D-Link®

DFL-2100 / DFL-2400

Intrusion Detection System

User Manual

First Edition (December 2002)

Printed In Taiwan

RECYCLABLE

1. Limited Warranty

Hardware:

D-Link warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following periods measured from date of purchase from D-Link or its Authorized Reseller:

Product Type	Warranty Period
Complete products	One year
Spare parts and spare kits	90 days

The one-year period of warranty on complete products applies on condition that the product's Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. Failing such timely registration of purchase, the warranty period shall be limited to 90 days.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid; D-Link will ordinarily reimburse Purchaser for mailing/shipping/insurance expenses incurred for return of defective product in accordance with this warranty. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product, which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

LIMITATION OF WARRANTIES

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An addresses/
telephone/fax list of D-Link offices is provided in the back of this manual.

Trademarks

Copyright Statement

FCC Warning

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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

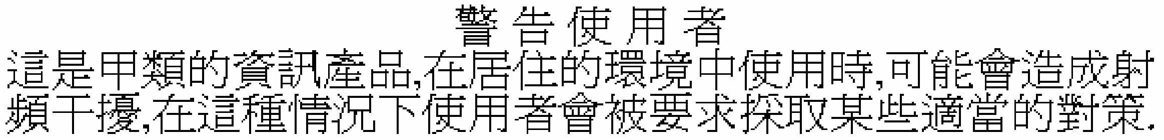
Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

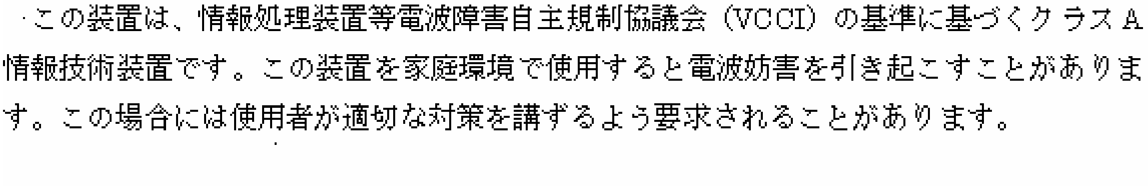
BSMI Warning



警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,在這種情況下使用者會被要求採取某些適當的對策.

VCCI A Warning



この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Table of Contents

ABOUT THIS GUIDE

This User Manual provides instruction for installing and manager the DFL-2100/DFL-2400 and Policy Server. The first will show how to connect DFL-2100/DFL-2400 with other Network equipments and Networks. The latter is a description for manager DFL-2100/DFL-2400 via Policy Server to make sure the intrusion detection system will protect your network and servers.

Overview of this User Manual

- Chapter 1, *Introduction*. Describes the Intrusion Detection System and its features.
- Chapter 2, *Installation and Initial Setup*. Helps you get started with the basic installation of the IDS.
- Chapter 3, *IDS Command Shell*. Describes the IDS Command mode and shell functions.
- Chapter 4, *IDS Management System*. A more detailed discussion of some of the management features of the IDS including, device management, Policy management, User management.
- Chapter 5, *Policy base IDS.* Talk about what is a policy?
- Chapter 6, *Define Your Own Defense Policy.* A more detailed discussion of the policy.
- Chapter 7, *Policy Definition Process.* A more detailed discussion of some of the management features of the Policy including, Address book, Group book, and Service book.
- Chapter 8, *IDS Reporting System.* Describes the advance reporting system, including the real time attack monitor, real time traffic monitor, attack events search and graph report.

1

INTRODUCTION

What is DFL-2100/DFL-2400?

DFL-2100/DFL-2400 is an active and on-line Network-based Intrusion Detection System (NIDS). Its responsibility is to detect malicious and suspicious packets on computer network and take actions in real time. It analyzes the incoming and outgoing packets with a mixed approach combined with misused and anomaly model. With this hybrid mechanism, DFL-2100/DFL-2400 can detect unknown type packet flooding and extend the ability to detect new pattern-based attack type easily, since a flexible rule-set is provided that new policies can be added easily. DFL-2100/DFL-2400 is built on real-time OS equipped with high performance appliance enables us to do much more than other software-based IDS.

Key Features

- Real-time detection and reaction:
  - Detect the validity of packets in great performance
  - The ability of instant traffic control: block packets, cut off connections, generate alarm and log suspicious packets.
  - Complete packet inspection.
- Robustness:
  - Based on dedicated Real-Time OS with strengthen TCP/IP protocol stack, DFL-2100/DFL-2400 minimizes the risk of being attacked and maximizes the durability.
- Policy based detection and access control:
  - Policy based detection rules with schedule function support.
  - Prioritized Policy.
  - Bi-directional detection and protection.
  - Layer 3 and Layer 4 are under control, and specially enhance the URL detection and access control.
- Manageability:
  - Web based management interface: the administrator can take advantage of the simplicity of user interface to manage DFL-2100/DFL-2400
  - Using policy server, administrators can control DFL-2100/DFL-2400 anywhere anytime via web browser.
  - Standard RS232 console port.
  - Remote Telnet control support.
  - SNMP aware.
  - Remote kernel updates support.
- Extensibility:

  - Within built-in anomaly detection model, DFL-2100/DFL-2400 can detect potential attacks.
  - By taking advantage of flexible policies, DFL-2100/DFL-2400 can be updated to detect new attack instantly that reduces the exposure time of attack cycle.
- Reporting feature:
  - Organized reporting and event trace back provides a clear view of what happened on the network.
  - Long-term events management.
  - Logged packet header decoding.
  - Template based printing function that fits the need of different level of management.

Network Architecture

DFL-2100/DFL-2400 is a transparent device and it does not change the network architecture. A Policy Server with DFL-2100/DFL-2400 Management System and DFL-2100/ DFL-2400 Reporting System provides a very friendly user-interface to configure DFL-2100/DFL-2400. Administrators could use DFL-2100/ DFL-2400 Management System to set up some policies for their network architecture. Policy server can manages multiple DFL-2100/DFL-2400s concurrently, and receive system logs, attack events from DFL-2100/DFL-2400s.

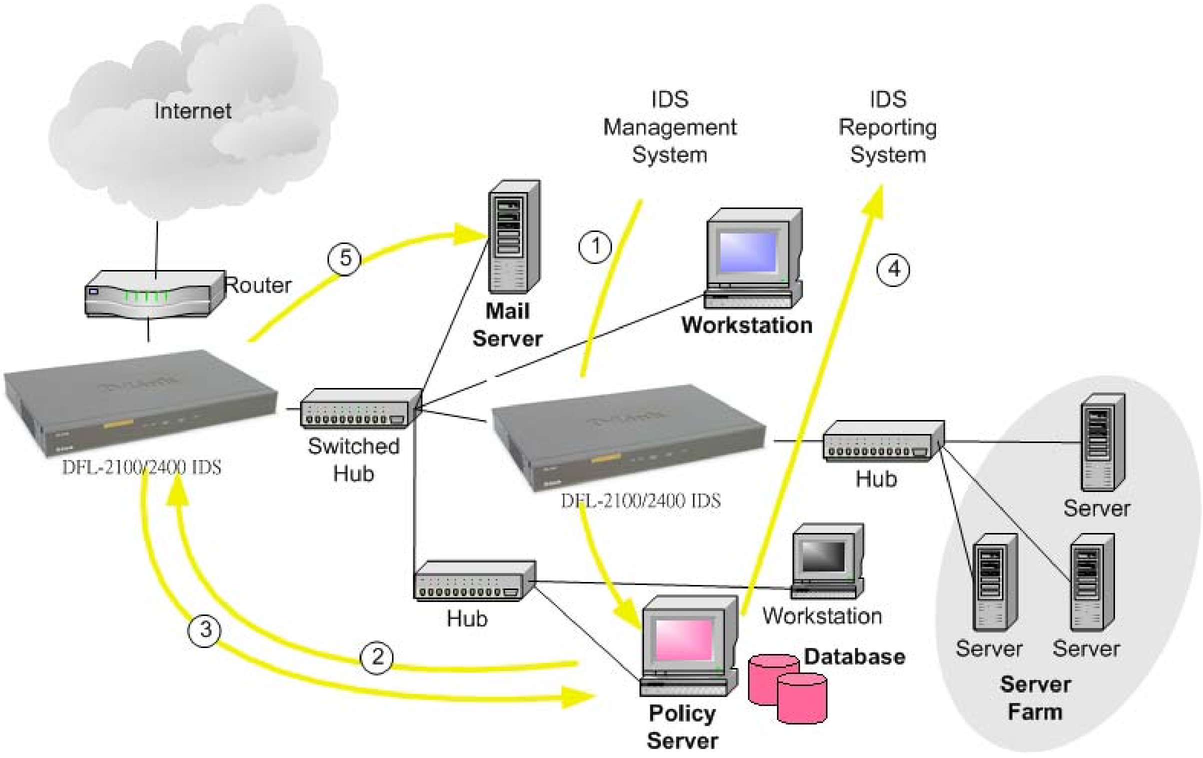


Figure 1-1: DFL-2100/DFL-2400 IDS Network Architecture

The DFL-2100/DFL-2400 Family

The DFL-2100/DFL-2400 Family consists of the following products:

- The DFL-2100 is a hardware and software solution that is optimized for medium sites. The DFL-2100 supports wire-speed Network Intrusion Detect, and can accept up to 8,000 simultaneous connections.
- The DFL-2400 is a high performance system that is optimized for supporting larger sized network configurations. The DFL-2400 supports wire-speed Network Intrusion Detect, and can support 128,000 simultaneous connections.

2

INSTALLATION AND INITIAL SETUP

Install DFL-2100/DFL-2400

Connecting the DFL-2100/DFL-2400 to the Network

Hardware install

A DFL-2100/DFL-2400 unit can be mounted in a standard 19-inch equipment rack or on a desktop or shelf. Mount the device onto the rack, using four rack-mounting screws.

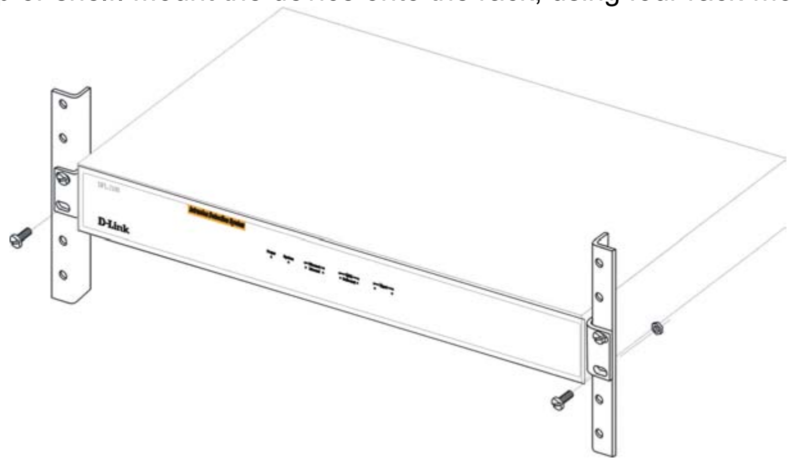


Figure 2-1：Installing the DFL-2100/DFL-2400 onto a rack

Check the target device

- ♦ Network Devices (like switching router, switch, hub...)
  If DFL-2100/DFL-2400 connects with Network Devices, generally you use “through” UTP patch core.
- ♦ CPE (like router, Desktop PC, notebook…)
  If DFL-2100/DFL-2400 connects to CPE devices, you must use “cross-over” line (included with the device)

Attach the line to the backend of the DFL-2100/DFL-2400

The DFL-2100/DFL-2400 comes standard with three 10/100 Half/Full duplex Ethernet interfaces. Since the DFL-2100/DFL-2400 is placed on the internal side of your access router, the DFL-2100/DFL-2400 will have three ports: “Ethernet”, “WAN” and “Manager”. The “Ethernet” port of the DFL-2100/DFL-2400 is the side that interfaces to your LAN. The “WAN” port of the DFL-2100/DFL-2400 is the side that interfaces to the WAN side of your network via your access router. The “Manager” port of the DFL-2100/DFL-2400 is the safety connection with Policy Server.

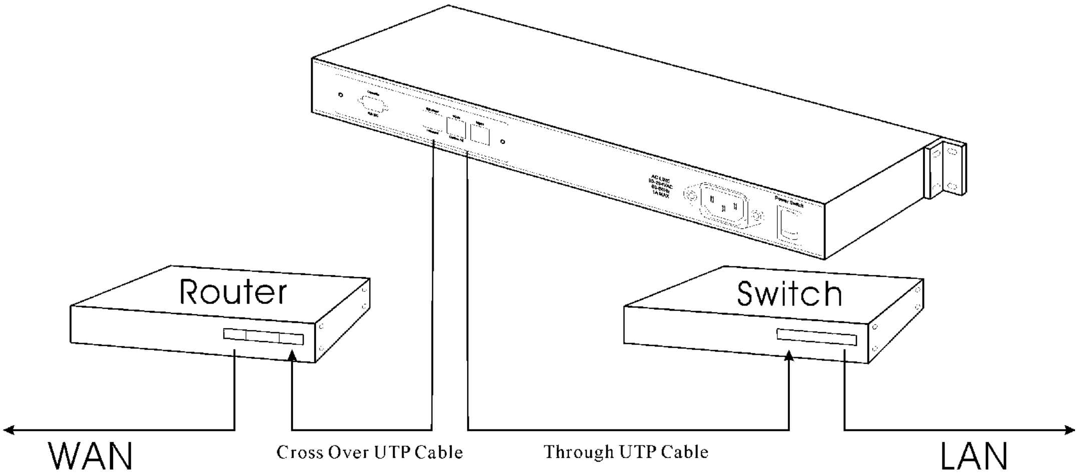


Figure 2-2：Cable Connection

Install Policy Server Software

Policy Server Hardware and Operating System Requirement

Before install the DFL-2100/DFL-2400 Policy Server, we must understand a few points about the DFL-2100/DFL-2400 Policy Server.

- The Operation System should be Windows 2000, Windows XP or Windows NT with service pack 6.0 and above.
- The host can support Internet access.
- DFL-2100/DFL-2400 will send log data to Policy Server and Policy Server will save it in hard disk. Therefore, your hard disk may have 30G free space.
- We suggest that your CPU would be Pentium III 1000 and memory would be 256 MB or more.

Installation Procedure

Step 0. Install NT service pack 6.0
Step 1. Install Policy Server
  Step 1-1 Install Java Run Time Environment（JRE）
  Step 1-2 Install MySQL database server
  Step 1-3 Install Apache Web server for Win32
  Step 1-4 Install Policy Server software
Step 2. Auto Configuration
Step 3. Close and reboot

Note: The detail installation describe can refer to “Quick Installation Guide”

Configure the DFL-2100/DFL-2400

Before you can begin to manage the DFL-2100/DFL-2400 device (i.e. protect your network and servers), it must first be initialized. This procedure is accomplished through the DFL-2100/DFL-2400 Command Shell, which resides in the DFL-2100/DFL-2400 device. Access to the Command Shell can be made either through SSH or from a terminal (or terminal emulator) connected directly to the DFL-2100/DFL-2400 device. These methods are described below.

Starting the System

The Power on/off switch of the DFL-2100/DFL-2400 is located near the power cable. To start the system, switch it to the ON position. You will be prompted for a login ID and a password after the system is started.
The login ID is **admin** and the password is **DLink** (to change the password, see Change Password, on page 15)

Setting System Parameters

Once you have accessed the Command Shell with SSH or a terminal connection, press any key and the following prompt will appear:

```
Login as: admin
admin@192.168.168.201’s Password:
D-Link IDS -- Protect your network and servers!
```

1. Setting DFL-2100/DFL-2400 Device IP
   ```
   >> set system ip <IDS Device IP>
   ```

2. Setting DFL-2100/DFL-2400 Gateway IP
   ```
   >> set system gateway xxx.xxx.xxx.xxx
   ```
   (XXX.XXX.XXX.XXX is your gateway IP)

3. Setting DFL-2100/DFL-2400 Network mask
   ```
   >> set system mask xxx.xxx.xxx.xxx
   ```
   (xxx.xxx.xxx.xxx is your network mask)

4. Setting DFL-2100/DFL-2400 Policy Server IP
   ```
   >> set psserver ip <Policy Server IP>
   ```

Getting Started

Once you have completed the initial setup, as described in the previous chapter, you can now connect to the DFL-2100/DFL-2400 Policy Server and manage your DFL-2100/DFL-2400 via web browser.

Connect the DFL-2100/DFL-2400 Policy Server from browser

➢ Open your browser, and enter:
http://<IP Address of the Policy Server>:6592/IDS/

Policy Server Initial Screen

The Initial Screen of Policy Server is the first Web page that you will see when you connect to the DFL-2100/DFL-2400 Policy Server. This is the main screen for Policy Server; by clicking on a particular Manu Tab, you can start to use its respective functions:

Manager DFL-2100/DFL-2400 Management System; It allows users to manage one or more DFL-2100/DFL-2400 devices concurrently. (See DFL-2100/DFL-2400 Management System)

Get Certification Downloading the Certification files to your client machine to ensure that your browser will consider the DFL-2100/DFL-2400 Management System and Reporting System applets as “trusted”.

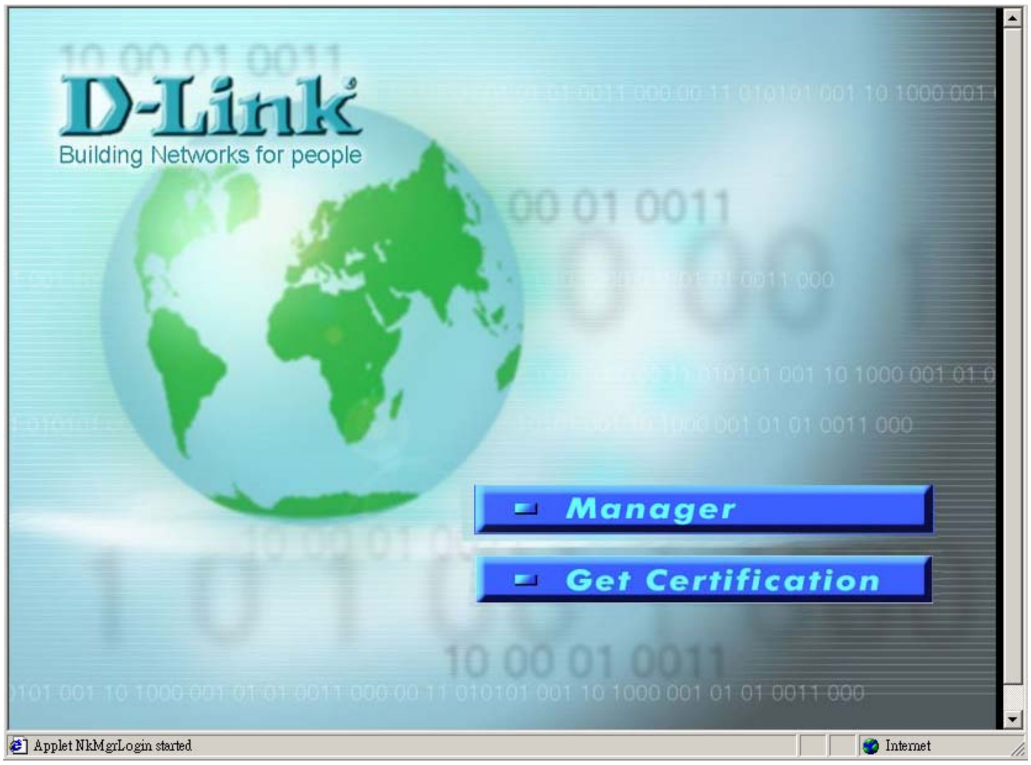


Figure 2-3: The DFL-2100/DFL-2400 Main Page

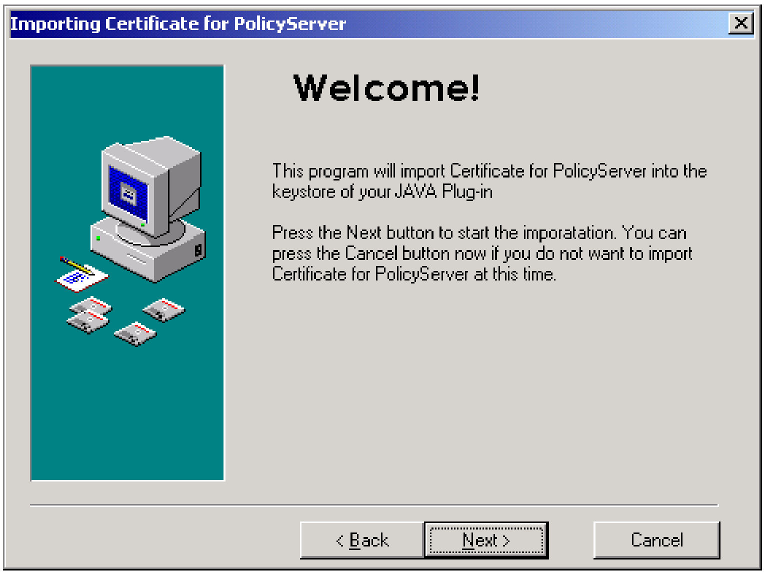
The Java Plug-In

The DFL-2100/DFL-2400 Management System and Reporting System run as Java applets with the assistance of Sun Microsystems Java Plug-in. You will install the Java Plug-in from the Policy Server automatically, when your browser connecting the Policy Server at the first time.

Getting Certification

Once you have completed the installation of the Java Plug-in, you must get certification.

To get the certification, click on “**Get Certification**” and it will install certification files automatically.



Welcome!

This program will import Certificate for PolicyServer into the keystore of your JAVA Plug-in

Press the Next button to start the imporatation. You can press the Cancel button now if you do not want to import Certificate for PolicyServer at this time.

Figure 2-4: Get Certification

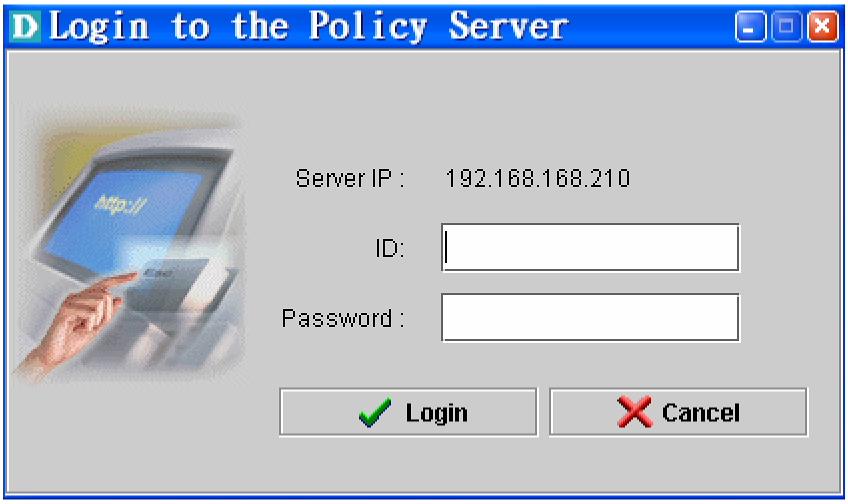
Once you have finished downloading the certification, you must restart your browser.

Manage your DFL-2100/DFL-2400

Start DFL-2100/DFL-2400 Management System

- Select Manager from the DFL-2100/DFL-2400 Main Page, the following login dialog will appear.
- Enter the Password and click Login to login to the DFL-2100/DFL-2400 Management main screen.

(Default ID: **admin**; password: **admin**)



Server IP : 192.168.168.210

ID:

Password :

Figure 2-5: DFL-2100/DFL-2400 Management System Login Screen

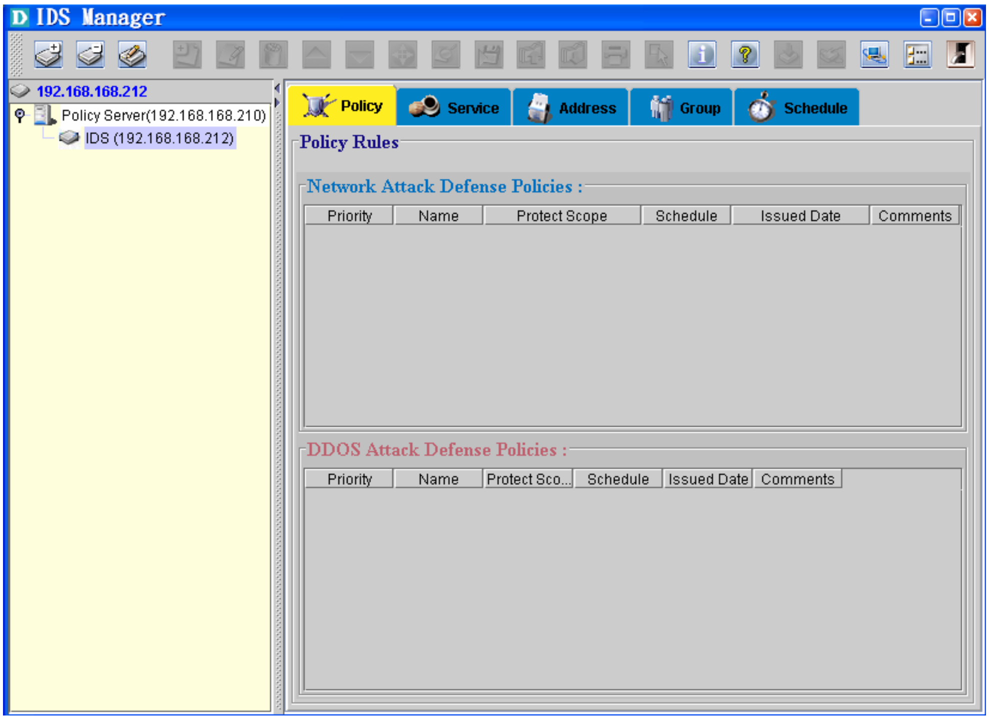
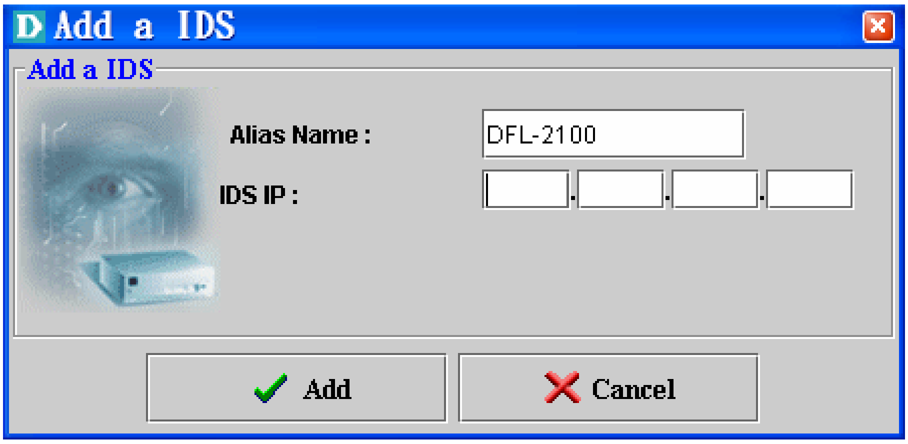


Figure 2-6: DFL-2100/DFL-2400 Management main screen

Add New DFL-2100/DFL-2400

1. Click Add DFL-2100/DFL-2400 button
2. Enter the Alias Name of the DFL-2100/DFL-2400.
3. Enter the IP of the DFL-2100/DFL-2400, which you want to add.
4. Click “Add” to add the DFL-2100/DFL-2400 device to the DFL-2100/DFL-2400 Tree.

5. Double click the device icon, which you add and you can manage the DFL-2100/DFL-2400 device.



Alias Name : DFL-2100

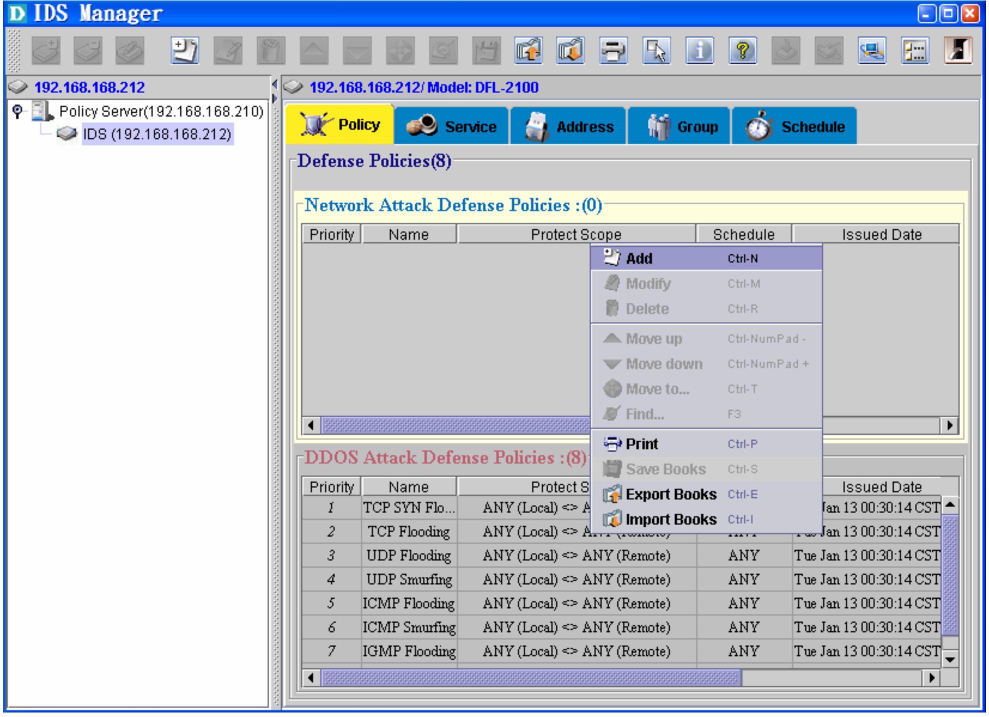
IDS IP : . . .

Figure 2-7: ” Add a DFL-2100/DFL-2400” Dialog

Load Newest Defense Policies

The policies are the most important information in the DFL-2100/DFL-2400 Management System. Policies indicate to DFL-2100/DFL-2400 how to detect an attack and how to response when an attack is detected. To start your DFL-2100/DFL-2400, you first need to load latest defense policies.

- ➢ Select “Add” button or click the right button of mouse on the Network attack Defense Policies window to add new policies.

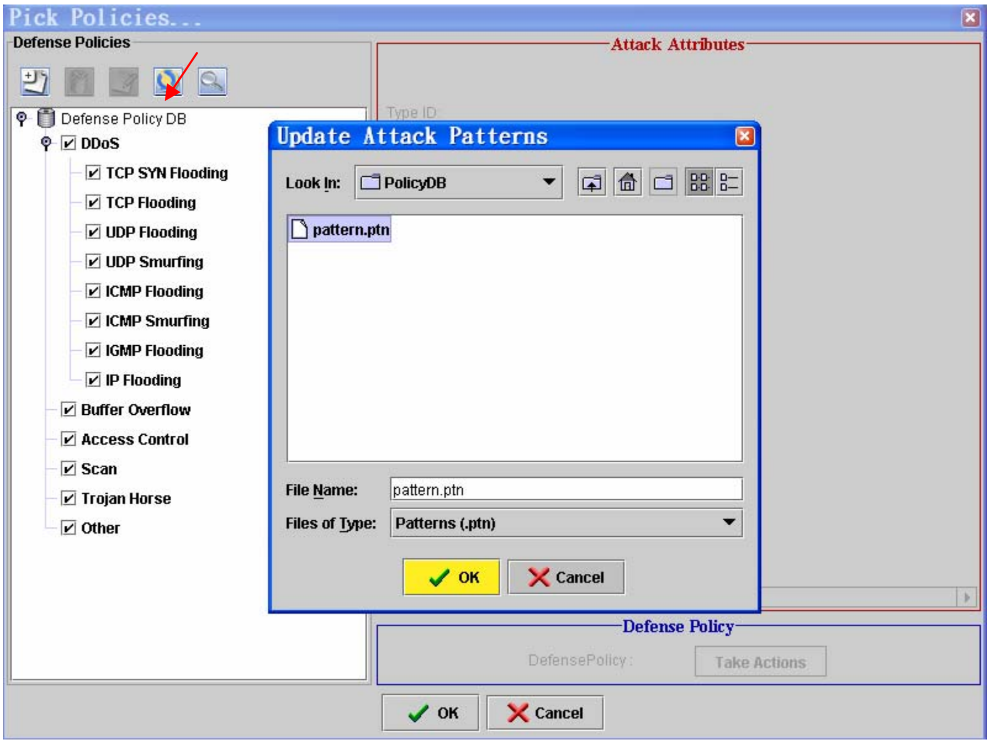


Priority	Name	Protect Scope	Schedule	Issued Date

Priority	Name	Protect S		Issued Date
1	TCP SYN Flo...	ANY (Local) <> A		Jan 13 00:30:14 CST
2	TCP Flooding	ANY (Local) <> A		Jan 13 00:30:14 CST
3	UDP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
4	UDP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
5	ICMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
6	ICMP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
7	IGMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST

Figure 2-8:” Add Policies” Dialog

- ➢ There is a default policy database on the DFL-2100/DFL-2400 Policy Server, administrator must select “Download latest attack pattern via network” to update latest pattern from Administrator Utility CD ~/Policy Server/PolicyDB/ policyXXX.ptn.



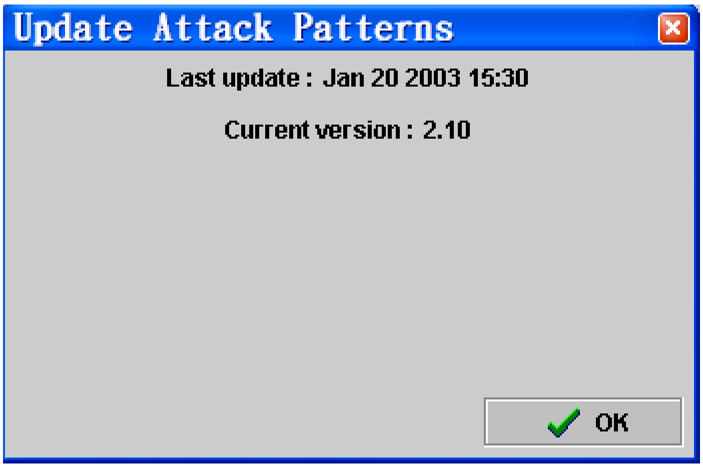
- ☑ DDoS
  - ☑ TCP SYN Flooding
  - ☑ TCP Flooding
  - ☑ UDP Flooding
  - ☑ UDP Smurfing
  - ☑ ICMP Flooding
  - ☑ ICMP Smurfing
  - ☑ IGMP Flooding
  - ☑ IP Flooding
- ☑ Buffer Overflow
- ☑ Access Control
- ☑ Scan
- ☑ Trojan Horse
- ☑ Other

File Name: pattern.ptn

Files of Type: Patterns (.ptn)

Figure 2-9: download latest attack pattern

➢ You can find new defense policies in the policy list when you finish the update.

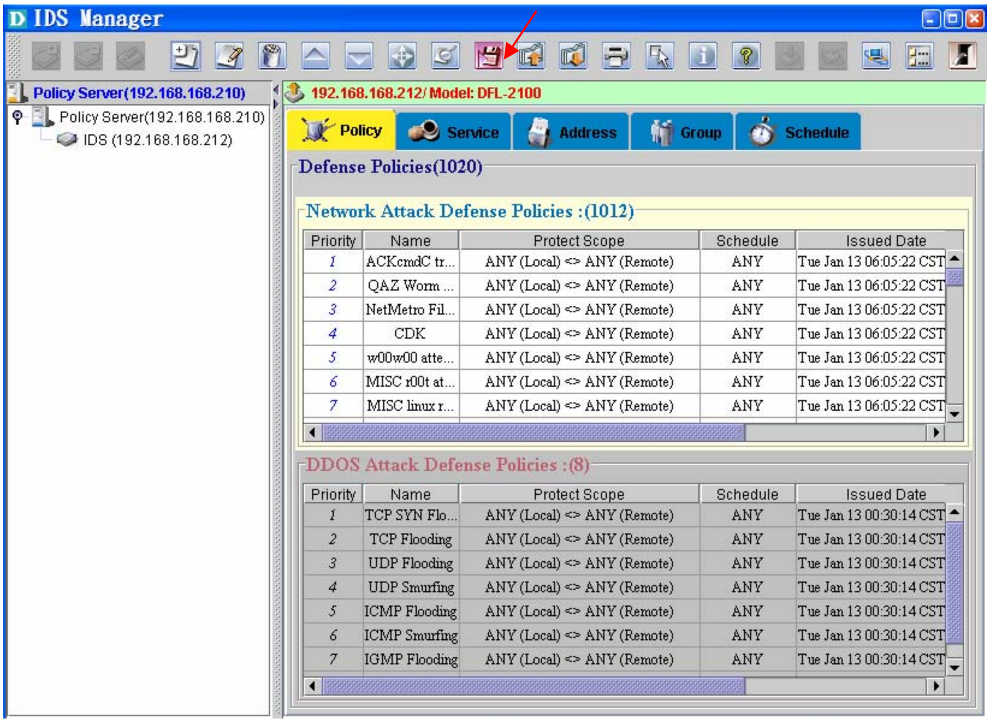


Last update : Jan 20 2003 15:30

Current version : 2.10

Figure 2-10: download latest attack pattern

➢ All the changes to the defense policies will not take effect until the red-lighted Confirm button is clicked.


IDS Manager
Policy Server(192.168.168.210)
Policy Server(192.168.168.210)
IDS (192.168.168.212)
192.168.168.212/ Model: DFL-2100
Policy
Service
Address
Group
Schedule

Defense Policies(1020)

Network Attack Defense Policies :(1012)

Priority	Name	Protect Scope	Schedule	Issued Date
1	ACKcmdC tr...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
2	QAZ Worm ...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
3	NetMetro Fil...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
4	CDK	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
5	w00w00 atte...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
6	MISC r00t at...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
7	MISC linux r...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST

DDOS Attack Defense Policies :(8)

Priority	Name	Protect Scope	Schedule	Issued Date
1	TCP SYN Flo...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
2	TCP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
3	UDP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
4	UDP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
5	ICMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
6	ICMP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
7	IGMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST

Figure 2-11: make sure the defense policies to take effect

Summary of Steps

In summary, you can make sure your DFL-2100/DFL-2400 have protected your servers and networks.

1. Connecting your DFL-2100/ DFL-2400 Policy Server via your browser.
2. Manage your DFL-2100/DFL-2400 via your Policy Server management windows.
3. Download the latest attack pattern and make sure the defense policies to take effect.

3

IDS COMMAND SHELL

DFL-2100/DFL-2400 Console/SSH System

The Console Service on DFL-2100/DFL-2400 provides a text mode interface for administrators to configure DFL-2100/DFL-2400 via RS-232 serial line. It runs as a shell, when legal commands are given, it performs the requested tasks.

And, the SSH Service do things like the console service do, actually, they use the same shell, but there are three points of difference.

i. SSH provides a mechanism that administrator can configure DFL-2100/DFL-2400 remotely via computer network.

ii. Since remote access is considered more risky than accessing from console, some functions are limited to the console service only. The list of limited functions will be showed in next section.

iii. For the sake of security, the SSH service can be suspended.

In security field, the common way to protect against brute-force password guess is increasing the delay time between login attempts. For the console service, it is not necessary. But for the SSH service, it is necessary. Thus, the SSH login attempt is confined to 3 times and 60 seconds. If the login failed over 3 times or the user hang on login procedure over 60 seconds, the SSH connection is cut-off and the resource is released.

Starting DFL-2100/DFL-2400 Command Shell

Once you have accessed the Command Shell with SSH or a Terminal connection, press any key and the following prompt will appear:

```
Login as: admin
IDS admin@192.168.168.201's Password:
D-Link IDS -- Protect your network and servers!
```

Please enter the login ID（Login：）and password（Password:）

(default login ID：**admin**；password：**DLink**)

Login successful user can see the prompt （user can key help or ? to get the setting information）

```
>>help
help   - This message.
get    - Get system information.
set    - Set system parameters.
ping   - Ping utility
arp    - Show & handle arp table.
netstat - Show system network status.
reset  - Reset system configurations to manufacturing defaults.
reboot - Reboot system.
>>
```

The Command Classes

All Commands are divided into four classes, **Help**, **Query**, **Set**, and **Miscellaneous**. The Commands in the 'Help' class are used to give user other command's information. The Commands in the 'Query' class are used by prefix command 'get' to retrieval system information and configuration. And the Commands in 'Set' class are used by prefix command 'set' to given parameters for system. Other functions not belonged to above two classes are in the 'Miscellaneous' class.

Help Command

The get command can display the arguments of others.

help get

Description: Use the help get command to display the arguments of "get command"

Syntax: help get

Arguments: none

Example:

```
>>help get
get    - Get system information. Available commands:
        system    - System configurations, including IP, password and etc.
        log       - System logs.
        time      - Device clock setting.
        interface  - Interface stealth function and working link mode.
        state      - Device operation state.
        psserver   - Policy server configurations.
        snmp      - snmp parameters.
```

help set

Description: Use the help set command to display the arguments of "set command"

Syntax: help set

Arguments: none

Example:

```
>>help set
set    - Set system parameters. Available commands:
        system    - System configurations, including IP, password and etc.
        time      - Device clock setting.
        interface  - Interface stealth function and working link mode.
        state     - Device operation state.
        psserver  - Policy server configurations.
        snmp      - snmp parameters.
>>
```

help ping

Description: Use the help ping command to display the arguments of “ping command”

Syntax: help ping

Arguments: none

Example:

```
>>help ping
ping   - Ping utility
>>
```

help arp

Description: Use the help arp command to display the arguments of “arp command”
Syntax: help arp
Arguments: none
Example:

```
>>help arp
arp    - Show & handle arp table.
>>
```

help netstat

Description: Use the help netstat command to display the arguments of “netstat command”
Syntax: help netstat
Arguments: none
Example:

```
>>help netstat
netstat- Show system network status.
```

help reset

Description: Use the help reset command to display the arguments of “reset command”
Syntax: help reset
Arguments: none
Example:

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

help reboot

Description: Use the help reboot command to display the arguments of “reboot command”
Syntax: help reboot
Arguments: none
Example:

```
>>help reboot

reboot - Reboot system.
```

Query Command

There are several query functions, and their command usage and description are illustrated in the following. All query functions are applicable to both console and telnet.

get

Description: Use the get command to display the arguments of “get command”
Syntax: get
Arguments: none
Example:

```
>>get

get    - Get system information. Available commands:

       system    - System configurations, including IP, password and etc.

       log       - System logs.

       time      - Device clock setting.

       interface  - Interface stealth function and working link mode.

       state     - Device operation state.

       psserver  - Policy server configurations.

       snmp      - snmp parameters.
```

get system

Description: Use the get system command to display the system information, include DFL-2100/DFL-2400 version, network states, policies, and DFL-2100/DFL-2400 status.
Syntax: get system
Arguments: none
Example:

```
>>get system

Version:  1.0.0 2002/12/20 Model: DFL-2100

Identification code: fbed2fe426fb392fed26e439

IDS IP Address:192.168.168. 201, netmask:255.255.255.0,
gateway:192.168.168.254
CPU utilization: 100%, free memory: 19MBytes
Current TCP connections: 3, TCP idle time limit: 1800 seconds
Maximum log number per second: 500
Detection parameters:
Maximum ping packet size: 100.
VPN bypass: off.  TCP state check bypass: off.
WCCP bypass: off. WCCP redirect IP :  0. 0. 0. 0
 Remote port: working policy number  861 < on> max ping  100.
 Local port:  working policy number  861 < on> max ping  100.
$>
```

get time

Description: Use the get time command to display the time information of DFL-2100/DFL-2400

Syntax: get time

Arguments: none

Example:

```
>>get time
Boot time: Thu Apr 11 15:21:35 2002 GMT +8.
Now time : Thu Apr 11 17:28:39 2002 GMT +8.
Up time  : 0 days, 2 hours, 7 minutes, 4 seconds.
>>
```

get log

Description: Use the get log command to display the log information of DFL-2100/DFL-2400

Syntax: get log

Arguments: none

Example:

```
>>get log
2002/05/16 19:53:05 U:SYS:Failed to open DDoS policy file!
2002/05/16 19:53:05 U:SYS:Failed to open policy file!
2002/05/16 19:53:05 I:SYS:DFL-2100/DFL-2400 startup!
2002/05/16 19:53:44 I:CON:Login OK!
2002/05/16 19:55:12 I:SSH:SSH user login from 192.168.168.65 OK!
---------------------------------------------------------------------------
 Event level  => I :Info, W : Warning, U : Urgent, F : Fatal
 Event source => CON : Console, SSH : SSH, SYS : System, PSS : Policy agent.
```

get interface

Description: Use the get interface command to display the interface information of DFL-2100/DFL-2400

Syntax: get interface

Arguments: none

Example:

```
>>get interface
Remote port:    AUTO    , MAC address  0:30:64: 1: 8: 2
Local port:     AUTO    , MAC address  0:d0:b7:b2:5f:ff
>>
```

get state

Description: Use the get state command to display the state information of DFL-2100/DFL-2400

Syntax: get log

Arguments: none

Example:

```
>>get state
State: NORMAL.
>>
```

get psserver

Description: Use the get psserver command to display the Policy Server's information, include IP Address and Log transfer interval time.

Syntax: get psserver

Arguments: none

Example:

```
>>get psserver
Policy server IP address : 192.168.168.160
Log transfer interval: 30 seconds
>>
```

get snmp

Description: Use the get snmp command to display the snmp information of DFL-2100/DFL-2400

Syntax: get snmp [system | community | trap]

Arguments:

system	Show the DFL-2100/DFL-2400's snmp information
community	Show the snmp network community setting
trap	Show the snmp trap information

Example:

```
>>get snmp
Options: [ system | community | trap ]
system:          Show SNMP System Information
```

```
community:     Show SNMP Community Setting
trap:               Show SNMP trap Information

>>get snmp system
SNMP Location: D-Link
SNMP Contact: service@dlink.com
SNMP Name: DFL-2100/DFL-2400

>>get snmp trap
SNMP Trap : Disable
SNMP Trap IP :   0.  0.  0.  0
$>get snmp community
SNMP Read-Only Community: public
SNMP Read-Write Community: private
SNMP Trap Community: SNMP_trap
```

Set Command

Use the set command to enter system configuration parameters. The usage and description are illustrated in the following. Some set functions are applicable to both console and telnet.

set

Description: Show the set command parameters and available commands
Syntax: set
Arguments: none
Example:

```
>>set
set    - Set system parameters. Available commands:
        system    - System configurations, including IP, password and etc.
        time      - Device clock setting.
        interface - Interface stealth function and working link mode.
        state     - Device operation state.
        psserver  - Policy server configurations.
        snmp      - snmp parameters.
>>
```

set system

Description: Use the set system command to configure DFL-2100/DFL-2400, include IP address, gateway, network musk and other information

Syntax: get system [ip | gateway | mask | passwd | rpasswd | detect | logmax]

Arguments:

ip <ip_address>
Set DFL-2100/DFL-2400 IP address

gateway <gateway_address>
The IP address of the router that forwards all traffic to the specified target address

mask<ip_mask>
Set DFL-2100/DFL-2400 network mask

passwd
Change the administrator password. If you change the password by console, you will change the console password. If you change the password by SSH, you will change the remote login password.

rpasswd
Change the remote login password. This command is applicable to console.

detect [tcptimeout|policy| pingmax|stateful | integrity | pinglen | wccp | vpnbypass]
Set the DFL-2100/DFL-2400 detect parameters

logmax <value:10-10000>
Set the DFL-2100/DFL-2400 can log event messages number.

Example:

Ex 1 :

```
>>set sys passwd


Change password...
Please type your current SSH passwd:
>>
```

Ex 2 :

```
>>set sys passwd


Change password...
Please type your current SSH passwd:
Please type your new passwd:
Please re-type your new passwd:
Password is changed successfully!
>>
```

Ex 3 :

```
>>set system ip
Need IP address: 000.000.000.000
>>
```

Ex 4 :

```
>>set sys logmax
```

```
Need value: 10 - 10000
>>set sys logmax 300
Change max log OK.
```

set system detect

Description: Use the set system detect command to configure DFL-2100/DFL-2400 intrusion detect parameters

Syntax: get system detect [tcptimeout|policy|pingmax|stateful | integrity | pinglen | wccp | vpnbypass] [ip | gateway | mask | passwd | rpasswd | detect | logmax]

Arguments:

tpctimeout <Value: 20-86400>	Set and modify the TCP connections timeout
policy <remote|local> <on|off>	Set and modify the policies work or not.
pingmax <remote|local> <Value:1-5000>	Allow how many users can ping a host in a second
stateful <on|off>	Checking the TCP state or not. Default setting is <off>.
integrity <on|off>	Checking the IP integrity or not. Default setting is <on>
pinglen <Value: 64-1500>	Set and modify the packet size of ping
wccp < bypass | redirect_ip >	Checking the WCCP packet or not , and specification the redirect host IP address.
vpnbypass < on | off >	Checking the VPN packet or not

Example:

Ex 1:

```
>>set system detect tcptimeout
Need value: 20-86400
>>set system detect tcptimeout 6000
Change TCP session time out limit to 6000 OK.
>>
```

Ex 2:

```
>>set system detect pingmax local
Need value : 1-5000
>>set system detect pingmax remote 3000
Change remote port maximum ping packet limit to 3000 OK.
```

Ex 3:

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

set time

Description: Use the set time command to set the system time on the DFL-2100/DFL-2400 Device

Syntax: set time

Arguments: none

Example:

```
>>set time
Current time  2002: 4:12 20:43:55 (GMT +8)
Specify year  [1980-2050] :
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!
```

set interface

Description: Use the set interface command to define the physical and logical interface settings for the DFL-2100/DFL-2400 Device

Syntax: set interface [link|stealth]

Arguments:

link <remote|local|manage><10|100|auto> <full|half>
Define the physical connection mode on the specified interface as auto sensing whether to operate at full or half duplex (as required by the device to which it is connected)

stealth <remote|local|manage>
Setting the stealth mode on the specified interface

Example:

```
 >>set interface
Need command: [ link | stealth ]
>>set int
Need command: [ link | stealth ]
```

set interface link

Description: Use the set interface link command to define the physical connection mode on the specified interface as auto sensing whether to operate at full or half duplex

Syntax: set interface link [remote|local|manage] [10|100|auto] [full|half]

Arguments:

<remote|local|manage>

remote — Specified remote(WAN) interface setting

local — Specified local(LAN) interface setting

manage — Specified manage interface setting

<10|100|auto>

10 — Set the physical connection at 10 Mbps

100 — Set the physical connection at 100 Mbps

auto — Setting the physical connection operate mode by auto sensing

<full|half>

full — Setting the physical connection operate mode at full duplex

half	Setting the physical connection operate mode at half duplex

Example:

```
>>set interface link

Need interface name : [remote | local | manage ]
```

Note This command is only applicable to console.

set interface stealth

Description: Use the set interface stealth command to set the stealth mode on the specified interface on the DFL-2100/DFL-2400 Device

Syntax: set interface stealth [remote|local|manage]

Arguments:

<remote|local|manage>

remote	Specified remote(WAN) interface setting
local	Specified local(LAN) interface setting
manage	Specified manage interface setting

Example:

```
>>set interface stealth remote

Need interface name: [ remote | local | manage ]
```

Note 1. This command is only applicable to console

set psserver

Description: Use the set psserver command to configure the Policy Server, which manage and log events for the DFL-2100/DFL-2400 Device

Syntax: set psserver [ip|interval]

Arguments:

ip <ip_address>	Set the Policy Server host IP
interval <value:10-600>	Configure the time interval of sending the events to the Policy Server.

Note: If Policy Server set behind the firewall, the IP address shouldn't the IP address of "real Policy Server". Please check your network status before you enter the IP address.

Example:

For example, A DFL-2100/DFL-2400 on the network 192.168.168.xxx and the Policy Server set behind the firewall at 10.0.0.xxx. The firewall or NAT must reconfigure a Virtual IP or Mapped IP for Policy Server. The DFL-2100/DFL-2400 set the Policy Server IP to the Virtual IP.

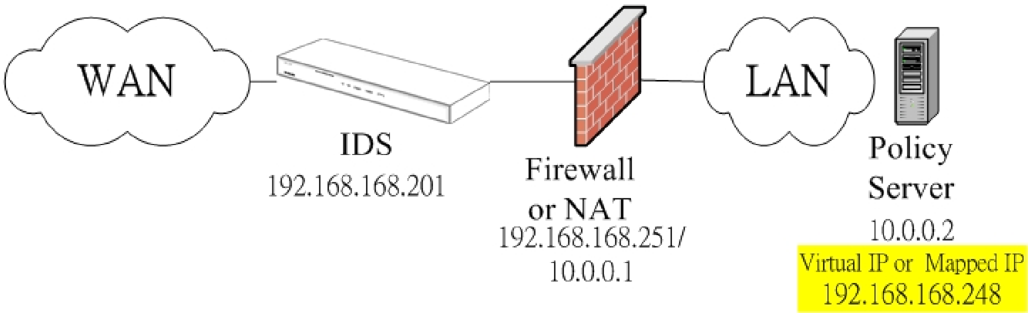


Figure 3-1: set policy server sample

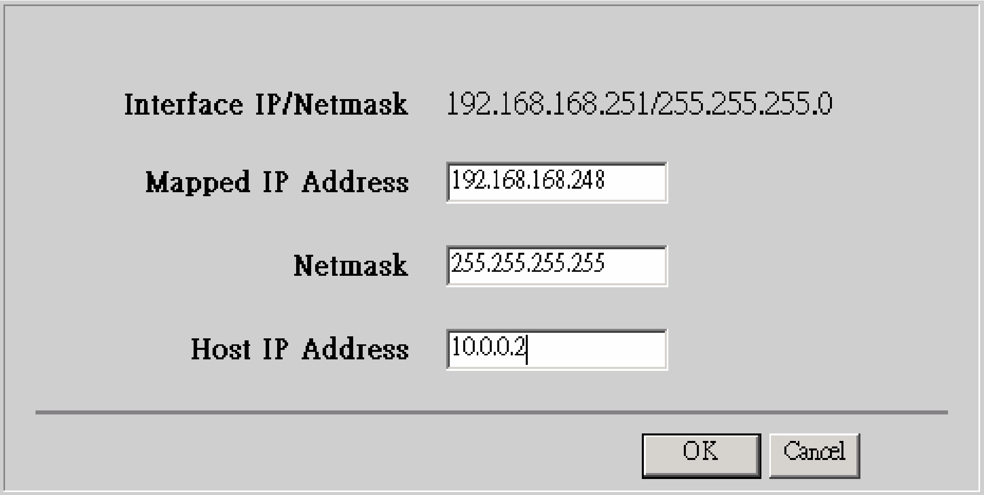
```
>>set psserver ip 192.168.168.248
```

The Firewall or NAT must reconfigure Port Mapping as :

192.168.168.248:7595	10.0.0.2:7595	TCP
192.168.168.248:7596	10.0.0.2:7596	UDP

Port 7595 and 7596 are private ports for DFL-2100/DFL-2400 Management System.

Firewall example: NetScreen



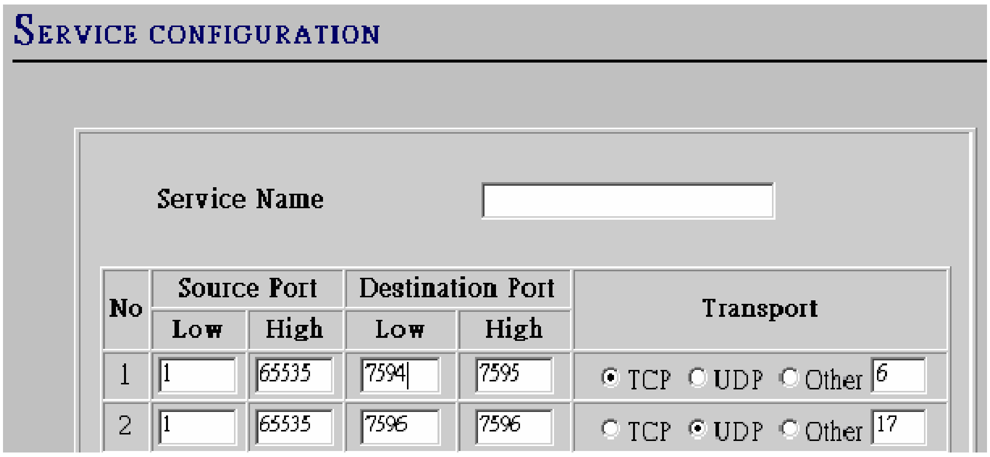
Interface IP/Netmask 192.168.168.251/255.255.255.0

Mapped IP Address 192.168.168.248

Netmask 255.255.255.255

Host IP Address 10.0.0.2

Figure 3-2: set policy server virtual IP sample

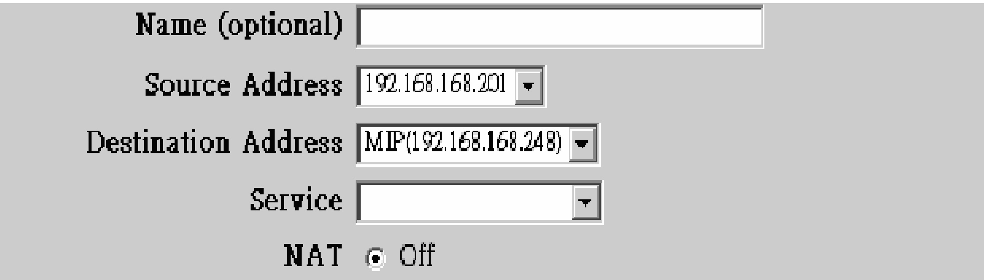


SERVICE CONFIGURATION

Service Name

No	Source Port		Destination Port		Transport
	Low	High	Low	High	
1	1	65535	7594	7595	● TCP ○ UDP ○ Other 6
2	1	65535	7596	7596	○ TCP ● UDP ○ Other 17

Figure 3-3: set private ports (service) for Policy Server



Name (optional):

Source Address: 192.168.168.201

Destination Address: MIP(192.168.168.248)

Service:

NAT: ● Off

Figure 3-4: firewall must open the private service for DFL-2100/DFL-2400

set state

Description: There are four states in DFL-2100/DFL-2400. ‘**Normal**’ means DFL-2100/DFL-2400 works normally according to given policies. ‘**Protect**’ means DFL-2100/DFL-2400 works like an access controller. It would let packets pass according to given policies. ‘**Stop**’ means DFL-2100/DFL-2400 would drop all the packets it receives. And ‘**Bypass**’ means DFL-2100/DFL-2400 would let all the packets pass through freely without any checks.

Syntax: set state [normal|protect|bypass|stop]

Arguments:

normal	Set DFL-2100/DFL-2400 works normally according to given policies
protect	Set DFL-2100/DFL-2400 works like an access controller
bypass	Set DFL-2100/DFL-2400 would let all the packets pass through freely without any checks
stop	Set DFL-2100/DFL-2400 drop all the packets it receives

Example:

Ex 1:

```
>>set state normal

Change system state to NORMAL mode.
```

Ex 2:

```
>>set state bypass

Change system state to BYPASS mode.
```

set snmp

Description: Use the set snmp command to configure the DFL-2100/DFL-2400 Device for Simple Network Management Protocol to gather statistical information from the DFL-2100/DFL-2400 device and receive notification when events of interest occur.

Syntax: set snmp [system | community | trap]

Arguments:

System<name>	Define the physical location, name and contract of the DFL-2100/DFL-2400
community < ro | rw | trap>	Defines the name and the permission for the SNMP community.

Trap<enable | disable | ip>	Enable or disable SNMP traps for the community. Define the IP address listen the trap.

Example:

```
>>set snmp trap
Need command: [ enable | disable | ip ]
>>
>>set snmp trap ip 192.168.168.65
Add SNMP Trap IP OK
```

Note 1. This command is only applicable to console.

Miscellaneous Commands

ping

Description: Use the ping command to check the network connection to another system

Syntax: ping [host_ip] [timeout] [count]

Arguments:

host_ip	Ping the host with IP address
timeout	The ping timeout in seconds
count	The ping count

Example:

```
>>ping 192.168.168.65
ping (192.168.168.65): 56 data bytes
192.168.168.65 is alive
>>ping -s 192.168.168.165 10
ping (192.168.168.165): 56 data bytes
64 bytes from 192.168.168.165: icmp_seq=0
64 bytes from 192.168.168.165: icmp_seq=1
64 bytes from 192.168.168.165: icmp_seq=2
64 bytes from 192.168.168.165: icmp_seq=3
64 bytes from 192.168.168.165: icmp_seq=4
64 bytes from 192.168.168.165: icmp_seq=5
64 bytes from 192.168.168.165: icmp_seq=6
64 bytes from 192.168.168.165: icmp_seq=7
64 bytes from 192.168.168.165: icmp_seq=8
64 bytes from 192.168.168.165: icmp_seq=9
10 packets transmitted, 10 packets received
>>
```

arp

Description: Use the arp command display the entries in the Address Resolution Protocol table

Syntax: arp [-a|-d host]

Arguments:

-a	Show the all ARP table entries
-d	Delete the host IP address in ARP table
host	Show the host IP address in ARP table

Example:

```
>>arp
usage: arp host
       arp -a
       arp -d host
       arp -s host ether_addr [temp]
       arp -f filename
>>arp 192.168.168.65
192.168.168.65 (192.168.168.65) at 0:0:e2:65:94:7d
>>arp -a
192.168.168.65 (192.168.168.65) at 0:0:e2:65:94:7d
192.168.168.70 (192.168.168.70) at 0:50:fc:2f:d3:6a
192.168.168.165 (192.168.168.165) at 0:50:ba:1a:9b:ab
192.168.168.254 (192.168.168.254) at 0:7:4f:d:60:1c
192.168.168.71 (192.168.168.71) at 0:50:22:0:38:27
>>
```

netstat

Description: Use the netstat command display the network status for debug

Syntax: netstat [-a]

Arguments:

-a	Show the network connected status, include the protocol, host IP, state.

Example:

```
>>netstat -a
Proto   Local Address      Foreign Address        (state)
udp     0.0.0.0.199
udp     0.0.0.0.1024
udp     0.0.0.0.161
tcp     127.0.0.1.1024     127.0.0.1.9728         ESTABLISHED
tcp     127.0.0.1.9728     127.0.0.1.1024         ESTABLISHED
tcp     0.0.0.0.7594       0.0.0.0                LISTEN
tcp     192.168.168.201.22  192.168.168.65.2455      ESTABLISHED
tcp      0.0.0.0.22            0.0.0.0              LISTEN
tcp      0.0.0.0.1024          0.0.0.0               LISTEN
>>netstat
Proto    Local Address      Foreign Address        (state)
tcp      127.0.0.1.1024     127.0.0.1.9728        ESTABLISHED
tcp      127.0.0.1.9728     127.0.0.1.1024        ESTABLISHED
tcp      192.168.168.201.22  192.168.168.65.2455     ESTABLISHED
```

reset

Description: Use the reset command to reload the manufacturing default setting. After reset to default, you must reboot the system to take efface.

Syntax: reset

Arguments: none

Example:

```
>>reset
Are you sure to reset all settings to manufacturing defaults? (y/n) yes
Reset to defaults OK, please reboot to apply change.
>>
```

reboot

Description: Use the reboot command to reboot the DFL-2100/DFL-2400 device.

Syntax: reboot

Arguments: none

Example:

```
>>reboot


Are you sure to reboot system?  yes
>>
```

4

IDS MANAGEMENT SYSTEM

DFL-2100/DFL-2400 Management System is a Web-based application that allows multi user to manage one or more DFL-2100/DFL-2400 devices concurrently. It can be used from any computer with access to the DFL-2100/DFL-2400 Policy Server via Web browser.

DFL-2100/2400 IDS Management Main Screen

Login

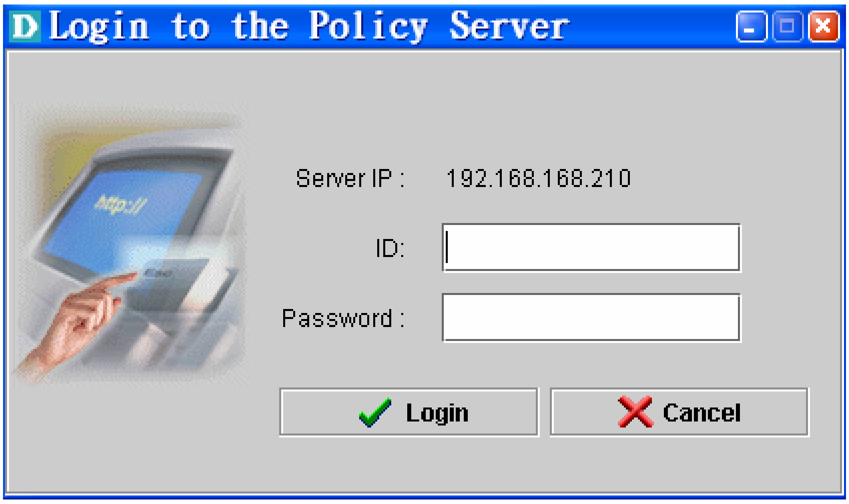
Connect the DFL-2100/DFL-2400 Policy Server from browser

- **Open your browser, and enter:**

http://<IP Address of the Policy Server>:6592/IDS/

1. Select ***Manager*** from the Policy Server web homepage, the following login dialog will appear.
2. Enter the ***Password*** and click ***Login*** to login to the DFL-2100/ DFL-2400 Management System.
   (Default ID: **admin**; Password : **admin**)

Note: The control mechanism of access to DFL-2100/DFL-2400 IDS Management System is password.


Login to the Policy Server

Server IP : 192.168.168.210

ID:

Password :

Figure 4-1: DFL-2100/DFL-2400 Management System Login Screen

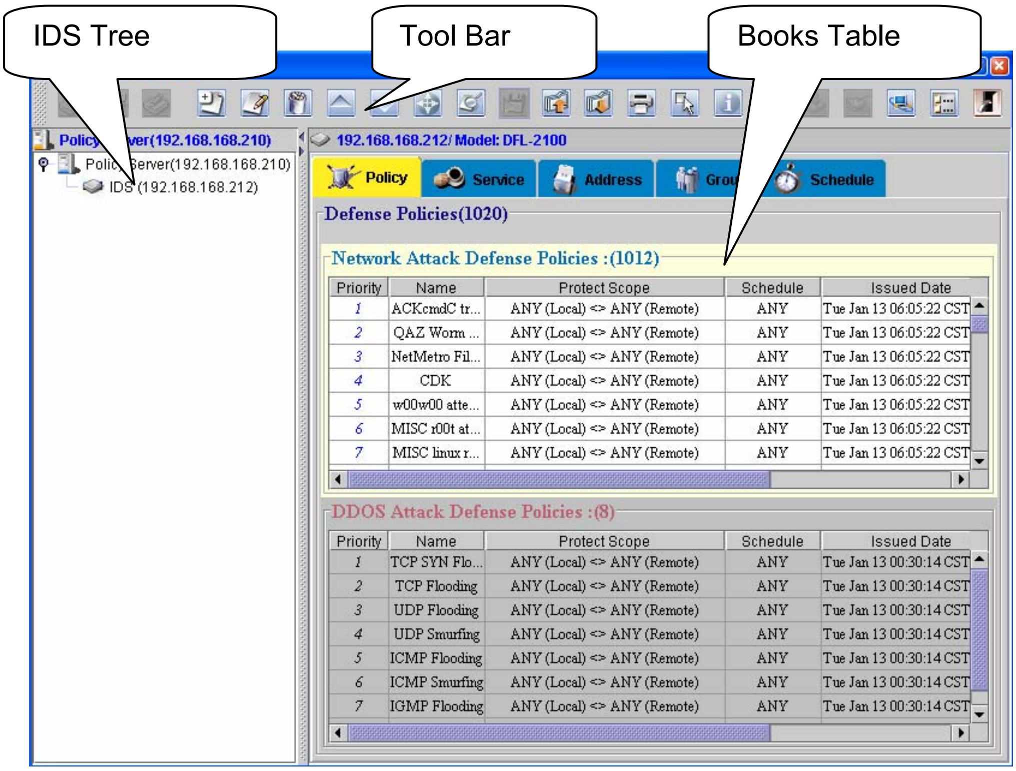
DFL-2100/DFL-2400 Management System Main Screen

The DFL-2100/DFL-2400 Management System main screen consist three windows:

IDS Tree: A tree-view of all the DFL-2100/DFL-2400 devices handled by the DFL-2100/DFL-2400 Policy Server you are current connected to. Tree-view Icons are described below.

Books Table: A table based setting environment for DFL-2100/DFL-2400. It consists five pages: Policy Book, Service Book, Address Book, Schedule Book, and Group Book. We will describe these books detail in the following chapters.

Tool Bar: It consists all of the function buttons for managing DFL-2100/DFL-2400.


IDS Tree
Tool Bar
Books Table
Policy ver(192.168.168.210)
Polic Server(192.168.168.210)
IDS (192.168.168.212)
192.168.168.212/ Model: DFL-2100
Policy
Service
Address
Grou
Schedule

Defense Policies(1020)

Network Attack Defense Policies :(1012)

Priority	Name	Protect Scope	Schedule	Issued Date
1	ACKcmdC tr...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
2	QAZ Worm ...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
3	NetMetro Fil...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
4	CDK	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
5	w00w00 atte...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
6	MISC r00t at...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
7	MISC linux r...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST

DDOS Attack Defense Policies :(8)

Priority	Name	Protect Scope	Schedule	Issued Date
1	TCP SYN Flo...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
2	TCP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
3	UDP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
4	UDP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
5	ICMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
6	ICMP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
7	IGMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST

Figure 4-2: DFL-2100/ DFL-2400 Management System Main Screen

Manage DFL-2100/DFL-2400

The DFL-2100/DFL-2400 IDS Management System can management multiple DFL-2100/DFL-2400s. To **manage** a DFL-2100/DFL-2400, you must first add the DFL-2100/DFL-2400 device to the DFL-2100/DFL-2400 IDS Management main screen. The device will be added to the IDS Tree of the tree-view window. After adding one or more DFL-2100/DFL-2400s to the IDS Tree, you can now load them to the DFL-2100/DFL-2400 IDS Management System and set up their Policy Rules and Books. Double click on one of the tree-node icons then the DFL-2100/DFL-2400 device specified by this node will be loaded and its Books will be shown in the Book Table window.

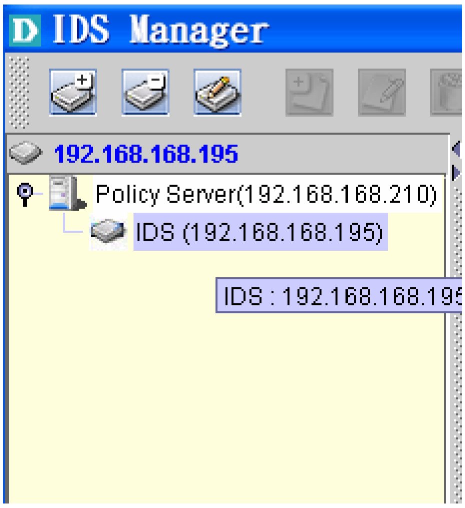


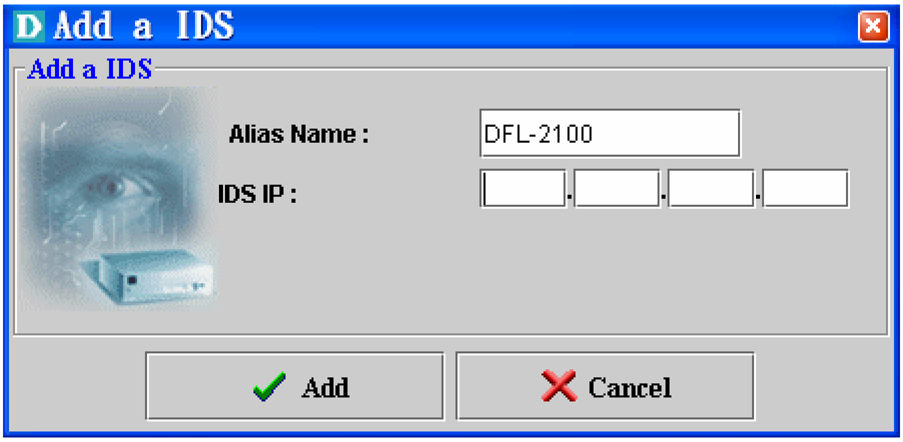
Figure 4-3: DFL-2100/ DFL-2400 IDS tree view

	Tree-View root, the DFL-2100/ DFL-2400 Policy Server with IP address being connected to. Double click this icon to expand the IDS tree.
	Tree-View root, the DFL-2100/ DFL-2400 Policy Server with IP address being connected to. Double click this icon to collapse the IDS tree.
	Designates an active DFL-2100/DFL-2400 device with alias name and IP address specified behind. Double click this icon to load the contents of this DFL-2100/DFL-2400 device.
	Designates the DFL-2100/DFL-2400 that has been loaded and modified its settings and has not been updated.
	Designates the DFL-2100/DFL-2400 is unavailable (broken of offline).

Table 4.1:Tree-View Icons and descriptions

Add a DFL-2100/DFL-2400

1. Click Add DFL-2100/DFL-2400 button on the tool Bar or right-click on the IDS tree window to bring up the pop-up menu. Select Add a DFL-2100/DFL-2400.
2. Enter the Alias Name of the DFL-2100/DFL-2400.
3. Enter the DFL-2100/DFL-2400 IP of the DFL-2100/DFL-2400 you wish to add.
4. Click Add to add the DFL-2100/DFL-2400 device to the IDS Tree.



Alias Name : DFL-2100

IDS IP : . . .

Figure 4-4: " Add a DFL-2100/DFL-2400" Dialog

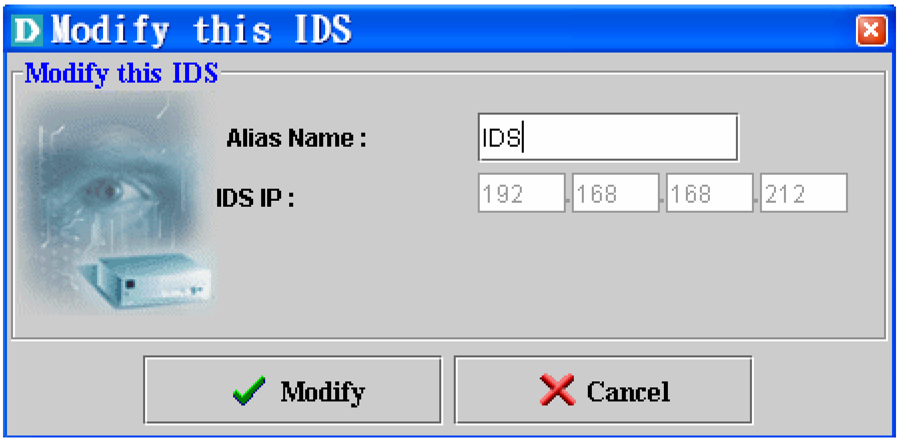
Remove a DFL-2100/DFL-2400

1. Select the DFL-2100/DFL-2400 you want to remove from the IDS Tree.
2. Click Remove DFL-2100/DFL-2400 button on the tool bar or right-click on the tree and select “Remove” from the pop-up menu. A warning message is displayed.
3. Click “Yes” to remove this DFL-2100/DFL-2400 from the IDS Tree, or “No” to cancel this action.

Note	Remove DFL-2100/DFL-2400 will also remove all the log files from the Policy Server. If you wish to keep these log files, backup these files on the Policy Server before removing this DFL-2100/DFL-2400.

Modify a DFL-2100/DFL-2400

1. Click Modify DFL-2100/DFL-2400 button or right-click on the IDS tree window to bring up the pop-up menu. Select Modify DFL-2100/DFL-2400.
2. Enter the new Alias Name of the DFL-2100/DFL-2400.
3. Click “Modify” to update the property of this DFL-2100/DFL-2400 or “Cancel” to cancel the modification.



Alias Name : IDS

IDS IP : 192 . 168 . 168 . 212

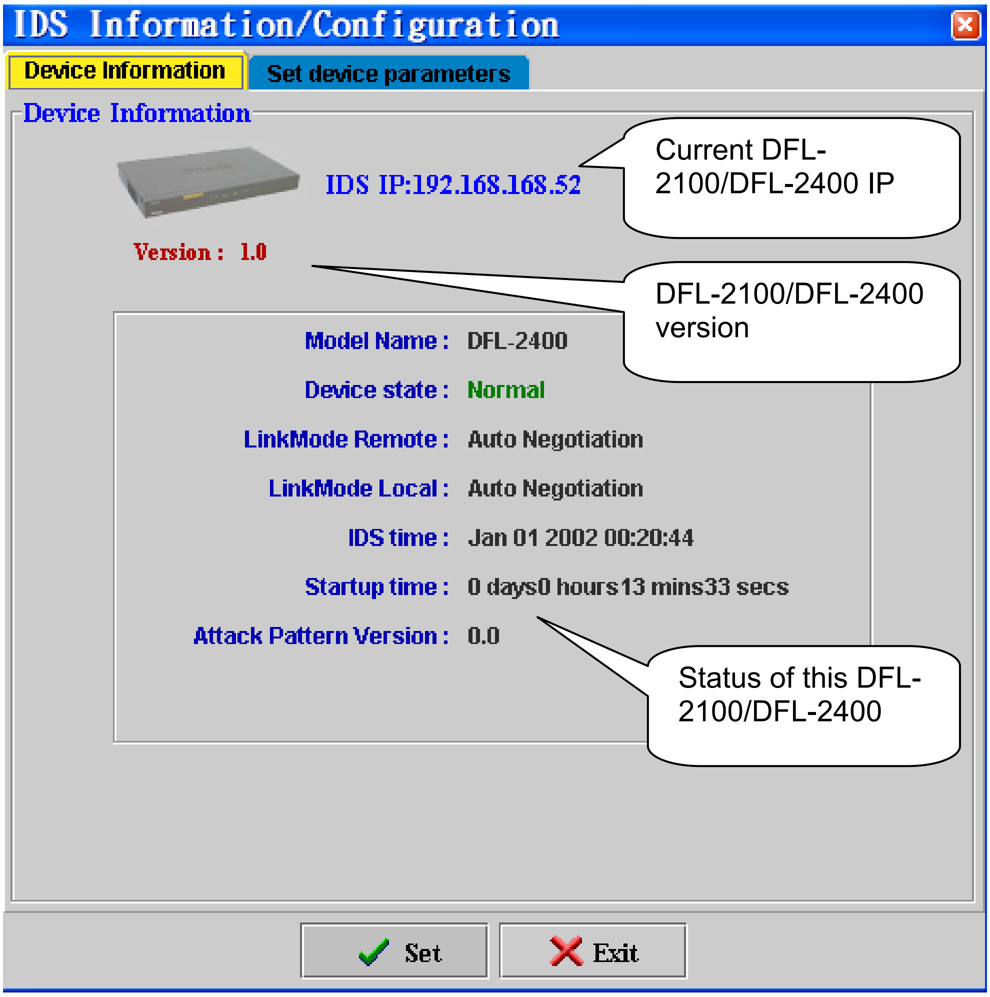
Figure 4-5:”Modify this DFL-2100/DFL-2400” Dialog

DFL-2100/DFL-2400 configure and setting

Once a DFL-2100/DFL-2400 has been added in the IDS tree, double click the icon in the tree-view to load the contents of this DFL-2100/DFL-2400 device.

DFL-2100/DFL-2400 Device Information

To see the information of the DFL-2100/DFL-2400 device you have loaded, and click preference/system information button on the Tool Bar. The following dialog appears.



Device Information

IDS IP:192.168.168.52

Version : 1.0

Model Name : DFL-2400

Device state : Normal

LinkMode Remote : Auto Negotiation

LinkMode Local : Auto Negotiation

IDS time : Jan 01 2002 00:20:44

Startup time : 0 days0 hours13 mins33 secs

Attack Pattern Version : 0.0

Current DFL-2100/DFL-2400 IP

DFL-2100/DFL-2400 version

Status of this DFL-2100/DFL-2400

Figure 4-6: ”DFL-2100/DFL-2400 Device Information” Dialog

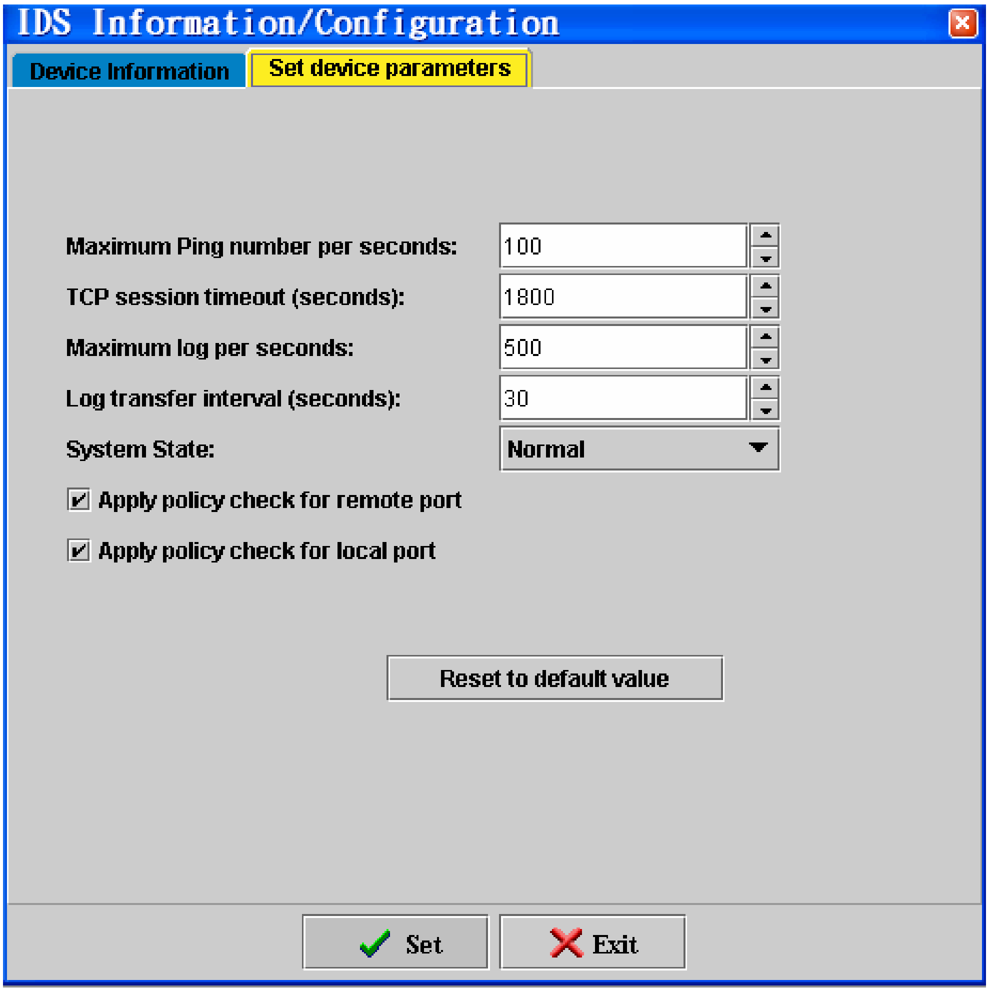
Setting DFL-2100/DFL-2400 parameters

With getting the information of the DFL-2100/DFL-2400 device at last section, you can set DFL-2100/DFL-2400 device some parameters at same button. Click **preference/system information** button on the Tool Bar and select “**set device parameters**” Tab. The following dialog appears.

There are five parameters can be set.

1. Maximum ping number per second.
2. TCP session timeout times

3. Maximum log per second
4. Set the DFL-2100/DFL-2400 state. There are four states in DFL-2100/DFL-2400. '***Normal***' means DFL-2100/DFL-2400 works normally according to given policies. '***Protect***' means DFL-2100/DFL-2400 works like an access controller. It would let packets pass according to given policies. ***'Stop***' means DFL-2100/DFL-2400 would drop all the packets it receives. And '***Bypass***' means DFL-2100/DFL-2400 would let all the packets pass through freely without any checks.
5. Set Policy will apply to which interface.



Maximum Ping number per seconds: 100

TCP session timeout (seconds): 1800

Maximum log per seconds: 500

Log transfer interval (seconds): 30

System State: Normal

☑ Apply policy check for remote port

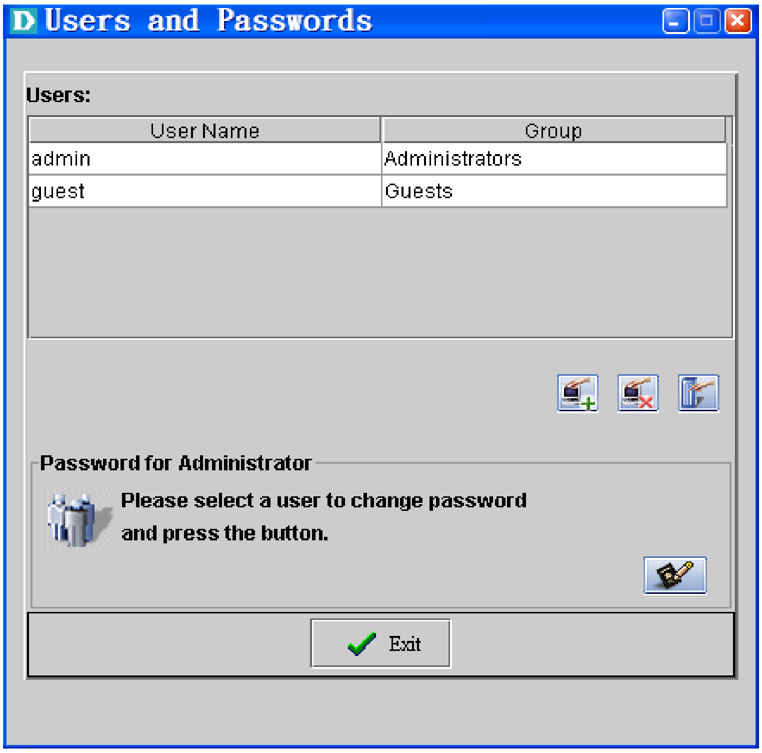
☑ Apply policy check for local port

Figure 4-7: "set device parameters" Dialog

User Manage

A user is some one who can use or access DFL-2100/ DFL-2400 IDS Management System. As the Management System administrator, you decide who has permission to access modify policy, select policy, search report.

Click **User Management** button on the tool bar. The Management Windows will appear. There are two default users in DFL-2100/DFL-2400 Policy Server. One is Admin (administrator), another is guest (guests).



Users and Passwords

Users:

User Name	Group
admin	Administrators
guest	Guests

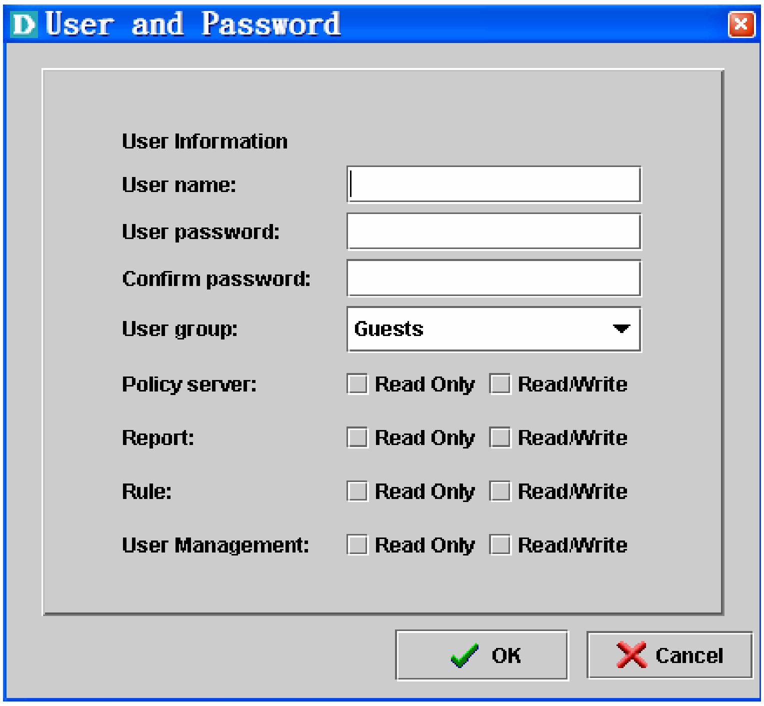
Password for Administrator

Please select a user to change password and press the button.

Figure 4-8: User Manage Window

Add new user

1. Click Add User button on the dialog. The following dialog appears.
2. Enter the User Name, User password.
3. Confirm the password.
4. Select a user group.
5. Give the Read / Write permission about policy service, report service and user management.



User and Password

User Information

User name:

User password:

Confirm password:

User group: Guests

Policy server: □ Read Only □ Read/Write

Report: □ Read Only □ Read/Write

Rule: □ Read Only □ Read/Write

User Management: □ Read Only □ Read/Write

Figure 4-9: Add New User Dialog

Delete user

1. Click Delete User button on the dialog.
2. The confirm dialog will appear.

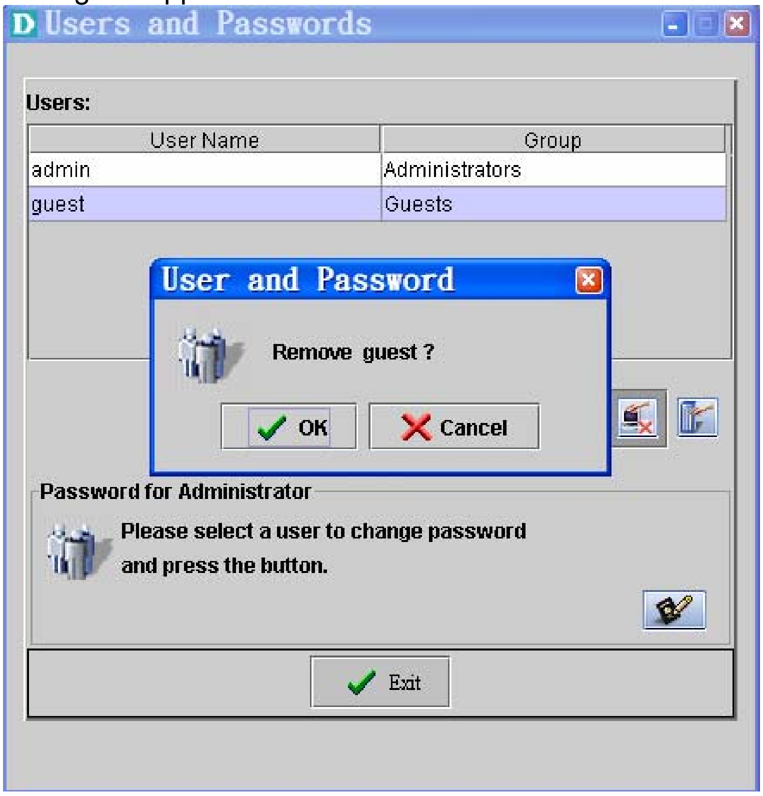
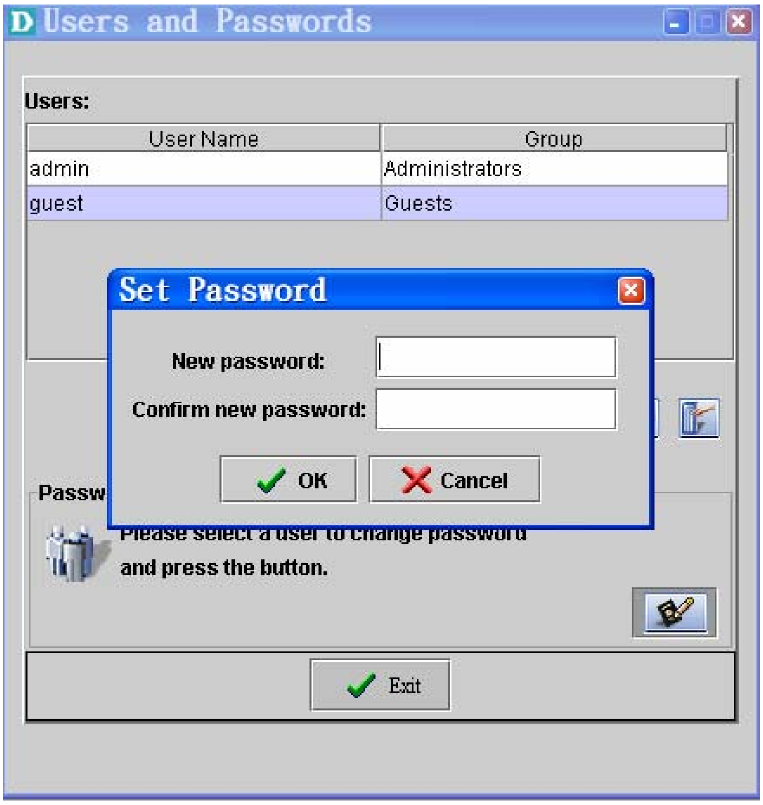


Figure 4-10: Remove User Dialog

Edit user

Once you click user management button, it will show the user list. Select one user you can change the password by click change password button. Or you can click the manage button in the dialog to edit the user parameters. There are three levels of parameters can be changed.

1. User password.
2. User group.
3. Policy Server Access permission.



Users and Passwords

Users:

User Name	Group
admin	Administrators
guest	Guests

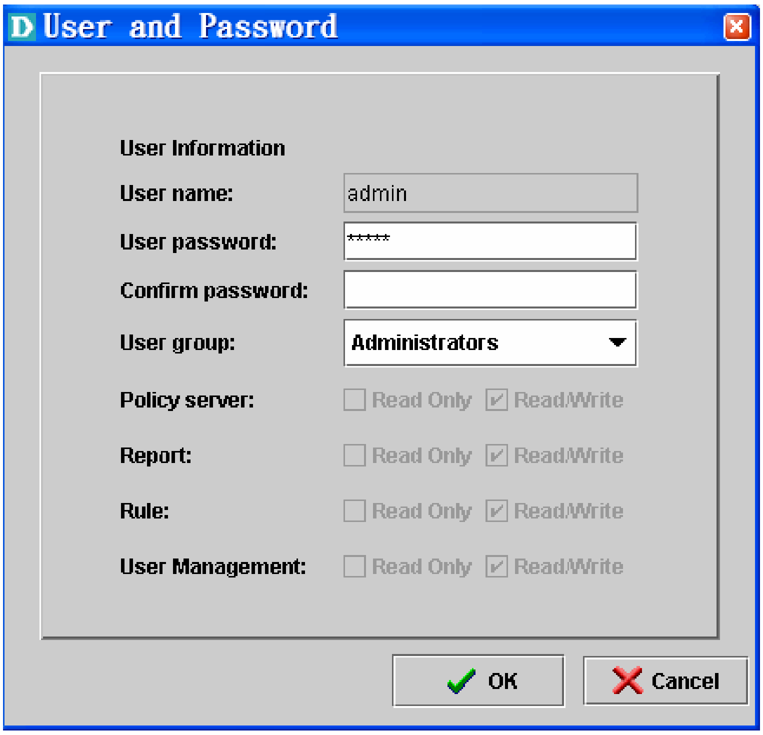
Set Password

New password:

Confirm new password:

Please select a user to change password and press the button.

Figure 4-11: Change Password Dialog



User and Password

User Information

User name: admin

User password: *****

Confirm password:

User group: Administrators

Policy server: □ Read Only ☑ Read/Write

Report: □ Read Only ☑ Read/Write

Rule: □ Read Only ☑ Read/Write

User Management: □ Read Only ☑ Read/Write

Figure 4-12: Edit User Permission Dialog

IDS Management system miscellaneous functions

DFL-2100/ DFL-2400 Management System tool bar include a manager tools that manages devices and edit network security policy and show other information. The first class DFL-2100/DFL-2400 device manage tools include add, delete and edit device. The secondary class policy manage tools include add, delete, edit, change priority, push policy, import/export policy and print function. The last class management system tools include Internet Register, live update, reporting system and user manage functions.

Toolbar icons	Function
	Add, Delete, Edit DFL-2100/DFL-2400 device
	Add, Delete, Edit security Policy
	Up and Down the priority, Find the policy
	Push the policy to DFL-2100/DFL-2400 device
	Import, Export, Print the policy
	Device information, About system, Help, Exit
	Register, Live update, User manager
	Reporting System

Table 4-1: The function list of DFL-2100/ DFL-2400 Management System

Export Books

Administrator can duplicate all the policy and books from DFL-2100/DFL-2400 to either Policy Server or local host. This function can be used when administrator want to change the deployment or copy books to other DFL-2100/DFL-2400. The procedure is as followings:

1. Load the DFL-2100/DFL-2400 that wants to export its books.
2. Click the "Export" button in the toolbar. And the following dialog will show up
3. Choose the target: either the Policy Server of local host.
4. If "To Policy Server" is chosen, a filename must be given. Otherwise, you can specify the local host directory that you want to store the books.

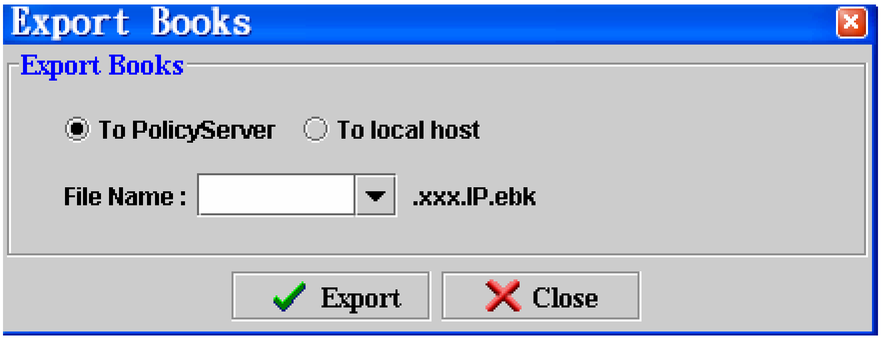
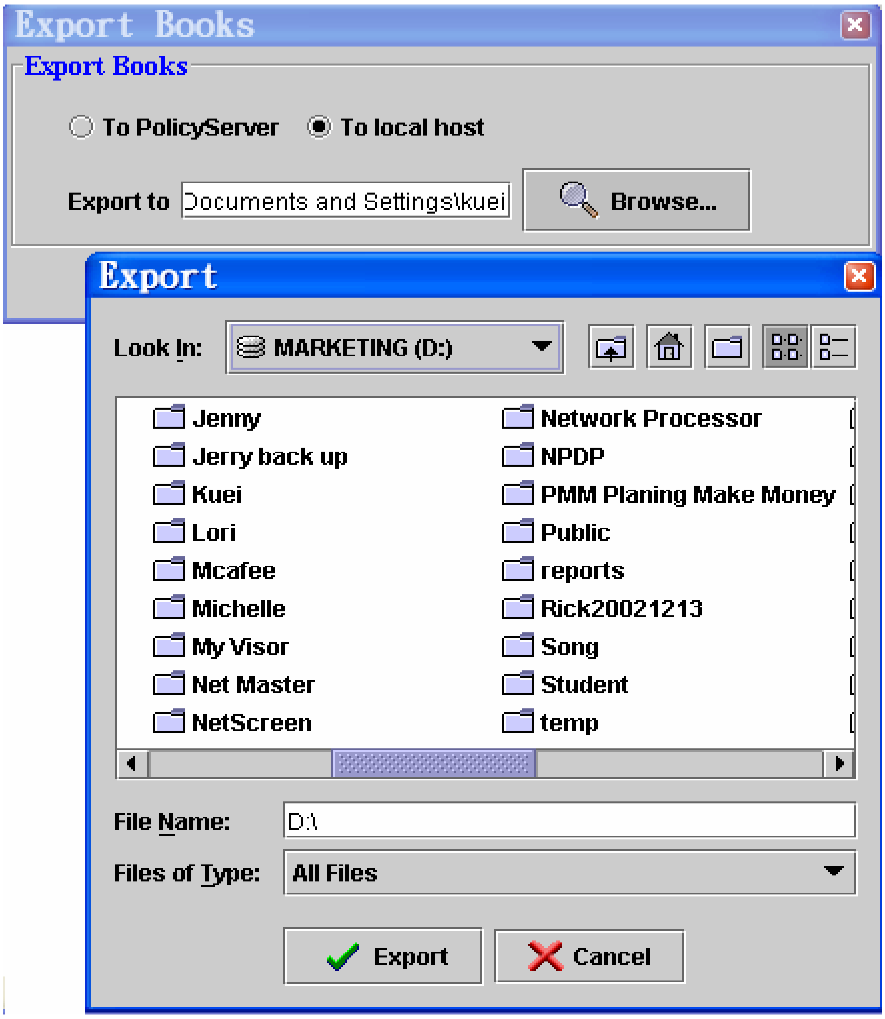


Figure 4-13: Export policy and books to policy server dialog



Export Books

○ To PolicyServer ● To local host

Export to: Documents and Settings\kuei

Export

Look In: MARKETING (D:)

File Name: D:\

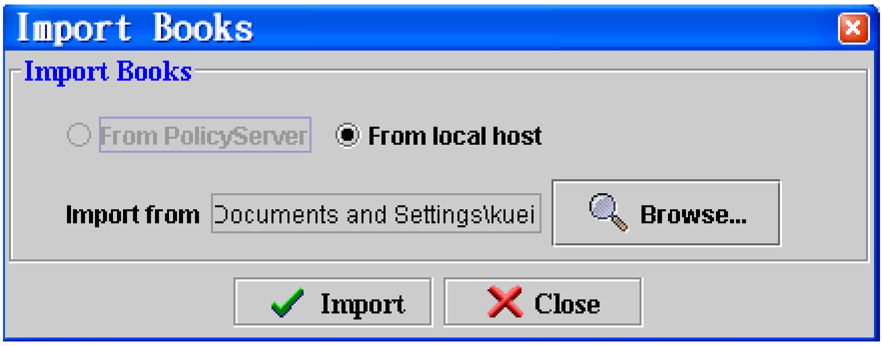
Files of Type: All Files

Figure 4-14: Export policy and books to local host dialog

Import Books

Administrator can import the books from either Policy Server or local host. The can be used when administrator want to change the deployment or copy books to other DFL-2100/DFL-2400. The procedure is as followings:

1. Load the DFL-2100/DFL-2400 that wants to import books.
2. Click the “Import” button in the toolbar. And the following figure will show up.
3. Choose the source: either the Policy Server of local host.
4. If “From Policy Server” is chosen, you can choose from different filenames. Otherwise, you can specify the local host directory that has the books.



Import Books

○ From PolicyServer ● From local host

Import from: Documents and Settings\kuei

Figure 4-15: Import policy from Policy Server dialog

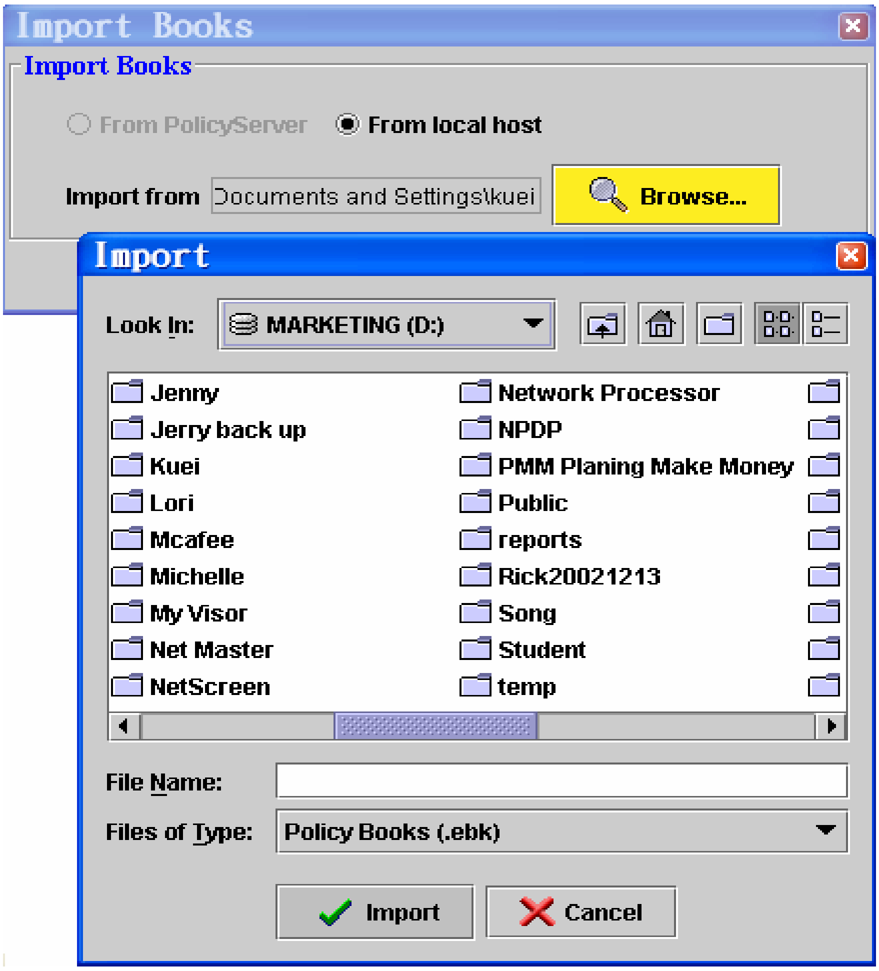
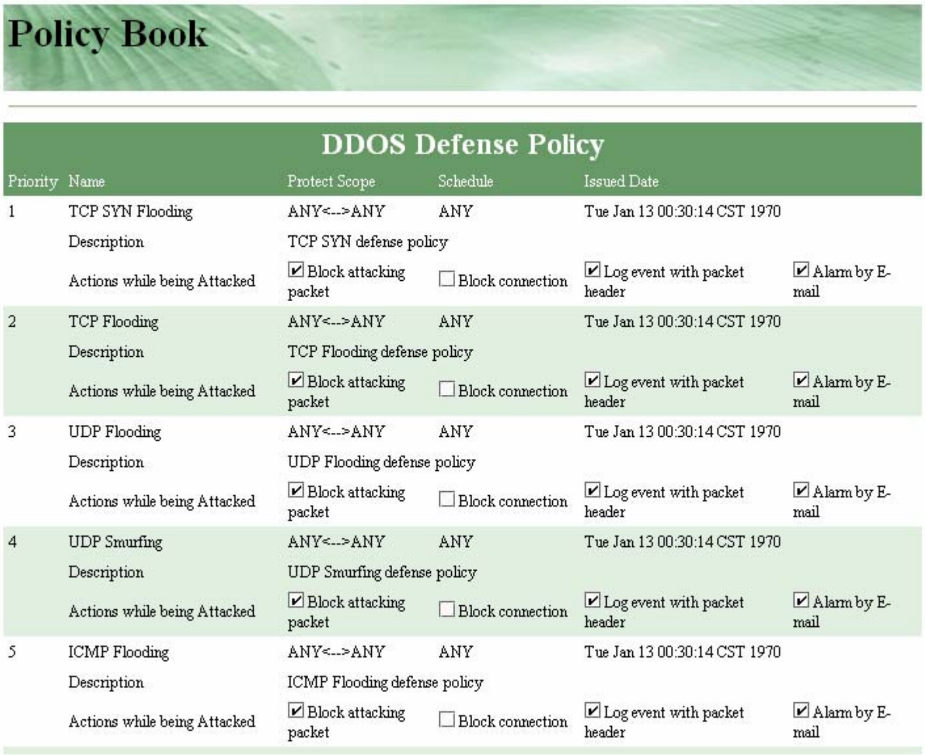


Figure 4-16: Import policy from local host dialog

Print Books

Another way to back up books is to print them out in papers. When the "Print" button 🖨 on the toolbar is pressed, the current loaded book will be prepared to print out. The print preview screen as the following figure will show up. Click "Print" to print it out, otherwise click "Cancel" to close this screen.



Policy Book

DDOS Defense Policy

Priority	Name	Protect Scope	Schedule	Issued Date	
1	TCP SYN Flooding	ANY<-->ANY	ANY	Tue Jan 13 00:30:14 CST 1970	
	Description	TCP SYN defense policy			
	Actions while being Attacked	☑ Block attacking packet	☐ Block connection	☑ Log event with packet header	☑ Alarm by E-mail
2	TCP Flooding	ANY<-->ANY	ANY	Tue Jan 13 00:30:14 CST 1970	
	Description	TCP Flooding defense policy			
	Actions while being Attacked	☑ Block attacking packet	☐ Block connection	☑ Log event with packet header	☑ Alarm by E-mail
3	UDP Flooding	ANY<-->ANY	ANY	Tue Jan 13 00:30:14 CST 1970	
	Description	UDP Flooding defense policy			
	Actions while being Attacked	☑ Block attacking packet	☐ Block connection	☑ Log event with packet header	☑ Alarm by E-mail
4	UDP Smurfing	ANY<-->ANY	ANY	Tue Jan 13 00:30:14 CST 1970	
	Description	UDP Smurfing defense policy			
	Actions while being Attacked	☑ Block attacking packet	☐ Block connection	☑ Log event with packet header	☑ Alarm by E-mail
5	ICMP Flooding	ANY<-->ANY	ANY	Tue Jan 13 00:30:14 CST 1970	
	Description	ICMP Flooding defense policy			
	Actions while being Attacked	☑ Block attacking packet	☐ Block connection	☑ Log event with packet header	☑ Alarm by E-mail

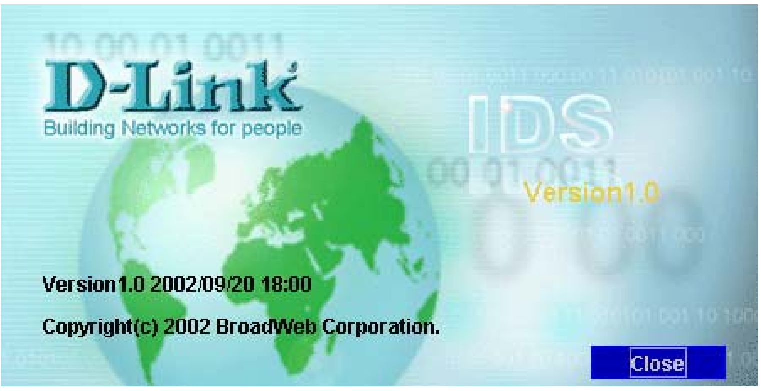
Figure 4-17: Print Policy Book Preview Screen

DFL-2100/DFL-2400 IDS Reporting System

The DFL-2100/DFL-2400 IDS Reporting System is an advance report system. Its include the real time attack monitor, real time traffic monitor, and advance attack event search system. We will show the subsystem detail at chapter 8. When the "Reporter" button on the toolbar is pressed, we will go into the "DFL-2100/ DFL-2400 IDS Reporting System" and get the more detail attack events messages.

About DFL-2100/DFL-2400 IDS Management System

When the "About" button on the toolbar is pressed, the current version information will be show by the popup window. Click "Close" to close this screen.



Version1.0 2002/09/20 18:00

Copyright(c) 2002 BroadWeb Corporation.

Figure 4-18: DFL-2100/ DFL-2400 Management System information

5

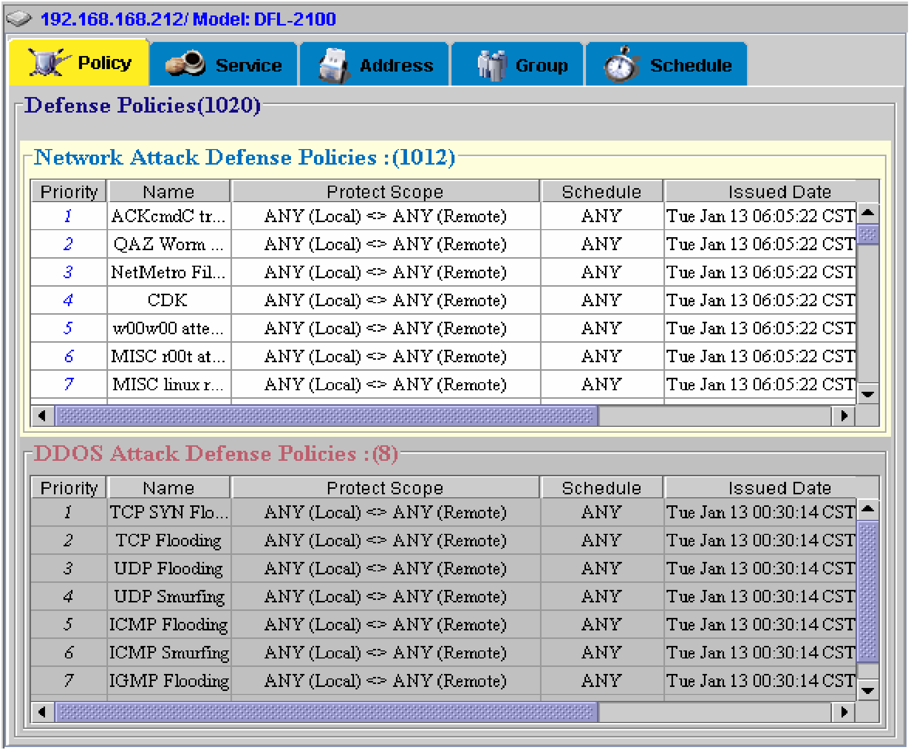
POLICY BASED IDS

What is a Policy?

The policy is the most important information in the DFL-2100/ DFL-2400 IDS Management System. A policy tells DFL-2100/DFL-2400 how to detect an attack, how to response when an attack is detected, what to protect and when to protect. Therefore, a policy consists of policy information, defense describe, protect scope, schedule, actions and some high level information such as class, issued date and etc.

The Policy Book

The policy book is divided into two tables. The upper table is “Network Attack Defense Policies” and the lower table is “DDoS Attack Defense Policies”. The reason of dividing these policies into different categories is because the detection methods are quite different inherently. The “Network Attack Defense Policies” employ the pattern matching while the “DDoS Attack Defense Policies” use statistical modeling.



Defense Policies(1020)

Network Attack Defense Policies :(1012)

Priority	Name	Protect Scope	Schedule	Issued Date
1	ACKcmdC tr...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
2	QAZ Worm ...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
3	NetMetro Fil...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
4	CDK	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
5	w00w00 atte...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
6	MISC r00t at...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
7	MISC linux r...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST

DDOS Attack Defense Policies :(8)

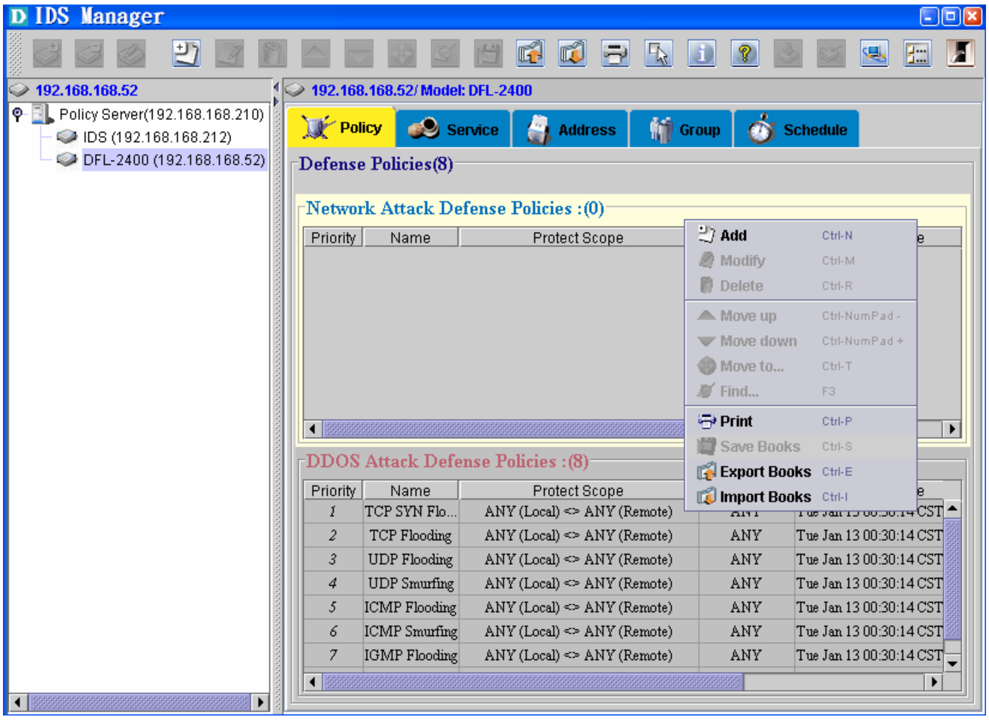
Priority	Name	Protect Scope	Schedule	Issued Date
1	TCP SYN Flo...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
2	TCP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
3	UDP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
4	UDP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
5	ICMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
6	ICMP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
7	IGMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST

Figure 5-1: Policy Book

Load latest attack pattern

The policies are the most important information in the DFL-2100/ DFL-2400 Management System. Policies indicate to DFL-2100/DFL-2400 for how to detect an attack and how to response when an attack is detected. To begin using your DFL-2100/DFL-2400, you need to load the latest defense policies.

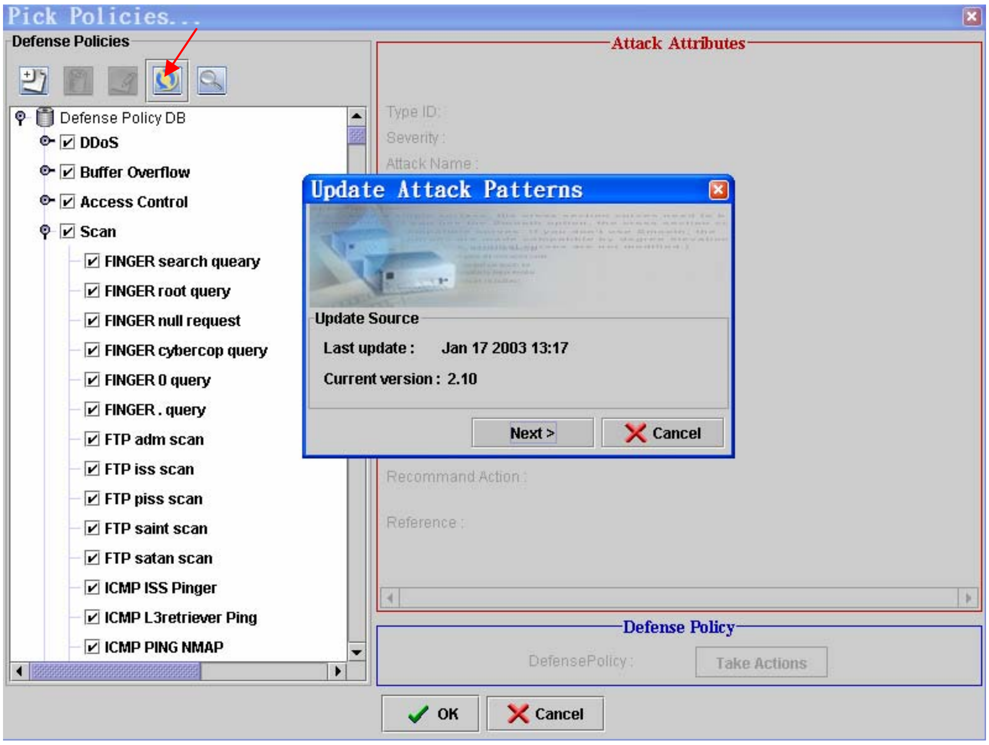
1. Select "Add" button or right-click on the Network attack Defense Policies window to add new policies.



Priority	Name	Protect Scope		e
1	TCP SYN Flo...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
2	TCP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
3	UDP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
4	UDP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
5	ICMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
6	ICMP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
7	IGMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST

Figure 5-2: Add new Policy

2. There is a default policy database on the DFL-2100/DFL-2400 Policy Server, administrator must select "Update latest attack pattern" button to update latest pattern from Administrator Utility CD ~/Policy Server/ PolicyDB/ policyXXX.ptn.
3. After register, DFL-2100/ DFL-2400 Management System will check the update server for latest pattern.



Pick Policies...

Defense Policies

- Defense Policy DB
  - ☑ DDoS
  - ☑ Buffer Overflow
  - ☑ Access Control
  - ☑ Scan
    - ☑ FINGER search queary
    - ☑ FINGER root query
    - ☑ FINGER null request
    - ☑ FINGER cybercop query
    - ☑ FINGER 0 query
    - ☑ FINGER . query
    - ☑ FTP adm scan
    - ☑ FTP iss scan
    - ☑ FTP piss scan
    - ☑ FTP saint scan
    - ☑ FTP satan scan
    - ☑ ICMP ISS Pinger
    - ☑ ICMP L3retriever Ping
    - ☑ ICMP PING NMAP

Attack Attributes

Type ID :

Severity :

Attack Name :

Recommand Action :

Reference :

Defense Policy

DefensePolicy :

Update Attack Patterns

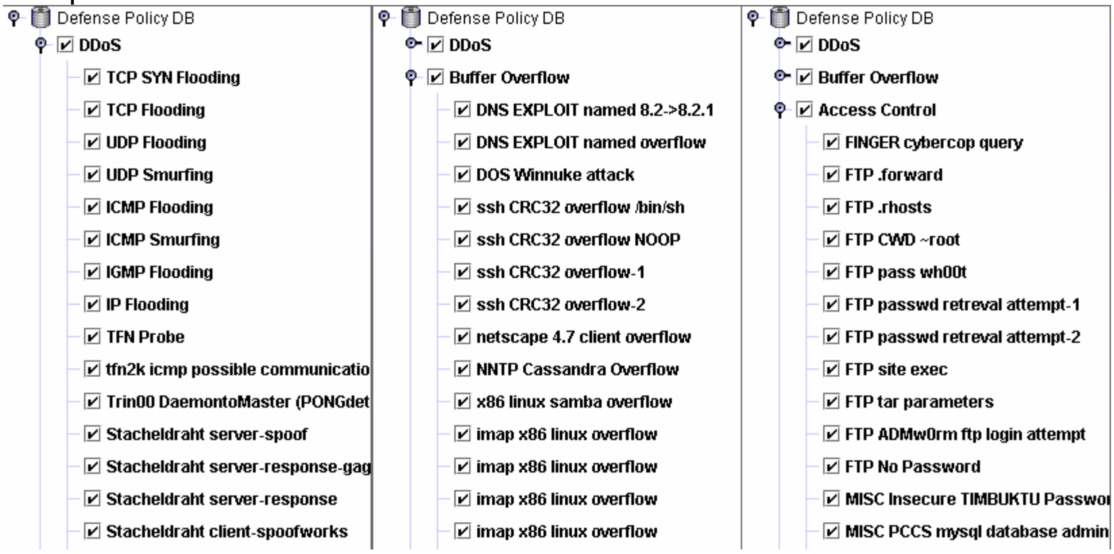
Update Source

Last update : Jan 17 2003 13:17

Current version : 2.10

Figure 5-3: download latest attack pattern

4. You can find new defense policies in the policy list when you finish the update.



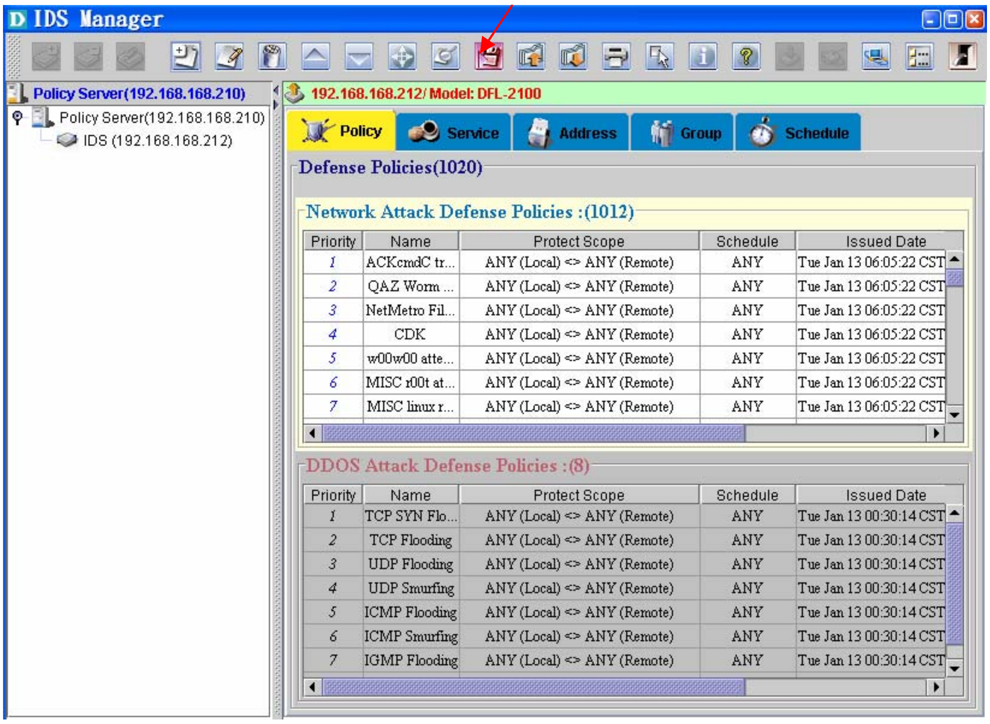
- Defense Policy DB
  - ☑ DDoS
    - ☑ TCP SYN Flooding
    - ☑ TCP Flooding
    - ☑ UDP Flooding
    - ☑ UDP Smurfing
    - ☑ ICMP Flooding
    - ☑ ICMP Smurfing
    - ☑ IGMP Flooding
    - ☑ IP Flooding
    - ☑ TFN Probe
    - ☑ tfn2k icmp possible communicatio
    - ☑ Trin00 DaemontoMaster (PONGdet
    - ☑ Stacheldraht server-spoof
    - ☑ Stacheldraht server-response-gag
    - ☑ Stacheldraht server-response
    - ☑ Stacheldraht client-spoofworks

- Defense Policy DB
  - ☑ DDoS
  - ☑ Buffer Overflow
    - ☑ DNS EXPLOIT named 8.2->8.2.1
    - ☑ DNS EXPLOIT named overflow
    - ☑ DOS Winnuke attack
    - ☑ ssh CRC32 overflow /bin/sh
    - ☑ ssh CRC32 overflow NOOP
    - ☑ ssh CRC32 overflow-1
    - ☑ ssh CRC32 overflow-2
    - ☑ netscape 4.7 client overflow
    - ☑ NNTP Cassandra Overflow
    - ☑ x86 linux samba overflow
    - ☑ imap x86 linux overflow
    - ☑ imap x86 linux overflow
    - ☑ imap x86 linux overflow
    - ☑ imap x86 linux overflow

- Defense Policy DB
  - ☑ DDoS
  - ☑ Buffer Overflow
  - ☑ Access Control
    - ☑ FINGER cybercop query
    - ☑ FTP .forward
    - ☑ FTP .rhosts
    - ☑ FTP CWD ~root
    - ☑ FTP pass wh00t
    - ☑ FTP passwd retreval attempt-1
    - ☑ FTP passwd retreval attempt-2
    - ☑ FTP site exec
    - ☑ FTP tar parameters
    - ☑ FTP ADMw0rm ftp login attempt
    - ☑ FTP No Password
    - ☑ MISC Insecure TIMBUKTU Passwo
    - ☑ MISC PCCS mysql database admin

Figure 5-4 : select your defense policies

5. When we select the defense policies, click the “OK” button return to the main manage window. All the changes to the defense policies will not take effect until the red-lighted Confirm button is clicked.


IDS Manager
Policy Server(192.168.168.210)
Policy Server(192.168.168.210)
IDS (192.168.168.212)
192.168.168.212/ Model: DFL-2100
Policy
Service
Address
Group
Schedule

Defense Policies(1020)

Network Attack Defense Policies :(1012)

Priority	Name	Protect Scope	Schedule	Issued Date
1	ACKcmdC tr...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
2	QAZ Worm ...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
3	NetMetro Fil...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
4	CDK	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
5	w00w00 atte...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
6	MISC r00t at...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST
7	MISC linux r...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 06:05:22 CST

DDOS Attack Defense Policies :(8)

Priority	Name	Protect Scope	Schedule	Issued Date
1	TCP SYN Flo...	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
2	TCP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
3	UDP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
4	UDP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
5	ICMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
6	ICMP Smurfing	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST
7	IGMP Flooding	ANY (Local) <> ANY (Remote)	ANY	Tue Jan 13 00:30:14 CST

Figure 5-5: Click the “Confirm button” after change defense policies

Change the Priority of Policies

The detection policies may not mutual exclusive, i.e. a single packet may match different policies concurrently. In order to solve this kind of conflicts, a priority mechanism is introduced. The rule is: policy with higher priority is checked first, and the action is determined according to first matched policy.

For administrators to change the priority of policies, there are two buttons on the toolbar: “Higher Priority”▲ and “Lower Priority” ▼.

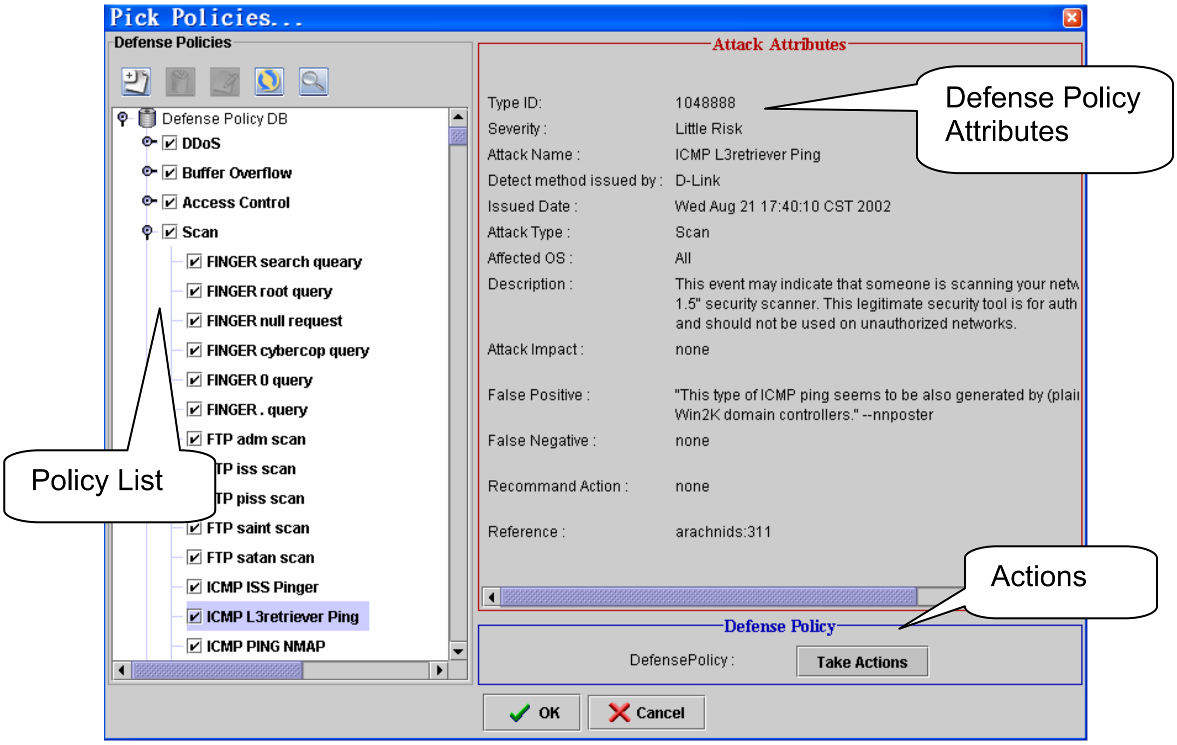
Note	In order to change the priority of policies, you have to double click the policy book table first, a selected table will be highlighted. And then select a policy to move it up or down. When it moves up, it gets higher priority; otherwise, it gets lower priority.

Network Defense Policies Database

There is a policy database on the Policy Server, administrator can pick up policies from this predefined database. Or user can click the “Add a Policy” button on the toolbar to add a policy to the database.

The “Network Defense Policies Database” window consists of three parts:

- The policy list: List of policies and group by class.
- Attack Attributes: The attack name, ID, type, protected OS and other attack descriptions.
- Defense Policy: Define the actions when the policy is matched.



Type ID: 1048888
Severity : Little Risk
Attack Name : ICMP L3retriever Ping
Detect method issued by : D-Link
Issued Date : Wed Aug 21 17:40:10 CST 2002
Attack Type : Scan
Affected OS : All
Description : This event may indicate that someone is scanning your netw
1.5" security scanner. This legitimate security tool is for auth
and should not be used on unauthorized networks.
Attack Impact : none
False Positive : "This type of ICMP ping seems to be also generated by (plai
Win2K domain controllers." --nnposter
False Negative : none
Recommand Action : none
Reference : arachnids:311

DefensePolicy :

Figure 5-6: Network Defense Policies Database

Select Defense Policy

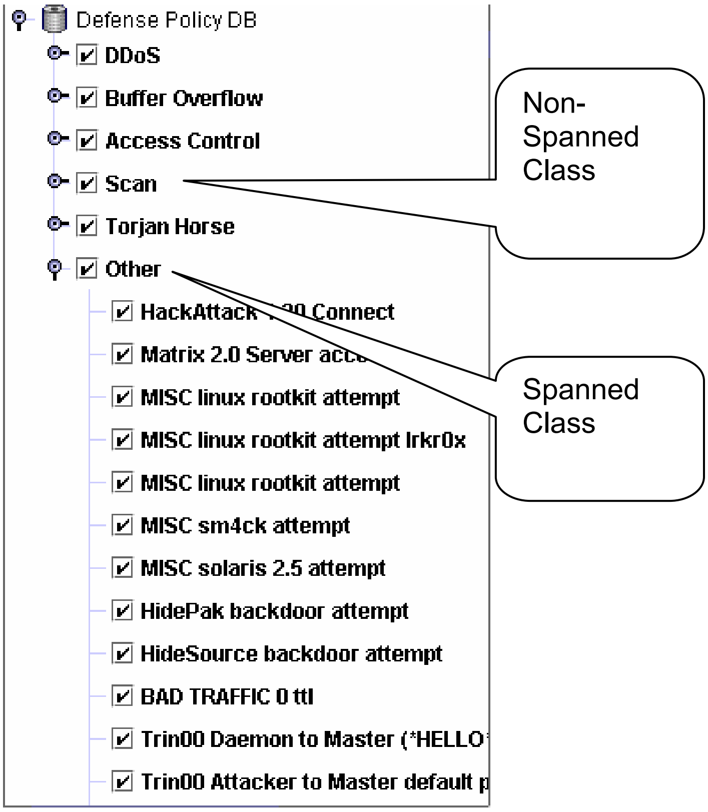
The procedure of picking up a defense policy is:

1. **Select a defense policy in policy list.**
2. **Set actions when this policy is met.**
3. **Define it's protect scope or DDoS parameters.**

Note	For DDoS attack defense policies, there are no protect scope field, because they always protect all hosts by default. However, they have another field called "DDoS Parameters". See section of "Setting DDoS Parameters".

Select a Defense Policy

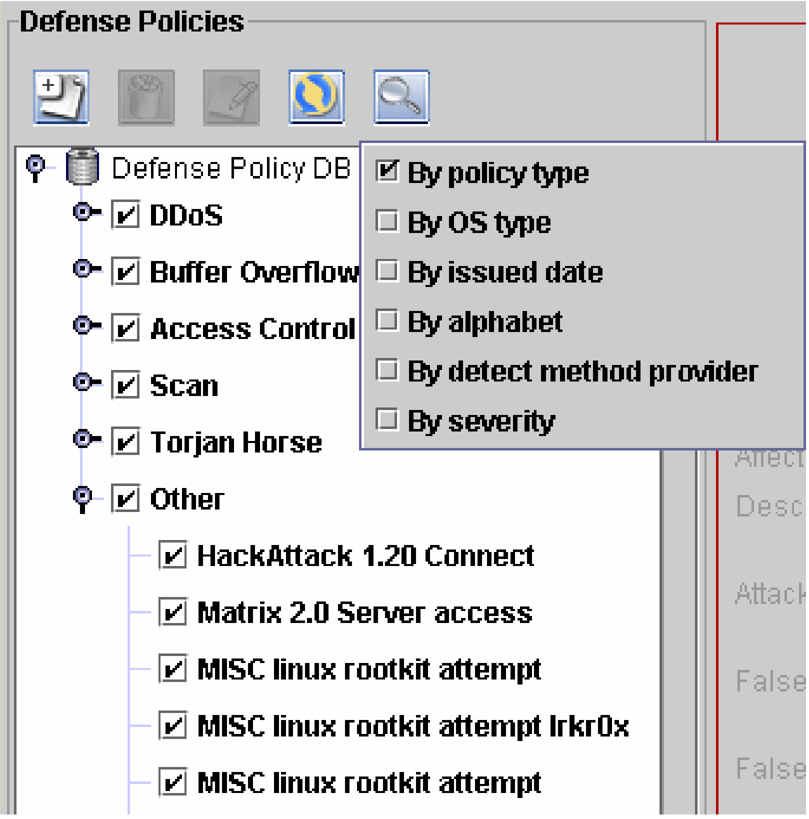
In policy list, you can double click the class item to span/close the items in the class. If the icon before the policy name is checked then it was selected. Otherwise if it is unchecked, then this defense policy is not selected. When a policy is selected, you can see its attributes and property in the "Attack Attribute" window and "Defense Policy Property" window.



Defense Policy DB
- ☑ DDoS
- ☑ Buffer Overflow
- ☑ Access Control
- ☑ Scan
- ☑ Torjan Horse
- ☑ Other
  - ☑ HackAttack 1.20 Connect
  - ☑ Matrix 2.0 Server acc
  - ☑ MISC linux rootkit attempt
  - ☑ MISC linux rootkit attempt lrkr0x
  - ☑ MISC linux rootkit attempt
  - ☑ MISC sm4ck attempt
  - ☑ MISC solaris 2.5 attempt
  - ☑ HidePak backdoor attempt
  - ☑ HideSource backdoor attempt
  - ☑ BAD TRAFFIC 0 ttl
  - ☑ Trin00 Daemon to Master (*HELLO
  - ☑ Trin00 Attacker to Master default p

Figure 5-7: Policy List Screen

Tip In order to find the policy you want quickly, you can sort the policies in the list. Press the “Arrange Policies” button and choose the listing method. The default setting is “by Policy Type”. You can try “by OS type” to group target machine specific policies, “by Issued Date” to get new released policies, “by alphabet” to list policies by alphabet, “by detect method provider” to group different policies released by different authority (Including user defined policies, see “define policy” section.), or “by severity” to group different severity policy.



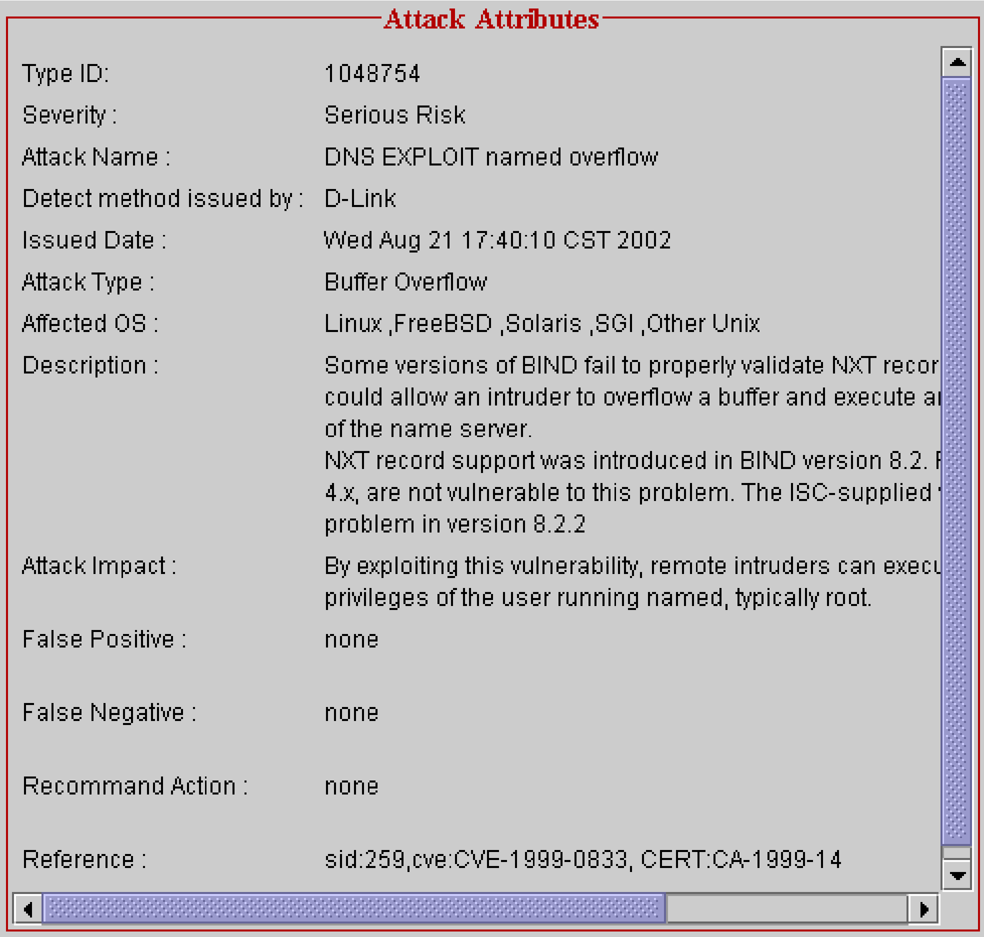
☑ DDoS
☑ Buffer Overflow
☑ Access Control
☑ Scan
☑ Torjan Horse
☑ Other
☑ HackAttack 1.20 Connect
☑ Matrix 2.0 Server access
☑ MISC linux rootkit attempt
☑ MISC linux rootkit attempt lrkr0x
☑ MISC linux rootkit attempt

☑ By policy type
□ By OS type
□ By issued date
□ By alphabet
□ By detect method provider
□ By severity

Figure 5-8: Arrange Policies Options

Policy Attribute

Each Policy has detail description about defense attack attributes. Administrator can get the detail description and recommend action.



Attack Attributes

Type ID: 1048754

Severity : Serious Risk

Attack Name : DNS EXPLOIT named overflow

Detect method issued by : D-Link

Issued Date : Wed Aug 21 17:40:10 CST 2002

Attack Type : Buffer Overflow

Affected OS : Linux ,FreeBSD ,Solaris ,SGI ,Other Unix

Description : Some versions of BIND fail to properly validate NXT recor
could allow an intruder to overflow a buffer and execute a
of the name server.
NXT record support was introduced in BIND version 8.2. F
4.x, are not vulnerable to this problem. The ISC-supplied
problem in version 8.2.2

Attack Impact : By exploiting this vulnerability, remote intruders can execu
privileges of the user running named, typically root.

False Positive : none

False Negative : none

Recommand Action : none

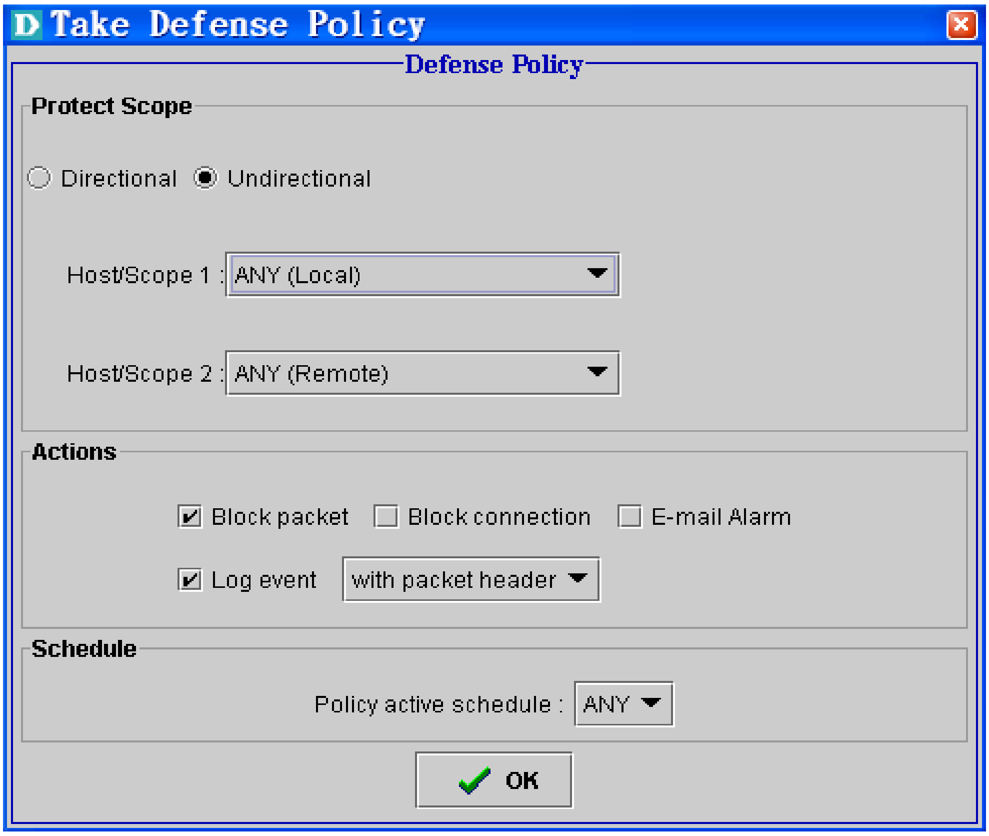
Reference : sid:259,cve:CVE-1999-0833, CERT:CA-1999-14

Figure 5-9: The Attack Attributes Frame

Defense Policy

Define Policy Protect Scope

The protect scope of a policy confine the detection range of a policy. An idea is to set the protect scope to be "Any" to "Any", but it's not practical. Since the resources and computing power of DFL-2100/DFL-2400 is limited, in order to maximize the utilization, carefully defining protect scope is necessary. For example, those policies dedicated for UNIX machines only can protect UNIX hosts, not including Windows hosts.



Take Defense Policy

Defense Policy

Protect Scope

○ Directional ● Undirectional

Host/Scope 1 : ANY (Local)

Host/Scope 2 : ANY (Remote)

Actions

☑ Block packet □ Block connection □ E-mail Alarm

☑ Log event: with packet header

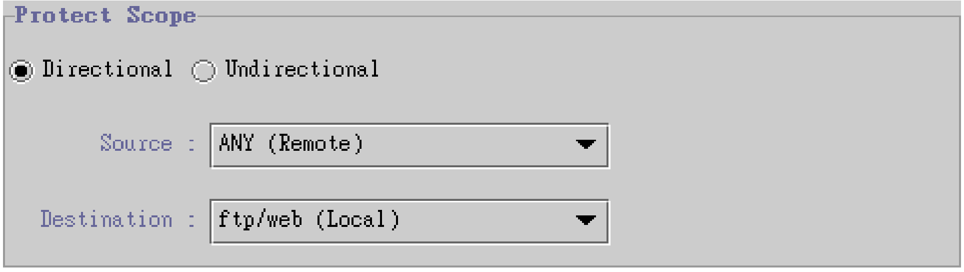
Schedule

Policy active schedule : ANY

Figure 5-10: The "Defense Policy Property" Frame

If the protect scope is defined as 'Directional', the scope are distinguished by source and destination. If it is defined as "Un-directional", the policy will protect the traffic from both directions.

Pick the protect scope by pull down the combo box; it will list available addresses and groups.



Protect Scope

● Directional ○ Undirectional

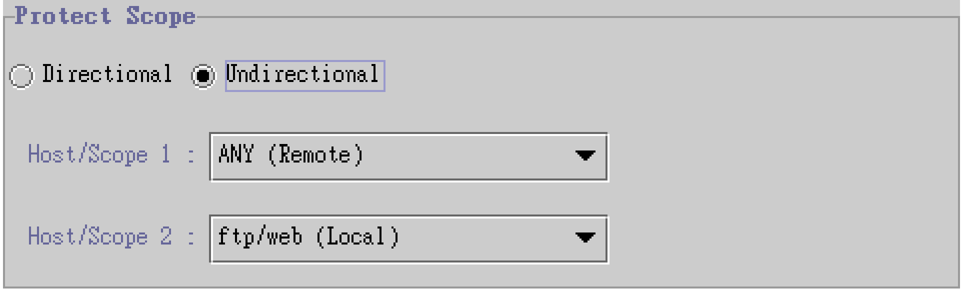
Source : ANY (Remote)

Destination : ftp/web (Local)

Figure 5-11: Directional Protect Scope

Note	Only addresses and groups already defined in Address Book and Group Book will show in the combo box. If you want to add a host in the protect scope, you have to define it in the Address Book first. See chapter 7 Policy definition Process

Note	When a “Local” address or “Local” group is chosen, the opposite field must be a “Remote” address or “Remote” group. Only traffic from “Local” to “Remote” or from “Remote” to “Local” will pass through DFL-2100/DFL-2400.



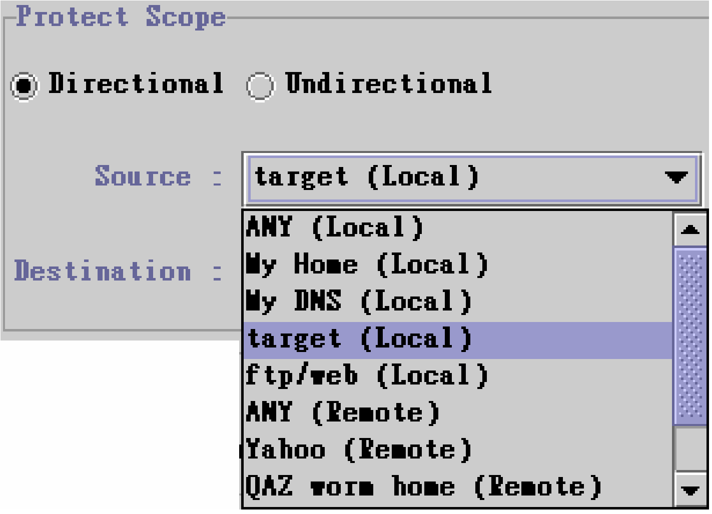
Protect Scope

○ Directional ● Undirectional

Host/Scope 1 : ANY (Remote)

Host/Scope 2 : ftp/web (Local)

Figure 5-12: Un-directional Protect Scope



Protect Scope

● Directional ○ Undirectional

Source : target (Local)

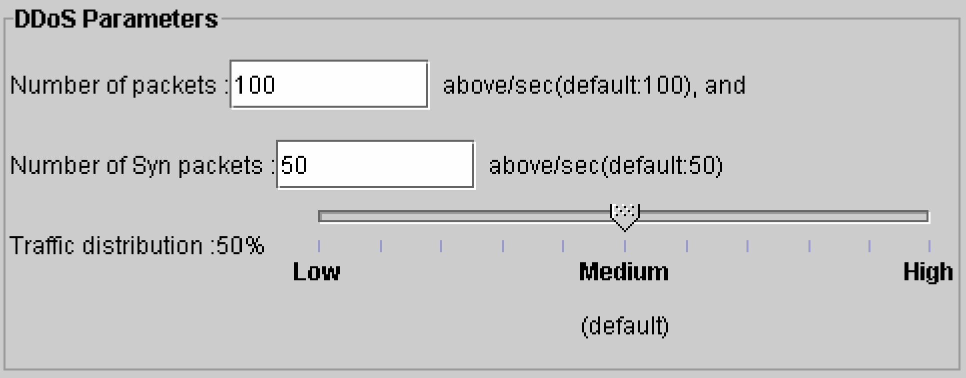
Destination :

Figure 5-13: Pick Protect Scope

Set DDoS Parameters

If a DDoS Attack Defense Policy is selected, there is no protect scope window. But the administrators need to set some parameters needed by statistical detection model. The parameters are

1. Number of packets: The lower bound number of packet passed through in a second.
2. Number of flooding/smurfing packets: The lower bound number of packets that are identified as flooding/smurfing packets in a second.
3. Traffic distribution: A number to tune the sensitivity of detection model. Range from 0 to 100. If you give a large number, the internal model of DFL-2100/DFL-2400 will be more sensitive to the variance of traffic distribution.



DDoS Parameters

Number of packets : 100 above/sec(default:100), and

Number of Syn packets : 50 above/sec(default:50)

Traffic distribution :50%

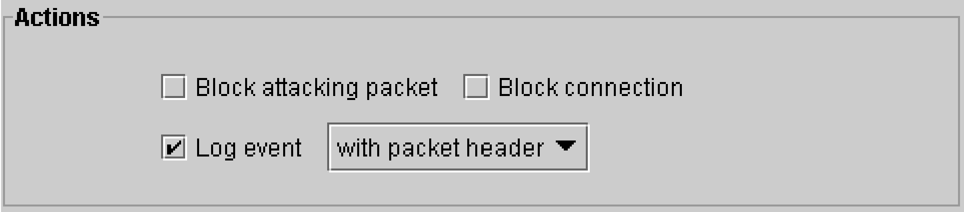
Figure 5-14: The DDoS Parameters Setup

Tip If you got a lot of false alarm of DDoS attack, you could try to lower this value. But before doing this, you had better check the DFL-2100/DFL-2400 Reporting System and inspect the logged packet headers. That makes sure that they are really false alarm or not.

Define Policy Actions

The final procedure to edit a policy is to define what kind of action will be applied when this policy conditions are matched. There are several actions are available:

1. Alarm by Email: the DFL-2100/DFL-2400 will send a mail contain the information of this attack to the email addresses of administrators defined in email trap instantly.
2. Log: the attack will be logged and managed by DFL-2100/ DFL-2400 Reporting System.
3. Block Packet: this attack packet would be dropped.
4. Block Connection: this attack packet would be dropped and its connection would be cut off.
5. Log packet headers: this attack packet header (the first 64 bytes) will be logged.



Actions

□ Block attacking packet □ Block connection

☑ Log event with packet header ▼

Figure 5-15:The Actions Setup

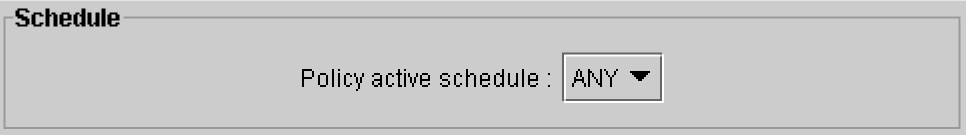
Note The logged attack event will transfer from DFL-2100/DFL-2400 to Reporting System every fixed time interval. To change this setting, see the section in DFL-2100/DFL-2400 Console/Telnet System.

Tip For some policies that are not ambiguous, uncheck “Log packet headers” will increase the utilization of DFL-2100/DFL-2400 system.

Note Only TCP policies will have the option of “Block Connection”, since other Layer 4 protocol is

Define Policy Action Schedule

At least, you must define when the defense policy will active. The default setting is all the time.


Schedule

Policy active schedule : ANY

Figure 5-16: The Schedule Setup

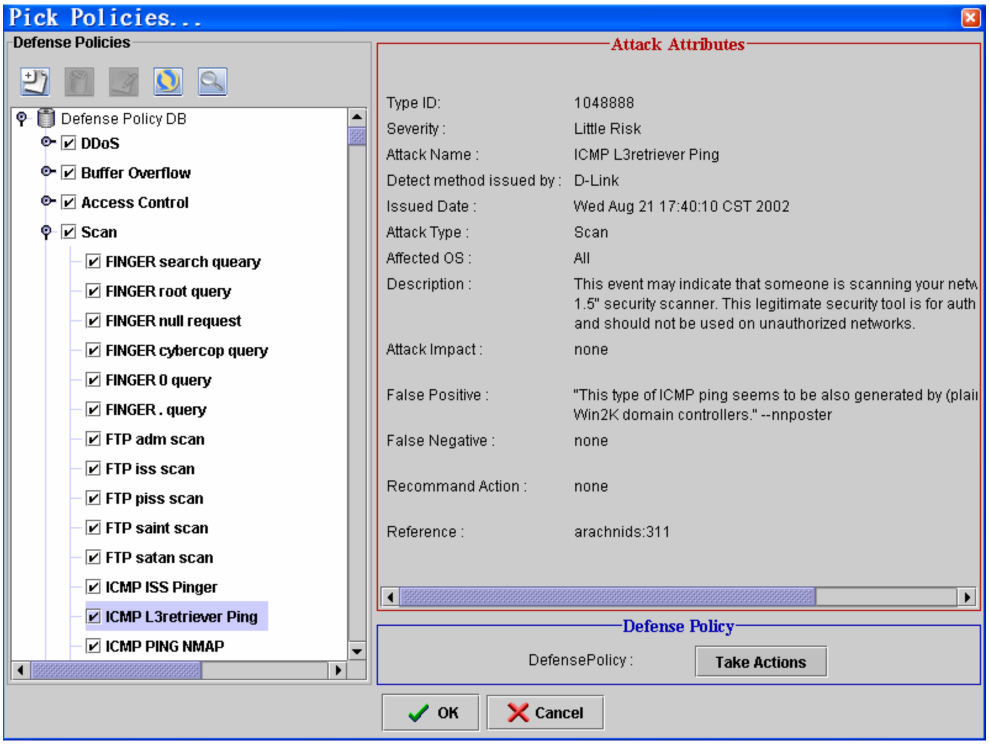
Note Only Schedule already defined in schedule Book will show in the combo box. If you want to add a schedule, you have to define it in the Schedule Book first. See chapter 7 Policy definition Process

6

DEFINE YOUR OWN DEFENSE POLICY

Define Your Own Defense Policy

The DFL-2100/ DFL-2400 IDS Management System provides a mechanism that allows multiple authorities to release attack detection database for DFL-2100/DFL-2400 users. Therefore users can get extensive support from vender or third parties. Check the "Detect method provider" from Arrange Policies button to show the policies group by provider.



- Defense Policy DB
  - ☑ DDoS
  - ☑ Buffer Overflow
  - ☑ Access Control
  - ☑ Scan
    - ☑ FINGER search queary
    - ☑ FINGER root query
    - ☑ FINGER null request
    - ☑ FINGER cybercop query
    - ☑ FINGER 0 query
    - ☑ FINGER . query
    - ☑ FTP adm scan
    - ☑ FTP iss scan
    - ☑ FTP piss scan
    - ☑ FTP saint scan
    - ☑ FTP satan scan
    - ☑ ICMP ISS Pinger
    - ☑ ICMP L3retriever Ping
    - ☑ ICMP PING NMAP

Type ID: 1048888

Severity : Little Risk

Attack Name : ICMP L3retriever Ping

Detect method issued by : D-Link

Issued Date : Wed Aug 21 17:40:10 CST 2002

Attack Type : Scan

Affected OS : All

Description : This event may indicate that someone is scanning your netw 1.5" security scanner. This legitimate security tool is for auth and should not be used on unauthorized networks.

Attack Impact : none

False Positive : "This type of ICMP ping seems to be also generated by (plai Win2K domain controllers." --nnposter

False Negative : none

Recommand Action : none

Reference : arachnids:311

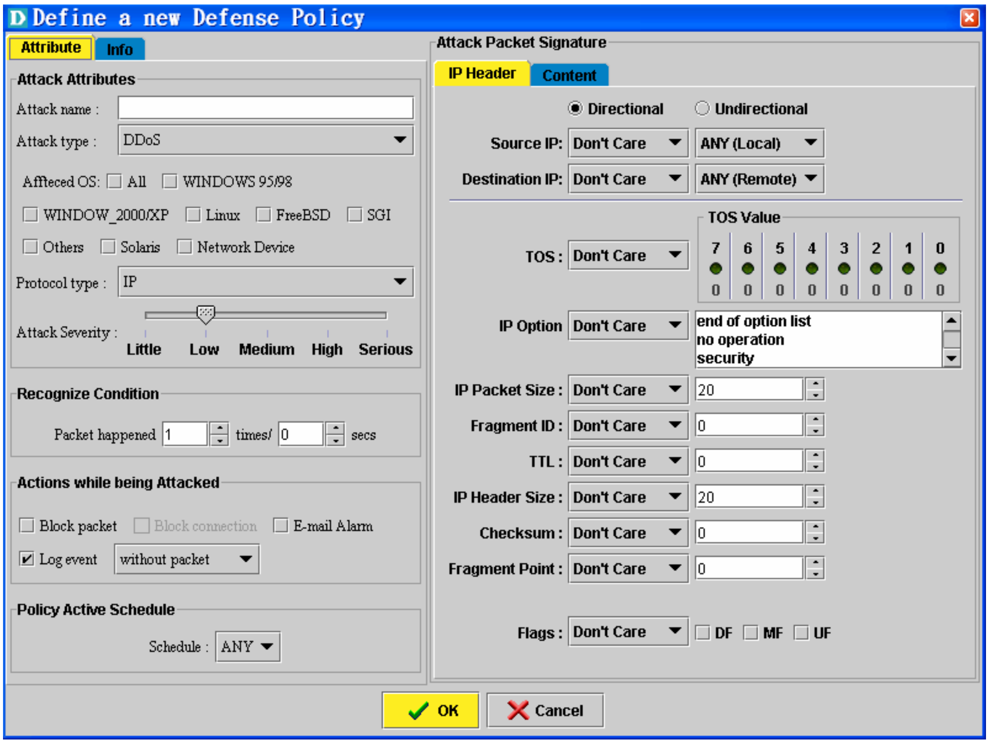
DefensePolicy : Take Actions

Figure 6-1: The Defense Policy database widow

But the DFL-2100/ DFL-2400 Management System also allows users to define their own policies. Press the "**Define a New Policy**" button in the "Defense Policy database" Window, a "Define New Policy" window will show as following figure.

Note All policies created by users are labeled as "User Defined". And only "User Defined" policies can be modified and deleted. Policies issued by vender or third parties can not modified or deleted, users can change their protect scope, schedule and actions only.

Note Before you define your own policies, be sure that you know how the network works. There are lots of fields in the “Define your own policy” procedure.



Define a new Defense Policy

Attack Attributes

Attack name :

Attack type : DDoS

Affeced OS: □ All □ WINDOWS 95/98 □ WINDOW_2000/XP □ Linux □ FreeBSD □ SGI □ Others □ Solaris □ Network Device

Protocol type : IP

Attack Severity : Little Low Medium High Serious

Recognize Condition

Packet happened 1 times/ 0 secs

Actions while being Attacked

□ Block packet □ Block connection □ E-mail Alarm

☑ Log event without packet

Policy Active Schedule

Schedule : ANY

● Directional ○ Undirectional

Source IP: Don't Care ANY (Local)

Destination IP: Don't Care ANY (Remote)

TOS : Don't Care

TOS Value							
7	6	5	4	3	2	1	0
●	●	●	●	●	●	●	●
0	0	0	0	0	0	0	0

IP Option Don't Care — end of option list / no operation / security

IP Packet Size : Don't Care 20

Fragment ID : Don't Care 0

TTL : Don't Care 0

IP Header Size : Don't Care 20

Checksum : Don't Care 0

Fragment Point : Don't Care 0

Flags : Don't Care □ DF □ MF □ UF

Figure 6-2: The” Define new Defense Policy” Window

The procedure of defining your own policy is:

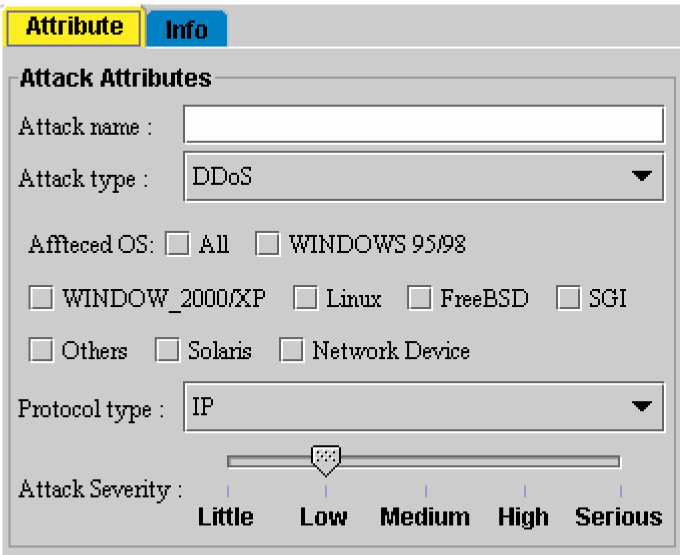
1. Fill the “Defense Policy Attributes” frame.
2. Determine the “Recognize condition” constraint of a policy.
3. Determine the “Action while being attacked” for this policy.
4. Determine the “Policy active schedule” for this policy.
5. Fill the “Packet Criteria” frame.

We will illustrate the procedure in details in the following sections.

Fill Defense Policy Attributes

In “Defense Policy Attribute” frame, you have to give some information about the attack you want to detection or the access you want to control.

1. **Attack name:**
   The name is given to identify, to show on the reporting system or emails. It must be a unique one.
2. **Attack type:**
   Determine what kind of attack that this belongs to. Available options are: DDOS, Buffer Overflow, Access Control, Scan, Trojan Horse and etc.
3. **Affected OS type:**
   Determined what kind of OS would be suitable to apply this policy. This field can have multiple options.
4. **Protocol type:**
   What kind of layer 4 protocol that this policy is on, it can be TCP, UDP, ICMP and IGMP. If you want to detect IP packets only, choosing IP is fine.
5. **Attack Severity:**
   It defines the dangerous level of the attack that this policy wants to detect.



Attack Attributes

Attack name :

Attack type : DDoS

Affteced OS: □ All □ WINDOWS 95/98 □ WINDOW_2000/XP □ Linux □ FreeBSD □ SGI □ Others □ Solaris □ Network Device

Protocol type : IP

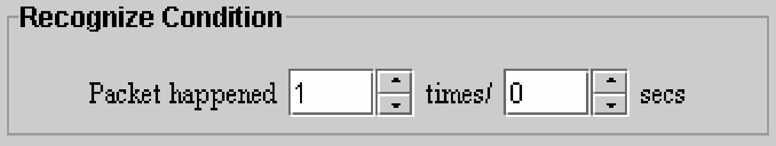
Attack Severity : Little Low Medium High Serious

Figure 6-3: The” Defense Policy Attributes” Frame

Determine the Recognize Condition.

For some defense policies, a single packet doesn't harm the network integrity; we must collect enough packets to identify an attack. Two parameters "**Repetition**" and "**Duration**" are introduced to increase to precision.

"Packet happened times" means we must collect enough repetitive packets. The default value is 1. "In every sec" means the time interval from first packet detected to the last packet that qualified the repetition constraint. If the DFL-2100/DFL-2400 doesn't collect enough matched packets during this duration time, the repetition count is reset to zero.



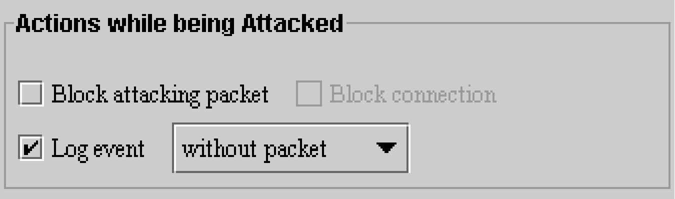
Recognize Condition

Packet happened 1 times/ 0 secs

Figure 6-4: The" Recognize condition" Frame

Determine the Action While Being Attacked

It is the same as section "Define Policy Actions".



Actions while being Attacked

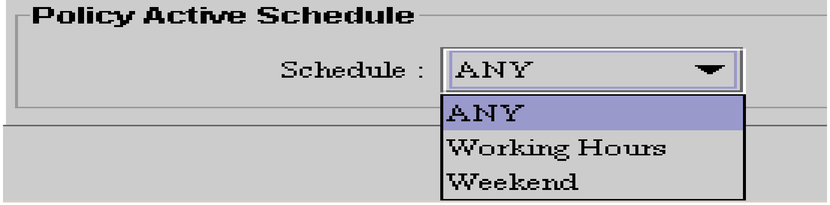
□ Block attacking packet □ Block connection

☑ Log event without packet

Figure 6-5: The" Actions" Frame

Pick Up the Schedule

Determine the enabled time slot for this policy; pick the schedule you want from the combo box.



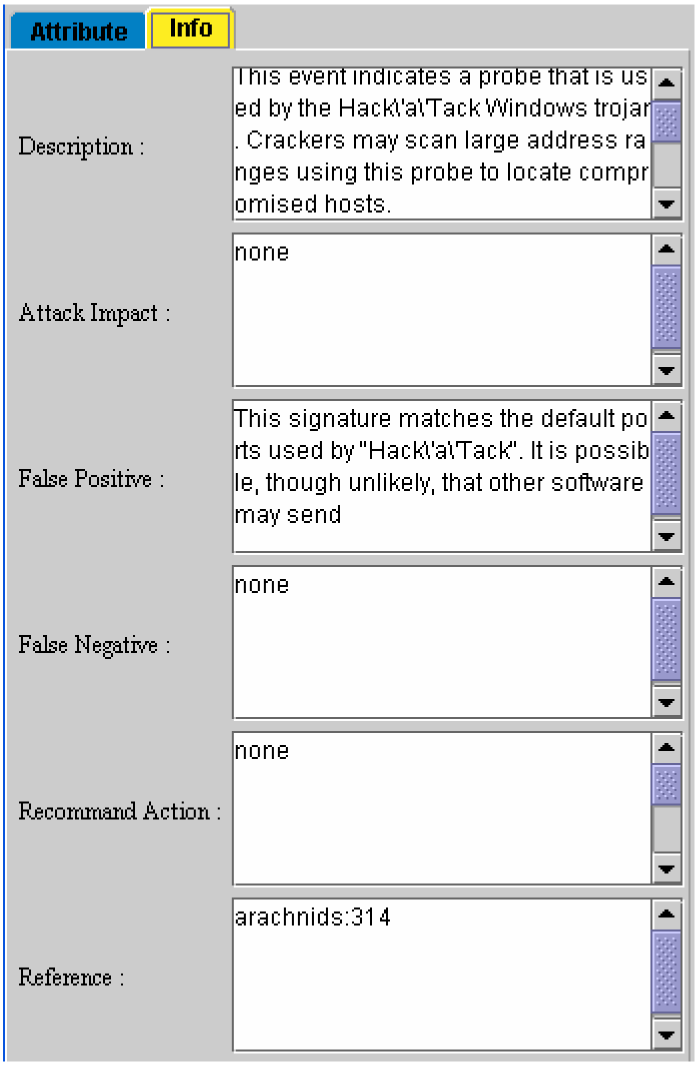
Policy Active Schedule

Schedule : ANY

Figure 6-6: The" Schedule" Frame

Description:

When we define a new attack policy, we should give some reference information about this attack. It will be very useful for other user to understand the policy. There is some information filed about the policy should be descript.



Description : This event indicates a probe that is used by the Hack\'a\Tack Windows trojan. Crackers may scan large address ranges using this probe to locate compromised hosts.

Attack Impact : none

False Positive : This signature matches the default ports used by "Hack\'a\Tack". It is possible, though unlikely, that other software may send

False Negative : none

Recommand Action : none

Reference : arachnids:314

Figure 6-7: The policy information

Fill the Packet Criteria

The packet criteria section is the heart of a policy. It defines lots of parameters to detect attacks or control access. There are tabs in this frame. And the tabs are shown according to your selection of “Protocol type” in “Policy Property”:

Protocol Type	Policy Property Tabs
IP	IP, Content
TCP	IP, TCP, Content
UDP	IP, UDP, Content
ICMP	IP, ICMP, Content
IGMP	IP, IGMP, Content

Table 6-1: ”Protocol Type” and “Policy Property Tabs”

The Comparison Operations

There are lots of fields in each tab. When the value of a field is given, you should specify the comparison operations. There four sets of operations (see below figure).

Note If a value is given but the “Comparison Operation” is set to “Don’t Care”, then this field is discarding.

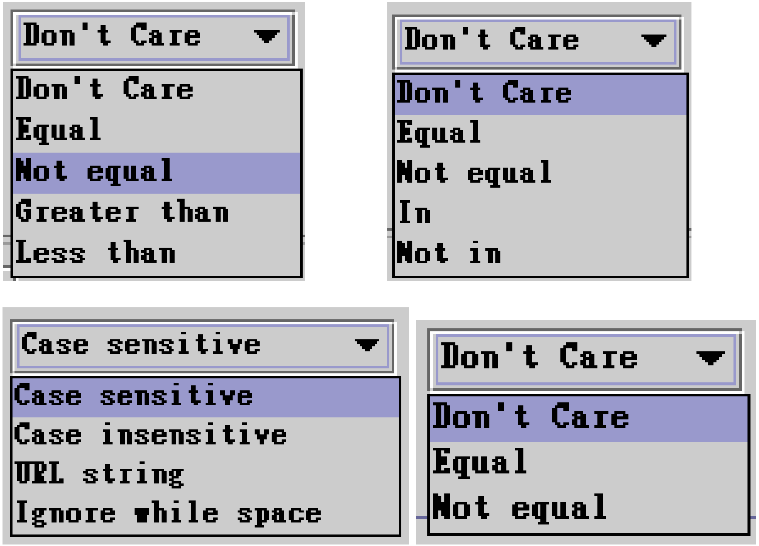
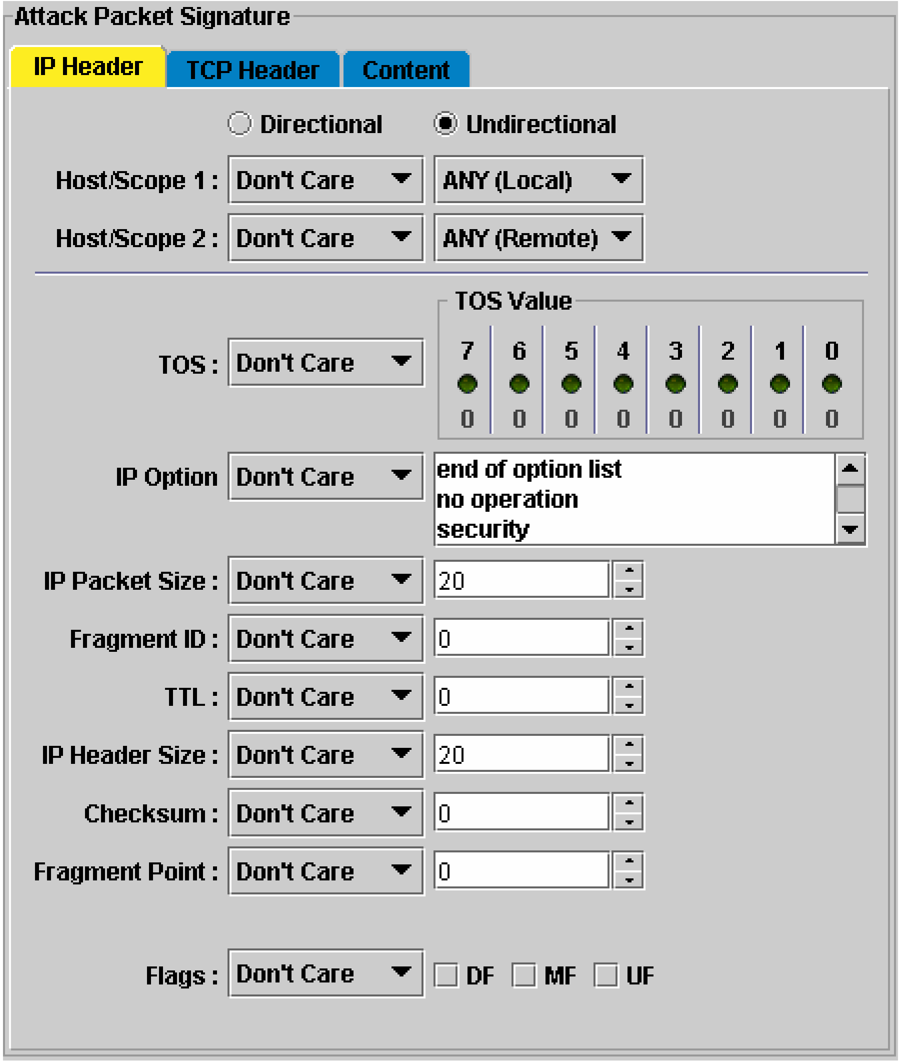


Figure 6-8: The ”Comparison Operations”

The IP Tab

The IP tab consists parameters for IP packet header field value settings:

1. Directional/Un-directional: This is the same as protect scope.
2. Source, Destination: Source and Destination addresses.
3. TOS: Type of service in IP header.
4. IP Packet Size: IP packet total size.
5. Fragment ID: IP packet identification field.
6. TTL: IP time to live field.
7. IP Header size: IP header size.
8. Checksum: IP checksum field.
9. Fragment Pointer: IP fragment pointer value.
10. Flags: DF-Don’t Fragment, MF-More Fragment, UF-Unused Flag.



○ Directional ● Undirectional

Host/Scope 1 : Don't Care | ANY (Local)

Host/Scope 2 : Don't Care | ANY (Remote)

TOS : Don't Care

TOS Value

7	6	5	4	3	2	1	0
●	●	●	●	●	●	●	●
0	0	0	0	0	0	0	0

IP Option Don't Care

end of option list
no operation
security

IP Packet Size : Don't Care | 20

Fragment ID : Don't Care | 0

TTL : Don't Care | 0

IP Header Size : Don't Care | 20

Checksum : Don't Care | 0

Fragment Point : Don't Care | 0

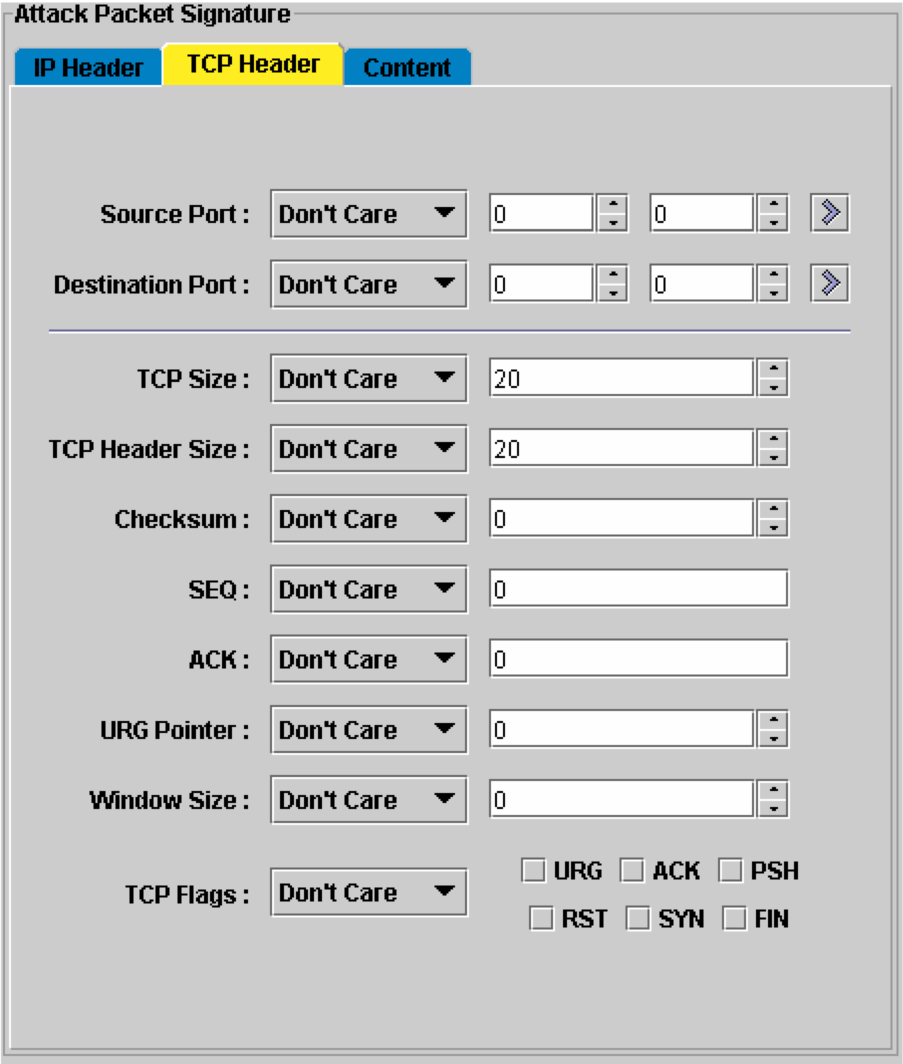
Flags : Don't Care | □ DF □ MF □ UF

Figure 6-9: The ”IP Tab”

The TCP Tab

The TCP tab consists parameters for TCP packet header field value settings:

1. Source, Destination Port: Source and Destination port number
2. TCP Size: TCP packet total size.
3. TCP Header size: TCP header size.
4. Checksum: TCP checksum field.
5. SEQ: TCP sequence number.
6. ACK: TCP acknowledgement number.
7. URG Pointer: TCP urgent pointer value.
8. Window size: TCP window value.
9. TCP Flags: URG-urgent, ACK-acknowledgement, PSH-push, RST-reset, SYN-synchronization, FIN-finish.



Source Port : Don't Care 0 0

Destination Port : Don't Care 0 0

TCP Size : Don't Care 20

TCP Header Size : Don't Care 20

Checksum : Don't Care 0

SEQ : Don't Care 0

ACK : Don't Care 0

URG Pointer : Don't Care 0

Window Size : Don't Care 0

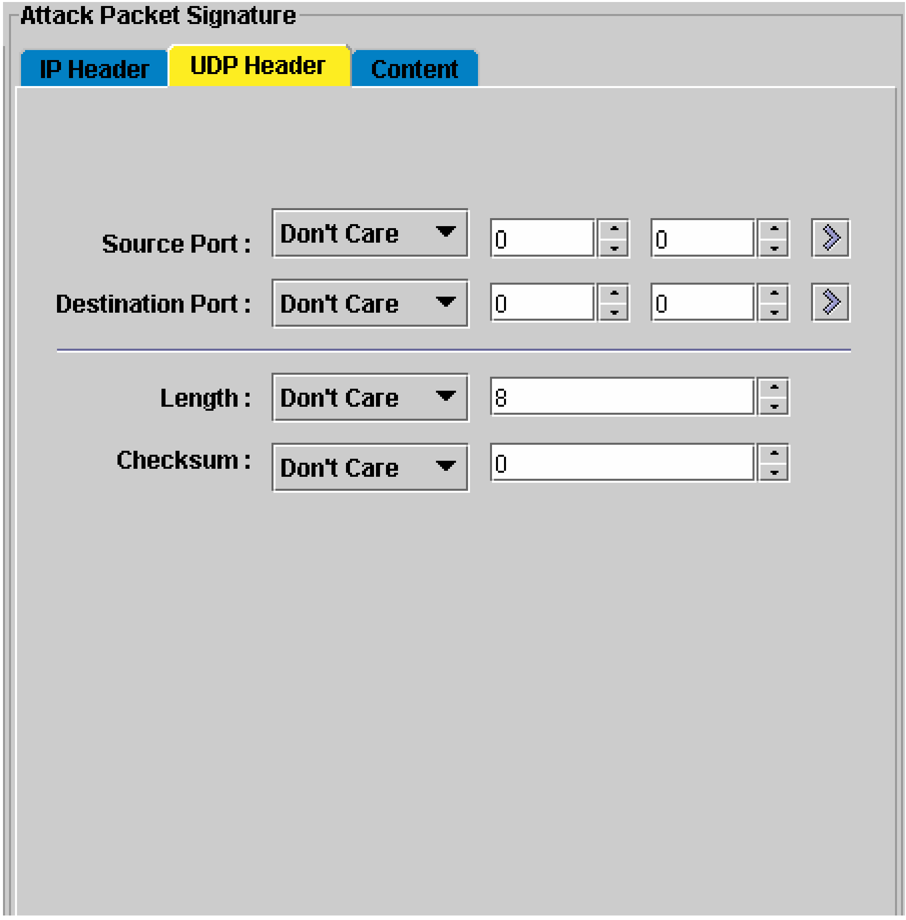
TCP Flags : Don't Care □ URG □ ACK □ PSH □ RST □ SYN □ FIN

Figure 6-10: The ”TCP Tab”

The UDP Tab

The UDP tab consists parameters for UDP packet header field value settings:

1. Source, Destination Port: Source and Destination port number
2. Length: UDP packet total size.
3. Checksum: UDP checksum field.



Source Port : Don't Care 0 0

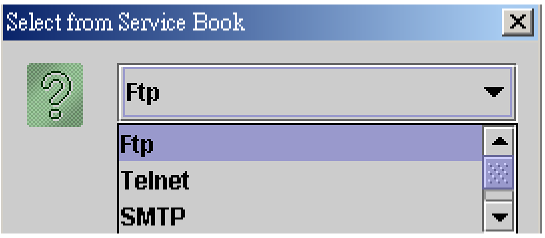
Destination Port : Don't Care 0 0

Length : Don't Care 8

Checksum : Don't Care 0

Figure 6-11: The "UDP Tab"

Note The port number can be chosen by the button › . It will show the service name that defined in the service.



Ftp

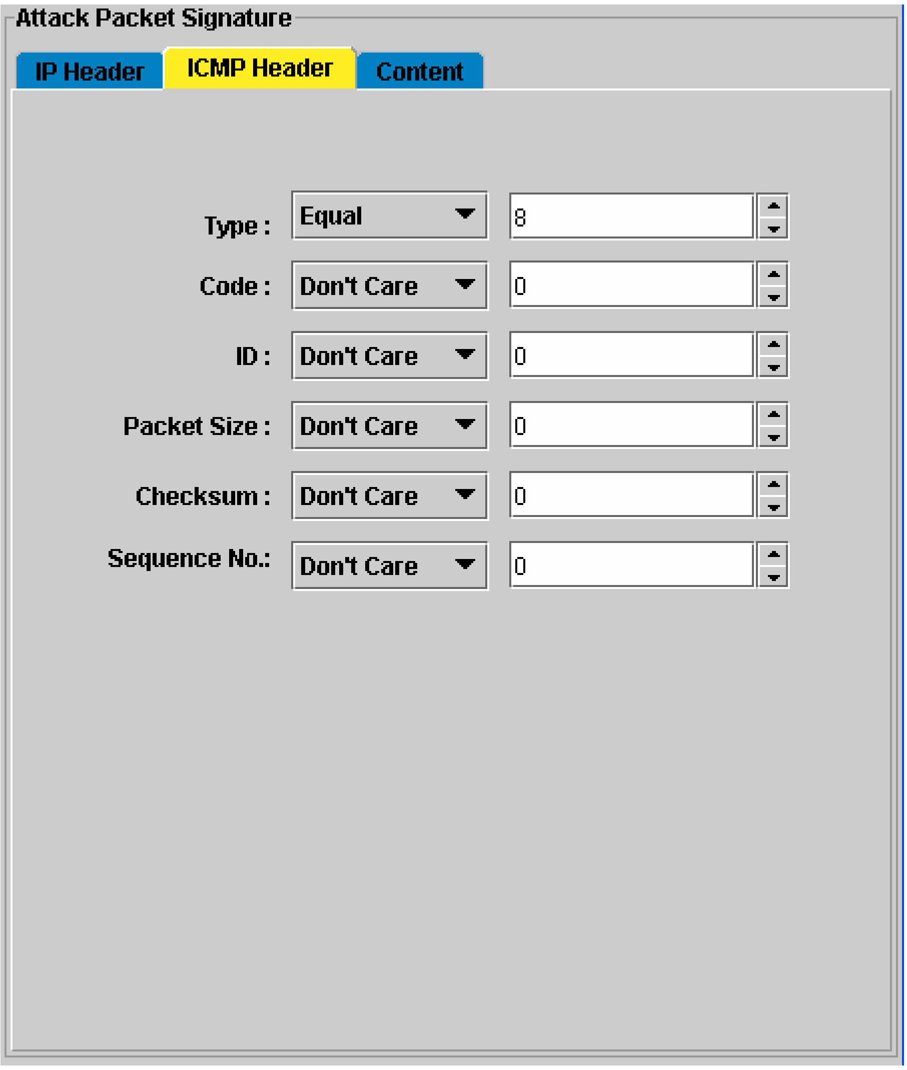
Ftp
Telnet
SMTP

Figure 6-12: The "Select from Service Book"

The ICMP Tab

The ICMP tab consists parameters for ICMP packet header field value settings:

1. Type: ICMP type field.
2. Code: ICMP code field.
3. ID: ICMP identification value
4. Packet Size: ICMP packet total size.
5. Checksum: ICMP checksum field.
6. Sequence: ICMP sequence number.



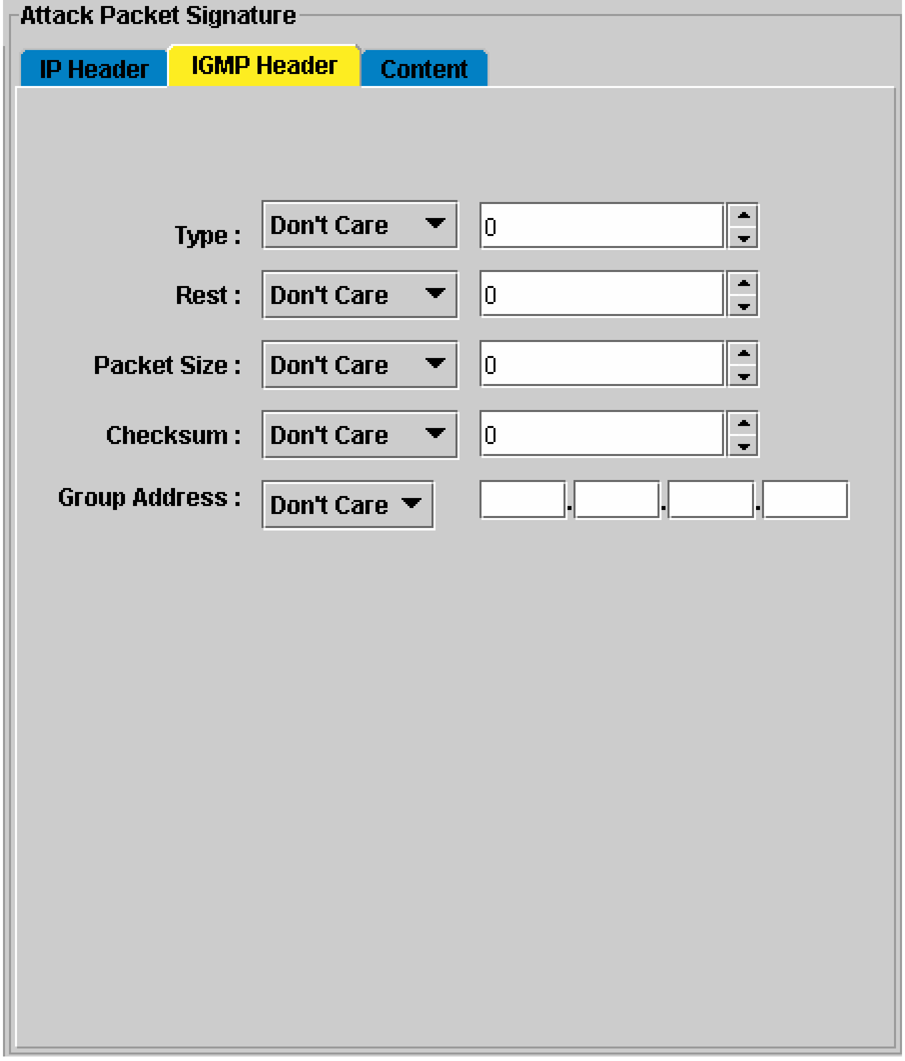
Type : Equal 8
Code : Don't Care 0
ID : Don't Care 0
Packet Size : Don't Care 0
Checksum : Don't Care 0
Sequence No.: Don't Care 0

Figure 6-13: The ”ICMP Tab”

The IGMP Tab

The IGMP tab consists parameters for IGMP packet header field value settings:

1. Type: IGMP type field.
2. Rest: IGMP max response time field.
3. ID: IGMP identification value
4. Packet Size: IGMP packet total size.
5. Checksum: ICMP checksum field.
6. Group Address: IGMP group address value.



Type : Don't Care 0

Rest : Don't Care 0

Packet Size : Don't Care 0

Checksum : Don't Care 0

Group Address : Don't Care . . .

Figure 6-14: The ”IGMP Tab”.

The Content Tab

The Content tab consists parameters for searching payload of packets.

Note If “Protocol Type” is IP, the matching starting point is at the end of IP (layer 3) header, otherwise, it would start matching from the end of layer 4 headers.

1. Match String: the string can be ASCII or HEX strings. If HEX string is used, allowable alphabet is ‘0’-‘9’, ‘A’-‘F’, ‘a’-‘f’.
2. Matching offset: the offset from the start point of payload.
3. Matching method: the matching method can be,

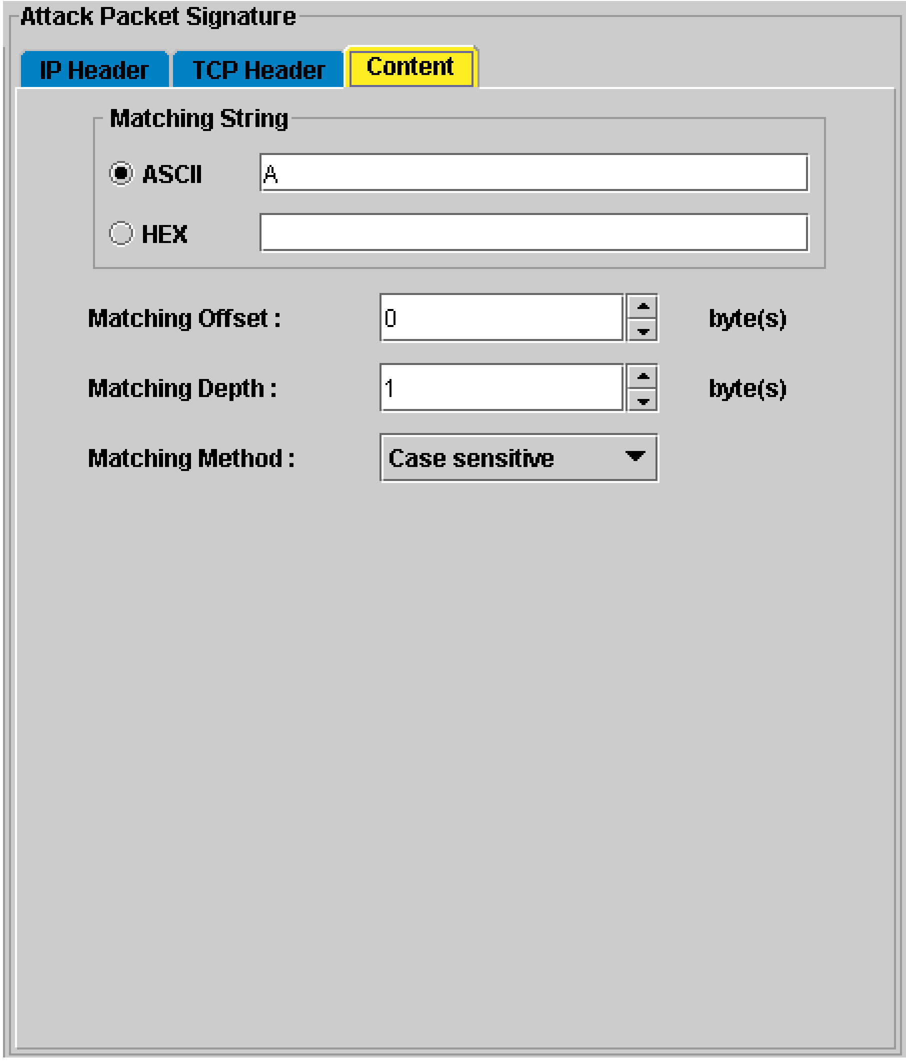
- Case sensitive: lower case and upper case characters are different. This is the default value.
- Case insensitive: ignore the differences of upper case and lower case characters.
- Ignore white space: ignore the white space occurred in the payload, such as blank, tab, new line, linefeed, carriage return.
- URL strings: the URL portion of payload will be extracted and parsed. And the sub string of pattern before the character ‘?’ will be regarded as the base part of URL, and the others are the parameters of URL. The URL matching is case insensitive by default, but it won’t remove the white spaces.

Note The order of URL parameters doesn’t matter. For example, given a pattern “/cgi-bin/foo.exe?p1=abc&p2=def”. An URL packet with URL request “/cgi-bin/foo.exe?p2=def&p1=abc” is considered as a match.

Note The extra parameters in the payload don't matter, too.

For example, given a pattern "***/cgi-bin/foo.exe?p1=abc&p2=def*** ".

An URL packet with URL request "***/cgi-bin/foo.exe?p0=xyz&p1=abc&p2=def***" is considered as a match.



Attack Packet Signature

Matching String

● ASCII: A

○ HEX:

Matching Offset : 0 byte(s)

Matching Depth : 1 byte(s)

Matching Method : Case sensitive

Figure 6-15: The "Content Tab".

7

POLICY DEFINITION PROCESS

In this Chapter we will discuss setting the parameters of books. These books will be used in Policy definition.

Edit Service Book

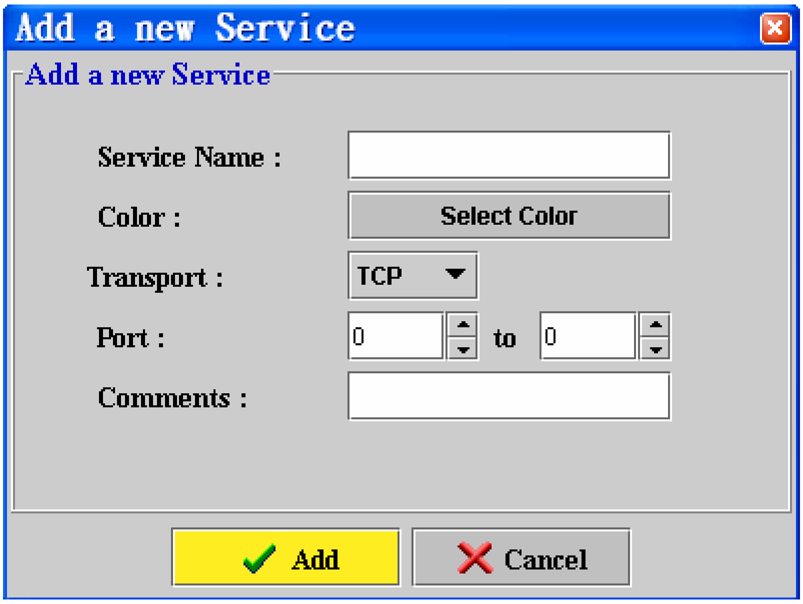
DFL-2100/DFL-2400 can support attack detection on the different types of Services, such as FTP, HTTP, SMTP, and so on. These Services are defined in the Service Book. DFL-2100/DFL-2400 has predefined several Services commonly seen in the network. You can also define your own Services and add them to the Service Book.

Click **Service Book** button to display the content of Service Book showing in the Book Table window.

> **Note**
>
> All the changes to the Service Book will not take effect until the red - lighted **Confirm** button is clicked.

Add a Service

1. Click **Service Book** button to switch to the Service Book page.
2. Click **Add** button or right-click on the Book Table and select **Add**. The following dialog appears.
3. Assign a unique **Service Name**.
4. Assign a unique **Color** as an identifier in the Reporting System.
5. Select a type (TCP or UDP) from the **Service Type** pull-down menu.
6. If the type of Service is other than a FTP service, the **From Port** and **To Port** field must be specified, else check the **View as FTP Service** box and specify the **Control Port** and **Data Port**.
7. Enter your **Comment** for this Service.
8. Click **Add** to add the Service to the Service Book.


Add a new Service

Add a new Service

Service Name :

Color : Select Color

Transport : TCP

Port : 0 to 0

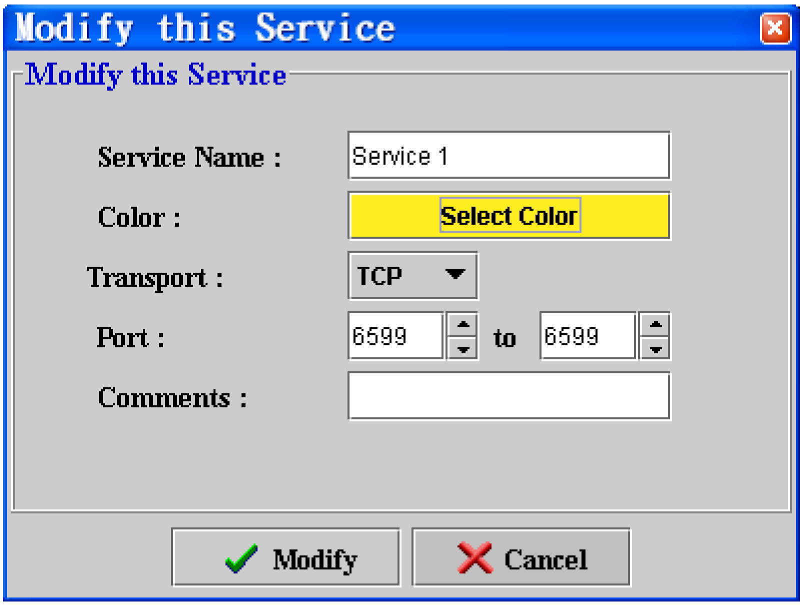
Comments :

Figure 7-1: ”Add a Service” Dialog

Modify a Service

1. Click **Service Book** button to switch to the Service Book page.
2. Click **Modify** button or right-click on the Book Table and select Modify. The following dialog appears.
3. Modify any of these fields as you wish.
4. Click **Modify** to update this Service.

Note	You cannot modify a default Service.


Modify this Service

Modify this Service

Service Name : Service 1

Color : Select Color

Transport : TCP

Port : 6599 to 6599

Comments :

Figure 7-2: ”Modify a Service” Dialog

Delete a Service

Select the Service to be deleted from the Service Book Table and click the Delete button or right-click on the table and select “Delete”.

Note	You cannot delete a Service that is currently referenced by the Policy Rules.

Edit Address Book

An Address is a target element of your network such as a PC or a LAN. You can specify an Address with its own IP, MAC, and net mask so that detection can be managed for a specific IP host or subnet with the same net mask. Because for different machines that with different operating systems and different services, the policies applied for each host are varied. For example, DNS and web servers may run on UNIX machines while end user may use Windows at their PC. Attack detection policies for UNIX and Windows are quite different. Therefore, administrator can define specific name for each host, and the names will be used in the policies. The Addresses defined in the *Address Book* are listed in the Address Book Table.

Addresses can be classified into two categories:

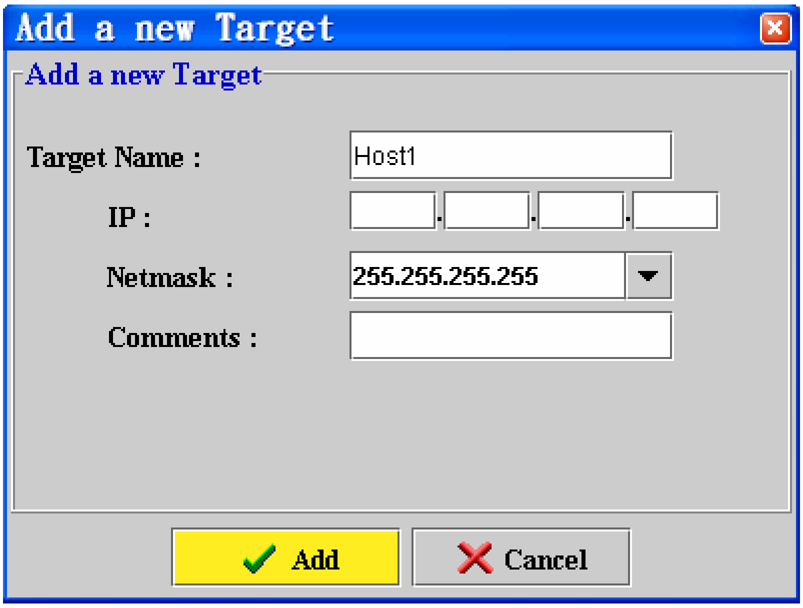
1. **Remote Address:** Addresses beyond the DFL-2100/DFL-2400.
2. **Local Address:** Addresses behind the DFL-2100/DFL-2400.

Click Address Book button to display the content of Service Book showing in the Book Table window.

Note	All changes to the Address Book will not take effect until the red - lighted **Confirm** button is clicked.

Add an Address

1. Click **Address Book** button to switch to the Address Book page.
2. Click **Add** button or right-click on the Book Table and select **Add**.
3. Specify a unique **Device Name**.
4. Enter the **IP Address**.
5. Select a net mask from the **Net mask** pull-down menu or enter your own net mask.
6. Enter your **Comment** for this Address.
7. Click **Add** to add this Address to the Address Book.



Add a new Target

Add a new Target

Target Name : Host1

IP : . . .

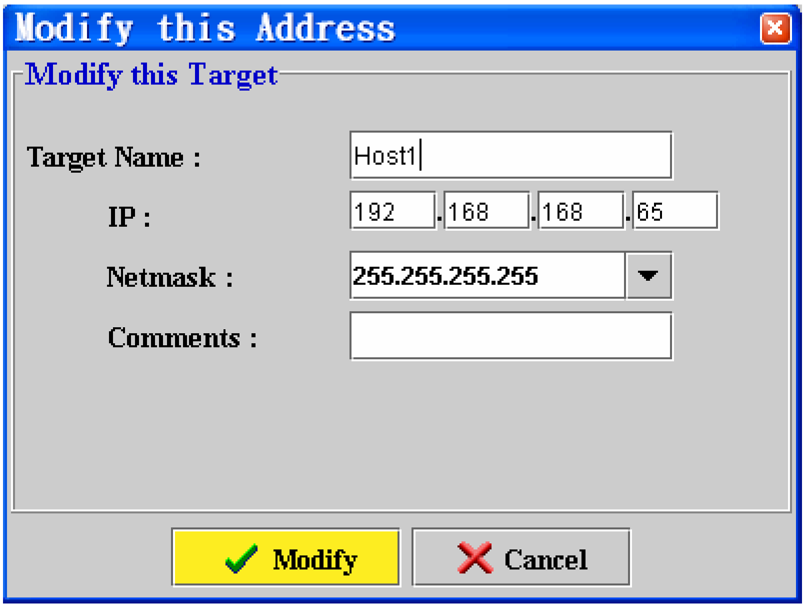
Netmask : 255.255.255.255

Comments :

Figure 7-3: ”Add a new Address” Dialog

Modify an Address

1. Click Address Book button to switch to the Address Book page.
2. Click Modify button or right-click on the Book Table and select Modify. The following dialog appears.
3. Modify any of these fields as you wish.
4. Click Modify to update this Address or Cancel to remain unchanged.



Target Name : Host1
IP : 192.168.168.65
Netmask : 255.255.255.255
Comments :

Figure 7-4: "Modify an Address" Dialog

Delete an Address

Select the entries to be deleted on the Address Book Table and click the **Delete** button or right-click on the table and select "Delete" from the pop-up menu.

Note	You cannot delete an Address that is currently referenced by the Policy Rules.

Edit Group Book

Groups are used to organize a set of Policy Rules so that they can be enabled or disabled together. For example, you can put a set of Rules in Group_A and another set of Rules in Group_B, then you can disable all the Rules in Group_A by just disabling Group_A instead of disabling all the Rules in Group_A one bye one.

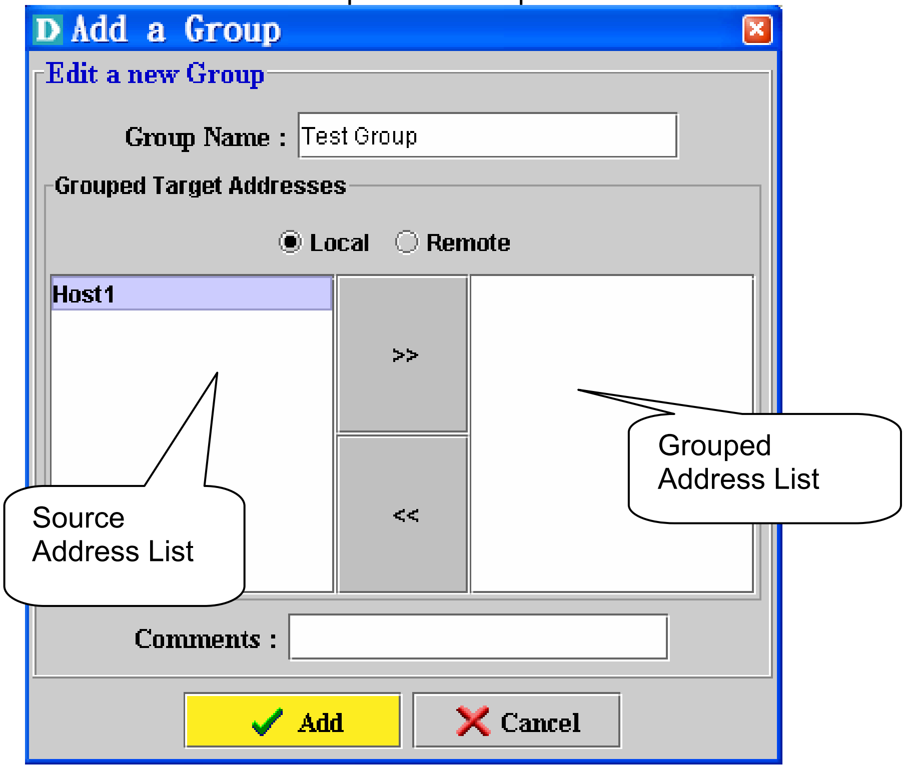
Note

(a) All the changes to the Schedule Book will not take effect until the red -lighted **Confirm** button is clicked.

(b) A disabled Rule in an enabled Group is still disabled, and a enabled Rule in a disabled Group is still disabled.

Add a Group

1. Click Group Book button to switch to the Group Book page.
2. Click Add button or right-click on the Book Table and select Add. The following dialog appears.
3. Enter the Group Name.
4. Select one or more Addresses from the Source Address List and click >>, the selected Addresses then be added to the Grouped Address List.
5. Enter your Comment for this Group.
6. Click Add to add the Group to the Group Book.



Group Name : Test Group

● Local ○ Remote

Comments :

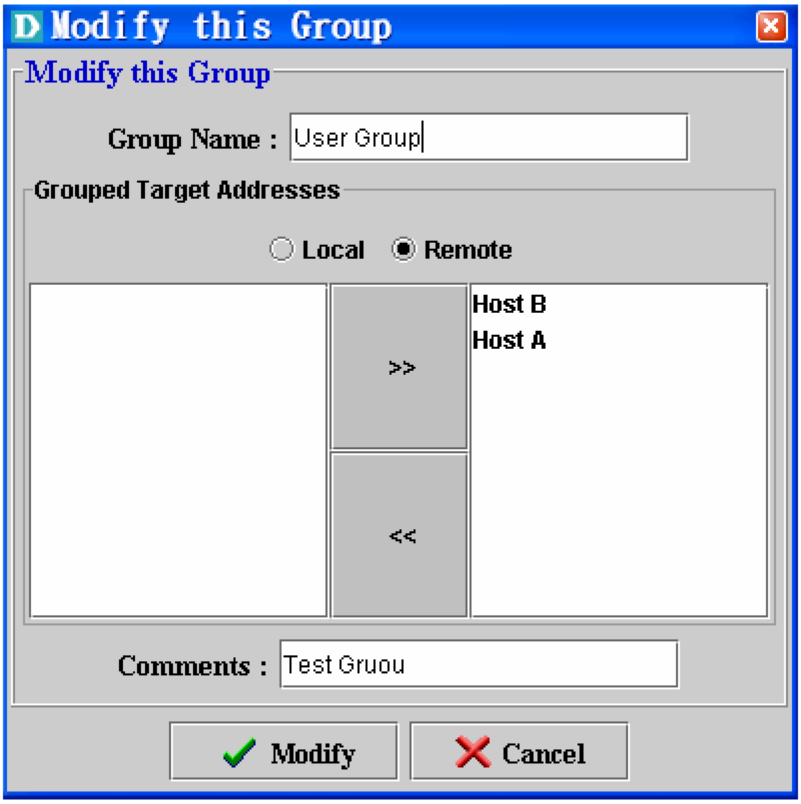
Source Address List

Grouped Address List

Figure 7-5: "Add a new Group" Dialog

Modify a Group

1. Click Group Book button to switch to the Group Book page.
2. Click Modify button or right-click on the Book Table and select Modify. The following dialog appears.
3. Modify any of these fields as you wish.
4. Click Modify to update this Schedule or Cancel to remain unchanged.



Group Name : User Group

○ Local ● Remote

Host B
Host A

Comments : Test Gruou

Figure 7-6: ”Modify a Group” Dialog

Delete a Group

Select the entries to be deleted on the Group Book Table and click the Delete button or right-click on the table and select “Delete” from the pop-up menu.

Note	You cannot delete a Group, which is currently referenced by the Policy Rules.

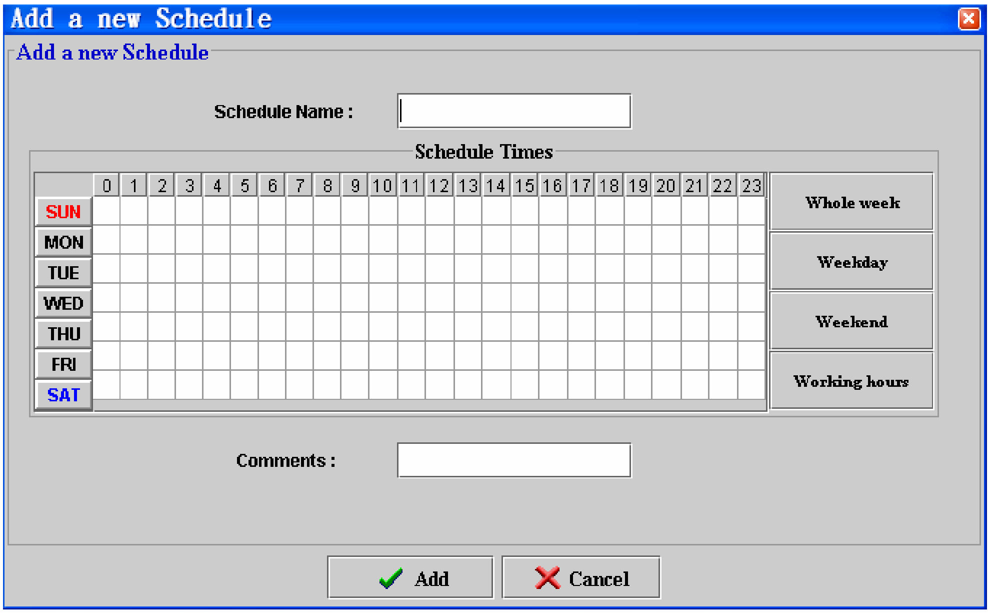
Edit Schedule Book

DFL-2100/DFL-2400 allows you to define policy enable time based on the schedule predefined in the Schedule Book. You can specify a Schedule as one or more periods of time slots that composed of any hour in a week.

Note All the changes to the Schedule Book will not take effect until the red -lighted **Confirm** button is clicked.

Add a Schedule

1. Click **Schedule Book** button to switch to the Schedule Book page.
2. Click **Add** button or right-click on the Book Table and select **Add**.
3. Specify a unique **Schedule Name**.
4. Click or drag a scope with your mouse on the **Schedule Time Table** to select the time that rule is to be triggered. The selected time box will be checked. You can also use the predefined schedule time by clicking the **Weekday, Weekend, Working Hours,** and Whole Week button on the right side of the table. Duplicate selection on the same time box will uncheck it.
5. Enter your **Comment** for this Schedule.
6. Click **Add** to add the Schedule to the Schedule Book.



Add a new Schedule

Add a new Schedule

Schedule Name :

Schedule Times

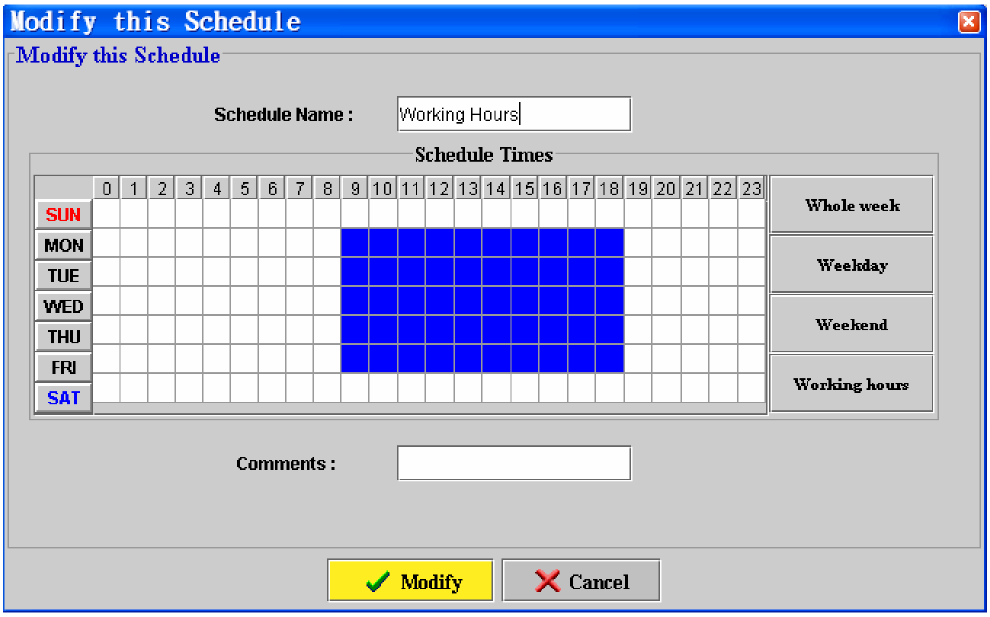
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SUN																								
MON																								
TUE																								
WED																								
THU																								
FRI																								
SAT																								

Comments :

Figure 7-7: ”Add a new Schedule” Dialog

Modify a Schedule

1. Click **Schedule Book** button to switch to the Schedule Book page
2. Click **Modify** button or right-click on the Book Table and select Modify. The following dialog appears.
3. **Modify** any of these fields as you wish.
4. Click **Modify** to update this Schedule or **Cancel** to remain unchanged.



Schedule Name : Working Hours

Schedule Times

	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										■	■	■	■	■	■	■	■	■	■					
SAT																								

Comments :

Figure 7-8: "Modify this Schedule" Dialog

Delete a Schedule

Select the entries to be deleted on the Schedule Book Table and click the Delete button or right-click on the table and select "Delete" from the pop-up menu.

Note	You cannot delete a Schedule that is currently referenced by the Policy Rules.

8

IDS REPORTING SYSTEM

The DFL-2100/DFL-2400 IDS Reporting System

DFL-2100/ DFL-2400 IDS Reporting System is an analysis tool that manages network attacks events and the records of DFL-2100/DFL-2400 system. It cannot only inquire about any network attack, but also simultaneously monitor network traffic and attacks circumstances. In terms of operation, DFL-2100/ DFL-2400 IDS Reporting System can support any Java Runtime Environment (JRE) by web servers. Users with authority are able to use browsers supporting Java Program (such as Internet Explorer or Netscape Navigator) to monitor the whole condition of network attacks through web-based IDS Reporting System.

Function	Description
Real-time network attacks monitor	Provides a real-time monitor for network attacks and classifies attacks according to their threatening levels to monitor.
Network attack reports	The reports can review detected attacks according to IP address, attack names, the level of attacks and attack time. It also provides analysis in the forms of statistical charts and bar charts.
Real-time traffic monitor	Provides options of different printing formats.
System events	Reviews operational events of DFL-2100/DFL-2400 system.

Table 8-1: The function list of DFL-2100/ DFL-2400 Reporting System

Main screen

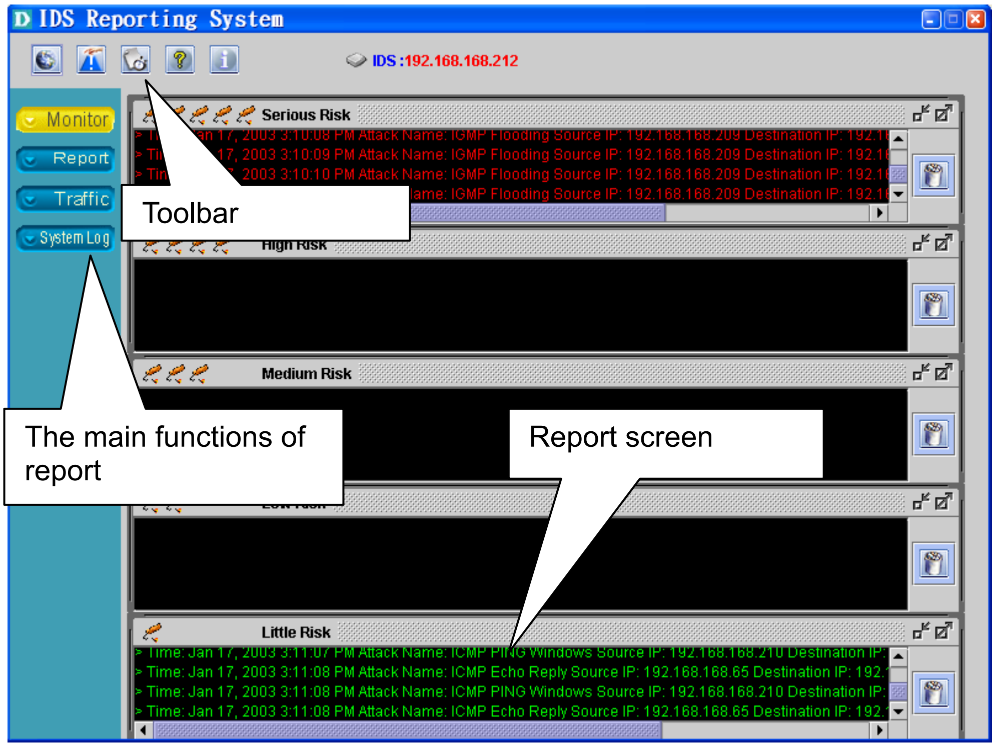
The main screen of DFL-2100/ DFL-2400 IDS Reporting System is composed of three parts.

1. The toolbar of DFL-2100/ DFL-2400 IDS Reporting System:

Toolbar icons	Function
🌐	Changes the language of display
⚠	Changes the level of warming
🖫	Sets up the export method of reports
?	The help functions
ℹ	Version information

Table 8-2: The toolbar of DFL-2100/ DFL-2400 Reporting System

2. The main functions of report: The system manager can select the events or contents that user wants to monitor through 4 options including “Real-time network attack monitor”, “Network attack report”, “Real-time traffic monitor”, and “System events”.
3. Report screen: The main display area displays information and charts according to selected options on the reporting system.



```
> Ti     an 17, 2003 3:10:08 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Ti      17, 2003 3:10:09 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Tin      7, 2003 3:10:10 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
                                 lame: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
```

```
> Time: Jan 17, 2003 3:11:07 PM Attack Name: ICMP PING Windows Source IP: 192.168.168.210 Destination IP:
> Time: Jan 17, 2003 3:11:08 PM Attack Name: ICMP Echo Reply Source IP: 192.168.168.65 Destination IP: 192.
> Time: Jan 17, 2003 3:11:08 PM Attack Name: ICMP PING Windows Source IP: 192.168.168.210 Destination IP:
> Time: Jan 17, 2003 3:11:08 PM Attack Name: ICMP Echo Reply Source IP: 192.168.168.65 Destination IP: 192.
```

Figure 8-1: The main screen of DFL-2100/ DFL-2400 Reporting System

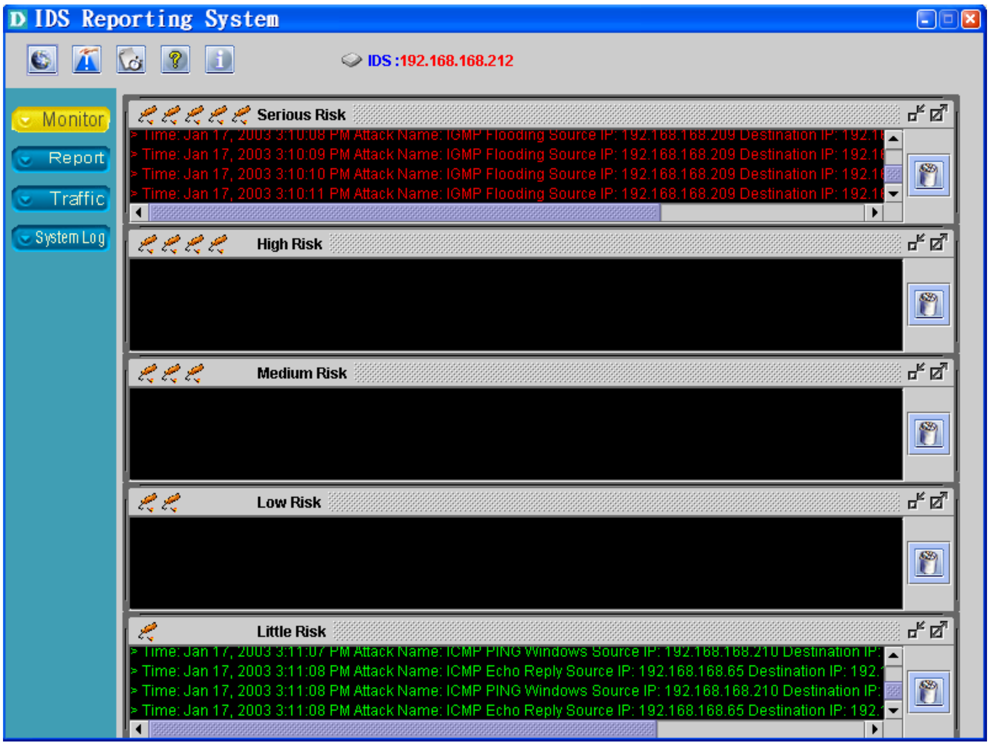
Start to use DFL-2100/DFL-2400 IDS Reporting System

The system manager just clicks on “Reporting System” button on the screen of DFL-2100/ DFL-2400 IDS Management System to open DFL-2100/ DFL-2400 IDS Reporting System.

- When the system manager clicks the button to enter DFL-2100/ DFL-2400 IDS Reporting System, the system will pre-load the real-time network attack monitoring screen of DFL-2100/DFL-2400 that the user is currently managing. (If DFL-2100/ DFL-2400 IDS Management System has not loaded any equipment of DFL-2100/DFL-2400, the reporting system will not be able to work by clicking the button directly.)
- Select one of the 4 main report functions (The system pre-loads the function of Real-time network attack monitor).

Real-time network attack monitor

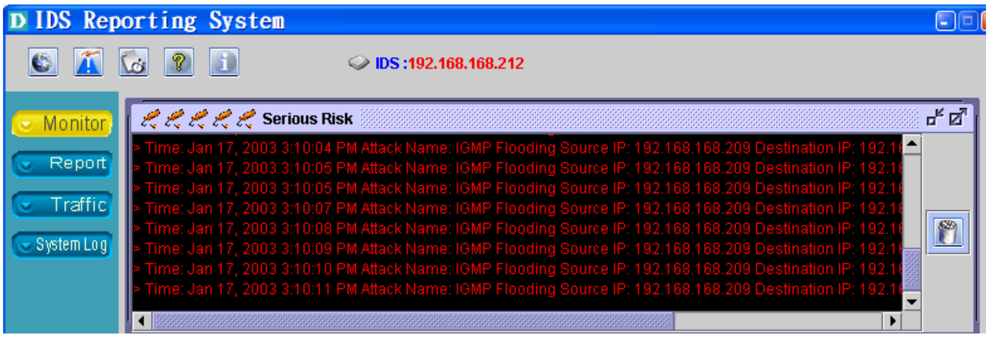
The on-line "Real-time network attack monitor" Monitor of DFL-2100/ DFL-2400 IDS Reporting System provides real-time warnings of network attacks in the form of text. For the system manager to fully understand the current situation of network at a glance, the monitoring function classifies the threatening levels of network attacks into 5 real-time monitoring screens - serious threat, high-level threat, medium-level threat, low-level threat and slight threat.



```
> Time: Jan 17, 2003 3:10:08 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:09 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:10 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:11 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
```

```
> Time: Jan 17, 2003 3:11:07 PM Attack Name: ICMP PING Windows Source IP: 192.168.168.210 Destination IP:
> Time: Jan 17, 2003 3:11:08 PM Attack Name: ICMP Echo Reply Source IP: 192.168.168.65 Destination IP: 192.
> Time: Jan 17, 2003 3:11:08 PM Attack Name: ICMP PING Windows Source IP: 192.168.168.210 Destination IP:
> Time: Jan 17, 2003 3:11:08 PM Attack Name: ICMP Echo Reply Source IP: 192.168.168.65 Destination IP: 192.
```

Figure 8-2: On-line real-time monitoring network attack

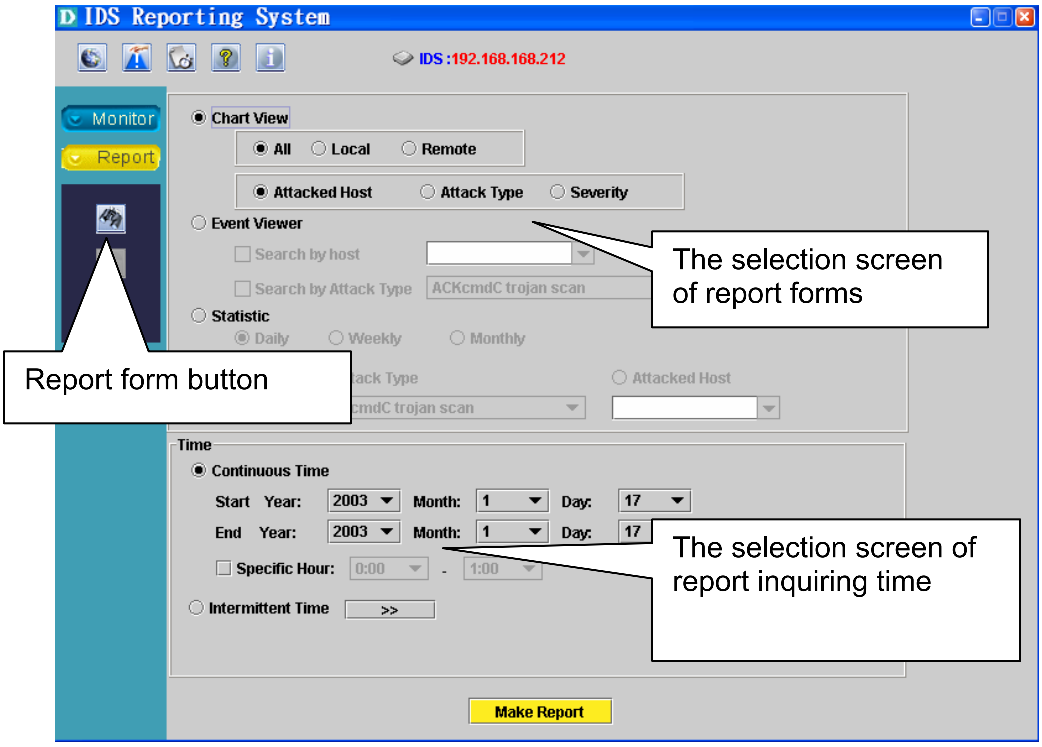


```
> Time: Jan 17, 2003 3:10:04 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:05 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:05 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:07 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:08 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:09 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:10 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
> Time: Jan 17, 2003 3:10:11 PM Attack Name: IGMP Flooding Source IP: 192.168.168.209 Destination IP: 192.1
```

Figure 8-3: Enlarge and narrow the real-time monitoring screen of network attack

Network Attack Report

When the system manager clicks "Report" Report button, DFL-2100/ DFL-2400 IDS Reporting System will provide review, inquiry and analysis functions of network attacks. The system manager then selects "Report Form" button to open "Report Inquiry Screen" (refer to Figure 8-4). User will select a needed report form and inquiring time and then click "Generate Report" to get needed network attacks or analysis.



IDS :192.168.168.212

● Chart View

● All ○ Local ○ Remote

● Attacked Host ○ Attack Type ○ Severity

○ Event Viewer

□ Search by host

□ Search by Attack Type ACKcmdC trojan scan

○ Statistic

● Daily ○ Weekly ○ Monthly

ack Type ○ Attacked Host

cmdC trojan scan

Time

● Continuous Time

Start Year: 2003 Month: 1 Day: 17

End Year: 2003 Month: 1 Day: 17

□ Specific Hour: 0:00 - 1:00

○ Intermittent Time >>

The selection screen of report forms

Report form button

The selection screen of report inquiring time

Figure 8-4: Report inquiry screen of attacks

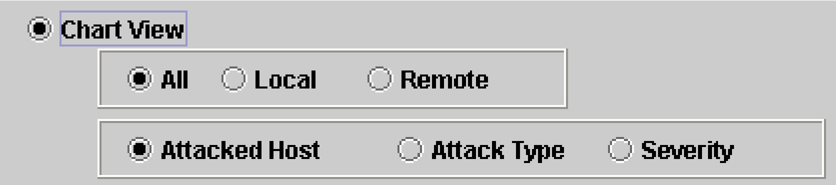
On the selection screen of report forms, the inquiries of network attacks can be categorized into three groups.

1. The attack report: a report of main network attacks. The manager can check the ranking of attacked hosts, the ranking of attack types, the risk ranking of attacks and etc.
2. The event search: An inquiry about serious attacks. It can search the network attacks events distinguished by host attacks or network attacks.
3. The final type is Statistics: a statistical analysis of network attacks, including daily report, weekly report, monthly report and various statistics of occurred network attacks or hosts attacks.

Note: All attack events in report forms inquiry accurate "Inquiring Time", otherwise the search information may not be found.

Browse of main attack events

On the select screen of report forms, the system manager selects "**Attack event Report**" and then selects the inquiry scope, object and time to inquire about the ranking of attacked hosts, attack types and warning levels.



● Chart View

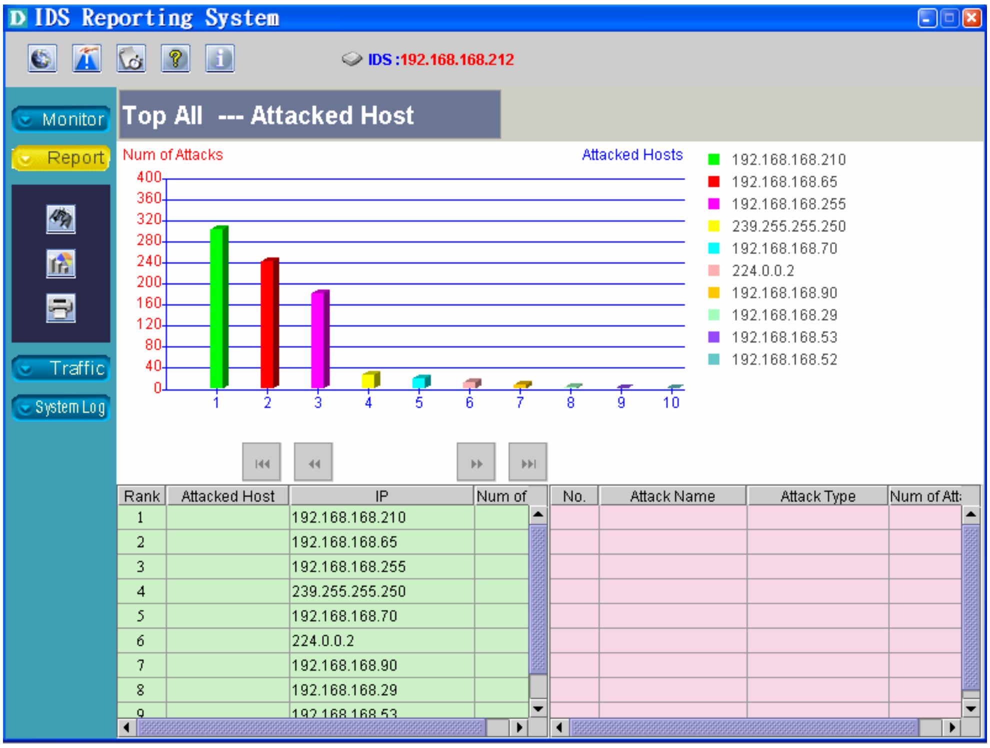
● All ○ Local ○ Remote

● Attacked Host ○ Attack Type ○ Severity

Figure 8-5: The inquiry screen of attack events ranking report

Ranking of attacked hosts:

In the options of attack events report, select the scope as "All" or other scopes as; local or remote, then select "Attacked Host Name" and the corresponding time, and click "Generate Chart" to see the Host attacked ranking report (similar to Figure 8-6).



Rank	Attacked Host	IP	Num of
1		192.168.168.210	
2		192.168.168.65	
3		192.168.168.255	
4		239.255.255.250	
5		192.168.168.70	
6		224.0.0.2	
7		192.168.168.90	
8		192.168.168.29	
9		192.168.168.53	

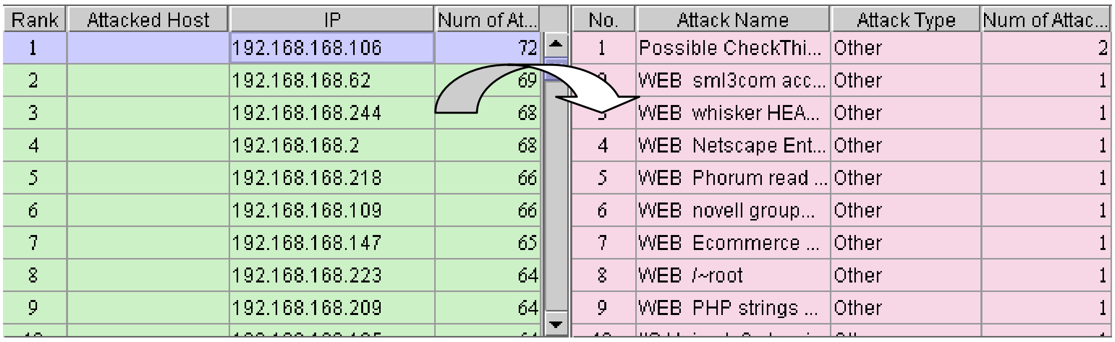
No.	Attack Name	Attack Type	Num of Att:

Figure 8-6: The inquiry screen of the host attacked ranking

The content description of inquiry screen:

- Ranking: the host attacked ranking.
- Name of attacked hosts: the host names defined on the address list.
- IP address: the IP address of attacked hosts.
- Attacked number: Numbers of IP address been attacked.

Users can double-click the content of this form to see the detail information display like the one on the right side of the following screen.



Rank	Attacked Host	IP	Num of At...
1		192.168.168.106	72
2		192.168.168.62	69
3		192.168.168.244	68
4		192.168.168.2	68
5		192.168.168.218	66
6		192.168.168.109	66
7		192.168.168.147	65
8		192.168.168.223	64
9		192.168.168.209	64

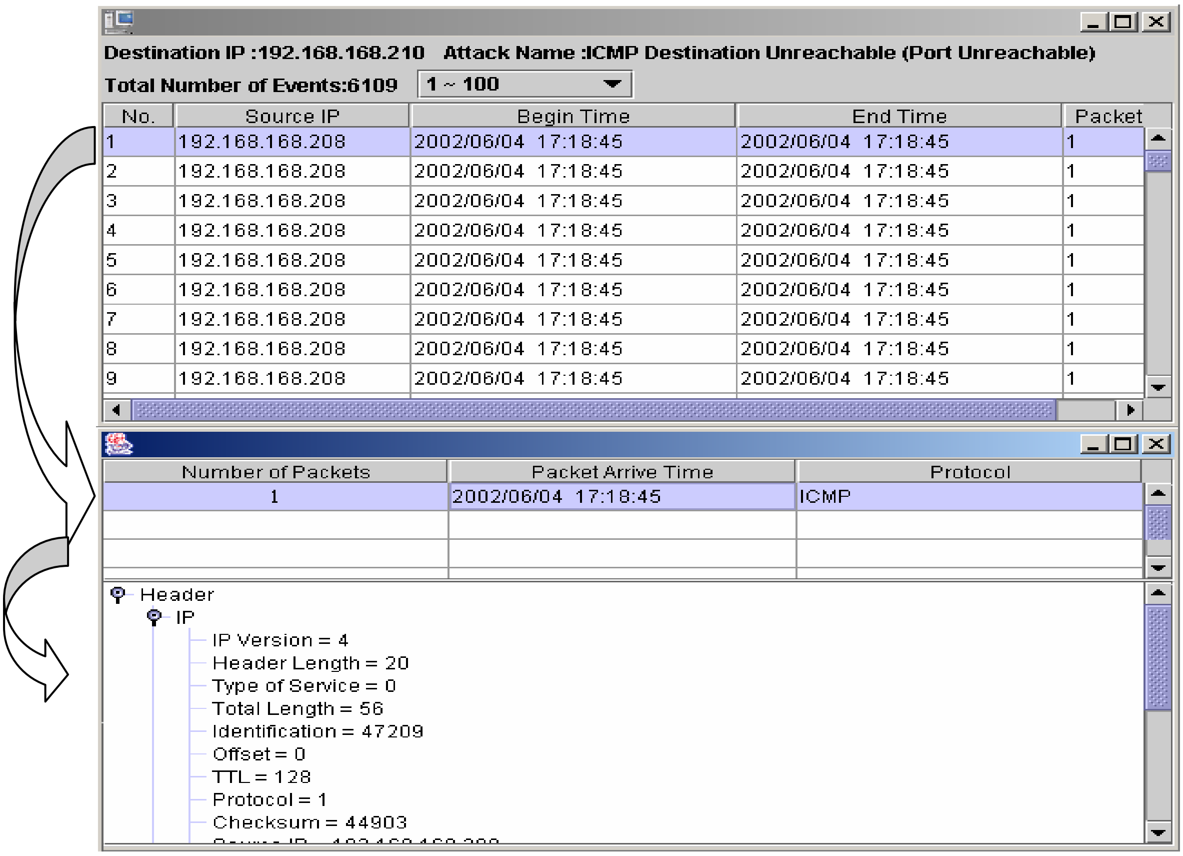
No.	Attack Name	Attack Type	Num of Attac...
1	Possible CheckThi...	Other	2
2	WEB sml3com acc...	Other	1
3	WEB whisker HEA...	Other	1
4	WEB Netscape Ent...	Other	1
5	WEB Phorum read ...	Other	1
6	WEB novell group...	Other	1
7	WEB Ecommerce ...	Other	1
8	WEB /~root	Other	1
9	WEB PHP strings ...	Other	1

Figure 8-7: The detail information on the inquiry screen of attacked host

<u>The content description of inquiry screen:</u>

- Serial number: the ranking of network attacks to this host.
- Attack names: name of the attacks to this host.
- Attack types: types of these attacks.
- Numbers of attacked: numbers of the attacks to this IP address.

When users **double-click** the content of the **right** form, user will get a screen displaying more detail information such as attack time, source data and etc. User can **double-click** the content on this screen to analyze the packet content of this attack. DFL-2100/ DFL-2400 Reporting System not only provides the entire safety status of the system manager's network, but also instinctively gets a detailed and complete network intrusion record to handle network crisis well.



Destination IP :192.168.168.210 Attack Name :ICMP Destination Unreachable (Port Unreachable)

Total Number of Events:6109 1 ~ 100

No.	Source IP	Begin Time	End Time	Packet
1	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
2	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
3	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
4	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
5	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
6	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
7	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
8	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1
9	192.168.168.208	2002/06/04 17:18:45	2002/06/04 17:18:45	1

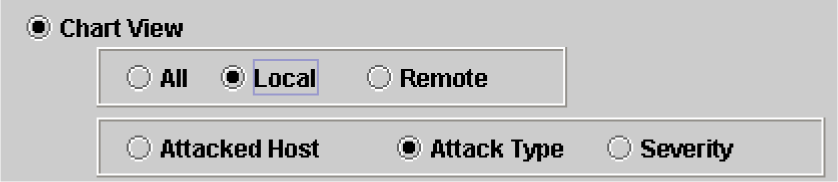
Number of Packets	Packet Arrive Time	Protocol
1	2002/06/04 17:18:45	ICMP

```
Header
  IP
    IP Version = 4
    Header Length = 20
    Type of Service = 0
    Total Length = 56
    Identification = 47209
    Offset = 0
    TTL = 128
    Protocol = 1
    Checksum = 44903
```

Figure 8-8: The detailed analysis screen of attack packet

Ranking of network attack types:

In the options of attack report, selects the scope as “Local” or other scopes (all or remote, then selects “**Attack Type**” and the corresponding time, and then click “Generate Chart” to see the ranking report of attacks (similar to Figure 8-10).

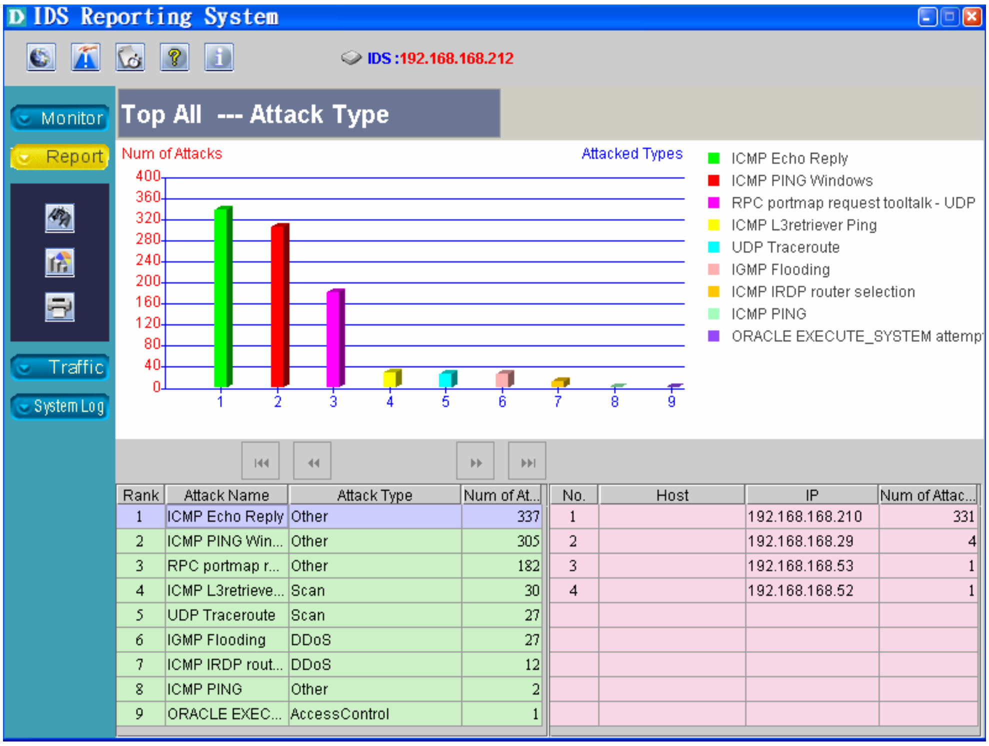


● Chart View

○ All ● Local ○ Remote

○ Attacked Host ● Attack Type ○ Severity

Figure 8-9: The inquiry screen of attack types ranking



Rank	Attack Name	Attack Type	Num of At...
1	ICMP Echo Reply	Other	337
2	ICMP PING Win...	Other	305
3	RPC portmap r...	Other	182
4	ICMP L3retrieve...	Scan	30
5	UDP Traceroute	Scan	27
6	IGMP Flooding	DDoS	27
7	ICMP IRDP rout...	DDoS	12
8	ICMP PING	Other	2
9	ORACLE EXEC...	AccessControl	1

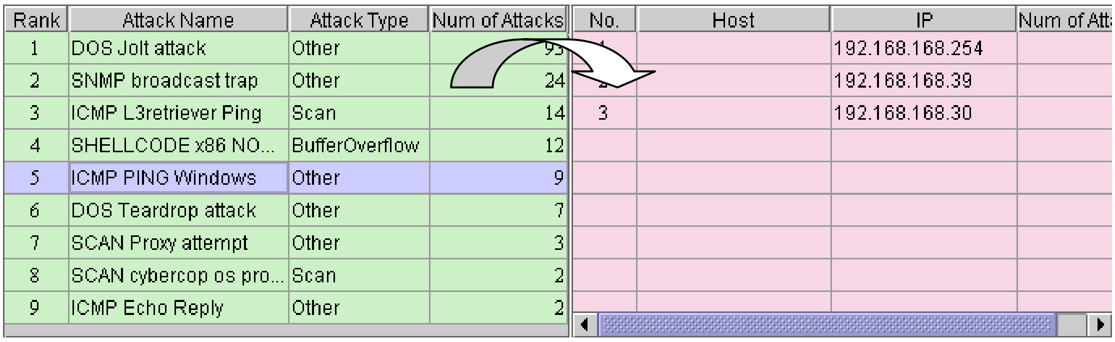
No.	Host	IP	Num of Attac...
1		192.168.168.210	331
2		192.168.168.29	4
3		192.168.168.53	1
4		192.168.168.52	1

Figure 8-10: The inquiry screen of attack types ranking

The content description of inquiry screen:

- Ranking: the ranking of attack names.
- Attack names: the names of the detected network attacks.
- Attack types: the type of network attacks, such as Scan, BufferOverflow, and etc..
- Numbers of the attack: the number of this attack.

Users can double-click the content of this form to see a detailed information display like the one on the right side of the following screen.



Rank	Attack Name	Attack Type	Num of Attacks
1	DOS Jolt attack	Other	93
2	SNMP broadcast trap	Other	24
3	ICMP L3retriever Ping	Scan	14
4	SHELLCODE x86 NO...	BufferOverflow	12
5	ICMP PING Windows	Other	9
6	DOS Teardrop attack	Other	7
7	SCAN Proxy attempt	Other	3
8	SCAN cybercop os pro...	Scan	2
9	ICMP Echo Reply	Other	2

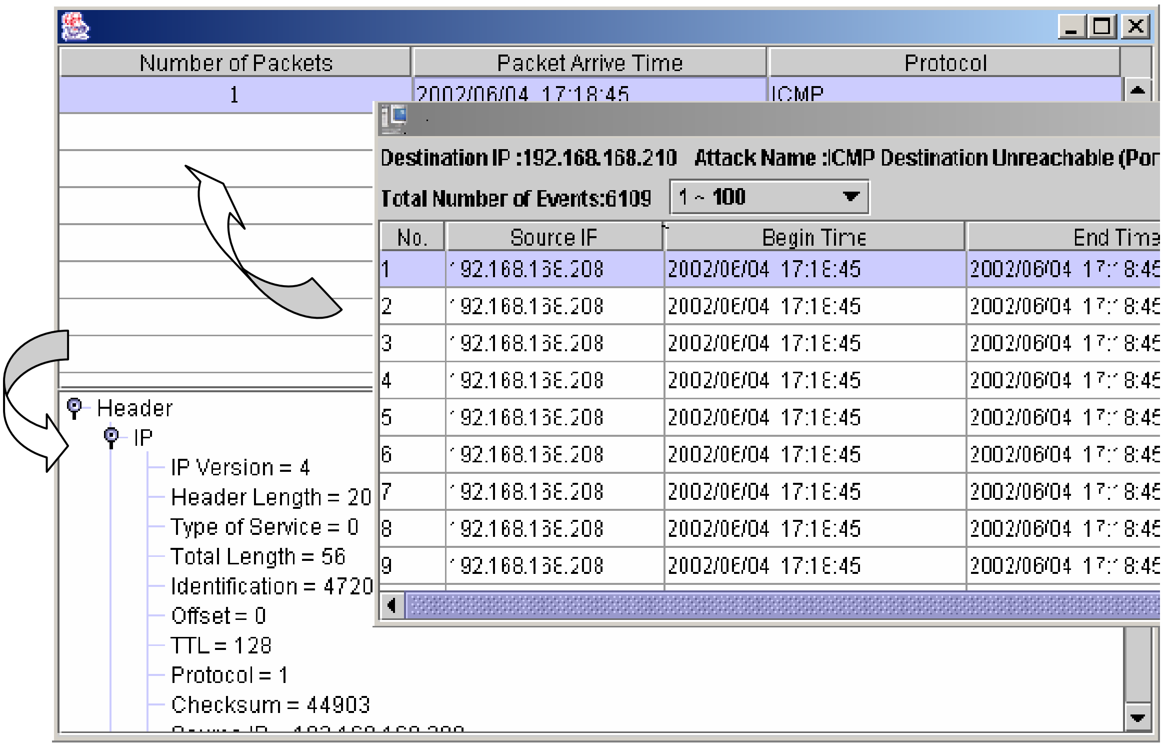
No.	Host	IP	Num of Att
1		192.168.168.254	
2		192.168.168.39	
3		192.168.168.30	

Figure 8-11: The inquiry screen of detailed information on attack events

<u>The content description of inquiry screen:</u>

- Serial number: the attacked hosts ranking.
- Host name: the names of attacked hosts.
- IP address: the IP addresses of attacked hosts.
- Number of attacks: the numbers of this IP address been attacked.

When user **double-click** the content of the **right** form, user will get a screen displaying more detailed information such as attack time, sources and etc. User can double-click the content on this screen to analyze the packet contents of this attack. DFL-2100/ DFL-2400 Reporting System not only provides the entire network safety status to system manager, but also instinctively gets a detailed and complete network intrusion record to handle the network crisis well.



Number of Packets	Packet Arrive Time	Protocol
1	2002/06/04 17:18:45	ICMP

Destination IP :192.168.168.210 Attack Name :ICMP Destination Unreachable (Por

Total Number of Events:6109 1 ~ 100

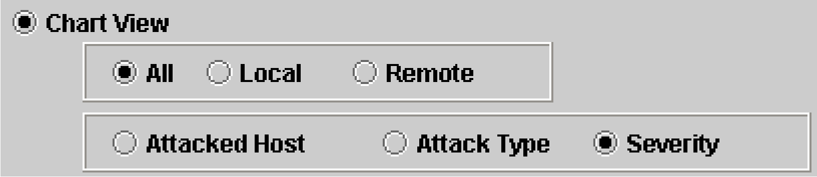
No.	Source IF	Begin Time	End Time
1	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
2	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
3	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
4	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
5	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
6	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
7	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
8	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45
9	192.168.138.208	2002/06/04 17:18:45	2002/06/04 17:18:45

```
Header
  IP
    IP Version = 4
    Header Length = 20
    Type of Service = 0
    Total Length = 56
    Identification = 4720
    Offset = 0
    TTL = 128
    Protocol = 1
    Checksum = 44903
```

Figure 8-12: The detailed analysis screen of attack packets.

Warning ranking of attack:

In the options of attack event report, selects the scope as “All” or other scopes as; remote or local, then selects “Attack Warning Level” and the corresponding time, and click “Generate Chart” to see the report of the warning ranking of attacks (similar to Figure 8-14).

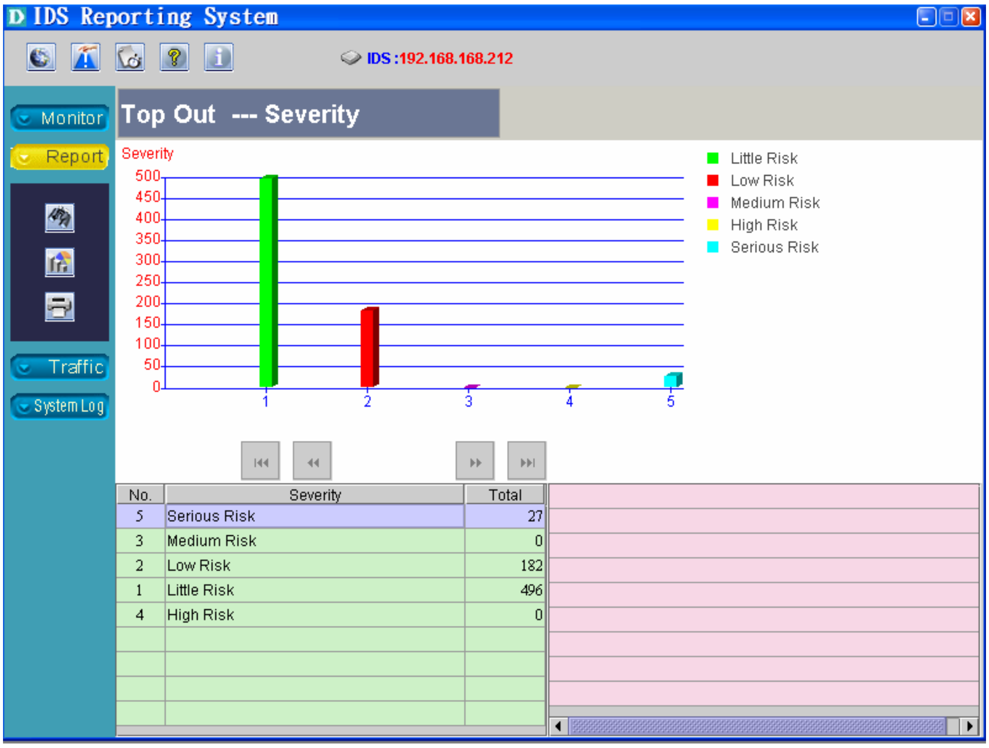


● Chart View

● All ○ Local ○ Remote

○ Attacked Host ○ Attack Type ● Severity

Figure 8-13: The inquiry screen of attack warning ranking



No.	Severity	Total
5	Serious Risk	27
3	Medium Risk	0
2	Low Risk	182
1	Little Risk	496
4	High Risk	0

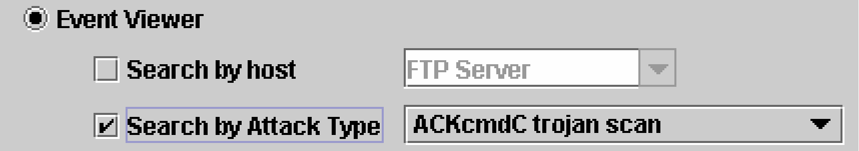
Figure 8-14: The inquiry screen of the danger attack ranking

The content description of inquiry screen of the danger ranking of attack:

- Serial number: the serial number of each attack warning level group.
- Display of the warning levels of attacks: the warning levels distinguished to 5 level: slight, low-level, medium-level danger, high-level danger and serious.
- Total: the accumulated attack numbers for all warning group.

Inquiry about important attacks

The system manager selects "Event Search" (refer to Figure 8-15) on the screen of report form options and then selects to search by attacked address, or by network attack names. The next step is to select a corresponding time period in order to inquire about all attacks occurring on the host, or hosts attacked by selected attacks during the selected time period.



● Event Viewer

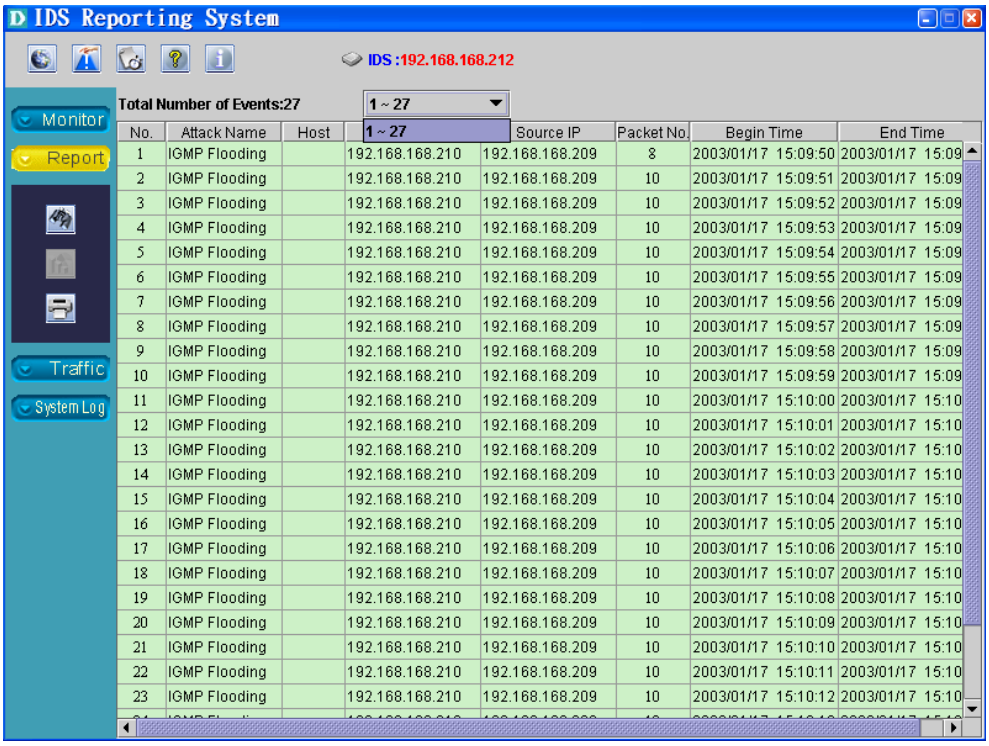
□ Search by host — FTP Server

☑ Search by Attack Type — ACKcmdC trojan scan

Figure 8-15: The browse and inquiry screen of attack events.

Note: If the addresses of the attacked targets have been input into an address list, they can be directly selected in the search. Besides, users can enter directly an IP address to search.

After clicks "Generate Chart" button, a list will display the detailed information about each attack on the report screen. Therefore, this screen provides not only the exhaustive information, but also the complete records and analysis of attack packets for system managers to search and to investigate the sources of attack packets.



IDS :192.168.168.212

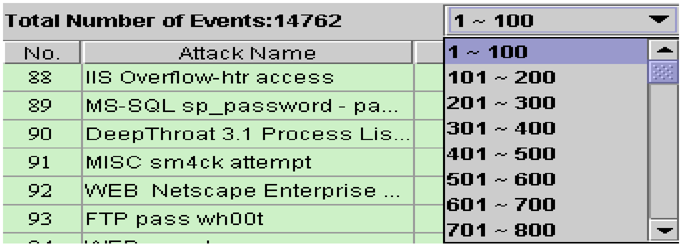
Total Number of Events:27 — 1 ~ 27

No.	Attack Name	Host	1 ~ 27	Source IP	Packet No.	Begin Time	End Time
1	IGMP Flooding		192.168.168.210	192.168.168.209	8	2003/01/17 15:09:50	2003/01/17 15:09
2	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:51	2003/01/17 15:09
3	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:52	2003/01/17 15:09
4	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:53	2003/01/17 15:09
5	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:54	2003/01/17 15:09
6	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:55	2003/01/17 15:09
7	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:56	2003/01/17 15:09
8	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:57	2003/01/17 15:09
9	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:58	2003/01/17 15:09
10	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:09:59	2003/01/17 15:09
11	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:00	2003/01/17 15:10
12	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:01	2003/01/17 15:10
13	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:02	2003/01/17 15:10
14	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:03	2003/01/17 15:10
15	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:04	2003/01/17 15:10
16	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:05	2003/01/17 15:10
17	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:06	2003/01/17 15:10
18	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:07	2003/01/17 15:10
19	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:08	2003/01/17 15:10
20	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:09	2003/01/17 15:10
21	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:10	2003/01/17 15:10
22	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:11	2003/01/17 15:10
23	IGMP Flooding		192.168.168.210	192.168.168.209	10	2003/01/17 15:10:12	2003/01/17 15:10

Figure 8-16: The screen of attack events result

The content description of attack displaying screen:

- Number of events: For user to conveniently review attacks, each screen will only display 100 records. User can use a pull-down screen to select needed section of attacks.



Total Number of Events:14762

1 ~ 100

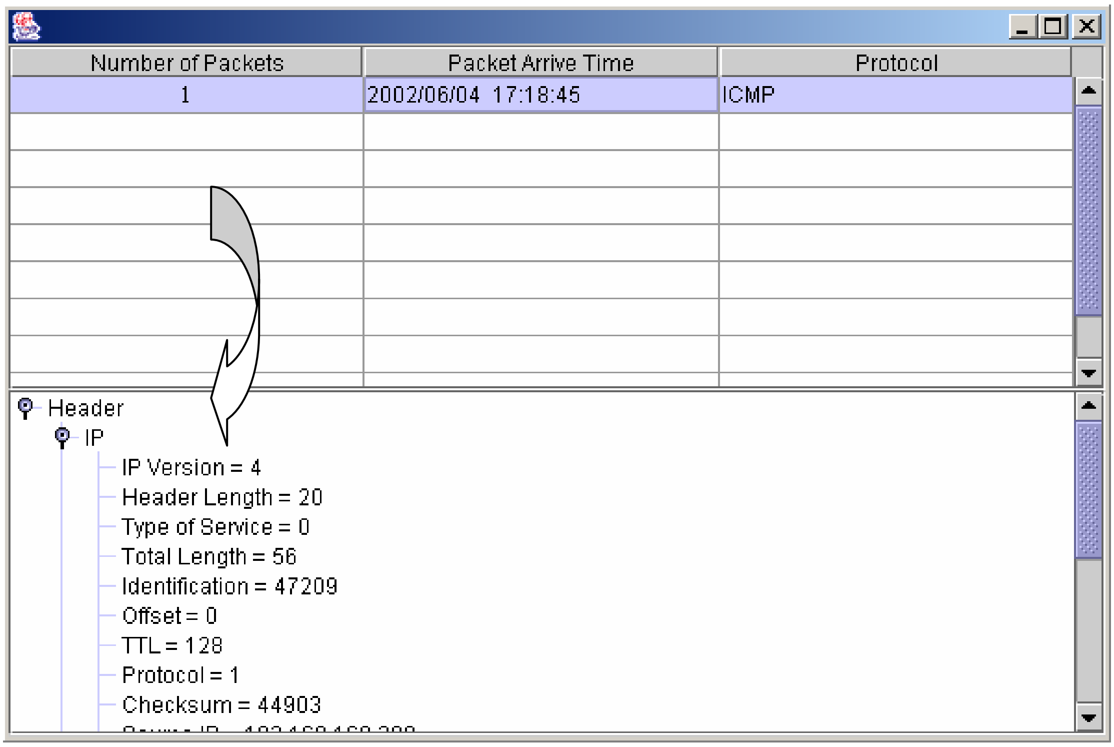
No.	Attack Name
88	IIS Overflow-htr access
89	MS-SQL sp_password - pa...
90	DeepThroat 3.1 Process Lis...
91	MISC sm4ck attempt
92	WEB Netscape Enterprise ...
93	FTP pass wh00t

1 ~ 100
101 ~ 200
201 ~ 300
301 ~ 400
401 ~ 500
501 ~ 600
601 ~ 700
701 ~ 800

Figure 8-17: The screen of number of attack events

- ◆ Serial number: the serial number of attacks.
- ◆ Attack name: the name of this attack.
- ◆ Host name: The names of attacked hosts pre-defined on the address list.
- ◆ Attacked IP address: the attacked IP address
- ◆ Number of packet: the number of packets accepted by this attack.
- ◆ Starting time: the time this attack begins.
- ◆ Finishing time: the time this attack ends.

When user double clicks the content of this form, user will be able to analyze the packet content of this attack. DFL-2100/ DFL-2400 IDS Reporting System not only provides the entire network safety status to system manager, but also instinctively gets a detailed and comprehensive network intrusion records to handle network crisis well.



Number of Packets	Packet Arrive Time	Protocol
1	2002/06/04 17:18:45	ICMP

Header
IP
IP Version = 4
Header Length = 20
Type of Service = 0
Total Length = 56
Identification = 47209
Offset = 0
TTL = 128
Protocol = 1
Checksum = 44903

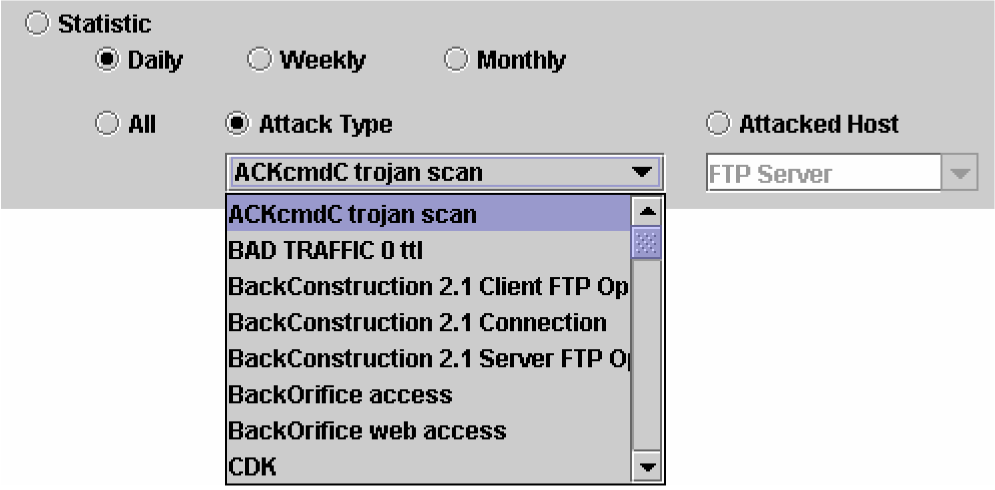
Figure 8-18: The analysis screen of attack packet.

- ◆ Serial number of packet: the serial numbers of packets.
- ◆ Event time: the event begins.
- ◆ Packet attacking time: the time when packets are received.
- ◆ Protocol: the protocol type of a packet. The protocol might be TCP, UDP, ICMP, or IGMP.
- ◆ Double click on a certain packet, and then the system will analyze this packet and display each field in a tree structure. (Refer to Figure 8-18.)

Statistical analysis of attack events

The system manager selects "Statistics" option (refer to Figure 8-19) on the screen of report form selection and then selects a "statistical analysis", the report could be selected in the form of daily, weekly, or monthly of **all** attacks, or one specific type of network attack, or **one host**.

Note: If the addresses of attacked targets have been input into an address list, they can be directly selected in a search. Besides, users can also directly enter an IP address to search.



○ Statistic

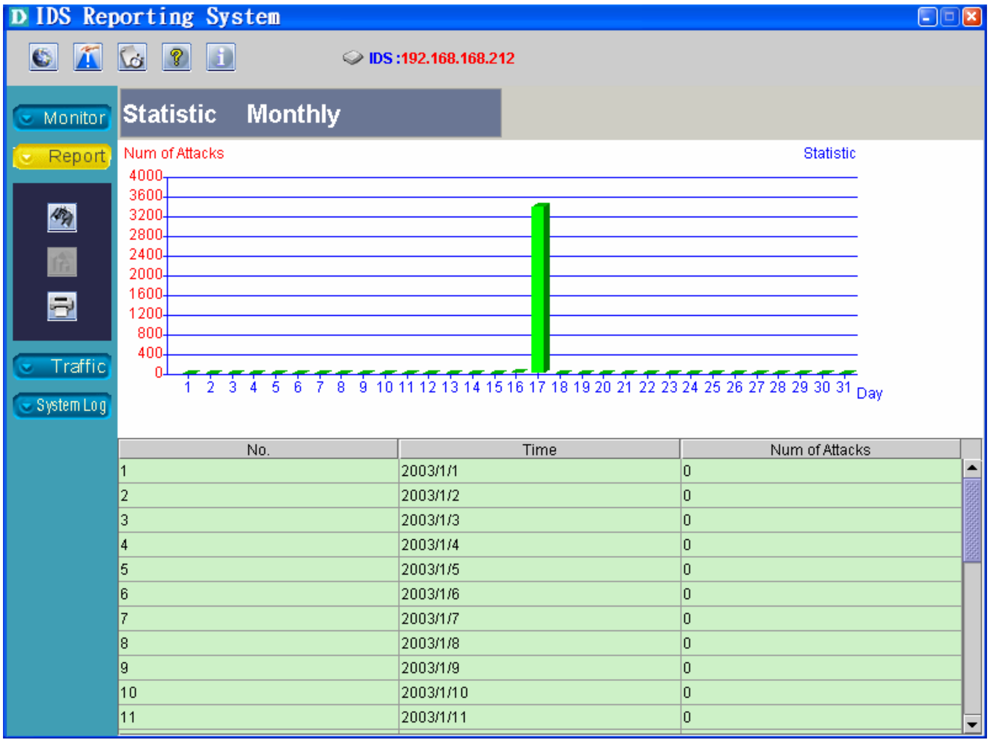
● Daily ○ Weekly ○ Monthly

○ All ● Attack Type ○ Attacked Host

ACKcmdC trojan scan ▼ FTP Server ▼

ACKcmdC trojan scan
BAD TRAFFIC 0 ttl
BackConstruction 2.1 Client FTP Op
BackConstruction 2.1 Connection
BackConstruction 2.1 Server FTP O
BackOrifice access
BackOrifice web access
CDK

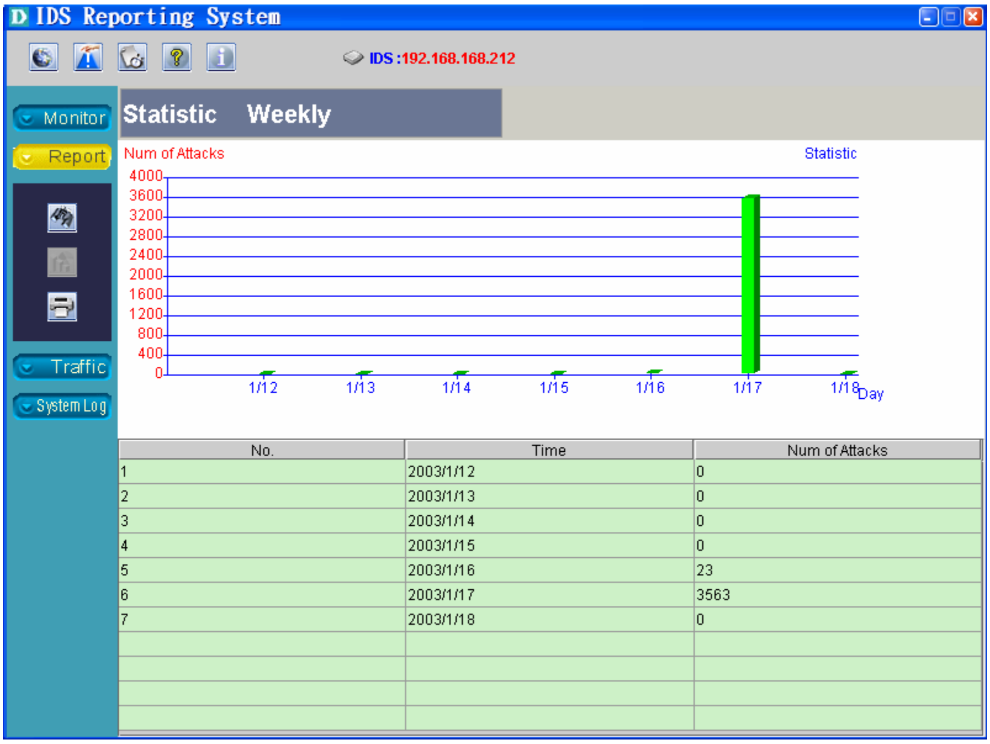
Figure 8-19: The screen of attack events results



Statistic Monthly

No.	Time	Num of Attacks
1	2003/1/1	0
2	2003/1/2	0
3	2003/1/3	0
4	2003/1/4	0
5	2003/1/5	0
6	2003/1/6	0
7	2003/1/7	0
8	2003/1/8	0
9	2003/1/9	0
10	2003/1/10	0
11	2003/1/11	0

Figure 8-20: A monthly report of attack events



No.	Time	Num of Attacks
1	2003/1/12	0
2	2003/1/13	0
3	2003/1/14	0
4	2003/1/15	0
5	2003/1/16	23
6	2003/1/17	3563
7	2003/1/18	0

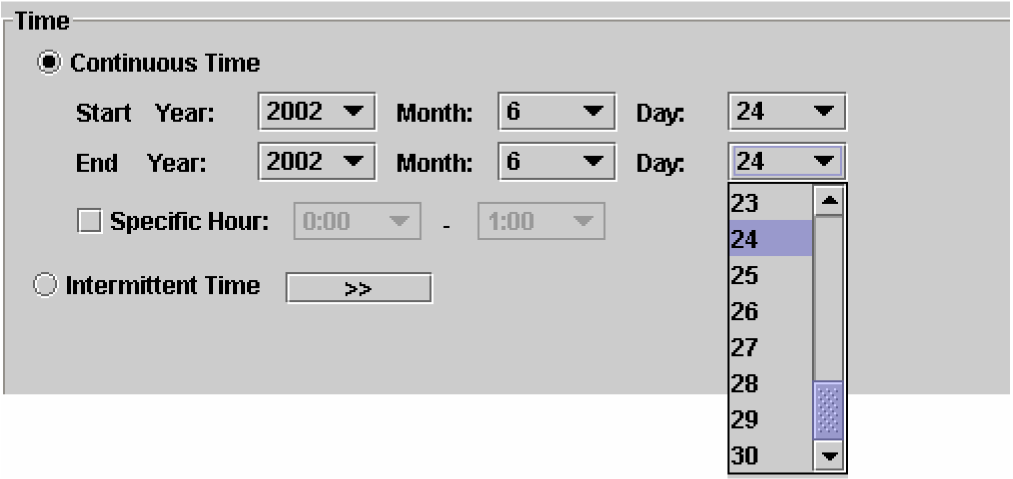
Figure 8-21: A weekly report of attack events

Selections of inquiring time

When the system manager inquires any form of reports, he/she should also select the corresponding time period. DFL-2100/ DFL-2400 IDS Reporting System provides two methods to select a time period; one continuous period, the other one as any combination of discontinuous time period.

Select one continuous period:

For a continuous period, the system manager can easily use a pull-down menu to select the starting and finishing time (Year, month and day), or even specific time (especially valuable for tracking the intrusion by the hacker.).



Time

● Continuous Time

Start Year: 2002 Month: 6 Day: 24

End Year: 2002 Month: 6 Day: 24

□ Specific Hour: 0:00 - 1:00

○ Intermittent Time >>

Figure 8-22: The selection of a continuous time period

Select discontinuous time period:

For discontinuous time period, DFL-2100/ DFL-2400 IDS Reporting System displays a visual calendar to select required dates after the system manager clicks on “>>” key. This calendar supports multiple choices and provides buttons for the system manager to conveniently quick select time periods. The details of all functions and components are described as following.

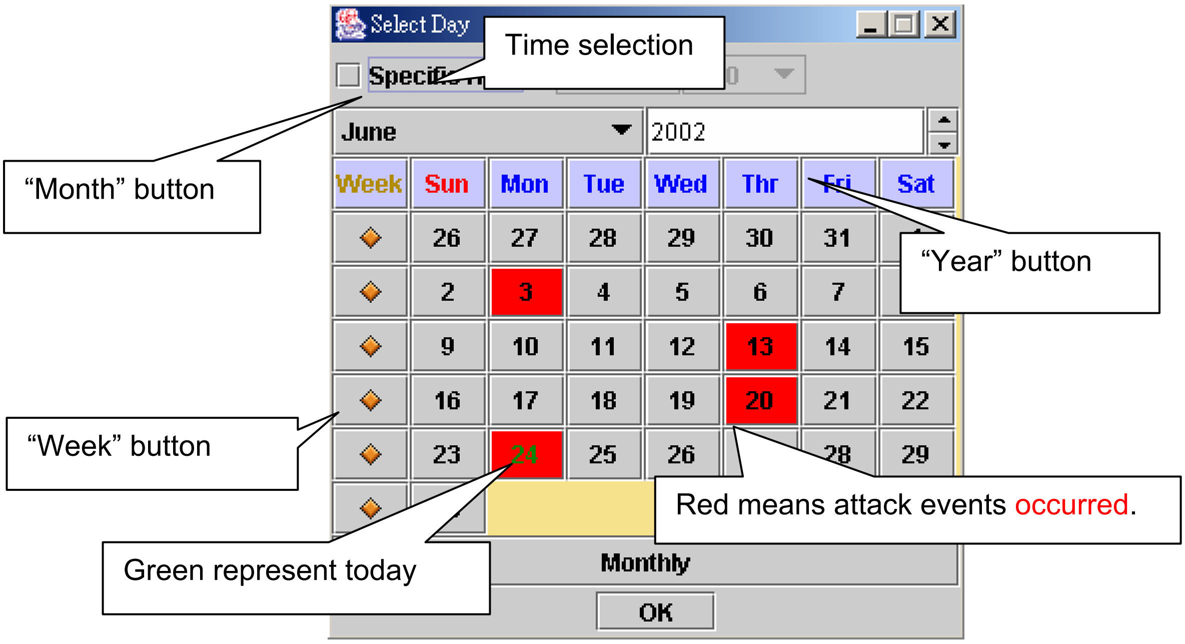
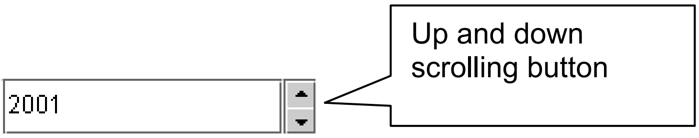


Figure 8-23: The selection of discontinuous periods

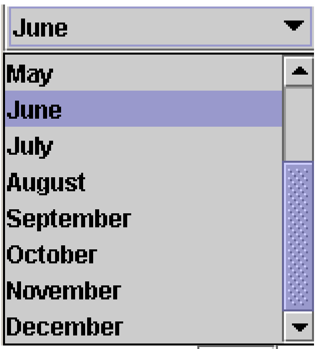
Notes of selection:

1. The field of year:



   Use the up and down scrolling button to decide which year to display.

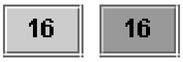
2. The field of month:



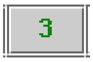
3. The selection button of week:

   Click on the week selection button to select a week and click once more to cancel this selection. When this button is selected, it is dark gray. Otherwise, it is bright gray.

4. The selection button of day:



Click on the day selection button to select a day and click once more to cancel this selection. When this button is selected, it is dark gray. Otherwise, it is bright gray.

5. The display of today: 

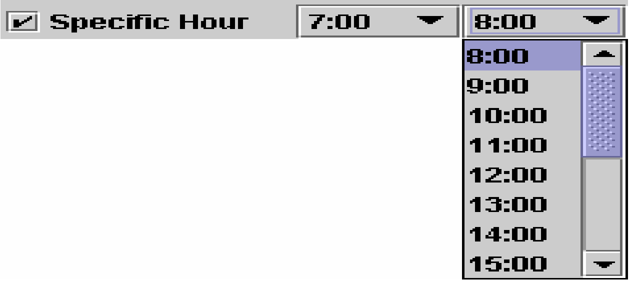
The letter on this button is displayed in green.

6. Monthly report button:

Click on this button to select the month displayed on the whole screen. To cancel, just click once more.

7. Specific time option:

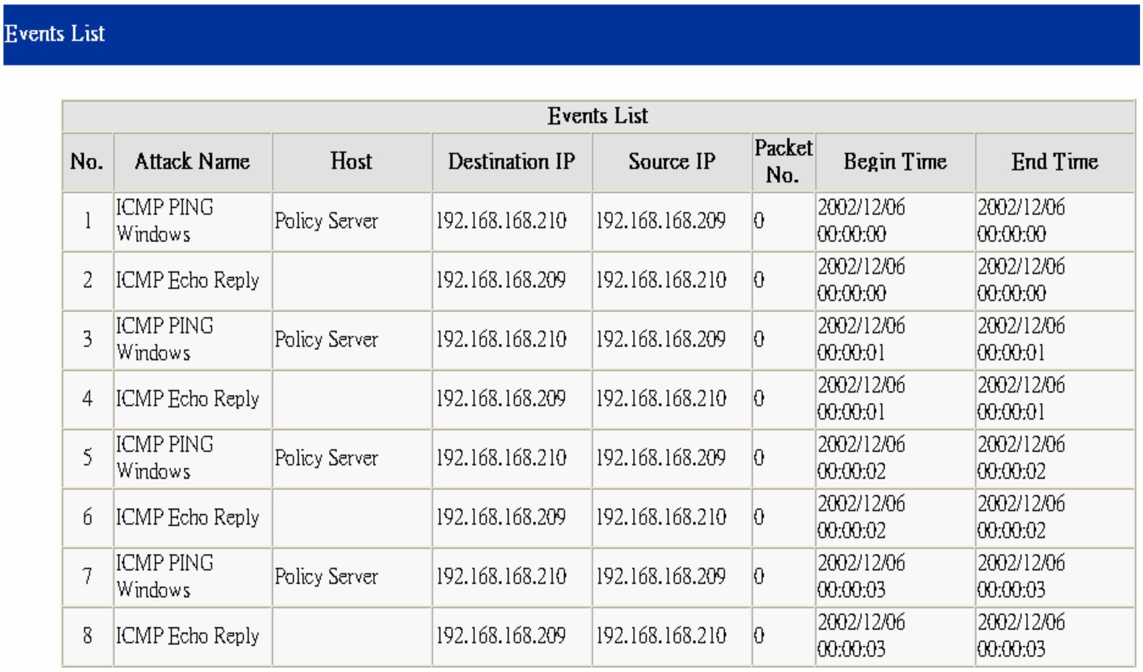
When this option is selected, the system would search for time information and display as the following.



The report print function

After getting any form of required reports, the system manager not only can review most of the reports on-line, but also print them out or switch to a bar chart, or to a pie chart for a further analysis and comparison.

1. The system manager just clicks on "Print" button in the options of report display, and the system would automatically generate a print preview in a browser. Then he/she just has to print out directly.

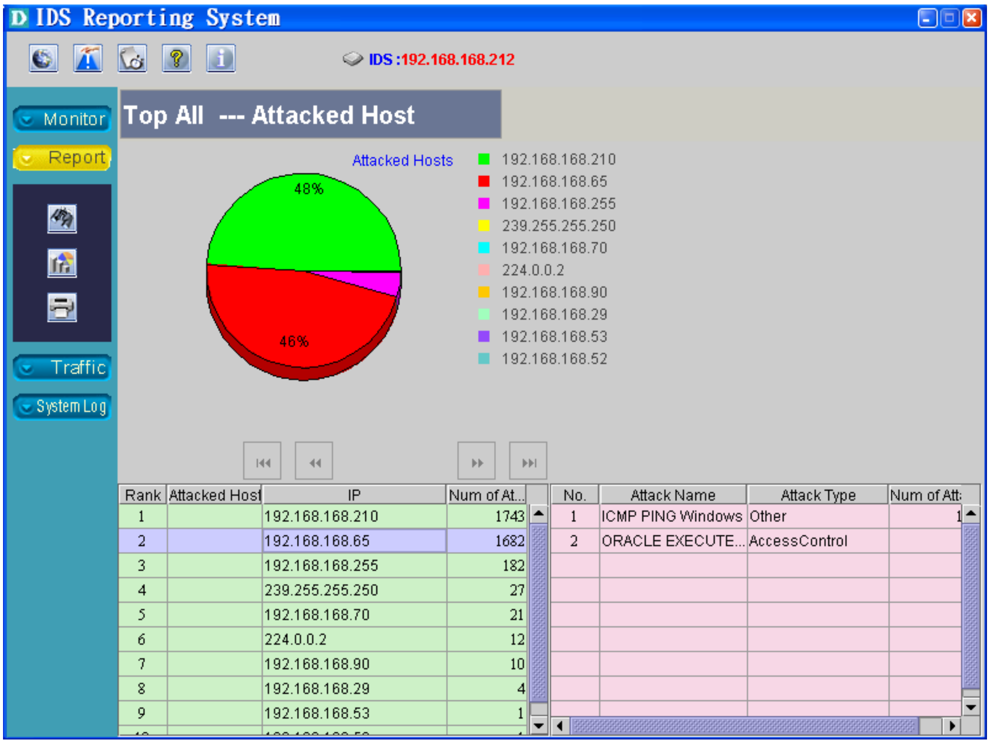


Events List

Events List							
No.	Attack Name	Host	Destination IP	Source IP	Packet No.	Begin Time	End Time
1	ICMP PING Windows	Policy Server	192.168.168.210	192.168.168.209	0	2002/12/06 00:00:00	2002/12/06 00:00:00
2	ICMP Echo Reply		192.168.168.209	192.168.168.210	0	2002/12/06 00:00:00	2002/12/06 00:00:00
3	ICMP PING Windows	Policy Server	192.168.168.210	192.168.168.209	0	2002/12/06 00:00:01	2002/12/06 00:00:01
4	ICMP Echo Reply		192.168.168.209	192.168.168.210	0	2002/12/06 00:00:01	2002/12/06 00:00:01
5	ICMP PING Windows	Policy Server	192.168.168.210	192.168.168.209	0	2002/12/06 00:00:02	2002/12/06 00:00:02
6	ICMP Echo Reply		192.168.168.209	192.168.168.210	0	2002/12/06 00:00:02	2002/12/06 00:00:02
7	ICMP PING Windows	Policy Server	192.168.168.210	192.168.168.209	0	2002/12/06 00:00:03	2002/12/06 00:00:03
8	ICMP Echo Reply		192.168.168.209	192.168.168.210	0	2002/12/06 00:00:03	2002/12/06 00:00:03

Figure 8-24: web-based print preview

2. The system manager just clicks on "Chart Switch" button in the options of report display, the system would automatically switch a bar chart to a pie chart.



	Attacked Hosts
🟩	192.168.168.210
🟥	192.168.168.65
🟪	192.168.168.255
🟨	239.255.255.250
🟦	192.168.168.70
■	224.0.0.2
🟧	192.168.168.90
🟩	192.168.168.29
🟪	192.168.168.53
🟦	192.168.168.52

Rank	Attacked Host	IP	Num of At...
1		192.168.168.210	1743
2		192.168.168.65	1682
3		192.168.168.255	182
4		239.255.255.250	27
5		192.168.168.70	21
6		224.0.0.2	12
7		192.168.168.90	10
8		192.168.168.29	4
9		192.168.168.53	1

No.	Attack Name	Attack Type	Num of Att:
1	ICMP PING Windows	Other	1
2	ORACLE EXECUTE...	AccessControl	

Figure 8–25: Attacks are displayed in the form of a pie chart.

Real-time traffic monitor

When the system manager clicks on "traffic Monitor" Traffic button, DFL-2100/ DFL-2400 IDS Reporting System would provide two real-time monitoring screens of network traffics. The upper screen displays the number of network packets received on-line and the number of real-time connections; the lower screen displays the number of packets that are identified as attacks and discarded by DFL-2100/DFL-2400. For users to more easily read the contents of monitored flows, DFL-2100/ DFL-2400 IDS Reporting System uses different colors to display different flows of protocol packets, which include most used TCP, UDP, ICMP, IGMP, IPX, NetBEUI and etc.

The traffic monitoring includes 4 options:

Toolbar icons	Function
L	Local flow monitoring, which refers to the flow delivered outward by an internal network.
R	Remote flow monitoring, which refers to the flow delivered inward by an external network.
⇅	Flow monitoring both of directions, inward and outward.
⏱	Set up time for data update

Table 8-3: The options of on-line real-time traffic monitor

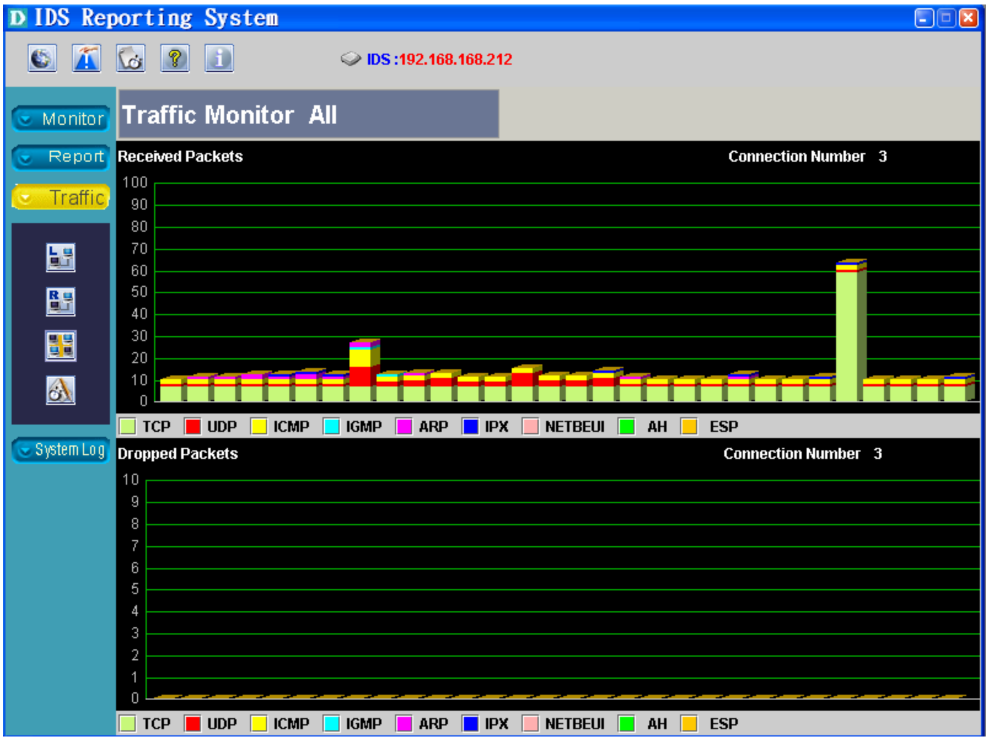


Figure 8-26: Real-time traffic monitoring

Set up time for real-time data update

The system manager can set up data-update time for flow monitoring. After 🛠 button is clicked, a dialogue box of time setup would appear for setting.

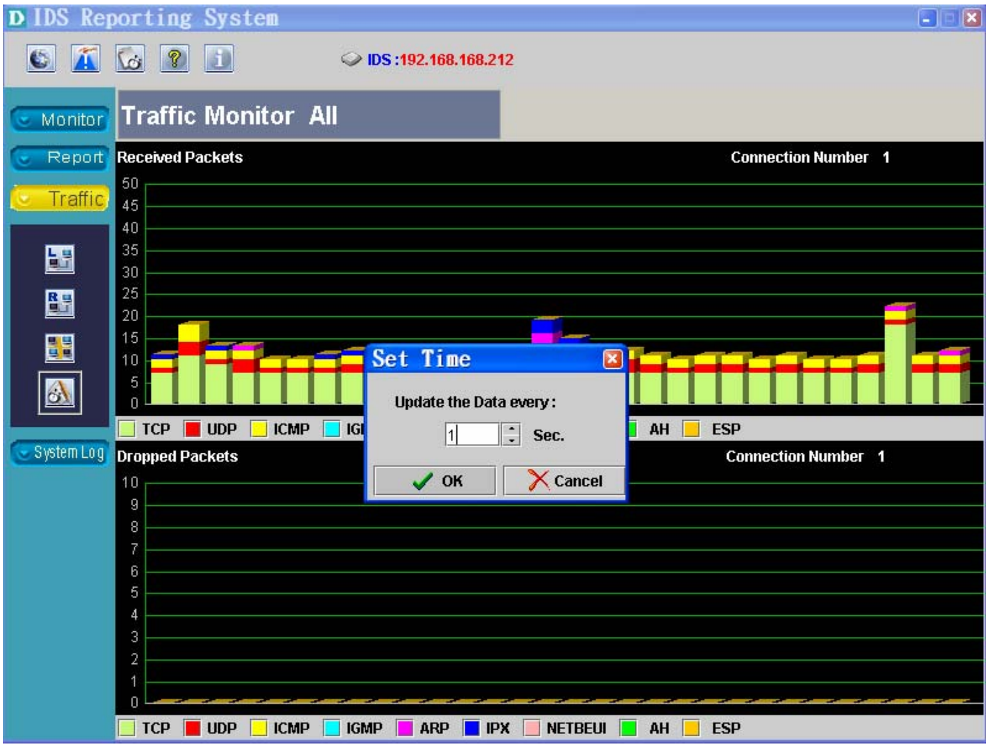
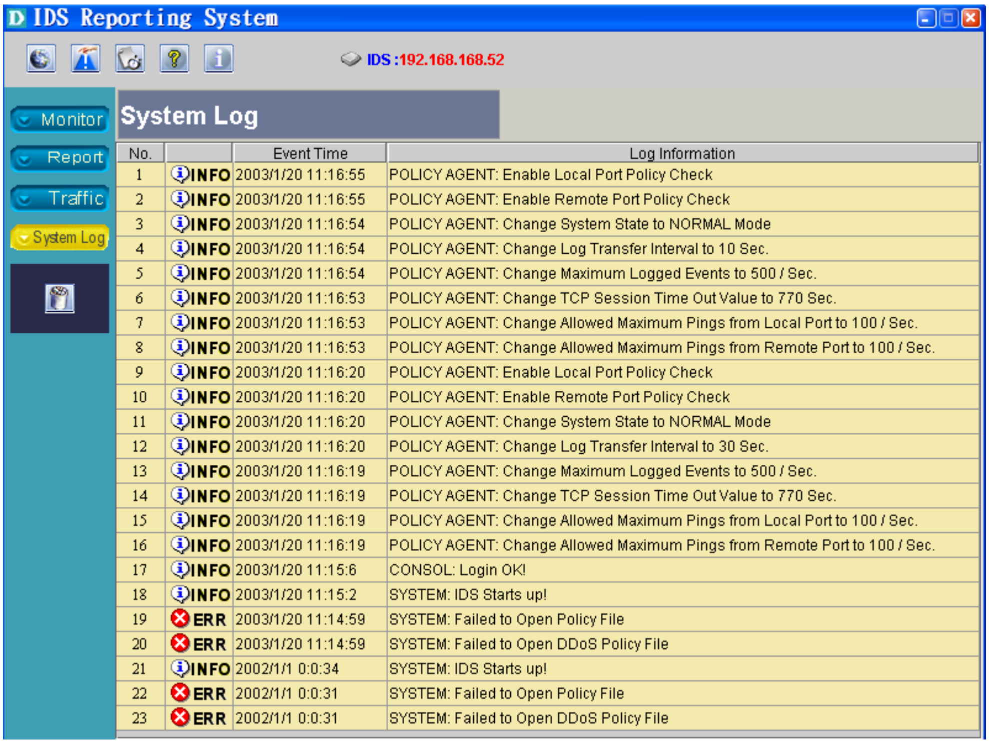


Figure 8-27: Set up data update time for real-time traffic monitoring

System events

When the system manager clicks on "System Event" System Log button, DFL-2100/DFL-2400 IDS Reporting System will provide reports of all system information, including the occurring time and contents of system information INFO, system warning WARN, system emergency ERR , and fatal system error FATAL.



No.		Event Time	Log Information
1	INFO	2003/1/20 11:16:55	POLICY AGENT: Enable Local Port Policy Check
2	INFO	2003/1/20 11:16:55	POLICY AGENT: Enable Remote Port Policy Check
3	INFO	2003/1/20 11:16:54	POLICY AGENT: Change System State to NORMAL Mode
4	INFO	2003/1/20 11:16:54	POLICY AGENT: Change Log Transfer Interval to 10 Sec.
5	INFO	2003/1/20 11:16:54	POLICY AGENT: Change Maximum Logged Events to 500 / Sec.
6	INFO	2003/1/20 11:16:53	POLICY AGENT: Change TCP Session Time Out Value to 770 Sec.
7	INFO	2003/1/20 11:16:53	POLICY AGENT: Change Allowed Maximum Pings from Local Port to 100 / Sec.
8	INFO	2003/1/20 11:16:53	POLICY AGENT: Change Allowed Maximum Pings from Remote Port to 100 / Sec.
9	INFO	2003/1/20 11:16:20	POLICY AGENT: Enable Local Port Policy Check
10	INFO	2003/1/20 11:16:20	POLICY AGENT: Enable Remote Port Policy Check
11	INFO	2003/1/20 11:16:20	POLICY AGENT: Change System State to NORMAL Mode
12	INFO	2003/1/20 11:16:20	POLICY AGENT: Change Log Transfer Interval to 30 Sec.
13	INFO	2003/1/20 11:16:19	POLICY AGENT: Change Maximum Logged Events to 500 / Sec.
14	INFO	2003/1/20 11:16:19	POLICY AGENT: Change TCP Session Time Out Value to 770 Sec.
15	INFO	2003/1/20 11:16:19	POLICY AGENT: Change Allowed Maximum Pings from Local Port to 100 / Sec.
16	INFO	2003/1/20 11:16:19	POLICY AGENT: Change Allowed Maximum Pings from Remote Port to 100 / Sec.
17	INFO	2003/1/20 11:15:6	CONSOL: Login OK!
18	INFO	2003/1/20 11:15:2	SYSTEM: IDS Starts up!
19	ERR	2003/1/20 11:14:59	SYSTEM: Failed to Open Policy File
20	ERR	2003/1/20 11:14:59	SYSTEM: Failed to Open DDoS Policy File
21	INFO	2002/1/1 0:0:34	SYSTEM: IDS Starts up!
22	ERR	2002/1/1 0:0:31	SYSTEM: Failed to Open Policy File
23	ERR	2002/1/1 0:0:31	SYSTEM: Failed to Open DDoS Policy File

Figure 8-28: The reviewing screen of system event records

The content description of system event screen:

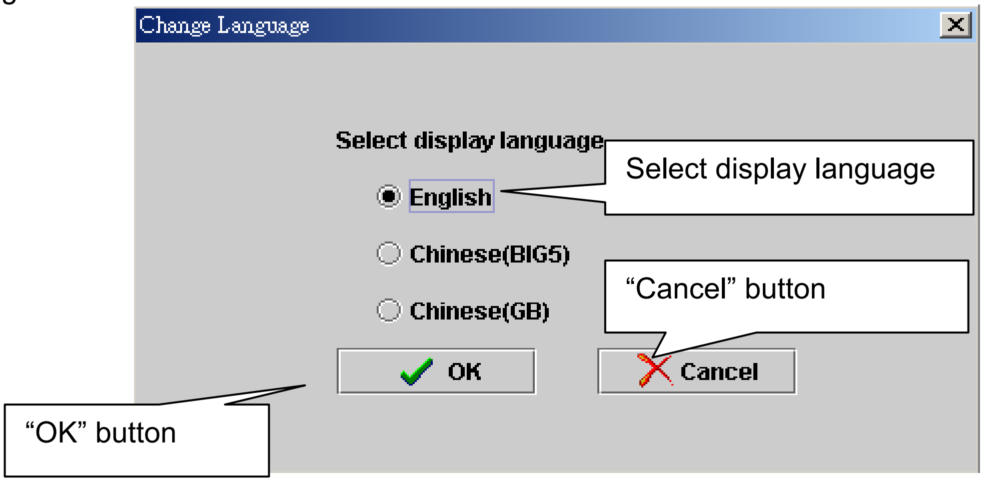
- Serial number: the serial number of historical records of system events.
- Type: there are four definitions of system event – system information INFO, system warning WARN, system emergency ERR , and fatal system error FATAL.
  1. System information: such as information about booting.
  2. System warning: Minor errors or events that temporarily do not influence system operation.
  3. System emergency: Serious errors that influence a normal operation or some functions of the system.
  4. Fatal system error: Events that influence the operation of main system functions.
- Time of System events: the occurring time recorded by the system.
- Information about system events: the descriptions of system events.

Introduction of other important tools

The toolbar provides users some tools to change language, warning level and report output setting on the main screen of DFL-2100/DFL-2400 IDS Reporting System.

Change display language

When users click on "Language Selection" button, they can see a dialogue box in Figure 8-30.



Change Language

Select display language

● English

○ Chinese(BIG5)

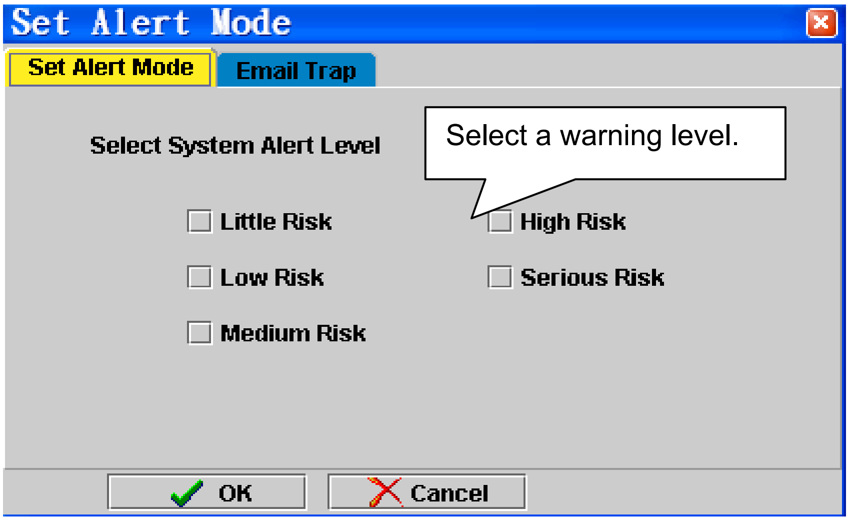
○ Chinese(GB)

Figure 8-29: Change display language

- Select display language: select a different language to display a different language version on program operation screens.
- "Ok" button: click on this button to accept the setting of a new language version.
- "Cancel" button: click on this button to exit this screen.

Change warning levels

When users click on "Warning level" button, they can change related settings of on-line warning levels and e-mail warning in a dialogue box (refer to Figure 8-30).



Set Alert Mode

Select System Alert Level

□ Little Risk □ High Risk

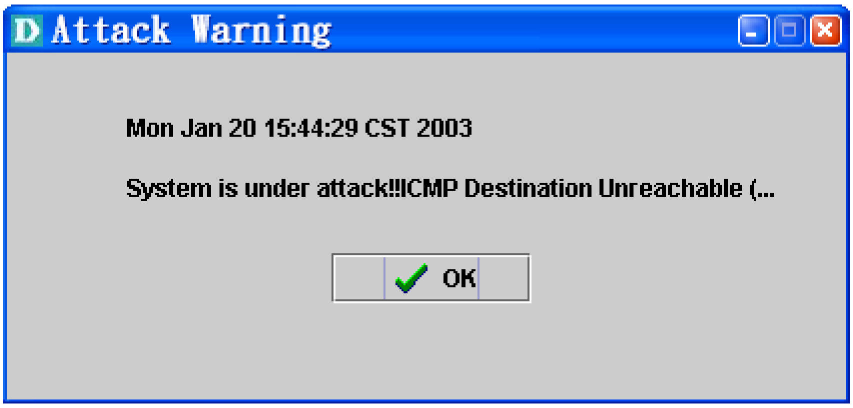
□ Low Risk □ Serious Risk

□ Medium Risk

Figure 8-30: Change warning levels

- Select a warning level: select the attack seriousness level that makes the system to inform occurrences of attacks.
- "Ok" button: click on this button to accept the setting of a new warning level.
- "Cancel" button: click on this button to exit this screen.
-

When network attacks occur, the system displays a warning screen according to settings.



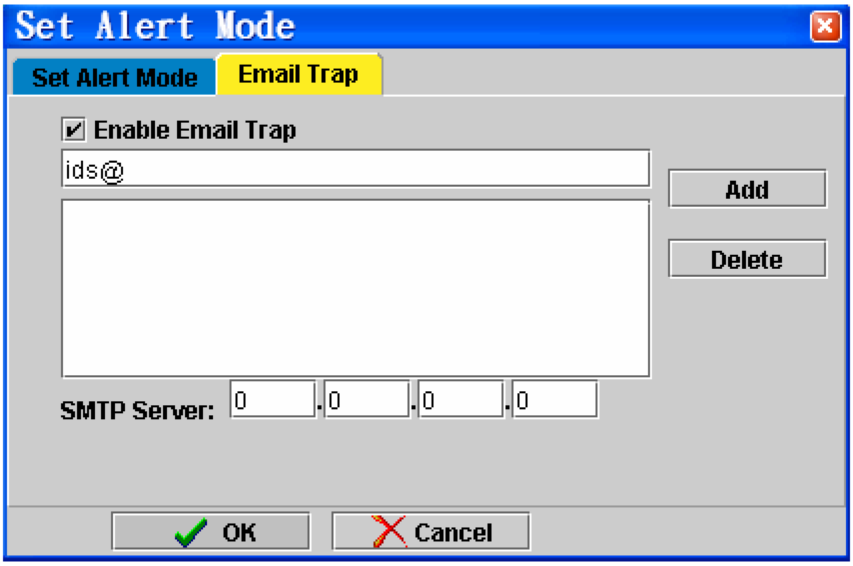
Attack Warning

Mon Jan 20 15:44:29 CST 2003

System is under attack!!!ICMP Destination Unreachable (...

Figure 8-31: The warning dialogue box displays when the system is attacked.

E-Mail tarp: Setting enable an e-mail trap when the system is attacked. These settings include a check box enabling mail notification and complete e-mail account and IP address of SMTP server.



Set Alert Mode

☑ Enable Email Trap

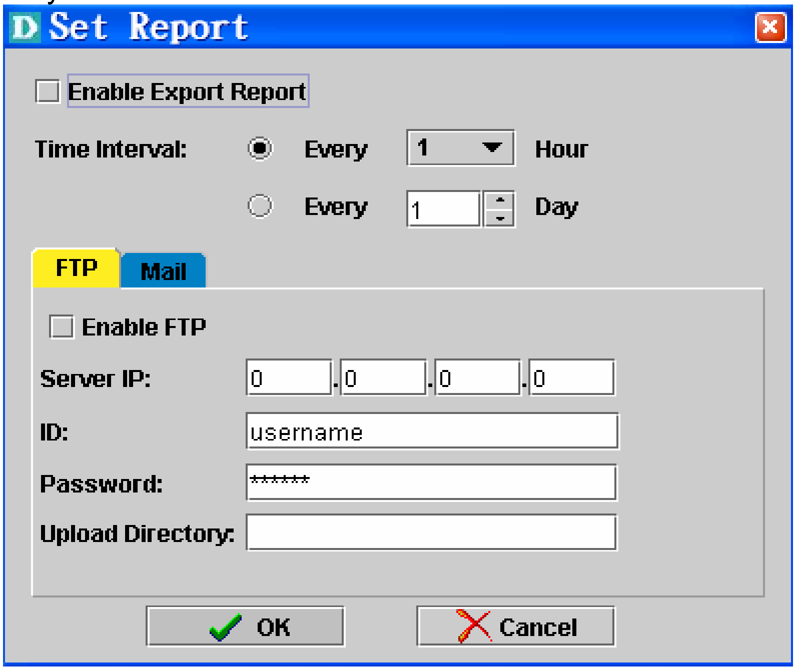
ids@

SMTP Server: 0 . 0 . 0 . 0

Figure 8-32: Use this dialogue box to enable the e-mail trap

Set up the schedule report output form

When users click on “Time Report” button, they can see a dialogue box in Figure 8-33 for the setting of report output. DFL-2100/DFL-2400 IDS Policy Server regularly outputs reports via e-mail or FTP. The interval of output time can be set as few hours or few days.



□ Enable Export Report

Time Interval: ● Every 1 Hour

○ Every 1 Day

□ Enable FTP

Server IP: 0.0.0.0

ID: username

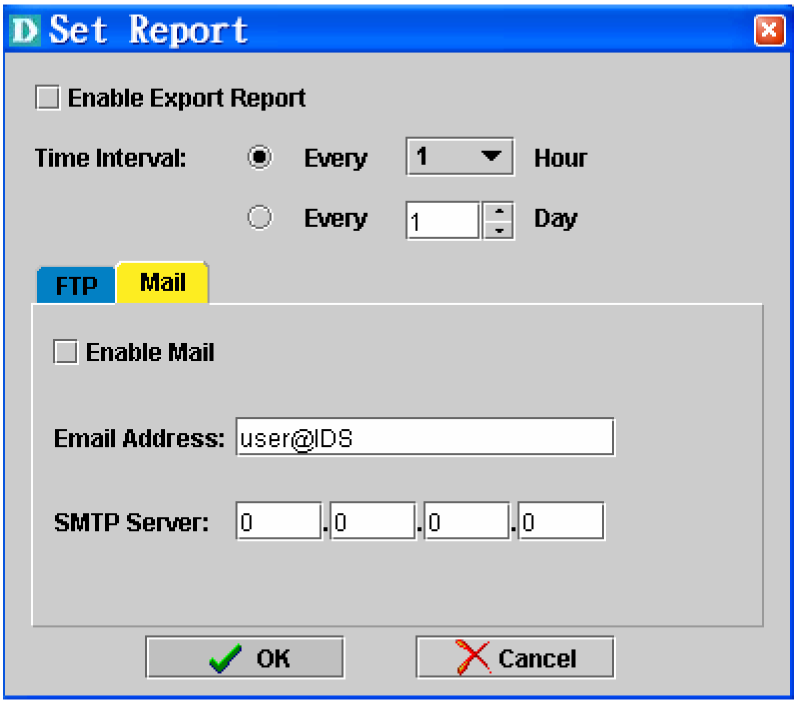
Password: ******

Upload Directory:

Figure 8-33: set up “Time Report” as FTP output.

1. Check the box of “Enable report output”.
2. Select an interval of data output by time (few hours) or by day (few days).
3. Select to receive report data with a FTP server.
4. Set up the IP address, account, password and upload directory of a FTP server.

Note: When the FTP outputs time reports is selected; the account of upload should have enough reading and writing authority on the upload directory of a FTP server.



Set Report

☐ Enable Export Report

Time Interval: ● Every 1 Hour

○ Every 1 Day

☐ Enable Mail

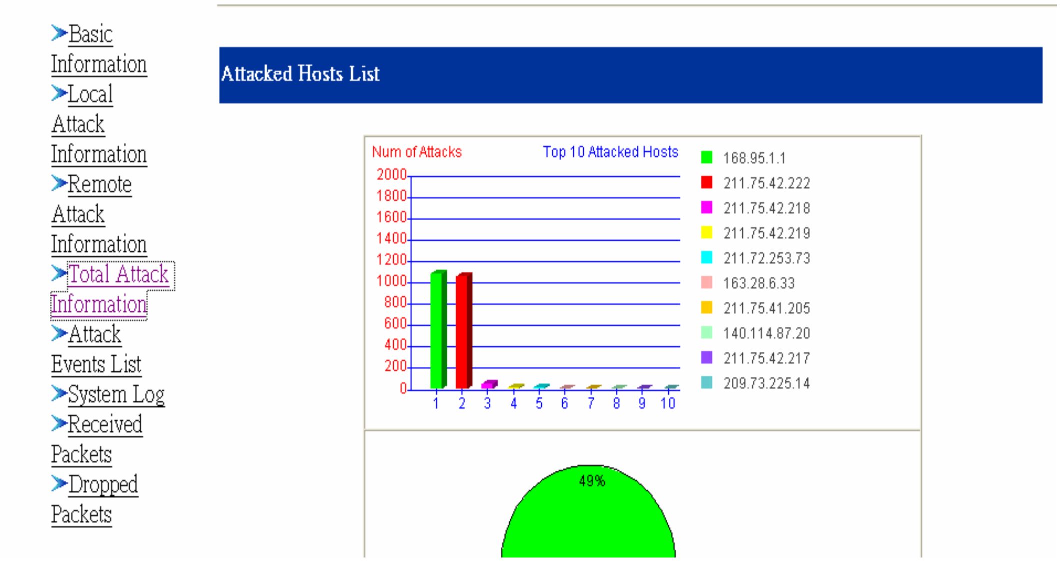
Email Address: user@IDS

SMTP Server: 0 .0 .0 .0

Figure 8-34: Set up a time report as mail output.

1. Check the box of “Enable Mail”.
2. Enter an e-mail address and click on “Finish” button.
3. Enter your STMP server.
4. Click on “Set up” button to finish the setting of enabling the time report output for e-mail received.

Time Report Output covers complete information about DFL-2100/DFL-2400 IDS Reporting System (including related information about network attacks and system information). DFL-2100/DFL-2400 Reporting System builds these time reports in a web-based form. Users just click on the index.htm of the home page to review reports through a browser while receiving reports.



- Basic Information
- Local Attack Information
- Remote Attack Information
- Total Attack Information
- Attack Events List
- System Log
- Received Packets
- Dropped Packets

Attacked Hosts List

Figure 8-35: The Schedule Summary report

Version information

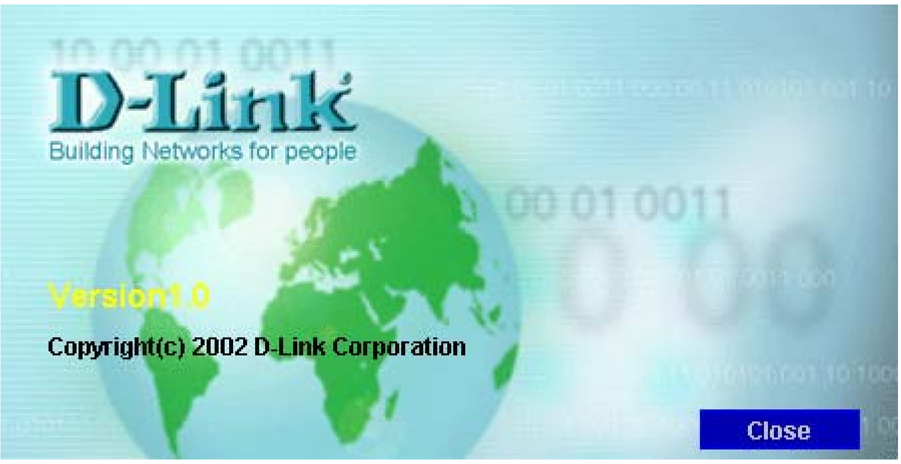

D-Link
Building Networks for people
Version1.0
Copyright(c) 2002 D-Link Corporation
Close

Figure 8-36: The dialogue box of DFL-2100/DFL-2400 version information

- “Close” button: click on this button to go back to the main screen.
- Version information: this field includes version information of the system.

D-Link Offices

AUSTRALIA
D-LINK AUSTRALASIA
Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077
TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand)
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au, info@dlink.com.au

CANADA
D-LINK CANADA
2180 Winston Park Drive, Oakville, Ontario L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5095 BBS: 1-965-279-8732
FREE CALL: 1-800-354-6522
URL: www.dlink.ca
FTP: ftp.dlinknet.com
E-MAIL: techsup@dlink.ca

CHILE
D-LINK SOUTH AMERICA
Isidora Goyenechea #2934 of.702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-2320923
URL: www.dlink.cl
E-MAIL: ccasassu@dlink.cl, tsilva@dlink.cl

DENMARK
D-LINK DENMARK
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL:45-43-969040 FAX:45-43-424347
URL: www.dlink.dk
E-MAIL: info@dlink.dk

EGYPT
D-LINK MIDDLE EAST
7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-2456176 FAX: 202-2456192
URL: www.dlink-me.com
E-MAIL: support@dlink-me.com, fateen@dlink-me.com

FRANCE
D-LINK FRANCE
Le Florilege #2, Allee de la Fresnerie
78330 Fontenay Le Fleury France
TEL: 33-1-30238688 FAX: 33-1-3023-8689
URL: www.dlink-france.fr
E-MAIL: info@dlink-france.fr

GERMANY
D-LINK CENTRAL EUROPE/D-LINK DEUSTSCHLAND GMBH
Schwalbacher Strasse 74, 65760 Eschborn Germany
TEL: 49-(0) 6196-7799-0 FAX: 49-(0) 6196-7799-300
URL: www.dlink.de
E-MAIL: mbischoff@dlink.de, mboerner@dlink.de

INDIA
D-LINK INDIA
Plot No.5, Kurla-Bandra Complex Road,
Off Cst Road, Santacruz (E), Bombay - 400 098 India
TEL: 91-22-652-6696 FAX: 91-22-652-8914
URL: www.dlink-india.com
E-MAIL: service@dlink.india.com

ITALY
D-LINK ITALY
Via Nino Bonnet No. 6/b, 20154 Milano, Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
E-MAIL: info@dlink.it
URL: www.dlink.it

JAPAN
D-LINK JAPAN
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141 Japan

TEL: 81-3-5434-9678
FAX: 81-3-5434-9868
URL: www.d-link.co.jp
E-MAIL: kida@d-link.co.jp

RUSSIA **D-LINK RUSSIA**
Michurinski Prospekt 49, 117607 Moscow, Russia
TEL: 7-095-737-3389, 7-095-737-3492 FAX: 7-095-737-3390
E-MAIL: vl@dlink.ru

SINGAPORE **D-LINK INTERNATIONAL**
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL: 65-774-6233 FAX: 65-774-6322
URL: www.dlink-intl.com
E-MAIL: info@dlink.com.sg

S. AFRICA **D-LINK SOUTH AFRICA**
Unit 2, Parkside 86 Oak Avenue
Highveld Technopark Centurion, Gauteng, Republic of South Africa
TEL: 27(0)126652165 FAX: 27(0)126652186
CELL NO: 0826010806 (Bertus Moller)
CELL NO: 0826060013 (Attie Pienaar)
E-MAIL: bertus@d-link.co.za, attie@d-link.co.za

SWEDEN **D-LINK SWEDEN**
P.O. Box 15036, S-167 15 Bromma Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
E-MAIL: info@dlink.se
URL: www.dlink.se

TAIWAN **D-LINK TAIWAN**
2F, No. 119 Pao-Chung Road, Hsin-Tien, Taipei, Taiwan
TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw
E-MAIL: dssqa@tsc.dlinktw.com.tw

U.K. **D-LINK EUROPE**
D-Link (Europe) Ltd. 4th Floor Merit House,
Edgware Road, Colindale, London NW95AB U.K.
TEL: 44-20-8731-5555 FAX: 44-20-8731-5511
URL: www.dlink.co.uk
E-MAIL: info@dlink.co.uk

U.S.A **D-LINK U.S.A.**
53 Discovery Drive, Irvine, CA 92618 USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
INFO LINE: 1-800-326-1688
BBS: 1-949-455-1779, 1-949-455-9616
URL: www.dlink.com
E-MAIL: tech@dlink.com, support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms____
Organization: ______________________________Dept.________________
Your title at organization:______________________________________
Telephone:________________________ Fax:______________________
Organization's full address:_____________________________________
____
Country:____
Date of purchase (Month/Day/Year):________________________________

Product Model	**Product Serial No.**	*** Product installed in type of computer (e.g., Compaq 486)**	*** Product installed in computer serial No.**

(* Applies to adapters only)

Product was purchased from:
Reseller's name:____
Telephone:________________________ Fax:______________________
Reseller's full address:____
____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
□Home □Office □Travel □Company Business □Home Business □Personal Use

2. How many employees work at installation site?
□1 employee □2-9 □10-49 □50-99 □100-499 □500-999 □1000 or more

3. What network protocol(s) does your organization use ?
□XNS/IPX □TCP/IP □DECnet □Others_____________________________

4. What network operating system(s) does your organization use ?
□D-Link LANsmart □Novell NetWare □NetWare Lite □SCO Unix/Xenix □PC NFS □3Com 3+Open
□Banyan Vines □DECnet Pathwork Windows NT Windows NTAS Windows '95
Others____

5. What network management program does your organization use ?
D-View HP OpenView/Windows HP OpenView/Unix SunNet Manager Novell NMS
NetView 6000 Others____

6. What network medium/media does your organization use ?
Fiber-optics Thick coax Ethernet Thin coax Ethernet 10BASE-T UTP/STP
100BASE-TX 100BASE-T4 100VGAnyLAN Others_________________________

7. What applications are used on your network?
Desktop publishing Spreadsheet Word processing CAD/CAM
Database management Accounting Others____________________________

8. What category best describes your company?
Aerospace Engineering Education Finance Hospital Legal Insurance/Real Estate
Manufacturing
Retail/Chainstore/Wholesale Government Transportation/Utilities/Communication VAR
System house/company Other______________________________________

9. Would you recommend your D-Link product to a friend?
Yes No Don't know yet

10.Your comments on this product? ______________________________
____
____
____
____
____

PLEASE
PLACE STAMP
HERE

TO: ______________________

____

____

D-Link®