	.1 .254
		< Back Next >	Cancel

3. Select the check boxes for the applications you want to block and click Next.

UDFL-M510	Information Security Gateway	
D-Link Building Networks for People	DINETDEI Dis V 🎱 Status V	trator ut 3 Help
U DFL-M510		
hterfaces	DFL-M510 Setup Wizard Application Policy Setting	
Ser Authentication		
Objects	Setup Check (by clicking the check boxes) the applications	
Eeal Time Monitor	1.Network Setting you would like to block	
Traffic Shaping	2 Application	
	Policy Setting 3.Real Time Montor Grant Control Cont	
	< Back Next > Cancel	



You can leave all the boxes unchecked to be sure the DFL-M510 is set up correctly. Later you can add applications to be blocked in the Policy menu. See Chapter 6 "**Policy**" on page 75.

4. Select the No radio button and click Finish.

DFL-M510	Information Security	Gateway	
D-Link Building Networks for People			et Defend et in as Administrator n- 192 168.9 103
DFL-M510			
system			
	DFL-M510 Setup	Wizard Real Time Monitor	0
User Authentication			
We Objects	Setup	Would you like to monitor the network now?	
Eal Time Monitor	1 Network Setting	,	
Traffic Shaping	2. Application Policy Setting 3. Real Time Monitor	 Yes No 	
		< Back Finish Can	281



If you select Yes in the screen above, you are taken to the Real Time Monitor screen when setup completes. See Chapter 7 "**Real Time Monitor**" on page 98.

It takes 30 seconds for the settings to be processed and then the following screen appears:



When the setup is successful, the following screen appears:



5. Click **OK.** The **System status** screen is shown for your information.



POLICY WIZARD

The **Policy Wizard** helps you to simplify the policy configurations and apply policy settings for the DFL-M510. Follow the steps as below to experience the easy use and convenience of **Policy Wizard**:

TO CREATE A NEW POLICY TEMPLATE VIA POLICY WIZARD

1. Go to Toolbar, click Wizard, Policy Wizard. The Policy Wizard window appears.



2. You can choose to manually setup Host/Group information here or latter in the tree view list. To setup the Host/Group information, click the "Set up Host/Group Now" button, otherwise, click Next to continue.

UDFL-M510	Policy Wizard)
	Host/Group Assignment Policy setting in DFL-M510 is operated at Group-Level, all system default or user-defined policies should be applied to the groups. Before starting the Policy Wizard, please make sure you have finished the Host/Group Setting. Or you could set up Host/Group NOW by clicking the button below.	
	< Back Next > Cancel	

3. In this step, you can choose either to create a new policy or to select an existing policy template.

UDFL-M510	Policy Wizard	0		
	Create/Choose Policy Template Create a new policy template by providing a template name, or select a policy from the existing templates			
	Create a new policy template Template Name Block Streaming Media			
	O Choose an existing policy template			
	Block P2P → Web Control → Streaming Media → Message Exchange (IM) → Message Exchange (IM) → Message File Sharing (P2P) → Mail			
	< Back Next > Cancel	:		

To create a new policy, you need to provide a policy name in the "**Template Name**" field, and click **Next** to continue. Here **Block Streaming Media** is the example.

To utilize an existing policy template, click the radio button "**Choose an existing policy template**", and select an existing policy template from the pull down list. The detail setting for the policy template you choose will appear in the three view list for your information, and click **Next** to continue.



If you select "**Choose an existing policy template**", and click **Next**, you are taken to the Step 5 for further configuration.

4. Specify the corresponding action and schedule for the "**Block Streaming Media**" template. Here the "**Block**" checkbox is checked, and the schedule is "**Always**". Click **Next** to continue.

UDFL-M510	Policy Wizard
	Set up Template Select the applications and assign their default behavior and schedule for mapping
	Template Name Block Streaming Media
	All Web Control Streaming Media Streaming 1 Streaming
	< Back Next > Cancel

5. Assign the "Block Streaming Media" template to a specific group. In this step, it is optional to assign the policy to a specific group. You can latter configure it in the "Policy Setting" Tab when you require. In this example, the policy does not apply to any specific group immediately. Click Save to save your setting for the new policy template.

DFL-M510	Policy	Afizard 🕘
	Assign to Specific Group Apply the template on the hosts or groups Block Streaming Media	s that you would like to manage
	Policy for the template	Host/Group
	Streaming MediaStreaming 1Streaming 1	All
	< Back Save	Setup another policy Finish



Do not forget to click the "**Save**" button in this step; otherwise you will lose your entire configuration for your new policy template.

6. After saving your new policy template, you can choose either to finish the Policy Wizard or to set up another policy template via the wizard.

UDFL-M510	Policy \	Mizard 📀
	Assign to Specific Group Apply the template on the hosts or groups Block Streaming Media	ः that you would like to manage
	Policy for the template	Host/Group
	Streaming MediaStreaming 1Streaming 1Streaming 1Streaming 1Streaming 1Streaming Multi-media CommunicationStreaming Multi-media CommunicationStreaming IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	All
	Save	Setup another policy



The Policy Wizard provides a simple and easy way to set up your policy setting, these configurations still can be modified latter in the configuration tabs of "Policy Setting". See Chapter 6 "**Policy**" on page 75 for more information.

TOOLS

The Tools includes the handy tools for the system maintenance, including Backup, Reset, Upgrade and Debug. Each of them will be described as below.

BACKUP

Go to the Toolbar, click Tools, Backup. The Backup window appears.

TG:	Backup unit's configuration
13	By assigning a file name and path for configuration download, and click the "Apply" button, you will receive a package
	file containing the unit's running configuration. This can later be uploaded to the unit to restore the configuration.
	Backup configuration to
	Browse Backup
000	
	Restore unit's configuration
	To restore a backup configuration, you can upload a previously downloaded backup file.
	Restore configuration from
	Browse

Backup configuration to	Press Backup configuration to store the currents settings to a file. The backup configuration dialog displays to ask the name of the stored file.
Restore configuration from	Press Restore configuration from to restore setting from a file on the management GUI. The restore configuration dialog would display to ask the name of the file.

RESTORING A CONFIGURATION BACKUP

- 1. Click Browse.
- 2. Locate the DFL-M510.cbk file and click **Open**.
- 3. Click **Restore** to send the file to the device.
- 4. When the update completes, click Reboot to reboot the device.



The configuration file includes the user-defined policy.

RESET

Go to the Toolbar, click Tools, Reset. The System Reboot window appears as below.



Reboot	After an update completes, press Reboot to boot the device from the new firmware.
Reset to Factory Default	Press Reset to Factory Default to restore the factory default settings.



Rebooting or resetting the device closes the GUI. Log back on as you normally do.

UPGRADE

Go to the **Toolbar**, click **Tools**, **Upgrade**. The **Firmware Upgrade** window appears, see below.

R	Firmware Update				
	To upgrade the unit's firmware, download the latest firmware from D-Link support web site and place it on your hard				
	drive. When the firmware is available, use this form to upload the new firmware to the unit. The unit will automatically				
	be restarted after completing the upgrade.				
	Note that this operation will take a while to complete. Do not click anywhere while the upload is in progress.				
	Firmware Update				
	File Path Browse Unhad				
150	Application Pattern Update				
	To undrade the unit's nattern database, download the latest nattern file from DJ ink sunnort web site and place it on				
	your hard drive. When the pattern file is available, use this form to upload it to the unit.				
	Note that this operation will take a while to complete. Do not click anywhere while the upload is in progress.				
	Application Pattern Lindeta				
	Application Fattern opdate				

File Path	Type the file path to the update file.
Browse	Press Browse to locate the update file. Then press Upload to send the newest file to the device.
Upload	Press Upload to begin the update.

DEBUG

Go to the Toolbar, click Tools, Debug. The Debug window appears, see below.



The Debug tool is a trouble shooting tool for your hardware provider. When you encounter hardware problems or configuration problems of DFL-M510, you can retrieve the debug information from the DFL-M510, and provide this file to your vendor for further analysis.

STATUS

The Status provides information on the current network and system settings. You can also find details of what applications can be monitored and incorporated into your policies.

After you log on, go to Toolbar, and click Status to open the following screen:



The Status screen gives you access to the following information:

- System Status
- Logging Status
- Report for Network Status
- Policy Status
- Pattern Status

System Status

The System tab information is updated every minute. You can also click the **Refresh** button to update the information. To view the **System Status**, click **Status/System**.

UDFL-M510		Information Security	Gateway		
D-Link Building Networks for People	Status 🔹			DNETI	Administrator 18.9.103 Logout 3 Help
DFL-M510 DFL-M510 System System Interfaces	Network	Status	System Status	3	
	IP Address	192.168.9.231	Model Name	DFL-M510	
E	Subnet Mask	255.255.255.0	Device Name	DFL-M510	
Real Time Monitor	Default Gateway	192.168.9.254 168.95.1.1	Kernel Version/ Last time updated	1.30.00 2006/10/03 15:17:41	
	Operation Mode	In-line	Pattern Version/ Last time updated	3.21 2006/07/11 07:08:28	
	Stealth Mode	WAN	Pattern number	423	
	LAN Link Mode	Auto Auto	Boot Time/Up Time	2006/10/03 15:18:34 / 0 Day(s) 0:31:50	
	DMZ Bypass		Device Time	2006/10/03 15:50:24	
			CPU Utilization		0%
	Host Bypass		RAM Usage		86%
			Flash Usage		10%
			Current Users	1	
			Current Sessions	2	
					Refresh

IP Address	Shows the IP Address (the default is 192.168.1.1)
Subnet Mask	Shows the subnet mask (the default is 255.255.255.0)
Default Gateway	Shows the default gateway (the default is 192.168.1.254
DNS Server	Shows the DNS server address
Operation Mode	Shows the defense status of the device
Stealth Mode	Shows if stealth mode is enabled
Lan Link Mode	Shows the LAN link mode
Wan Link Mode	Shows the WAN link mode
DMZ Bypass	Shows the DMZ bypass; packets are not monitored in DMZ
Host Bypass	Shows the host bypass
Model Name	Shows the model name
Device Name	Shows the device name
Kernel Version	Shows the kernel version
Last time updated	Shows last time the firmware was updated

Pattern Version	Shows the pattern version
Last time updated	Shows the last time the pattern was updated
Pattern number	Shows the pattern number
Boot Time/Up Time	Shows the last time the device was booted up
Device Time	Shows the system device time
CPU Utilization	Shows CPU utilization, monitor CPU usage to prevent overload
RAM Usage	Shows RAM usage, monitor memory usage to prevent overload
Flash Usage	Shows flash usage, monitor flash usage to prevent overload
Current Users	Shows the total number of hosts, monitor the host table to prevent it from running out
Current Sessions	Shows the total number of sessions, monitor the sessions table to prevent connection sessions from running out



CPU utilization, RAM and Flash Usage display the percentage being used, expressed as an integer percentage and calculated as a simple by time interval.
Logging Status

To view the Logging Status, click Status/Logging.

PE-M310					nformation	Security Gat	eway				
D-Link uilding Networks for People	Tools -	Statu	is 🗸						D NE S Logged ir admin - 1	A Administra 92.168.9.103	end itor
DFL-M510 @ System @ Interfaces		Logs—									
		Specifi	ic Time :	Since	2006/10/0	3 То	2006/10/03	Search			
Volicy Volicy Real Time Monitor		Displa	y Filter 🔺	MI	Al			Page	1	Next	>
www.anconaping		No.	Severity	r Time		Log Type	Host/Source IP	Host/Destinaiton IP	Category	Application	Action
		1	Info	2006/10/	3 15:36:20	System	06128NBVMNXP(1	N/A	System	N/A	N/A
		2	Info	2006/10/	33 15:30:35	System	U6128INBVVINXP(1	N/A	system	N/A	N/A
					13151910	System	Console	IN/A	System	N/A	M/A
		4	Info	2006/10/	03 15:19:00 03 15:18:34	System System	Console Console	N/A N/A	System System	N/A N/A	N/A N/A
		4	Info	2006/10/	13 15:19:00 13 15:18:34	System System	Console Console	N/A N/A	System System	N/A N/A	N/A N/A
		4	Info	2006/10/	13 15:19:00 13 15:18:34	System System	Console Console	N/A N/A	System System	N/A N/A	N/A N/A
		4	Info	2006/10/	13 15:19:00 13 15:18:34	System System	Console Console	N/A	System System	N/A N/A	N/A N/A
		4	Info	2006/10/	13 15:19:00 13 15:18:34	System System	Console	NA NA	System System	N/A N/A	N/A N/A
		4	nfo	2006/10/	<u>13 15:19:00</u> 1 <u>3 15:18:34</u>	System System	Console	NA MA	System System	N/A N/A	N/A N/A
		4	nfo	2006/10A 2006/10A	13 15:19:00 13 15:18:34	System System	Console	NA NA	System System	N/A N/A	N/A
		4	nto	2006/104	131519.00 131519.34	System	Console	NIA NA	System System		N/A
		4	nto	2006/10/	13151900 13151934	System	Console	N/A	System System	NA NA	N/A

The log involves three lists of records. The system log records the device status changes and firmware operational conditions. It will statically list out incidents on the log windows when there are any. It is the administrator's decision to activate the log display by clicking **Refresh**. On the log display list, the default setting of the system is to display all information regarding incidents, including the occurring, source, and message. Administrators can inspect data and filter out unnecessary events

SEARCHING FOR LOGS BY A SPECIFIC TIME

To search a log for a specific time, specify the time under **Specific Time** and click **Search**.

SETTING THE LOG DISPLAY

The **Display in one page** field lets you define how many log records display in one page. The default value is 10.

NAVIGATING LOGS

Use the navigation arrows </> to jump to the first or last page. Use **Prev/Next**, to go to the previous or next page. Go to a specific page by selecting it from the Page drop-down arrow.

THE REPORT for Network Status

To view the Report for Network Status, click Status /Report.

DFL-M510	Information Security Gateway	
CPL-MS10 CPL-MS10	Information Security Gateway	FEND trator ut @ Help
	Today Generate	B

In the **Report Title** field, type a title for the report, and click **Generate**.

INTERACTIVE REPORT





The above screen is described in the Real Time Monitor chapter. See "Monitoring Real Time Traffic". Click **Print** to print the report. Click **Save As** to save the report to the local computer. Click **Close** to close the report window.

VIEWING A SAVED REPORT

Reports are saved in HTML format and can be viewed in a Web browser.

1. Click Save As.

DFL-M510	Save As	
Look in: 🛅	Dlink	
File <u>N</u> ame:	Test	
Files of <u>T</u> ype:	Save As (.htm, html)	•
Files of <u>T</u> ype:	Save As (.htm, html)	la al la

- 2. Type a name for the report and click **Save As**.
- 3. Open the file you saved in your Web browser.

Report		
Report Title : Test		
Date : Tue Dec 20 17:34:56 CST 2005		
Device : 192.168.70.243		
Range : 2005/12/20 ~ 2005/12/20		
Traffic Chart		
Utilization - <mark>II</mark> All	Health Alert	Alla All M510
· M	tions	and Non Maria Non Non Non
OK B B	an B Time	an B B Time

4. Scroll down to view the details of the report.

POLICY STATUS

To view the Policy Status, click Status/Policy Status.

UDFL-M510	Information Security Gateway	00
D-Link Building Networks for People	D Status ↓	See In as Administrator amin-192.169.9.103
DFL-M510 def System def System def Interfaces User Authentication def Objects		
Real Time Monitor	Application Application Veb Control Veb Control Veb Mail : Yahoo/Hotmail/Gmail HTTP HTTPs NNTP	.
	User Request	
• (· · · · · · · · · · · · · · · · · · ·

APPLICATION STATUS

Click **Application** to select the application category which you want to know. It will display the current version in the right field. The following are the supported applications of Pattern version 3.21 on the DFL-M510. The latest pattern can be downloaded automatically after you register the product information and enable the auto download feature on the DFL-M510. To register product information, please visit the following hyperlink: <u>https://security.dlink.com.tw/member_registration.asp</u>.

Application	Support Version			
	Web mail: Yahoo/Hotmail/Gmail			
Wah Control	НТТР			
	HTTPS			
	NNTP			
Internet File Sharing	eDonkey2000-1.4.3			
(P2P)	eMule 0.46a			
	WinMX 3.53			
	BitTorrent 4.0.4			
	EzPeer 2.0			
	Overnet / eDonkey2000-1.1.2			
	MLdonkey 2.5			

	Shareaza v2.1.0.0
	Morpheus 4.9.2
	BearShare 5.1.0
	Kuro 6.0
	KaZaa 3.0
	Pigo 3.3
	GnuTella
	Grokster v2.6
	DirectConnect 2.2.0
	Beedo 2.0
	PP365 2004
	SoftEther 2.0
	PacketiX (Softether) 2.10 build 5080
	VNC 3.3.7
	RealPlayer 10.5
	Windows Media Player 10.0
	H.323
Streaming Media	RTSP
	iTunes 4.8
	WinAmp 5.09
	Radio365 1.1.11
	QuickTime 6.5.2
	General FTP Applications
File Transfer	GetRight 5.2d
	FlashGet 1.71
	MSN 7.5 Build 7.5.031
	Microsoft Live Messenger 8.0
	Web MSN
	AIM : 5.9.3759
	QQ V06.1.103.300
	TM 2006
Message Exchange	ICQ 5
(IM)	iChat 3.0.1
	Yahoo Messenger 7.0
	Odigo v4.0 Beta Build 689
	IRC MIRC 6.16
	Rediff BOL 7.0 Beta
	Google Talk 1.0.0.92
	Skype 1.3.0.57
Mail	SMTP

POP3
IMAP4
NNTP



The DFL-M510 manages P2P downloads by using the P2P Protocol. In this architecture, no matter what version of the client you use, the DFL-M510 can manage it.

REQUEST NEW APPLICATION SUPPORT

If there is a new application that the DFL-M510 can not support, you can use this function to request support.

1. Click User Request. The following screen appears.

UDFL-M510	Application	On Demand					
Notice: Th Su an Su ap	Notice: This Request Form is only for collecting applications in the field. Submission of a request does Not guarantee that D-Link will implement an application signature. Submission of a request will help D-Link to develop new and useful application signatures.						
	Category	Web Control	-				
	Application Name						
	Version						
	Application Link						
	Application Description						
	Reporter						
	Email Car	ncel Help					

2. Complete all information of the new application, and click **Send**. You will be contacted by the D-Link support team.

PATTERN STATUS

To view the Pattern Status, click Status/Pattern Status.



PATTERN INFORMATION

This page will display the Pattern Information

Last Update	Shows the last time the pattern was updated
Version of current pattern	Shows the pattern version
Number of pattern	Shows the pattern number

Pattern Updated Information

This page will show the log when you update pattern.

CHAPTER 2: SYSTEM

The System menu is where you carry out the basic setup of the DFL-M510 such as integration with your network. The System menu also lets you set local time settings and carry out maintenance.

THE SYSTEM SCREEN

After you log on, click **System** to open the following screen:



The System screen gives you access to the following screens:

- "Date and Time" on page 38
- "Remote Management" on page 40
- "Log Setting" on page 42

THE DATE AND TIME SCREEN

Use **Date and Time** to adjust the time for your location.

1. Click **System > Date and Time**. The **Date and Time** window appears.

Set the date, time, and	time zone information for this system.		
Current Date and Time	2006/10/03 16:06:17		
Time Zone :	(GMT) Greenwich Mean Time : Dublin,		
Enable daylight savi	ng time		
Offset :	0	Min(s)	
Start Date :	2006/04/02 06:00:00		
End Date :	2006/10/01 06:00:00		

2. Click \blacksquare to the right of **Current Date and Time**.

UDFL-M5	10					0
November						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
45		1	2	3	4	5
46 6	7	8	9	10	11	12
47 13	14	15	16	17	18	19
48 20	21	22	23	24	25	26
49 27	28	29	30			

3. Select the current date and click 🧟 to return to the **Date and Time** screen.

- 4. In the **Current Date and Time** field, type in the current time and then choose the time zone for your location from the drop-down list.
- 5. Click **Apply** to confirm your settings. The following screen appears:



6. Click OK to exit.



THE REMOTE MANAGEMENT SCREEN

Use **Remote Management** to enable system administration remotely. The following screen appears.

DFL-M510	Information Security Gateway	
D-Link Building Networks for People	► Lug Status ►	IETDEFEND ed in as Administrator in - 192. 168.9. 103
DEL-M510 System System Constant of the second se	Server Access Secure Client IP Address Al Server Port 80 0	Add : Delete :
	Server Access Secure Client IP Address AI Selected IP Address	Add Delete
	Αρριγ	Reset

The DFL-M510 can be remotely managed via HTTP or SSH. The Remote Access tab lets you control access rights.

HTTP/SSH

The descriptions for the HTTP and SSH fields are the same.

Server Access	Options are All, Disabled , Allowed from LAN, or Allowed from WAN. The default is All.
Secure Client IP Address	Options are All or Selected IP Address.
Add/Delete	Use Add/Delete to add IP Addresses or a Subnet address to the Selected IP Address window.

Configuring Server Access for SSH for Specific IP Addresses

- 1. Select WAN in the Server Access field.
- 2. Click the Selected IP Address radio button and click Add.

UDFL-M510	Add Client IP	
IP Address : Subnet Mask :	192 . 168 . 9 255.255.255.0	.0
:	OK Cance	el

3. Type in the IP Address and Subnet Mask for the PC that will access the DFL-M510 and click **OK**. The IP Address is added to the Selected IP Address window. Repeat steps 2 and 3 to add other IP Addresses.

Secure Client IP Address		
Selected IP Address	192.168.9.250/32	Add
	Apply	Reset

4. Click **Apply**. The new settings are processed.



When the settings are processed, the following screen appears:



5. Click **OK** to finish.

THE LOG SETTING SCREEN

Configure Log Type and Severity Notification to view log information on the device. Click **System/Log Setting**, the following screen appears.

DFL-M510		Information Secu	rity Gateway	
D-Link Building Networks for People	Status -			D NETDEFEND Logsee in at: Administrator aimin: 172.15.643
UFL-M510	Aemory Log Log Receiver			
Date and Time Semote Management	Configure Log Type and Sev	erity Notification to v	iew log and event information on this devic	e.
Log Setting	Log Type and Severity M	lotification ———		
		Warning	idenfo	
Real Time Monitor	Policy			
	Critical	Warning	Info	
	Malware Detection			
	Critical	Warning	Info	
				lumlu Consol
				: Apply : Cancel :

The Log Setting screen has two tabs. Click on a tab to view the settings.

MEMORY LOG TAB

Click the Memory Log tab. The following screen appears.

⊠System				
Critical	Warning	⊠Info		
Policy				
Critical	Warning	Info		
Malware Detection	1			
Critical	Warning	Info		

On DFL-M510, there are three log types, including **System**, **Policy** and **Malware Detection**. System log setting enables you to log and view system related information on the DFL-M510. Policy log setting enables you further configure the logging for individual policy template. For Malware Detection log setting, it allows DFL-M510 log the information while the device detects any network health concern activities in your internal network. Each log type has three corresponding severity notification, including Critical, Warning and Info. You can configure severity notification for each log type to enable the logging on DFL-M510 according to your audit requirement.

LOG RECEIVER TAB

Click the Log Receiver tab. The following screen appears.

Activate		System		
IP Address	0.0.0	Critical	Warning	Minfo
Facility	Local Use 3	Policy		
Port	(Default Port: 514)	Critical	Warning	Info
		Malware Det	ection	
		Critical	VVarning	Info

To export the logging information to external Syslog server, you need to activate the Server setting, meanwhile provide the IP address and port configuration of your Syslog server. Then specify the log type and severity notification you would like to export to and view on your Syslog server.

CHAPTER 3: INTERFACES

THE INTERFACE SCREEN

The Network screen lets you configure settings for your network.

1. Click Interface. The Network Setting window appears.

DFL-M510	Information Security Gateway	
D-Limk Building Networks for People	DNET Logged in a Status •	Administrator 168.9.103
DFL-M510 System System Objects Objects Real Time Monitor Traffic Shaping	Network Setting Interface Parameter VLAN General Setting Image: Setting Image: Setting Image: Setting Device Name Image: Setting Image: Setting Image: Setting Del-MS10 Image: Setting Image: Setting Image: Setting Inactivity Timeout Image: Setting Image: Setting Image: Setting Inactivity Timeout Image: Set Setting Image: Setting Image: Setting Inactivity Timeout Image: Set Setting Image: Setting Image: Setting Image: Set Setting Inactivity Timeout Set Community Set Community Set Community Image: Set Setting Image: Set Setting Set Community Set Community Set Community Set Community Image: Set Setting Image: Set Setting Trap Server Image: Ima	Server Check
6	Apply	Reset

The Network screen has four tabs. Click on a tab to view the settings.

NETWORK SETTING TAB

Click the Network Setting tab. The following screen appears.

UDFL-M510	Information Security Gateway	
Home Multication System		ed in as Administrator - 192.168.9.103 Dogout ① Help
	Device Name IP Address 192.168.9.231 Email Address DFL-M510 Subnet Mask 255.255.0. SMTP Server 0 Inactivity Timeout DNS Server 168.95.1.1 ID ID 120 Min. Default Gateway 192.168.9 254 Password	, 0 , 0 , 0
	Set Community Server Access	
	Get Community Secure Client IP Address	, dad
	Trap Server 0 .0 .0 .0	Delete
	Apr	yy Reset

General Setting			
Device Name			
DFL-M510			
Inactivity Timeout			

Device Name	Type a name for the device.
Inactivity Timeout	Set the inactivity time out.



When more than one DFL-M510 is installed in your location, assign device names to help identify different units.

DEVICE SETTING

These fields display the IP address and related network information of the device.

Device Setting —				
IP Address	192	. 168	.1	.1
Subnet Mask	255.2	255.255.0)	
DNS Server	0	.0	.0	.0
Default Gateway	192	. 168	. 1	. 254

IP Address	Device IP Address	
Subnet Mask	Device Subnet Mask	
DNS Server	Device DNS Server	
Default Gateway	Device Default Gateway	

ADMIN EMAIL

To enable the network administrator to receive emails from the DFL-M510, the following fields must be completed.

Admin Email	
Email Address	
SMTP Server	0.0.0.0
ID	
Password	
	Server Check

Email Address	Type the administrator's email address
SMTP Server	Type the IP of the SMTP server
ID	Type an ID if sender authentication is required
Password	Type a password if sender authentication is required
Server Check	When the above fields are completed, click Server Check to verify the mail account.



The ID/Password field must be filled in if your mail server requires authentication.

SNMP CONFIGURATION

To set up SNMP (Simple Network Management Protocol), the SNMP communities have to be set and access control to the SNMP server has to be enabled

Set Community		Server Access Disable	
Get Community		Secure Client IP Address	
Trap Community		All Selected IP Address	Add :
Trap Server	0.0.0.0		Delete

Set Community	Type the SNMP community that allows the SNMP set command. You can use SNMP software to configure the device such as System Contact, Name, and Location.
Get Community	Type the SNMP community that allows the SNMP get command. You can use SNMP software to retrieve configuration information from the device such as System description, Object ID, Up time, Name, Location, and Service.
Trap Community	Type the SNMP community that allows the SNMP trap command. When the device reboots, the device sends the trap to the trap server.
Trap Server	Type the IP of the SNMP management center that should be reported.
Server Access	Options are: Disable -No access from LAN or WAN All - Access from LAN and WAN (Note: This setting has no remote access restrictions; any IP address will have access to the DFL-M510.) WAN -Access from WAN only LAN - Access from LAN only The default option is Disable.
Secure Client IP Address	Options are All or Selected IP Address , which the SNMP commands are restricted to come from.
Add/Delete	Use Add/Delete to select IP addresses.

Configuring Server Access for LAN and WAN for Specific IP Addresses

1. Select All in the Server Access field.

Note: This setting has no remote access restrictions; any IP address will have access to the DFL-M510.

2. Click the **Selected IP Address** radio button and click **Add**.

UDFL-M510	Add Client IP	-	0
IP Address :	192 . 168 . 9 . C)	
Subnet Mask :	255.255.255.0		
	OK Cancel	-	

3. Type in the IP Address and Subnet Mask for the PC that will access the DFL-M510 and click **OK**. The IP Address is added to the Selected IP Address window. Repeat steps 2 and 3 to add other IP Addresses.

Server Access	1 1 1	
Secure Client IP Address		
) All		
Selected IP Address	192.168.9.1/24	Add
		Delete

4. Click **Apply**. The new settings are processed.



When the settings are processed, the following screen appears:



5. Click OK to finish.

INTERFACE TAB

Click the Interface tab. The following screen appears.

UDFL-M510	Information Security Gateway	00
D-Link Building Networks for People	NETD Support in as ad Support in as ad Support in as ad	efend ministrator 9.103
🔮 Home 🛛 🎑 Wizard 🔻 🛛 🐒 Tools	▼ 🏐 Status ▼ 📔	Logout 🕜 Help
😳 DFL-M510	Network Setting Interface Parameter VLAN	
System	-Link Setting	
Interfaces	Link voting	
	Interface Link Setup	
E Ko Policy	WAN Port 10 100 Half Full O Auto	
🦕 Real Time Monitor	Inned	
	LAN Port 10 100 Half Full O Auto	
	Apply	Reset
	rinterlace stealth Setting	
	Stealth Mode	
	WAN Port 🥑 On 🔷 Off	
	LAN Port 🔘 On 🥝 Off	
	Apply	Reset
• (]		

LINK SETTING

Set the Ethernet ports for the speed you want and click Apply.

Interface Link Setun	WAN - 10/100/Half/Full/Auto
	LAN -10/100/Half/Full/Auto

INTERFACE STEALTH SETTING

The LAN/WAN Ports can be configured in Stealth Mode by selecting **On**.

Staalth Mada	WAN - On/Off
	LAN - On/Off
Subnet Mask	LAN Port

After you make changes, click **Apply**. The new settings are processed and the following screen appears:





Click OK to finish.

PARAMETER TAB

Click the Parameter tab. The following screen appears.

DFL-M510		Information Sec	urity Gateway				
D-Link Building Networks for People						Logged in as Ac admin · 192.168	efend Iministrator .9.103
🏠 Home 🛛 🏟 Wizard 👻 🛛 🐒 To	ols 🔻 🛛 🅙 Status 👻 📔						Logout 🛛 🕜 Help
DFL-M510	Network Setting Interface	Parameter VI AN					
🗄 🍈 🍈 System	notific the second second	1	1				
	Operation Mode	DMZ Bypass					
- 독 User Authentication	OIn-Line	IP Address	0.0.0	.0	Subnet Mask	0.0.0.0	
- 😻 Objects							
E-W Policy	O Bypass	D Address			C. Land March	0.000	
Traffic Shaning	Monitor	IP Address	0.0.0		Subhet Mask	0.0.0.0	1
Tranc Shaping	Owneritor						
		IP Address	0.0.0	.0	Subnet Mask	0.0.0.0	-
	-Group/Host Bypass			> . >> . < <	Bypassed User/	Sroup	
						Apply	Cancel
				_			D

This tab defines management parameters.

OPERATION MODE

Operation Mode
In-Line
Bypass
O Monitor

In-Line	In In-Line mode, the DFL-M510 works as a transparent gateway in your network. All traffic is inspected as it passes through the DFL-M510. The DFL-M510 responds to illegal activities based on policy rules. When attacks are detected, the DFL-M510 can take the following action: • Drop the Packet • Reset the Connection • Log the Event • Save the Packet Message Content
Bypass	In Bypass mode, the DFL-M510 works like a bridge with all rules and actions disabled. This mode is designed to help network administrators to debug and trace network abnormalities. When Bypass mode is selected, the DFL-M510 will not detect or take action to security events in the network.
Monitor	Monitor mode allows you to analyze network activities and make early-stage diagnosis before deployment. The DFL-M510 will detect all events by inspecting all packets. In this mode, the DFL-M510 will log all events, but will not take any countermeasure (reset, drop actions). It is suggested to monitor net-work traffic in this mode before setting In-Line mode, in order to fine tune your security policy and network performance.



The DFL-M510 only protects and monitors your net-work when set to In-Line mode. The other modes offer limited monitoring and are used for integrating the DFL-M510 smoothly with your network.

DMZ BYPASS

In order to speed up traffic from the intranet to DMZ, hosts within the given DMZ subnet addresses are not checked and all packets from or to those hosts pass unhindered.

CDMZ Bypass				
IP Address	0.0	.0.0	Subnet Mask	0.0.0
IP Address	0.0	.0.0	Subnet Mask	0.0.0.0
IP Address	0.0	.0.0	Subnet Mask	0.0.0.0

IP Address	Type in the IP Address
Subnet Mask	Type in the Subnet Mask



The IP addresses of the hosts in a subnet must be continuous. That is, the network mask contains only two pairs: the leading 1s, and the following 0s.



SETTING UP THE DMZ BYPASS FUNCTION

In the following example, a mail server with the IP address 10.10.10.250 is added to DMZ Bypass.

1. Type in the IP address and the Subnet mask of the mail server.

CDMZ Bypass			
IP Address	10 .10 .10 .250	Subnet Mask	255.255.255.255
IP Address	0.0.0.0	Subnet Mask	0.0.0.0
IP Address	0.0.0.0	Subnet Mask	0.0.0.0

2. Click Save.

HOST/GROUPS BYPASS

Hosts within the intranet which do not need to be monitored are added to the Bypassed User/Group. These hosts have unhindered access to the WAN, but may be less secure than In-Line hosts.



The IP addresses of the hosts in the bypass list must be in the host table first. That is, the host must be learned or entered before you can select it. Otherwise, the host must be within a group and specified by a subnet. Such a host is automatically added to the bypass list when it is learned.

Host/Group Bypass		
Available User/Group	_	Bypassed User/Group
	, ≻ ,	
	>>	
	<	
	<<	
	1 - 	Save Cancel Help

Available User/Group	Select the User or Group and click >> to add the User/Group to the Bypassed User/Group list.
Bypassed User/Group	Lists Users and Groups that have been added.

After you make changes, click **Save**. The new settings are processed and the following screen appears:



Click **OK** to continue.



An IP address in the Host Bypass implies bypass source IP. To provide more throughputs, you could set up the servers IP (ERP/mail/ftp) in the Host Bypass if the servers are located in the internal network.

VLAN TAB

Click the VLAN tab. The following screen appears.

DFL-M510	Information Security Gateway	
D-Link Building Networks for People	D NETD D NetD Status V	EFEND Inistrator 103 ogout ? Help
DFL-M510	Network Setting Interface Darameter VLAN	
system		
	CVLAN Setting	
👆 😽 User Authentication	VLAN Enabled	
	VLAN ID (Enter the VLAN Number in your Network)	
+ lolicy		
- 🦕 Real Time Monitor	VID1 0 VID6 0	
	VID2 0 - VID7 0 -	
	VID3 0	
	VID4 0 Management Group PVD Adva	nced
	(Atist be one of the above VI ANIDe VID1_VID7)	
	Apply	Reset
	-1/1 BB Statue	
	401420 0.124	
	Management P. 132,100.3.231	
	Management VLAN : PVID	
	VLAN Enabled	
	VID1 VID2 VID3 VID4	

A VLAN (Virtual LAN) is a group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

The IEEE 802.1Q standard defines VLAN ID #1 as the default VLAN. The default VLAN includes all the ports as the factory default. The default VLAN's egress rule restricts the ports to be all untagged, so it can, by default, be easily used as a simple 802.1D bridging domain. The default VLAN's domain shrinks as untagged ports are defined in other VLANs.



If your have VLAN environment, and require the DFL-M510 recognize the VLAN tags, please configure VLAN settings before connecting the DFL-M510 to the intranet.

CONFIGURING VLAN SETTINGS

The following is an example of a network environment with four VLAN sets.

ltem	Description
VID1	1
VID2	3
VID3	5
VID4	7
Management	VID2

Refer to the following to configure the VLAN setting.

1. Click **Interface** and then select the **VLAN** tab.

DFL-M510	Information Security Gateway
D-Link Building Networks for People	NetDefend Sugad in as Administrator samin-ligo 168 2 103
🏠 Home 🛛 🏩 Wizard 👻 🖌 🐒 To	ols 🕶 🛛 🗢 Status 👻 📔 🖉 Logout 🛛 🥥 Help
DFL-M510	Network Setting Interface Decemeter VIAN
🗄 🍈 System	
	LAN Setting
🛶 😽 User Authentication	VLAN Enabled
	VLAN ID (Enter the VLAN Number in your Network)
B 🌆 Policy	
Real Time Monitor	VID1 0 VID6 0
	VID2 0 VID7 0
	VID3 0 *
	VID5 0 - (Must be one of the above VLAN IDS, VID1 - VID7)
	Anniv
	- Hour - Hour -
	rVLAN Status
	Management IP 192 168 9 231
	Management VLAN: PVID
	VLAN Enabled

VLAN Enabled	Enables or disables the VLAN function
VID1 - VID7	Type in the VLAN ID.
Management Group	Select the Management VLAN Group

- 2. Click the VLAN Enabled checkbox to enable VLAN.
- 3. Type in each VID in the VID1 to VID7 boxes.



The DFL-M510 supports up to seven VLANs. The Management VID must be either PVID, or VID1 to VID7. Configurations depend on your environment.

4. Click **Apply**. The screen updates as follows.

DFL-M510	Information Security Gateway	
D-Link Building Networks for People	D NETDEFE Suppedin az Administrat samin 192 198 0.103	IND or
👔 Home 🛛 🎒 Wizard 👻 🛛 🔭 Took	l ♥ ♥ Status ♥ 22 Logout	Help
DFL-M510	Network Setting Interface Parameter VLAN	
B 🏟 System	-VII BU Setting	
Interfaces	-VLAN Secting	
	WVLAN Enabled	
	VLAN ID (Enter the VLAN Number in your Network)	
🛶 Real Time Monitor	VID1 1 VID6 0	
	VID2 3 VID7 0	
	VID4 7 Management Group VID2 Advanced	
	VID5 (Must be one of the above VLAN IDs, VID1 - VID7)	
	1-1	
	Apply Rese	nt -
	rVLAN Status	
	Management IP 192 168 9 231	
	Management VLAN : VID2	
	VI AN Enabled	
	VID1 1 VID2 3 VID3 5 VID4 7	
	VID5 VID6 VID7	

VLAN STATUS

LAN Status Management IP :	192.168.9.231			
Management VLAN :	VID2			
VLAN Enabled				
VID1 1	VID2 3	VID3 5	VID4 7	
VID5	VID6	VID7		

Management IP Shows the device IP address	
Management VLAN Shows the Management VLAN Group ID	
VID1 - VID7	Shows the ID of each VLAN

CHAPTER 4: USER AUTHENTICATION

THE USER AUTHENTICATION SCREEN

UDFL-M510			Information Security Gateway		
D-Link Building Networks for People	nis 🗶 🔍 Status	* 1		D NETDI Cosee in ar Admi Cosee in ar Adminication	FEND
DFL-M510	-Accounts-	1.0	la.	Lend Time Lends	
User Authentication	1 1	admin	Administrator	23:20:45 10/03/2006	
	2	amber	Read Only	22:09:43 07/12/2006	
🗄 🧔 Policy					
				Delete	
			Add : Edit	Delete Login	Status
< C					

After you log on, click User Authentication to open the following screen.

ACCOUNTS

No.	Shows the current number of accounts
Name	Shows the name for each account
Role	Shows the shows the level of the user's policy: Administrator; Read Only; or Write.
Last Time Login	Shows the last time the account was accessed



Only users that are assigned the Administrator role can edit the Account and Hosts/Groups menus.
CREATING A NEW ACCOUNT

To create a new account click Add. The Account Edit dialog box appears.

DFL-M510 Account Edit
Name
Amber
Password

Confirm Password

Drivilare
OK

Name	Type a name for the account.
Password	Type a password.
Confirm Password	Retype the password.
Privilege	Assign privilege status: Administrator; Read Only; or Write.

Click OK to confirm. The account is added to the Accounts list.

Control Contro Control Control Contecontrol Control Control Control Control Con	DFL-M510		Int	ormation Security Gateway		
Water Tools Status Logod Help DFL-M510 System Image: Control of the system <	D-Link Building Networks for People				DNE Logged in Statistics	as Administrator 2.168.1.101
Water Authentication Objects Policy Real Time Monitor Traffic Shaping	Home Wizard V X Tools V	-Accounts-		- Park	I tot Text tot	2 Logout 3 Help
	User Authentication	NO.	admin	Administrator	12:06:12 10/04/2006	
Policy Real Time Monitor Traffic Shaping		2	Amber	Read Only	N/A	
Real Time Monitor	Policy					
	Laffic Shaping					
Add Edt Login Status						
Add Edt Login Status						
Add Edt Delete Login Status						
Add Edt Login Status						
Add Edt Login Status						
Adid Edit Delete Login Status						
Add Edt Login Status						
Avid Edit Delete Login Status						
Adid Edit Delete Login Status						
				Add	Edit Delete	Login Status

To review or audit an account, click Login Status. The following screen appears:

Account	Role	IP	Time	Detail
admin	Administrator	172.17.5.243	11:14:47 10/03/2006	Login Success
admin	Administrator	172.17.5.243	11:18:36 10/03/2006	User Logout
admin	Administrator	172.17.5.243	11:22:33 10/03/2006	Login Success
admin	Administrator	172.17.5.243	11:23:00 10/03/2006	User Logout
admin	Administrator	172.17.5.243	11:23:24 10/03/2006	Login Success
admin	Administrator	172.17.5.243	11:24:08 10/03/2006	User Logout
admin	Administrator	172.17.5.91	13:50:03 10/03/2006	Login Success
admin	Administrator	172.17.5.91	13:53:32 10/03/2006	User Logout
admin	Administrator	172.17.5.91	13:53:56 10/03/2006	Login Success
admin	Administrator	172.17.5.91	14:04:11 10/03/2006	User Logout
admin	Administrator	172.17.5.243	12:06:12:10/04/2006	Login Success

A log is created each time a user logs on or logs out. Monitor this list for added security. See "**Toolbar, Logging**" on page 28.

CHAPTER 5: OBJECTS

In DFL-M510, the term "**Objects**" mainly refers to **Hosts** and **Groups**. A host is a client computer with a network interface. A group is a set of hosts. The DFL-M510 learns host information from packets passing through the device. Host information includes the MAC address, IP address and VLAN address. In order to manage the host internet access, we can lock a host with a MAC address and/or an IP address.

Assign names to hosts to make them easier to manage. Otherwise, the DFL-M510 learns the device name from the network. Assigned names take priority over learned names.

THE OBJECTS SCREEN

After you log on, click **Objects** to open the following screen:

DFL-M510			Information Se	ecurity Gateway				1	00
D-Link Building Networks for People	Status	•				II. II	D NET	Administrator 68.1.101	D Help
System	octup nosta	setup	roroups						
	Current M	lode: N	IAC Based Management	Switch to IP B	ased Ma	nagement			
	-Hosto Tab								
E Olicy	-nosts rat	ле —							
	No.	State	Host/IP Address	MAC	VLAN	Name	MAC-IP Bind	MAC-Lock	
	1		172.17.5.243 06128NB / 172.17.5.91	00-90-0B-05-EB-04 00-E0-18-2E-23-E8	0				
	H	osts with	in 200						
	B	ypass Ho ther Host	ISTS		Re	fresh	Add	Delete	
		Forwa	rd						
	0	Block			<u>:</u> A	pply : I	mport	Export	
<0									•

The **Objects** screen has the following two tabs:

- "The Setup Hosts Tab"
- "The Setup Groups Tab"

THE SETUP HOSTS TAB

The **Setup Hosts** tab lets you add new hosts and manage current hosts.

1. To view the Setup Hosts tab, click Objects > Setup Hosts.

DFL-M510			Information Se	ecurity Gateway				
Home Witzard Tools Tools	Setup Hosts	• Setup	Groups				DNET Saged in as again - 192.1	Administrator 68.1.101 2 Logout 2 Help
E				-				
	Current Mo	ode: M	IAC Based Management	Switch to IP Ba	ised Ma	nagement		
Objects	-Hosts Tabl	le ——						
Policy								
	No.	State	Host/IP Address	MAC	VLAN	Name	MAC-IP Bind	MAC-Lock
	1	-	172.17.5.243 06128NB (172.17.5.91	00-90-0B-05-EB-04 00-E0-18-2E-23-E8	0			
	Ho By Oth	sts with pass Ho her Host	in 200 sts s		Re	tresh	Add ·	Delete
		DIUCK)

MAC Based Management / IP Based Management

After DFL-M510 connects into your network, the DFL-M510 can automatically learn host information according to MAC or IP address information. In general circumstance, MAC Based Management is enough to fulfill the deployment environment where a switch is attached to the LAN port of your DFL-M510. However, if there is a router attached to your LAN port, the DFL-M510 will recognize the router mac address only, it cannot recognize the hosts automatically behind the routers, thus the IP Based Management mode is required in order to have your DFL-M510 correctly recognize the hosts behind your router.

No.	Shows the current number of hosts
State	Shows the status for each host (refer to color legend at the bottom of the screen)
Host/IP Address	Shows the host IP address
MAC	Shows the host MAC address

Host Table

Name	Shows the host name
MAC-IP Bind	Check this box to lock an IP address to the host's MAC address
MAC-Lock	Check this box to lock the MAC address
Hosts within 150	Hosts all within 200 hosts
Bypass Hosts	Hosts that are not monitored
Other Hosts	The DFL-M510 can manage 200 hosts. If you select Block , hosts that exceed 200 have no Internet access. If you select Forward , those hosts will be allowed to access the Internet, but will not be monitored by the DFL-M510.

CHANGING THE STATUS OF A HOST

In the following example, the status of No. 1 is changed from **Hosts within 200** to **Other Hosts**.

1. Right-click on the host you want to change the status of.

Without Stor Poole Image: Store of the store store of the store store of the store of the store of the store	DFL-M510			Information Se	curity Gateway					0
DFL-M510 Setup Hosts Setup Groups User Authentication Objects Policy Real Time Monitor Traffic Shaping No. State Host/P Address MAC-JOENE // Move to Standby 8-25-23-F8 Swap Swap	D-Link Building Networks for People	ools 🔻	•				П П	D NET S Logged in as admin - 192.	Administrator 168.1.101	D
System Interfaces User Authentication Objects Policy Real Time Monitor Traffic Shaping No. State Host/IP Address MAC VLAN Name MAC-IP Bind MAC-Lock VLAN Name MAC-IP Bind MAC-Lock Image: Control of the state of the	DFL-M510	Setup Host	Satur	Groupe						
Interfaces Current Mode: MAC Based Management Switch to IP Based Management Objects Image: Contract Mode: MAC Based Management Image: Contract Mode: MAC Based Management Iter and the state Monitor Real Time Monitor Image: Contract Mode: MAC Based Management Iter and the state Mode: MAC Based Management Image: Contract Mode: MAC Based Management Image: Contract Mode: MAC Based Management Iter and the state Monitor Image: Contract Mode: MAC Based Management Image: Contract Mode: MAC Based Management Iter and the state Monitor Image: Contract Mode: MAC Based Management Image: Contract Mode: MAC Based Management Iter and the state Monitor Image: Contract Mode: MAC Based Management Image: Contract Mode: MAC Based Management Iter and the state Monitor Image: Contract Mode: MAC Based Management Image: Contract Mac Based Management Iter and the state Monitor Image: Contract Mac Based Management Image: Contract Mac Based Management Iter and the state Monitor Image: Contract Mac Based Management Image: Contract Mac Based Management Iter and the state Monitor Image: Contract Mac Based Management Image: Contract Mac Based Management Iter and the state Monitor Image: Contract Mac Based Management Image: Contract Mac Based Management Iter an	system	, ootup noot	Jetup	oroups						
Wiser Authentication Objects Policy Real Time Monitor Traffic Shaping No. State Not New York Standby 012040511 Move to Standby 022 0612040511 Move to Standby 0225-23-76 Swap Swap		Current I	Mode: M	IAC Based Management	Switch to IP B	ased Ma	pagement			
Image: State Hosts Table Image: Shaping Hosts Table Image: Shaping Image: Shaping Image: Shaping Image: Shaping <th>🛶 🌜 User Authentication</th> <td>Guirointi</td> <td></td> <td></td> <td>, on the b</td> <td></td> <td>gonon</td> <td></td> <td></td> <td></td>	🛶 🌜 User Authentication	Guirointi			, on the b		gonon			
Policy Real Time Monitor Traffic Shaping No. State HostsP Address MAC VLAN Hame MAC-IP Bind MAC-Lock 1 172:17:5243 00:90:08:05:68:04 0 2 0:120:8711 Move to Standby Swap Swap Hosts within 200 Bypass Hosts Other Hosts Prevent Add Delete	- 🍓 Objects	Letter Le	ble ——							_
No. State MostlP Address MAC VLN Name MAC-Lock Image: Traffic Shaping Image: Traffic Shapi	E 🕠 Policy									
Intartic Shaping	- View Real Time Monitor	No.	State	Host/IP Address	MAC	VLAN	Name	MAC-IP Bind	MAC-Lock	
Swap Swap Hots within 200 Bypass Hosts Other Hosts Other Hosts Frence Frence Add Delete Delete Export Export	{(0) Fraπic Snaping	2		06128NB / 1 Move to Stan	by 8-2E-23-F8	0				
Hosts within 200 Sypass Hosts Other Hosts Conversion Refresh Add Delete				Swap						
Diuck Contraction of the second			Hosts with Bypass Ho Dther Host Prorwa O Block	in 200 sts s rd		Ret	fresh .	Add nport	Delete	

2. Select Move to Standby.

			Information S	ecurity Gateway	-			1
D-Link ilding Networks for People						IL LI	D NET S Logged in as admin - 192.1	DEFEND Administrator 168.1.101
Home 🛛 🏟 Wizard 👻 🛛 🐒 Tools	🔻 🛛 🍮 Sta	tus 🔻 📔		_		_		🖉 Logout 🛛 🕜 H
DFL-M510	Setup Ho	sts Setu	o Groups					
🔹 System								
interfaces	Currer	nt Mode: N	MAC Based Management	Switch to IP Ba	ased Ma	nagement		
User Authentication								
Policy	[Hosts	Table ——						
🖕 Real Time Monitor		lo. State	Host/IP Address	MAC	VLAN	Name	MAC-IP Bind	MAC-Lock
Traffic Shaping		1	06128NB / 172.17.5.91	00-E0-18-2E-23-F8	0			2
		2	172.17.5.243	00-90-0B-05-EB-04	0			S
		Hosts with Bypass H Other Hos	nin 200 osta ta		Re	rresh	Add :	Delete
		Hosts with Bypass H Other Hos Other Hos Block	nin 200 osts ts ard		Re	fresh	Add :	Delete Export

Notice, the **State** icon is now green, indicating the host is now in the **Other Hosts** category.

ADDING A HOST

Refer to the following to add a host.

1. Click Add.

UDFL-M510	Host Edit	
Name :	Joy	
IP Address :	192 . 168 . 9 . 120	
MAC :	00-08-A1-12-22-45	
O MAC_IP Bind	G MAC Lock	
:	OK Cancel	

2. Type in the required information and click **OK**. The new host is added to host table.

No.	State	Host/IP Address	MAC	VLAN	Name	MAC-IP Bind	MAC-Lock
1		06128NB1VMNXP / 192.168	00-11-95-5A-FF-25	0			S
2		192.168.9.120	00-08-A1-12-22-45	0	Joy		

EXPORTING A HOST DATABASE

You can export a host database to reuse or to import into another DFL-M5 10. Refer to the following to export a host database.

1. Click Export.

UDFL-M510	Export Host	. 🥥
Export to file		
	OK	

2. Click . The Save dialog box appears.

DECHIOTO		Save		1	(
Save In: 🛅	Export		1		
l File <u>N</u> ame:					
l File <u>N</u> ame: Files of <u>T</u> ype:	Export (.ho)				

3. Enter a file name and click **Save**.

UDFL-M510	Export Host	1	0
Export to file	D:\Export\Host_List_Export.ho		
	OK Cancel		

4. Click $\boldsymbol{\mathsf{OK}}$ to confirm the export.



5. Click **OK** to continue.

THE SETUP GROUPS TAB

There is one **Default** Setup Group in the DFL-M510. The **Setup Groups** tab lets you add and configure additional Setup Groups.

1. To view the Setup Groups tab, click Objects > Setup Groups.

UDFL-M510	Information Security Gateway	
D-Link Building Networks for People	D	Logged in as Administrator admin - 192.108 1.101 Cogout 3 Help
👿 DFL-M510	Setup Hosts Setup Groups	
🛓 💩 System		
	Group Setting	
	Add	
E Real Time Monitor	Delete Available Hosts	osts in Selected Group
Traffic Shaping		06128NB(172 17 5 91)
	Down	172.17.5.243
	· · · · · · · · · · · · · · · · · · ·	
	Add Subnet	
		piy cancel
< ()		

GROUP SETTING

Add	Click to add a new Setup Group
Delete	Click to delete a Setup Group
Up	Click to move a Setup Group up
Down	Click to move a Setup Group down

QUICK ASSIGN USER/GROUP

Group Name	Type in the group name
Quota	Total available space to a group
Session	Total sessions available to a group
Available Hosts	Lists the available hosts
Hosts in Selected Group	Lists the hosts in the selected group

Add Subnet	Click to add a sequential IP address range to a group.
------------	--

ASSIGNING HOSTS TO GROUPS

You can assign a host to a group by checking the button crossing the host and the group. Refer to the following to add a host to a group.

1. Click Add.

UDFL-M510 Add	d Group Name	00
Group Name	PM	
ок	Cancel]

2. Type a group name and click **OK.**

-Quick Assign User/Group	
Group Name PM	
Available Hosts	Hosts in Selected Group
06128NB(172.17.5.91) 172.17.5.243	>> <
	Apply Cancel

- 3. Select the host and click to add it to the Hosts in Selected Group window.
- 4. Click **Apply**.



5. Click **OK** to finish. The new group is added to the Group Setting list.

UDFL-M510	Information Security Gateway	
CORLANSIO	de Status Croups Croup Setting Croup Setting Croup Name M Add Delete Down Croup Name M Available Hosts 172:17:5:243 Croup Croup Name M Add Subnet	n Selected Group
		Cancel

CHAPTER 6: POLICY

Policy is the most important information in the DFL-M510 Management System. A policy can consist of thousands of patterns. Each pattern defines how to detect an application, how to respond when an application is detected, what to block, and when to block. You can view and modify the settings, including applying scope, acting schedule, actions and information such as category, and constraints.

THE POLICY SCREEN



After you log on, click **Policy** to open the following screen:

The **Policy** screen gives you access to the following screens:

- The Policy Setting Screen
- User Defined Pattern
- The Schedule Screen
- Message Setting
- Keyword Filter
- Pattern Updates

After the policy database is published and fetched, it is uploaded to the DFL-M510. To manage the users and applications, policies are defined and each of them complies with a company policy. Then each policy can be applied to a host or a group. We define a policy before applying it or creating a template. A template can be defined manually or via the template wizard. Once a template is defined, it can be assigned to

a host or a group and it becomes a complete policy.

THE POLICY SETTING SCREEN

After you log on, click **Policy/Policy Setting** to open the following screen:

DFL-M510	Information Security Gateway	
DEL-MSIO	Importation Security Gateway Status Importate Setting Assign Policy Policy Viewer Importate Setting Assign Policy Viewer Importate List Name Wizard_Template Block MP2P Delete Importation Security Gateway Block All Delete Importation Security Gateway Important File Stating Painternet File Straining (P2P) Important File Straining (P2P) Block All Dupat Important File Straining (P2P) Important File Straining (P2P) Important File Straining Media Important File Straining Media Important File Straining Media	Very Popup Message Web Message Web Message Web Message MSN In-Vindow Message MSN against the security
		Apply Cancel

Every template, including the global template created by the device wizard, can be created or modified.

The protocols displayed on the policy are described as follows.

A. The IM Applications that can be managed by the DFL-M510

ltem	Protocol	Management Type	Support Version
Message Exchange	MSN	MSN Keyword	MSN 7.5 / Microsoft Live
(IM)		Login	Messenger : 8.0
		Chat	
		File Transfer	
		Audio Communication	
		Video Communication	
		Online Game	
		Encrypted with SIMP	

		Web MSN		
		Login	ICQ5/ AIM 5.9.3759/	
		Chat	iChat 3.0.1	
		File Transfer		
	ICQ/ AIM/ IChat	Audio Communication		
		Video Communication		
		Web ICQ		
		Login	6.0.0.1921	
		Chat		
	Yahoo	File Transfer		
	Messenger	Audio Communication		
		Video Communication		
		Web Yahoo IM		
	QQ/ TM	Login	QQ V06.1.103.300/ TM 2006	
	Gadu-Gadu	Login	Gadu-Gadu 7.1	
	Clarge	Login (Normal Mode)	Skype 1.3.0.60	
	Зкуре	Login (Strict Mode)		
		Login	MIRC 6.16	
		File Transfer		
	Odigo	Login	v4.0 Beta(Build 689)	
		Login	Rediff BOL 7.0 Beta	
	Rediff BOL	Chat		
		Audio Communication		
		File Transfer		
	Google Talk	Login	Google Talk 1.0.0.92	
		Chat		
		Audio Communication		
Web Control		Yahoo Mail		
Control	Web Mail	Gmail		
		Hotmail		
	Web	Web Page Keyword		

Application	URL Keyword	
	Upload	
	Java Applet/ Active X	
	Download	
	Web Post	
	Cookie	

B. The P2P/Remote Access Application that can be allowed/blocked by the DFL-M510

ltem	Protocol	Software Version
Internet File Sharing (P2P)		Shareaza 2.1.0.0
		BearShare 5.0.1.1
	Coutollo	LimeWire 4.8.1
	Giulena	Gnucleus 2.2.0.0
		Morpheus 5.0
		ezPeer2.0
		mldonkey 2.5.x
	FastTrack	Kazaa 3.0
		Grokster 2.6
	Kuro	Kuro 5.30.0704
		eDonkey2000-1.4.3
		Shareaza 2.1
	eDonkey2000	eMule 0.46a
		Morpheus 5.0
		mldonkey 2.5.x
		BitComet 0.59
	BitTorrent	Shareaza 2.1
		BitTorrect 4.0.4
		mldonkey 2.5.x
	DirectConnect	PeerWeb DC++ 0.300
		StrongDC++ 1.00 RC9
		RevConnect 0.674d

		DC++ 0.674	
		DirectConnect 2.2	
		Jubster MP3 Finder 3.0.0	
		BCDC++ 0.674b	
		DC Pro 0.2.3.45E	
	PiGO	PiGO V 3.0	
	PP365	PP365 1.11	
	WinMX	WinMX 3.53	
	PC Anywhere	PC Anywhere 11	
	VNC	VNC Ver. 3.37	
	SoffEbor	SoftEher Ver. 2.0	
	Soliener	PacketiX (SoftEther) 2.10 build 5080	
		File Transfer	
Eilo Tropofor	FIF Application	Command Execution	
	GetRight	GetRight 5.2d	
	FlashGet	FlashGet 1.71	
	POP3		
Moil	IMAP4		
IVIAII	SMTP		
	NNTP		
	RealPlayer	10.5	
	MS Media Player	10.0	
Streaming Media	iTunes	4.9.0.17	
	QuickTime	7	
	Winamp	5.09	
	Radio365	1.11	
	H.323		



The DFL-M510 manages P2P downloads by using P2P Protocol. In this architecture, no matter what version of client is used, the DFL-M510 can manage it.



The DFL-M510 only supports HTTP download via Getright.

The **Policy Setting** screen has the following three tabs:

- "The Template Setting Tab" on page 80
- "The Assign Policy Tab" on page 83
- "The Policy Viewer Tab" on page 87

THE TEMPLATE SETTING TAB

To view the **Template Setting** tab, click **Policy > Policy Setting > Template Setting**.



When you select a template from this list, its patterns are listed in the center pane. You can add, delete, and duplicate templates.



To quickly make a new template, find an existing template that has a similar pattern and duplicate it. Then modify the new template as desired.

Each time only one category, application, or pattern can be chosen and settings are shown in the **Options** pane. When a category is chosen, the options or the constraints show that all patterns of the category are the same. When an application is chosen, the options or the constraints show that all patterns of the application are the same. When a pattern is chosen, it shows all the options and all the constraints of it. The options or constraints which are not shown are grayed out.

Changes made in the fields under Options apply to all patterns.

THE OPTIONS PANE

When a pattern is detected, the DFL-M510 takes certain management actions, such as blocking the connection, or notifying the administrator. There are five actions that can be taken:



Action	Description
Block	The pattern packet is dropped and its connection cut off.
Pass	Just log the event.
Alert by Email	An email with details of the attack to the administrator defined in email management parameter.
Win Popup Message	Send a Windows popup message to the user.



When you turn off Messenger Service or enable Personal Firewall, the Win Popup Message function works correctly.

DEFINING THE ACTIVE SCHEDULE

It is possible to define the active time range of a pattern. The default setting is **Always** (all the time).

The Scope confines the detection ranges of a pattern rule to some hosts or some directions of traffic. This is very helpful for users who need to fine tune the policy so as to match their environment. For example, if you want to block your staff using P2P software, you can limit the detection range of the P2P policy to only intranet, and skip detection against DMZ. Thus, false-positives can be reduced, while maintaining performance.

If the detection scope is defined as Directional, the scope is distinguished by source and destination.

If it is defined as Non-directional, the rule will manage. Therefore, an administrator does not have to choose the detection scope from the combo box. Instead it is fine tuned before the policy database is published. The only thing the administrator needs to do is to apply the templates or the policy to the hosts or the groups.

Schedule	Always	-
	Always	
	Weekdays	
Keywood Cont	Weekend	
-Keyword Cont	Working Hours	



Only schedules already defined show in the combo box. If you want to use custom schedule, you need to define it first. See "**The Schedule Screen**" on page 93.

DEFINE KEYWORD CONTENT

Some patterns have constraint parameters. If such a pattern rule is selected, there is a constraint parameter section as following.

Keyword: The user defined keyword to match the content of packets.

Keywor	d Content	 	

THE ASSIGN POLICY TAB

To view the Assign Policy tab, click Policy > Policy Setting > Assign Policy.

DFL-M510	Information	Security Gateway	00
D-Link Building Networks for People	Status •		August 1922 (189.1.10) Support 1922 (189.1.10) Cogout 1 Help
U DFL-M510	Template Setting Assign Policy Policy V	iewer	
S User Authentication	-Template-		Group/Host
- Objects			
E	Available Templates	Policy for the template	E See PM
	Wizard_Template	Message Exchange (IM)	
	Bypass All	iulinternet File Sharing (P2P)	
	Block P2P	File Transfer	
	Block M+P2P	iMail	
	BIOCK AII		
Pattern Updates		+Streaming Media	
- Ve Real Time Monitor			
			Apply Cancel
			Curron Curron

HOW TO ASSIGN A POLICY

In the following example, the Security group is assigned a policy only allowing Web control such as Web browsing.

1. In the **Template Setting** tab, click **Add** to add a new template.

DFL-M510	Information Security Gateway	
borne Witzard forme Witzard forme Witzard forme System biterrares literrares		NETDEFEND ged in .a: Administrator min. 142. (18:1.10) 2 Logout 2 Help
	Wtzard_Template Add Image: Constraint of the state of the sta	y Email g All v pup Message ation blocked by s v lessage against the security v -Window Message Inst the security poli v Always v Intent
•		Apply Cancel

2. Configure Policy for application behavior management.

Building Networks for Propio More Mode and Additional Additional and Additional Addition

3. Click "Apply" to save the policy template.

Building Networks for Papels
B→W SS (COARMAChat(Mac) B→W SS (COARMAChat(Mac)) B→W SS (COARMAChat

4. Click the **Assign Policy** tab. Select the template you want to implement from the **Available Templates** pane

UDFL-M510	Information Secur	ity Gateway	
DELMSIO	Template Setting Assign Policy Policy Viewer Template Available Templates Vitzard_Template Bypass All Block P2P Block All No IM File Transfer	Policy for the template	CroupHost
			Apply Cancel
(2)半			

5. Under Group/Host, select PM and click Apply.



THE POLICY VIEWER TAB

In the Policy Viewer tab, you can view all policies of groups. In the example below, we check the policy of the **PM** group via the **Assign Viewer** tab, click **Policy > Policy Setting > Policy Viewer**, and then select **PM** in the **Group/Host** pane.

UDFL-M510	Information Security Gateway		00
DEL-MS10 DEL-MS10 DEL-MS10 DEL-M510 Ward Objects Dolicy Objects Objects	Information Security Gateway Image: Status Image: Status Status Template Setting Assign Policy Policy Viewer GroupHost Image: Status Image: Status Image: Status Image: Status <th>Adaption of the second second</th> <th></th>	Adaption of the second	
	Auto Communication Video Communication Video Communication Video Xahoo M		

USER DEFINED PATTERN

The pattern database is made by a team of professional signature researchers. They are familiar with protocols, system vulnerability, and application patterns.

After a new application pattern is detected, the pattern is put into the pattern database and published. Before publishing, there are still ways for a manager to define application patterns. If a specific application is always connecting to several specific servers or by several specific ports. The servers and the ports can be blocked by a user-defined pattern.

00 DFL-M510 Information Security Gateway D-Link NETDEFEND 0 🏠 Home 🛛 🕼 Wizard 👻 🛛 🌋 Tools 👻 🚔 Status 👻 📔 De Loc out 🛛 🕜 H 🔱 DFL-M510 -User-Defined Pattern 🛶 🎯 System Pattern Info By Protocol therfaces Add 🔙 Objects 🗤 🥡 Policy Edit Delete 🙀 User Defined Pattern Message Exchange (IM) Pattern Ports — --- 🐶 Message Setting 🏀 Keyword Filter TCP UDP 🤹 Pattern Updates 庙 Real Time Monitor Traffic Shaping From 0 + To From 0 To

Policies can be defined in the following Policy/User Defined Pattern screen:

After a pattern is defined, the pattern is displayed in the pattern list, contained in a template, and assigned with options and constraints. Click **Edit** to edit a defined rule. Click **Delete** to delete a defined rule.

DEFINING A PATTERN BY PROTOCOL

For example, a Streaming Media sees TCP 3001 ports to connect to Media servers. To block this Streaming Media game do the following.

1. In the **User Defined Pattern** screen, click **Add**.

DELEMER Building Networks for People Delement Status Status Delement De	UDFL-M510	Information Security Gateway		00
Pointy Setting Delete Category Message Exchange (M) Image: Schedule Message Setting Image: Schedule Image: Schedule Image: Schedule Pattern Updates Image: Schedule Image: Schedule Image: Real Time Monitor Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Image: Schedule Imag	COPLASSO	Information Security Gateway	Cogot P Help	
			Save	

2. Type in **Streaming1** for the pattern name and click **OK**.

UDFL-M510 Add	d Pattern Name	00
Pattern Name	Streaming1	
ОК	Cancel	

3. Input a pattern named **Streaming 1**, with category **Streaming Media** and TCP port 3001.

4. Click Save.

UDFL-M510	Information Security Gateway	00
CDELASSO	Status Status User-Defined Pattern Pattern Info By Protocol By Application Server Name Streaming Media Delete OPLANSIO Info The Ports Portocol Ports Ports Ports Ports Ports Ports Ports Ports Ports	Image: Constraint of the second strate Image: Constraint of the second strate
		Save

DEFINING A PATTERN BY SERVER

In this scenario, a web chat application is always connecting to a network server with the IP address 140.126.21.4. You can block this web chat application and then click the **Save** button to add a new rule as follows.

UDFL-M510	Information Security Gateway	
Vore Version	Information Security Gateway Image: Streaming Media Streaming Media Edit Delete OFLAMS10 Add Pattern Name Upped and and and the streaming for the streaming f	DEFEND Administrator 8.1.10 Logoat Pelo
Traffic Shaping	OK Cancel 3,001-2 To 3,001 Image: Concel I	Save

1. In the User Defined Pattern screen, click Add.

2. Type in **Web Chat 1** for the pattern name and click **OK**.

UDFL-M510 Add P	attern Name	00
Dation Maria	we and	
Pattern Name	Web Chat 1	
ок	Cancel	

3. Input a rule name **Web Chat 1**, with category **Web Control** and servers, 140.126.21.4.

UDFL-M510	Information Security Gateway	00
CPELASSO	VIETO State Vieto	EFEEND neristrator 1.00 Logout Pelp Pelp
< C		

4. Click Save.

UDFL-M510	Information Security Gateway	
COPELAISIO	Information Security Gateway Status User-Defined Pattern -Web Control -Web Control -Streaming Media -Streaming Media </th <th>bon Server Neb Control</th>	bon Server Neb Control
<)



The DFL-M510 supports 1500 sets of user-defined patterns by protocol and 1500 sets of user-defined patterns by Application Server.

THE SCHEDULE SCREEN

It is possible to define the active time range of a policy. The time range can be defined by the schedule. Each schedule has a name, and a time range. The time range is specified in units of hours.

Click **Policy > Schedule** to access the **Schedule** screen.

Information Security Gateway	
Available Schedule List :	Add Edit
	Available Schedule List Available Schedule List Schedule List Weekend Working Hours

There are four predefined schedules. The **Always** schedule means the policy is always active. The **Working Hours** schedule means the policy is active during working hours. The regular working hours are Monday to Friday from 9:00 AM to 5:00 PM. The **Weekdays** schedule means the policy is active during the whole workdays. The regular workdays are Monday to Friday. The **Weekend** schedule means the policy is not active during the whole workdays. The regular Weekend days are Saturday to Sunday.

To Add or Modify a schedule press the Add or Modify button to open the schedule editing dialog box. Modify the schedule name and check the hour tab to include or exclude the hour represented by the tab.

Wh	ole w	eek		W	/eekda	ay		VVe	eekend	a l] [:	Work	ting ho	ours										
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SUN																								
MON		::	_																					_
TUE																								
WED		:: 																				-		
THU																								
FRI																1							1	
SAT																							1	1

MESSAGE SETTING

In this section, you can edit popup or Web messages. Refer to the following to add a popup message.

1. Click **Policy > Message Setting**.

DFL-M510	Information Security Gate	way
D-Link Building Networks for People		Logged in as Administrator
Home Avizard Vizard Viz	Popup Message to User	Nep Logaut 🛛 🕐 Help
User Authentication	No. Message Description 1 Communication blocked by security policy	Message Text User defined text message
		Add : Edit : Delete :
- 09 Message Setting - 09 Keyword Filter - 09 Pattern Updates - 19 Real Time Monitor	Web Message to User	Message Text
Traffic Shaping	1 Veb site against the security policy	Your Application Communication has been blocked by a Policy
	rMSN In-Window Message to User	Add : Edit Delete :
	No. Message Description 1 MSN against the security policy	Vour Application Communication has been blocked by a Policy
		Edit Delete
[]	·	þ Þ

2. Under **Popup Message to User**, click **Add**.

UDFL-M510	Popup Message Property Add	0
Message ID :	2	
Description :	Message to Block Applications	
You cannot us	e this application.	_
Please contact	the system administrator for further information.	
	OK Cancel	

3. Type a description and the content of the message and click **OK**.

DFL-M510	Information Security Gateway	
D-Link Building Networks for People		D NETDEFEND S Logged in az Administrator admini 102.148.1.101
UFL-M510 System	Popup Message to User-	ne Text
	Communication blocked by security policy	ned text message
— 🍥 Objects	2 Message to Block Applications You cannot be a set used to block applications	not use this application. Please contact the system admi.
Policy Policy Setting		Add Edit Delete
	Web Message to User	ge Text
	Web site against the security policy Your App	ilication Communication has been blocked by a Policy
		Add Edit Delete
	No. Message Description Message	ge Text
	1 Misk against the security poicy Your App	lication Communication has been blocked by a Policy
		Add Edit Delete



When you turn off Messenger Service or enable Personal Firewall, the Win Popup Message function works correctly.

KEYWORD FILTER

The DFL-M510 provides the following keyword functions:

- Web page keyword
- URL keyword
- MSN keyword

These keyword functions are used to describe applications of MSN and Web browsers.

Since all the keyword policies and other policies are too complex to display in a page, an integrated GUI frame is designed to aggregate these rules to use more easily. The special keyword policy GUI is illustrated as following.

L-M510		Information Securit	y Gateway	
D-Link uilding Networks for People	Status		D N Stopped	In as Administrator 192.168.1.101
DEL M540				
System	-Keyword	Table		
interfaces	,			
S liser Authentication	No.	Keyword Name	Keyword Content	
	1	Web Page Keyword 1	-	
	2	Web Page Keyword 2		
- Volicy	3	Web Page Keyword 3		
	4	URL Keyword 1		
	5	URL Keyword 2		
	6	URL Keyword 3		
		MSN Keyword 1 MSN Keyword 2		
Newword Filter		MSN Keyword 3		
Pattern Undates				
Real Time Monitor				
Traffic Shaning				
Tanc Shaping				
			· · · · · · · · · · · · · · · · · · ·	
			Annlo	Edit
			Appay	LOR



This function only supports chapter by ASCII encoding.

PATTERN UPDATE

Constrained by the probability of the probabil	DFL-M510	Information Security Gateway	
Version	D-Link Building Networks for People	D NETDEFE Loged in az Administrat aprin: rtoz ráz	ND
Register for Pattern Update or view current status Download Now	DFL-M510 DFL-M510 System User Authentication Objects Defined Pattern Schedule Keyword Filter Pattern Updates Real Time Monitor Traffic Shaping	Pattern Updates Pattern Information Last update: 2006/09/14 10:23:54 Version of current pattern: 3:22 Number of pattern: 4:29 Please register the DFL-M510 in D-Link NetDefend Center by clicking on the Left button below. Only registered DFL-M510 can receive pattern update message. The current status of a registered DFL-M510 can also be viewed by clicking the same button.	Hap
		Register for Pattern Update or view current status	

PATTERN UPDATE

The DFL-M510 provides up-to-date protection for your network. Pattern information can be reviewed in this section such as last update, version of current pattern and number of pattern.

You can register the DFL-M510 in D-Link's security portal by clicking on the "Register for Pattern Update or view current..." button. By clicking "Download Now", you can immediately connect to the update server and manually download the latest pattern. To obtain the detailed information for the latest pattern before you download, please click "Check details before download" for further information.

CHAPTER 7: REAL TIME MONITOR

The Real Time Monitor provides real-time tracking of network usage in the form of text and graphs. System administrators can monitor significant application pattern events, quickly understand network status, and take imperative action.

THE REAL TIME MONITOR SCREEN

After you log on, click **Real Time Monitor** to open the following screen:





For Real-time Monitor to work properly, port 8801 - 8810 must be opened on the client PC to receive the analysis data from the DFL-M510.



D-Link recommends not managing the DFL-M510 through a WAN link, since the Real-time Monitor feature would get data from the DFL-M510.

The Real Time Monitor screen gives you access to the following:

- Monitoring Real Time Traffic
- Monitoring Real Time Application

MONITORING REAL TIME TRAFFIC

To monitor Real Time Traffic check the **Real Time Traffic** radio button.



ALL	The number of bytes of all packets received
ALL M510	The total amount of traffic the DFL-M510 can manage
Drop	The number of bytes of packets that are identified as an application patter and discard by DFL-M510
IM	The number of bytes of all application of the IM category
P2P	The number of bytes of all application of the P2P category
Mail	The number of bytes of all application of the Mail category
File Transfer	The number of bytes of all application of the File Transfer category
Web Control	The number of bytes of all application of the Web Control category
Streaming Media	The number of bytes of all application of the Streaming Media category
Misc.	The number of bytes of all traffic which does not belong to IM. P2P, Mail, File Transfer, or Streaming Media
Health Alert/Sec	The number of events that a packet was detected as a health concern packet
Administrators can accumulate and analyze detected application patterns by information revealed from their packets. These are explained in the Top N analysis section.

REFRESH TIME

The system provides the new traffic status every thirty seconds.

TRAFFIC LINES

One line in the traffic chart means one meter of current time. Each line can be hidden or shown by clicking the check box before the specified label.

SCOPE

Click the drop-down arrow to select a group or subnet to monitor. It filters hosts and doesn't affect the current traffic status but instead zooms into the subset of the hosts that are specific by each case.

MONITORING REAL TIME APPLICATION

To monitor Real Time Application check the **Real Time Application** radio button.

UDFL-M510		Informat	ion Security G	ateway		
D-Link Building Networks for People	• I 🕙 Status 🔹 I				ĨĨ	NETDEFEND Legged in as Administrator shinic 172. 175.43 Zogout 2 Help
100 DEL-M510						
	Real Time Traffic	Real Time A	pplication			Top 10 Categories / Top 10 Applications
Interfaces	Real Time Application					Top 10 Chart
user Authentication						By Hit @ By Byte
	Host	HTTP	HTTPS	SMTP	FTP	
E	172.17.5.243 06129NB(172.17.5.91)				_	Top 1 - Top 2
	06128NBWINXP(172.17.5.43)	~	~			
	Common Network Pro Health Checking EIM	otocol)		,	Top 10 Information Web Control 184.95 KB 88.76% Message Exchange (IM) 23.42 KB 11
			*			Reset Back

The Real Time Application page shows management information classified by pre-defined types and hosts.

The left of this screen displays the current application information; the right of this screen displays the accumulated application information for Top N analyzing. The right part is the same as the right part of real time traffic.

There are three tables: the common network protocol table; the EIM table; and the health checking table. Select the radio button to display each table. The EIM table is the default.

COMMON NETWORK PROTOCOL

The common network protocol table shows the current status of each host. This table is a layer 4 table and network applications are monitored at the network port number. The common network protocol contains HTTP, HTTPS, SMTP, FTP, TELNET, POP3, IRC, NNTP, and IMAP. If a host is connecting to the Internet via the above ports, the table shows a check mark to indicate the host is currently connecting.

DFL-M510		Informa	tion Security G	iateway			1	00
Building Networks for People Home Mome M	is 🔹 🔿 Status 🔹	Real Time /	Application			Top 10 Categories / Top 10 /	TDEFEND n as Administrator 72.17,6.43 2 Logout 2 He Applications	qie
	-Real Time Application					Top 10 Chart		
User Authentication Objects	Host	НТТР	HTTPS	SMTP	FTP	🛄 🕗	🔵 By Hit 💿 By Byte	
E To Policy	172.17.5.243		_	_	_	Top 1	- Top 2	
	06128NB(172.17.5.91) 06128NBWINXP(172.17	.5.43)						
	Common Networ Health Checking EIM	ork Protocol)		,	Top 10 Information Web Control : Message Exch	295.63 KB 90.85% hange (M) 29.77 KB 9.1	
10						Res	et : Back	

HEALTH CHECKING

The Health Checking table is a layer seven table. Instead of classifying the application pattern, several packets that come from attacking tools can damage the host. Some of the packets are assembled and stored in the file system and are detectable by anti-virus software. Some packets try to get system authorized control and run as an operating system's administrator without storing to the file system. These packets are invisible to almost all anti-virus software, but detectable by the DFL-M510. When those packets come from a host and are detected, the corresponding field shows a check mark to indicate the host has health concern problems.

Health-concern problems include network based worms, illegal agents, and tunnels. Network based worms do not include common viruses, since they are easy to discover by standard virus software.

Illegal agents include backdoors, trojans, spyware, and ad-ware.

Tunnels are host-based software. They provide a secure channel for communication. The purpose is to break through a firewall and escape content inspecting. For example, like soft ether, VNN, and VNC.

UDFL-M510		Informa	tion Security Gate	Nay		
bone Witard Sector	Status	Real Time .	Application	111	Construction of the second sec	Logout 2 Help
interfaces	Real Time Application —					
						v Hit 🕜 By Byte
	Host	Worm	Illegal Agent	Tunnel		, m 00,0,0
Policy	172.17.5.243				Top 1 - Top 2	
— 🚂 Real Time Monitor	06128NBWINXP(172.17.5.81)	43)				
					Top 10 Information Web Control 296.15 Message Exchange (I	KB 88,58% M) 37.79 KB 11
	Common Network	Protocol			•0	 ,
•			*		Reset	Back

EIM

The EIM table provides layer seven monitoring. A packet is classified by its application pattern and summarized into six categories: IM, P2P, Web application, file transfer, E-mail, and media.

If a host is connecting to the Internet and identified as a category application, the table shows a check mark to indicate the host is currently running the application with that specific category.

DFL-M510		Infor	mation	Security Gatev	vay			
Home Witzard V Tools	s 🕶 🍽 Status 💌						D NETD Logged in as Ad admin 1972 12 6	EFEND ministrator .43 Logout 3 Help
🛓 🍈 🎆 System	🔾 Real Time Traffic 🧯 🤅	🛛 Real Tir	me Appli	ication			Top 10 Categories / Top 10 Applicati	ons
	Real Time Application						Chart	
							🛛 🗤 🍊 🔹 🔿 🕫	v Hit 🖸 By Byte
- 🍓 Objects	Host	IM	P2P	Web Control	File Transfer	Mail		· · · ·
🕀 🧔 Policy	172.17.5.243 06128NB(172.17.5.91)						Top 1 - Top 2	
	06128NBV/INXP(172.17.5.43)			~		-		
	•					F	Top 10 Information Web Control 298.52 Message Exchange (II	KB 86.79% M) 45.42 KB 13
	Common Network Prof	tocol]					
							Reset	Back

TWO LEVELS TOP 10 ANALYSIS

Administrators can review detected application patterns by information revealed from its packets. All triggered incidents are categorized on the principle of sequence, health, time of occurrence, name of pattern, source address, destination address, counts, and responsive actions (dropping packets, disconnects, emailing the administrator in charge, or keeping logs of incidents,) and are all displayed in charts for administrators to quickly understand the present status of the network. These monitoring charts have two levels. First: choose one chart from the six charts; then pick one item from the first level to display the second level chart.

TOP 10 CATEGORIES/TOP 10 APPLICATION

In these charts, the first level shows the top 7 categories. When a category is chosen, the second level shows the top 10 applications in the chosen category. The following means that the top category is the IM category. The following means that the top category is Message Exchange (IM).

The lower list shows details of each category. When the IM category is chosen, the second level chart covers the first chart as follows:



The lower list shows details of each category. When the IM category is chosen, the second level chart covers the first chart as follows:

luli 🔿		O By Hit	Bv Bvte
	·	00,1	0,0,0,0
-	Top 1 -	Тор З	
		-	
-			
p 10 Inf	ormation		
op 10 Inf	ormation		
op 10 Inf	ormation	91.95%	
op 10 Inf	MSN 4.12 MB Skype 354.23	91.95% KB 7.9%	
op 10 Inf	MSN 4.12 MB Skype 354.23 Yahoo Messen	91.95% KB 7.9% ger 6.69 K	B 0.15%
op 10 Infe	MSN 4.12 MB Skype 354.23 Yahoo Messen	91.95% KB 7.9% ger 6.69 K	B 0.15%
op 10 Inf	MSN 4.12 MB Skype 354.23 Yahoo Messen	91.95% KB 7.9% ger 6.69 K	B 0.15%
op 10 Infi	MSN 4.12 MB Skype 354.23 Yahoo Messen	91.95% KB 7.9% ger 6.69 K	B 0.15%

It would be understood that the MSN is the most frequent application within the IM category.



TOP 10 APPLICATIONS / TOP 10 USERS

In these charts, the first level shows the top 10 applications. When an application is chosen, the second level shows the top 10 users in the chosen application.

The following means that the top application is MSN.

	Top 10 Applications / Top 10 Users
	Тор 1 - Тор 10
Top 40 lpf/	prostion
Top 10 Info	Veb Application 12.15 MB 40.09%
Top 10 Info	Web Application 12.15 MB 40.09% POP3 11.07 MB 36.56%
Top 10 Info	Web Application 12.15 MB 40.09% POP3 11.07 MB 36.56% MSN 4.36 MB 14.39%
Top 10 Info	Web Application 12.15 MB 40.09% POP3 11.07 MB 36.56% MSN 4.36 MB 14.39% Gnutella 1.84 MB 6.07%
Top 10 Info	Web Application 12.15 MB 40.09% POP3 11.07 MB 36.56% MSN 4.36 MB 14.39% Gnutella 1.84 MB 6.07% Skype 451.53 KB 1.49%
Top 10 Info	Vveb Application 12.15 MB 40.09% POP3 11.07 MB 36.56% MSN 4.36 MB 14.39% Gnutella 1.84 MB 6.07% Skype 451.53 KB 1.49% SMTP 194.86 KB 0.64%
Top 10 Info	VVeb Application 12.15 MB 40.09% POP3 11.07 MB 36.56% MSN 4.36 MB 14.39% Gnutella 1.84 MB 6.07% Skype 451.53 KB 1.49% SMTP 194.86 KB 0.64% ICQ/AlM/Chat(Mac) 180.62 KB 0.6
Top 10 Info	Web Application 12.15 MB 40.09% POP3 11.07 MB 36.56% MSN 4.36 MB 14.39% Gnutella 1.84 MB 6.07% Skype 451.53 KB 1.49% SMTP 194.86 KB 0.64% ICQ/AIM/Chat(Mac) 180.62 KB 0.6

TOP 10 GROUPS/TOP 10 APPLICATIONS

In these charts, the first level shows the top 10 groups. When a group is chosen, the second level shows the top 10 Applications. The following means that the top group is the default group.

	Obyrin Obybyre
	Top 1 - Top 1
p 10 Information	1
Default	45.34 MB 100%

TOP 10 USERS/TOP 10 APPLICATIONS

In these charts, the first level shows the top 10 users. When a user is chosen, the second level shows the top 10 applications in the chosen user. The following means that the top user is Jeffrey.

	Top 1 - Top 9
2	
o 10 Info	ormation
	JEFEREV J IVPA9S(192,168,70,240)
-	JEFFREY-LIVPA9S(192.168.70.240)
	JEFFREY-LIVPA9S(192.168.70.240) 192.168.10.6 11.21 MB 21.27% 192.168.0.109 8.77 MB 16.63%
	JEFFREY-LIVPA9S(192.168.70.240) 192.168.10.6 11.21 MB 21.27% 192.168.0.109 8.77 MB 16.63% 192.168.168.16 7.53 MB 14.28%
	JEFFREY-LIVPA9S(192.168.70.240) 192.168.10.6 11.21 MB 21.27% 192.168.0.109 8.77 MB 16.63% 192.168.168.16 7.53 MB 14.28% 192.168.0.110 4.16 MB 7.88%
	JEFFREY-LIVPA9S(192.168.70.240) 192.168.10.6 11.21 MB 21.27% 192.168.0.109 8.77 MB 16.63% 192.168.168.16 7.53 MB 14.28% 192.168.0.110 4.16 MB 7.88% 192.168.168.18 1.91 MB 3.62%
	JEFFREY-LIVPA9S(192.168.70.240) 192.168.10.6 11.21 MB 21.27% 192.168.0.109 8.77 MB 16.63% 192.168.168.16 7.53 MB 14.28% 192.168.0.110 4.16 MB 7.88% 192.168.168.18 1.91 MB 3.62%

TOP 10 HEALTH CONCERNS/TOP 10 USERS

In these charts, the first level shows the top 3 health concerns. When a health concern is chosen, the second level shows the top 10 users in the chosen health concern.

The following means that the top health concern is the illegal agent.

lill 🧠		3vte
	Тор 1 - Тор 1	- 1
		_
p N Information		_
p N Information	ING 37 Hits 100%	
p H Information	ING 37 Hits 100%	
p N Information	ING 37 Hits 100%	
p N Information	ING 37 Hits 100%	
p N Information	ING 37 Hits 100%	

TOP 10 USER WITH HEALTH CONCERNS/TOP 10 HEALTH CONCERNS

In these charts, the first level shows the top 10 users with health concerns. When a user is chosen, the second level shows the top 3 health concerns in the chosen user. The following means that the top user with health concern is CJHO.

		By Hit	By Byte
-	Top 1	- Top 2	
p N Infor	mation ——		
p N Infor	mation	8.16.6) 19 1	Hits 51.35%
p N Infor	mation — CJHO(192.16 KNIGHT-NB(1	8.16.6) 19 H 92.168.50.75	Hits 51.35%)18 Hits -
p N Infor	mation —— CJHO(192.16 KNIGHT-NB(1	8.16.6) 19 H 92.168.50.75	Hits 51.35%) 18 Hits (

CHAPTER 8: TRAFFIC SHAPING

The Traffic Shaping enables bandwidth control over the Internet applications. System administrators can specify the bandwidth either for user groups or for applications.

D-Link Description Building Networks for People Status Home V4zard Status	ID Help
10 DFL-M510	
tar file Shaping	- 1
- to Interfaces	
Enable traffic snaping and specify bandwidth or internet.	
Enable Traffic Shaping	
Define a traffic shaping policy by specifying what application group should have bandwidth limitation.	
No Name Application Group Port Schedule Limit	
no. name approator or prot scredule Linit	
Add for Application Add for Group Modify Delete Apply	5
	•

DEFINING A TRAFFIC SHAPING POLICY FOR APPLICATIONS

This scenario illustrates how to configure bandwidth limitation for applications. Here the example below demonstrates how to create a traffic shaping policy for BitTorrent. You can create a traffic shaping policy via click the **Add for Application** button, and then click the **Apply** button to add a traffic shaping policy as follows.

OBy User	Defined Service
Name	
Category	Message Exchange (IM) Application Any
Limit	10 - KB (Min 10KB, Max 5MB)
Schedule	Always

1. In the Traffic Shaping screen, click Add for Application.

 Select By Default Application, provide the policy name P2P_BitTorrent. In Category and Application menu, select Internet File Sharing (P2P) and BitTorrent, meanwhile assign bandwidth limitation, for instance 50KB for BitTorrent. Then click the Apply button to add a new policy.

Name	P2P_BitTorrent
Category	Internet File Sharing (P 💌 Application BitTorrent
Limit	50 KB (Min 10KB, Max 5MB)
Schedule	Always

3. Enable Traffic Shaping feature, and click **Apply** to take effective.

efine	a traffic shaping r	olicy by specifying what	application grou	n should have ban	dwidth limitation.	
	a a anno onapang p	ionoj oj opeenjing rina.	opprovion gi ot			
No.	Name	Application	Group	Port	Schedule	Limit
1	P2P_BitTorrent	Internet File Sharing (P			Always	50 KB
₹ (]						Ð
• (den den line den "		-			D
<	for Application	Add for Group	Modify	Dele	te	D
<	for Application	Add for Group	Modify	Dele	te	D

DEFINING A TRAFFIC SHAPING POLICY FOR USER GROUPS

This scenario illustrates how to configure bandwidth limitation for user groups. Here the example below demonstrates how to create a traffic shaping policy for the PM user group. You can create a traffic shaping policy via click the **Add for Group** button, and then click the **Apply** button to add a traffic shaping policy as follows.

1. In the Traffic Shaping screen, click Add for Application.

Name				
Group	Default			
Limit		10 KB (Min 10KB, Max S	imb)	
Schedule	Always			

2. Provide the policy name **UG_PM.** In Group menu, select the **PM** user group; meanwhile assign bandwidth limitation, for instance **300KB** for the user group. Then click the **Apply** button to add a new policy.

Name	UG_PM	
Group	PM T	
Limit	300 KB (Min 10KB, Max 5MB)	
Schedule	Always	

3. Click **Apply** to take the policy effective.

efine	a traffic shaping p	oolicy by specifying what	t application grou	p should have bar	ndwidth limitation.	
No.	Name	Application	Group	Port	Schedule	Limit
1	UG_PM		PM		Always	300 KB
2	P2P BitTorrent	Internet File Sharing (P.			Always	50 KB
	1					
۹ (-			Ð

APPENDIX A: THE COMMAND LINE INTERFACE

This section covers the following topics:

- Terminal/SSH (Secure Shell) Connection
- CLI Command List
- Help Command
- Get Command
- Set Command
- Exit Command
- Reboot Command
- Reset Command
- Ping Command

Terminal/SSH (Secure Shell) Connection

The DFL-M510 Console Service provides administrators a text-mode interface to configure the DFL-M510 and its arguments via an RS-232 serial cable. The DFL-M510 devices provides terminal emulation and SSH connection service. Administrators can attach an RS-232 cable to the RS-232 console port on the DFL-M510, and log in with the super terminal program provided by Windows 95/98/2000/NT/XP; or use the remote login command line interface by using terminal connection software with SSHv2 encryption function.

These two methods of accessing the command line interface have three major differences between them:

- 1. SSH service provides administrators an ISG remote control mechanism and higher security compared to a traditional Telnet connection.
- 2. Since remote access is considered more risky than accessing from a terminal connection, some functions are limited to the terminal connection service only. For example, the device booting message does not show on the remote access. (Details of the limited functions are provided in the next section.)
- 3. For the sake of security, the SSH service provided by ISG devices can be shut down. From security stand point, the best way to protect against brute force approach is to prolong the interval between login attempts. Therefore, the SSH login attempt is limited to 3 times, and each interval 60 seconds. If a user has failed logins that exceeds this or is stuck in the login process for more than 60 seconds, the SSH connection will be terminated, and login resources are released. In addition, the DFL-M510 only allows one SSH connection at a time for the consideration of the conformity of system configuration and the security of the remote connection.

Getting Started

Once you have accessed the Command Line Interface (CLI) with a terminal connection, press any key and the following prompt will appear. Enter the user name and password: the default user name is **admin**, the default password is **admin**.

Welcome to D-Link DFL-M510 Console Environment Copyright (C) 2005 D-Link Corp. <www.dlink.com> DFL-M510 login:

CLI Command List

You can use the console or SSH to connect the DFL-M510. After login, you can use the CLI commands to configure the DFL-M510. The complete CLI commands are described as follows.

Commands	Description
help	Getting information of all command's usage and argument configuration
get	Display all kinds of configuration information of the DFL-M510
set	Set the system parameter
history	Display all commands which you have used
exit	Exit command shell
reboot	Reboot system
reset	Reset system configuration to default settings, type "y" to load default setting.
ping	Send ICMP echo request messages

Help Command

Help is used for getting information of other command's usage and argument configuration.

Main command	Sub command	Example	Command description	
	get	help get	Display all information of "get" command.	
	set	help set	Display all information of "set" command.	
	history	help history	Display all information of "help" command	
h a ha	exit	help exit	Display all information of "exit" command	
neip	reboot	help reboot	Display all information of "reboot" command	
	reset	help reset	Display all information of "reset" command	
	ping	help ping	Display all information of "ping" command	

EXAMPLE

(A) help get

>> help get

get - Get system parameters. Available commands system - System configurations, including IP, password and etc.

time - Device clock setting state - Device operation state interface - Device interface configuration

(B) help set

>> help set

 set - Set system parameters. Available commands system - System configurations, including IP, password and etc. time - Device clock setting state - Device operation state remote - Setup remote access configuration. Interface - Change interface link mode

(C) help history

>> help history history - Show all command history

(D) help exit

>> help exit exit - Log out

(E) help reboot

>> help reboot reboot - Reboot system

(F) help reset

>> help reset reset - Reset system configurations to manufacturing defaults

(G) help set

>> help ping ping - Ping utility

Get Command

This command will display all kinds of configuration information of the DFL-M510.

Main command	Sub command	Example	Command description
	system	get system	Display system configurations, including IP, password and etc.
get	time	get time	Display device clock setting
	state	get state	Display device operation state
	interface	get interface	Display device interface configuration

EXAMPLE

(A) get system

>> get system

```
Device name: M510
MAC Address: 00:00:00:00:00:00
DFL-M510 IP Address:192.168. 80.244, netmask:255.255. 0. 0,
gateway:192.168.168.253
TCP cold start duration time: 300 seconds
VLAN function: off. VLAN ID: 1.
Detection parameters:
Detection parameters:
 Maximum ping packet size: 1024.
TCP state check bypass: off.
WAN port: policy check <off> Stealth < on> max ping
LAN port: policy check <off> Stealth < on> max ping
                                                                                                                                                                           10000.
                                                                                                                                                                           10000.
Remote access:
HTTP:
Access: all
1 - Client IP: all
2 - Client IP: 0.
3 - Client IP: 0.
                                                   11 Netmask: 255.255. 0.
0. 0. 0. 0 Netmask: 255.255.255.
0. 0. 0. 0 Netmask: 255.255.255.
                                                                                                                                                                               0
                                                                                                                                                                               0
                                                                                                                                                                              Õ
ŠSH:
Access: all
1 - Client IP: all
2 - Client IP: 0
3 - Client IP: 0

        11
        Netmask:
        255.255.255.

        0.
        0.
        0.
        Netmask:
        255.255.255.

        0.
        0.
        0.
        Netmask:
        255.255.255.

        0.
        0.
        0.
        Netmask:
        255.255.255.255.

                                                                                                                                                                               0
                                                                                                                                                                               0
                                                                                                                                                                               Ø
>> _
```

(B) get time

>> get time Current time : (GMT + 0) Mon Apr 18 08:34:37 2005 DST time : (GMT + 0) Mon Apr 18 08:34:37 2005 System duration: 0 days 0:43:10

(C) get state

>> get state Operation mode: In-Line

(D) get interface

>> get interface Interface: WAN: auto. LAN: auto.

Set Command

Use this command to set the system's parameter.

Main command	Sub command	Command description
	system	Set system configurations, including IP, password and etc.
	time	Set device clock
set	state	Set device operation mode
	remote	Set remote control mode
	interface	Set interface link mode

"SET SYSTEM" COMMAND

Prefix command	2 nd command	Example	Command description
set system	ір	set system ip 192.168.80.244	Set device's IP
	mask	set system mask 255.255.0.0	Set device's mask
	gateway	set system gateway 192.168.80.244	Set device's default gateway
	passwd	set system passwd	Set administrator's new password
	detect	set system detect	Set the relating arguments for ISG's outgoing and incoming packets detection.

vlan	set system vlan	Set the VLAN environment related parameters
name	set system name	Set device's name

Prefix command	2 nd command	3 rd command	Postfix comman d	Example	Command description
	tcptimeout	20 -2592000		set system detect tcptimeout 6000	Set TCP connection timeout
	policy	wap	On	set system detect policy wan on	Turn on wan port's policy check
		Wall	Off	set system detect policy wan off	Turn off wan port's policy check
		lan	On	set system detect policy lan on	Turn on lan port's policy check
			Off	set system detect policy lan off	Turn off lan port's policy check
set system detect	pingmax	wan	10 - 300000	set system detect ping wan 5000	Set max ICMP count of wan port
		lan	10 - 300000	set system detect ping lan 5000	Set max ICMP count of lan port
	stateful	on		set system detect stateful on	Turn on TCP state bypass
		off		set system detect stateful off	Turn off TCP state bypass
	pinglen	64 - 1500		set system detect pinglen 1024	Set max acceptable ICMP size 64 -1500
	tcpcoldstart	0 -300		set system detect art 250	Set TCP cold start timer

Prefix	2 nd command	3 rd command	Example	Command description
	on		set system vlan on	Turn on VLAN function
set system vlan	off		set system vlan off	Turn off VLAN function
Vian	vid	1 - 4094	set system vlan 1	Set VLAN ID

EXAMPLE

(A) set system ip

>> set system ip 192.168.1..245 Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(B) set system mask

>> set system mask 255.255.255.0 Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(C) set system gateway

>> set system gateway 255.255.255.0Do you want to apply this setting immediately?Your current ssh/http connection will be cut off. (y/n)

(D) set system passwd

>> set system passwd Original password: ***** New password: ***** Retype password: *****

(E) set system detect tcptimeout

>> set system detect tcptimeout 100000 Change TCP session time out limit OK.

(F) set system detect policy wan on

>> set system detect policy wan on Apply policy check for wan interface OK.

(G) set system detect policy wan off

>> set system detect policy wan off Remove policy check for wan interface OK.

(H) set system detect policy lan on

>> set system detect policy lan on Apply policy check for lan interface OK.

(I) set system detect pingmax wan 100000

>> set system detect pingmax wan 100000 Change wan port maximum ping packet limit OK.

(J) set system detect pingmax lan 100000

>> set system detect pingmax wan 100000 Change lan port maximum ping packet limit OK

(K) set system detect stateful on

>> set system detect stateful on Turn on TCP state check bypass

(L) set system detect stateful off

>> set system detect stateful off Turn off TCP state check bypass

(M) set system detect pinglen 1024

>> set system detect pinglen 1024 Change maximum length of ping packet OK.

(N) set system detect tcpcoldstart 250

>> set system detect tcpcoldstart 250 Change TCP cold start duration time OK.

(O) set system vlan on

>>set system vlan on Turn on VLAN function.

(P) set system vlan off

>>set system vlan off Turn off VLAN function.

(Q) set system vlan vid 1

>>set system vlan vid 1 Set VLAN ID OK

(R) set system name

>>set system name Press new device name: M510

"SET TIME" COMMAND

Main command	Sub command	Example	Command description
set	time	set time	Set device clock

EXAMPLE

(A) set time

```
>> set time

Current time : (GMT + 0) Mon Apr 18 10:57:15 2005

Specify year [ 2000 - 2099 ] :

Specify month [ 1 - 12 ] :

Specify date [ 1 - 31 ] :

Specify hour [ 0 - 23 ] :

Specify minute [ 0 - 59 ] :

Specify second [ 0 - 59 ] :

Specify timezone [ -12 to +12 ] :
```

Change time successfully ! Current time : (GMT + 0) Mon Apr 18 10:57:43 2005 DST time : (GMT + 0) Mon Apr 18 10:57:43 2005 System duration: 0 days 1:9:1

"SET STATE" COMMAND

Prefix	2 nd command	Example	Command description
set state	inline	Set state inline	Set ISG to execute normally based on its configured policy
	Monitor	Set state monitor	ISG only inspects and keep logs does not drop packets or disconnects on its own accord
	Bypass	Set state bypass	ISG will transmit all received packets to work on another port unconditionally, which can be regarded as bridge mode.
	Span	Set state span	ISG accept packets mirrored from hub or switch mirror port and is able to reset network connection; two connection ports of ISG work at this time.

EXAMPLE

(A) set state inline

>> set state inline Set system state to In-Line mode.

(B) set state monitor

>> set state monitor Set system state to MONITOR mode.

(C) set state bypass

>> set state bypass Set system state to BYPASS mode.

(D) set state span

>> set state span Set system state to SPAN mode.

"SET REMOTE" COMMAND

Prefix command	2nd command	3rd command	Postfix command	Command description
		wan		Enable remote access using browser from wan port
		lan	Enable remote access u browser from lan port	Enable remote access using browser from lan port
set remote	access	all		Enable remote access using browser from wan and lan port
		disable		Disable remote access using browser
nttp		1	xxx.xxx.xxx	Assign specify IP can use browser to remote access
	ір	2		
		3		device
		1		Accian specify subpet mask
	mask	2	xxx.xxx.xxx.xxx	can use browser to remote
	3	3		access device

Prefix command	2nd command	3rd command	Postfix command	Command description
	access	wan		Enable remote access using SSH from wan port
		lan		Enable remote access using SSH from lan port
		all		Enable remote access using SSH from wan and lan port
set remote		disable		Disable remote access using SSH
ssh	ip	1	xxx.xxx.xxx	Assign specify IP can use SSH to remote access device
		2		
		3		
r		1		Assign specify subnet mask can use SSH to remote access device
	mask 2 3	2	xxx.xxx.xxx.xxx	
		3		

EXAMPLE

(A) set remote http access wan

>> set remote http access wan Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(B) set remote http access lan

>> set remote http access lan Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(C) set remote http access all

>> set remote http access all Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(D) set remote http access disable

>> set remote http access disable Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(E) set remote http ip 1 192.168.1.230

>> set remote http ip 1 192.168.1.230 Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(F) set remote http mask 1 255.255.255.0

>> set remote http mask 1 255.255.255.0 Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(G) set remote ssh access wan

>> set remote ssh access wan Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(H) set remote ssh access lan

>> set remote ssh access lanDo you want to apply this setting immediately?Your current ssh/http connection will be cut off. (y/n)

(I) set remote ssh access all

>> set remote ssh access all Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(J) set remote ssh access disable

>> set remote ssh access disable Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(K) set remote ssh ip 1 192.168.1.230

>> set remote ssh ip 1 192.168.1.230 Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

(L) set remote ssh mask 1 255.255.255.0

>> set remote ssh mask 1 255.255.255.0 Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

"SET INTERFACE" COMMAND

Main command	Sub command	Command description
set	interface	Set interface link mode

EXAMPLE

(A) set interface

>> set interface Interface. WAN: auto LAN: auto

Setup WAN port configuration : Specify auto mode or speed [auto / 10 / 100] : Specify stealth mode [on / off] : Setup LAN port configuration : Specify auto mode or speed [auto / 10 / 100] : Specify stealth mode [on / off] :

Do you want to apply this setting immediately? Your current ssh/http connection will be cut off. (y/n)

History Command

This command will display all commands which you have used.

Main command	Sub command	Example	Command description
history	none	history	Display all commands which you have used

EXAMPLE

(A) history

- >> history
- 1 : get system
- 2 : history

Exit Command

Use this command to exit command shell.

Main command	Sub command	Example	Command description
exit	none	exit	Exit command shell

EXAMPLE

(A) exit

>> exit Logout Welcome to D-Link DFL-M510 Console Environment Copyright (C) 2005 D-Link Corp. <www.dlink.com> DFL-M510 login:

Reboot Command

Use this command to reboot system.

Main command	Sub command	Example	Command description
reboot	none	reboot	Reboot system, type "y" to reboot the system.

EXAMPLE

(A) exit

>> reboot Are you sure to reboot system? (y/n)

Reset Command

Use this command to reset system configuration to default settings.

Main command	Sub command	Example	Command description
reset	none	reset	Reset system configuration to default settings, type "y" to load default setting.

EXAMPLE

(A) reset

>> reset

This will set the system configuration to the default values, and then reboot the system.

Continue? (y/n)

Ping Command

Use this command to reset system configuration to default settings.

Main command	Sub command	Example	Command description
ping	xxx.xxx.xxx	Ping 168.95.192.1	Send ICMP echo request messages

EXAMPLE

(A) ping

>> ping 192.168.80.243 PING 192.168.80.243 (168.95.192.1) : 56 data bytes --- 168.95.192.1 ping statistics ---1 packets transmitted, 1 packets received, 0% packet loss Round-trip min/avg/max = 2.2/2.2/2.2 ms

APPENDIX B: GLOSSARY

Bandwidth

The transmission capacity of a given device or network

Bit

A Binary Digit (either a one or a zero); a single digit number in base-2. A bit is the smallest unit of computerized data.

Bridge

A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet.

Browser

A browser is an application program that provide a way to look at and interact with all the information on the World Wide Web

CLI (Command Line Interface)

In this interface, you can use line commands to configure the device or perform advanced device diagnostics and troubleshooting.

Console

This is a device (usually a computer) that you use to manage a networking device via a serial port (RS232) connection.

Crossover Cable

A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.

DNS (Domain Name System)

Domain Name System links names to IP addresses. When you access Web sites on the Internet you can type the IP address of the site or the DNS name.

Domain Name

The unique name that identifies an Internet site. Domain Names always have two or more parts that are separated by dots. The part on the left is the most specific and the part on the right is the most general.

Ethernet

A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.

Events

These are network activities. Some activities are direct attacks on your system, while others might be depending on the circumstances. Therefore, any activity, regardless of severity is called an event. An event may or may not be a direct attack on your system.

FCC (Federal Communications Commission)

The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.

Firewall

A hardware or software "wall" that restricts access in and out of a network. Firewalls are most often used to separate an internal LAN or WAN from the Internet.

Flash memory

A nonvolatile storage device that can be electrically erased and reprogrammed so that data can be stored, booted and rewritten as necessary.

FTP (File Transfer Protocol)

File Transfer Protocol is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

Gateway

A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages and/or architecture.

HTTP (Hyper Text Transfer Protocol)

The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certain kinds of attacks.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer)

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

ICMP (Internet Control Message Protocol)

A message control and error-reporting protocol between a host server and a gateway to the Internet ICMP uses Internet Protocol (IP) datagram, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.

IM (Instant Messaging)

IM (Instant Messaging) refers to chat applications. Chat is real-time, text-based communication between two or more users via networked-connected devices.

IP (Internet Protocol)

(Currently IP version 4 or IPv4) The underlying protocol for routing packets on the Internet and other TCP/IP-based networks.

IRC (Internet Relay Chat)

It is a way for multiple users on a system to "chat" over the network.

ISP (Internet Service Providers)

Provide connections into the Internet for home users and businesses. There are local, regional, national, and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.

LAN (Local Area Network)

A shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. LANs have different topologies, the most common being the linear bus and the star configuration.

Logs

Logs are device information that a device is scheduled to send out.

NAT (Network Address Translation)

The translation of an Internet Protocol address used within one network to a different IP address known within another network.

Network

Any time you connect two or more computers together, allowing them to share resources, you have a computer network. Connect two or more networks together and you have an internet.

NIC (Network Interface Card)

A board that provides network communication capabilities to and from a computer system. Also called an adapter.

P2P (Peer-To-Peer)

Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server.

Packet Filter

A filter that scans packets and decides whether to let them through or not.

Port

An Internet port refers to a number that is part of a URL, appearing after a colon (:), directly following the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, for example, Web servers normally listen on port 80.

Protocol

A "language" for communicating on a network. Protocols are sets of standards or rules used to define, format and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.

Router

A device that connects two networks together. Routers monitor, direct and filter information that passes between these networks.

RS-232

RS-232 is an EIA standard which is the most common way of linking data devices together.

Server

A computer, or a software package, that provides a specific kind of service to client software running on other computers.

SSL (Secured Socket Layer)

Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP Address that you entered. You do not need to change the computer subnet mask unless you are instructed to do so.

Switch

A layer-2 network device that selects a path or circuit to send a data packet through.

TCP (Transmission Control Protocol)

TCP is a connection-oriented transport service that ensures the reliability of message delivery. It verifies that messages and data were received.

Telnet

Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Terminal

A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard, display screen and some simple circuitry.

TFTP (Trivial File Transfer Protocol)

TFTP is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).

Transparent Firewall

A transparent firewall, also known as a bridge firewall, is a device that can act as a bridge and also filter/inspect packets. You do not have to change other network settings when you add a transparent firewall to the network.
URL (Uniform Resource Locator)

URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. A URL is basically a pointer to the location of an object.

WAN (Wide Area Networks)

WANs link geographically dispersed offices in other cities or around the globe including switched and permanent telephone circuits, terrestrial radio systems and satellite systems.

APPENDIX C: FEATURES AND SPECIFICATIONS

Hardware Specification

Ethernet	2 x 10/100 M auto-sensing auto-crossing with frog light
Other port	RS232(9 pin)
LCD Module	Blue background with white light LCD Panel
Power	AC LINE 100-240V AC 50-60Hz 0.8A MAX
Dimension (L*D*H, mm)	440mm * 250mm * 44mm

Features Specification

Application Detection / Prevention / Management

Application Class	Application Type	Application Name	Control Points
1. Message Exchange	*Instant Messengers (IM)	 MSN Yahoo Messenger ICQ AIM QQ IChat (MAC) Odigo Trillian 	 Login Send/Receive Message Send File File Type/Name/Size Receive File VoIP Establishment Video Establishment White Board
2. Internet File Sharing	*Peer-to-Peer (P2P)	 EzPeer eDonkey Skype eMule Kazaa Limwire BitTorrent Grokster Gnutella Shareaza 	Establishment 1. Connection Establishment

			11.	Morpheus		
			12.	WimMX		
3.	Web Application Control	Web Browser (HTTP/HTML) Java Applet /ActiveX Application	 1. 2. 3. 4. 5. 6. 7. 1. 2. 	Web Mail Web Uploading Web Download Web Posting Web IM Web URL Filter Web Content Anti-WebPage Kidnap Webpage	1. 2. 3. 4. 5. 6. 7. 1.	Login Post/Put Upload Download URL Keyword Cookie Retrieval ActiveX/Java Applet Download
4.	File	*FTP	1.	FTP Applications	1.	Login/Password
	Transfer		2.	FlashGet	2.	Download File
			3.	GetRight	3.	Upload File
			4.	NetTranport		
5.	Media	*Streaming Media	1.	Media Player	1.	Connection
			2.	RealOne		Establishment
			3.	Winamp		
		Internet Audio	Rad	lio on line	1.	Connection
6	Mail	SMTP			1.	Restricted "mail from" Address
					2.	Restricted "rcpt to"
		POP3			Log	in/Password
		IMAP4			Log	in/Password
		Mail Content			Key	word Matching
Intranet Illegal Agent		*Illegal Intranet-Internet Tunnel	1.	SoftEther	Connection Establishment	
		Spyware			Bloo Info	ck Outgoing rmation
		*Backdoor / Trojan	1. 2.	Backorifice Subseven	Der Hac	y Replying to ker
Trou	ubleshooting	Victim	1.	Worm affected	Det	ect affected packet

Helper	Identification		Hosts	generated by Victim
		2.	Trojan affected Hosts	
		3.	Spyware/ADware affected Hosts	
		4.	Intruded Hosts	

LCM Module

Main Menu	Sub-Menu	Description	
Device Status	System Info.	Firmware Ver	
		Policy Ver	
		Policy Number	
		Current Date	
		Current Time	
		Dev. Up Time	
		CPU Load	
		Memory Usage	
		Current Session	
	Traffic Info.	WAN RX	
		WAN Drop	
		LAN RX	
		LAN Drop	
		Traffic Level	
	Alert Monitor	Traffic Alert	
Device Config	IP Info,	Device Name	
		IP Address	
		IP Mask	
		Gateway IP	
		DNS IP	
		Operation Mode	
	Interface Info.	LAN Link Mode	
		LAN Stealth	

		WAN Link Mode
		WAN Stealth
Reset	Reset Confirm	
Reboot	Reboot Confirm	

Other Specifications

Performance: 30-40 Mbps (All function enabled), Wires peed for L3 switching Concurrent Users: 150 Concurrent TCP Sessions: 4,000

Mechanic & ID Design Front LED indicators

Function	Naming	Color	Status	LED description
Power	Power	Green	Off	Power off
			On	Power on
System	System	Green	Off	Power off (System not ready)
			On	System ready and running ok
Rypace	Bypass Bypass	Red	Off	System bypass not enable
Bypass			On	System bypass or failed
Inbound (left)	Inbound (LAN)	Green	Off	Ethernet link ok, and the speed is 10Mbps
			On	Ethernet link ok, and the speed is 100Mbps
	nbound right)	Yellow	Off	No packet forwarding
Inbound (right)			ON	Link
			Blinking	Act
Outbound (left)	Outbound (WAN)	Green	Off	Ethernet link ok, and the speed is 10 Mbps
			On	Ethernet link ok, and the speed is 100Mbps
Outbound			Off	No packets Send/Receive
(right)		Yellow	On	Link
			Blinking	Act

Physical Environment

Power

~ 25W Open Frame Switching Power Supply, Input AC range 100 ~ 240V 50/60Hz.

Operation Temperature 0-60

Storage Temperature

-20 – 70

Humidity Operation: 10%~90% RH Storage: 5%~90% RH

INDEX

А

Active schedule, template 64 Administrator, email notification 25 Application block, new 102 Application blocking, supported 100 Assign Policy tab 66

В

Bypass zone, DMZ 33 Bypass, hosts/groups 35

С

Command line interface 105 Common network protocol 82 Configuring, Command Line Interface 3 Configuring, Web-based Interface 7

D

Date and time, adjust 21

E

EIM 83

F

Front view 1

Н

Heath checking 82 Host database, exporting 50 Host, adding 49 Hosts, assigning to groups 53 HTTP/SSH, remote management 30

I

Interface tab 28

Κ

Keyword content, template 65 Keyword filter 76

L

LCM Button Description 2 Log tab 94 Log, searching for 95 Logging on the DFL-M510 7 Logs, navigating 95

Μ

Maintenance screen 39

Ν

Network analysis 84 Network screen 23 Network Setting tab 23 Network, status 98

0

Operation mode, inline, bypass, monitor 32

Ρ

Parameter tab 32 Pattern, user defined 68 Policy rule, by server 71 Policy rule, defining 69 Policy screen 55 Policy Setting screen 58 Policy Status tab 100 Policy Viewer tab 68 Policy, how to assign 66 Popup messages, editing 74 Ports, speed 29 Ports, stealth mode 29

R

Real Time Application, monitoring 81 Real Time Monitor screen 79 Real Time Traffic, monitoring 80 Rear View 3 Remote Access tab 29 Report tab 92 Report, interactive 92

S

Schedule screen 72 Server access, configuring 27 Server access, configuring for SSH 30 Setup Groups tab 51 Setup Wizard, run 10 SNMP, configuring 26 Status LEDs 2 System Screen 15 System, status 99

Т

Template Setting tab 63 Template wizard, running 56 Template, options 63