Use of IDP

The SG-1000 can detect the anomaly flow packets and notice the MIS engineer to handle the situation , in order to prevent any suspicious program to invade the destination PC. In other words, the SG-1000 can provide the instant network security protection as detects any internal or external attacks, in order to enhance the enterprises network stability .

The so called IDP configure is defined to be the IDP setting.

Setting

Setting

The SG-1000 can update signature definitions every 30 minutes or the MIS engineer can select to use manual update. It also shows the latest update time and version .

The MIS engineer can enable anti-virus to the compact or non-encryption files.

Virus engine：

Clam：The default setting is free to use .

The SG-1000 can send the NetBIOS notification through e-mail when system detected the attacks and infected files .

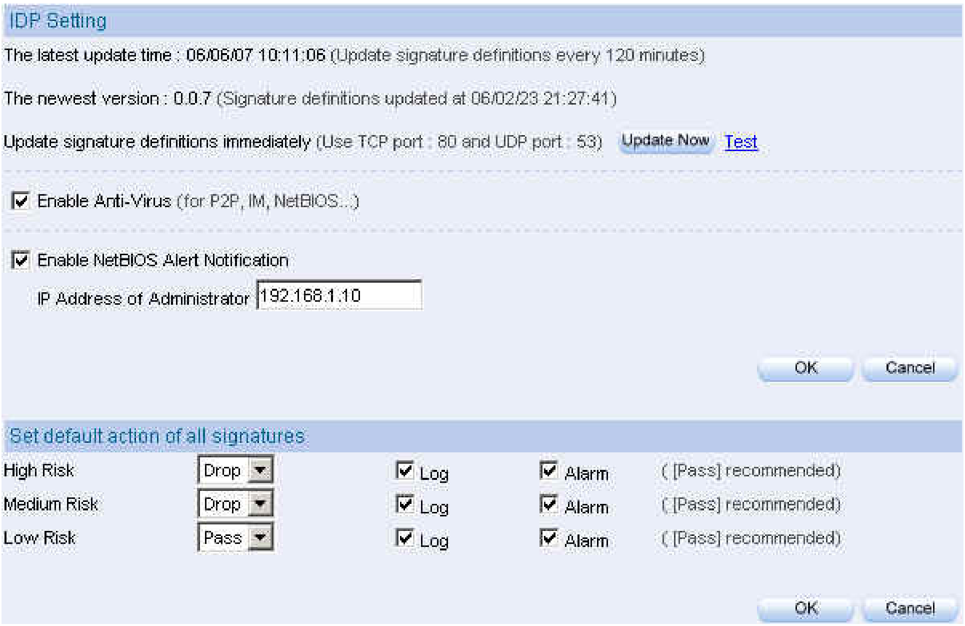
The MIS engineer can click Test , in order to make sure the SG-1000 can connect to the signature definition server normaly.

Set default action of all signatures

The internet attack risks included High, Medium and Low. The MIS engineer can select the action of Pass , Drop , Log or Alarm to the default signatures .

In **System → Configure → Setting**, select **Enable E-mail Alert Notification** , and add the following settings：

1. Select **Enable Anti-Virus** .
2. Select **Enable NetBIOS Alert Notification .**
3. **IP Address of MIS engineer** , enter 192.168.1.10 .
4. Click **OK** .
5. **High Risk** , select Drop , Log and Alarm .
6. **Medium Risk** , select Drop , Log and Alarm .
7. **Low Risk** , select Pass , Log and Alarm .
8. Click **OK** . (***Fig. 17-1***)
9. Select enable **IDP** in policy .



IDP Setting

The latest update time : 06/06/07 10:11:06 (Update signature definitions every 120 minutes)

The newest version : 0.0.7 (Signature definitions updated at 06/02/23 21:27:41)

Update signature definitions immediately (Use TCP port : 80 and UDP port : 53) Update Now Test

☑ Enable Anti-Virus (for P2P, IM, NetBIOS...)

☑ Enable NetBIOS Alert Notification

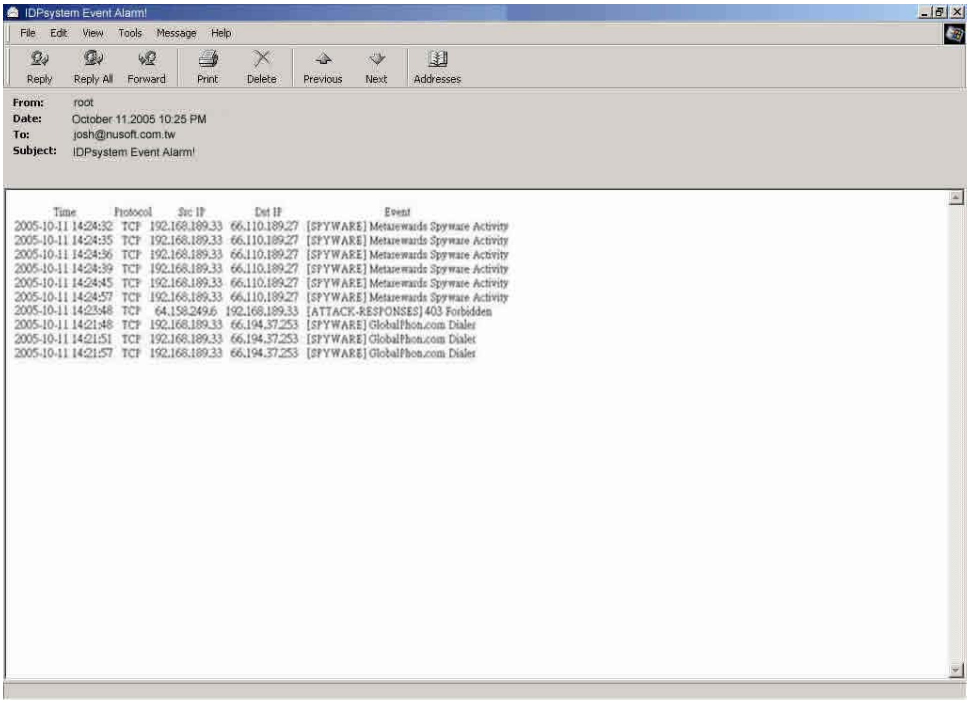
IP Address of Administrator 192.168.1.10

Set default action of all signatures

High Risk	Drop	☑ Log	☑ Alarm	([Pass] recommended)
Medium Risk	Drop	☑ Log	☑ Alarm	([Pass] recommended)
Low Risk	Pass	☑ Log	☑ Alarm	([Pass] recommended)

Fig. 17-1 The IDP setting

When the SG-1000 detected the attack types corresponded to the signature , then it will send the NetBIOS notification through e-mail and results the **Log** in **IDP → IDP Report**. (***Fig. 17-2, Fig. 17-3, Fig. 17-4***)

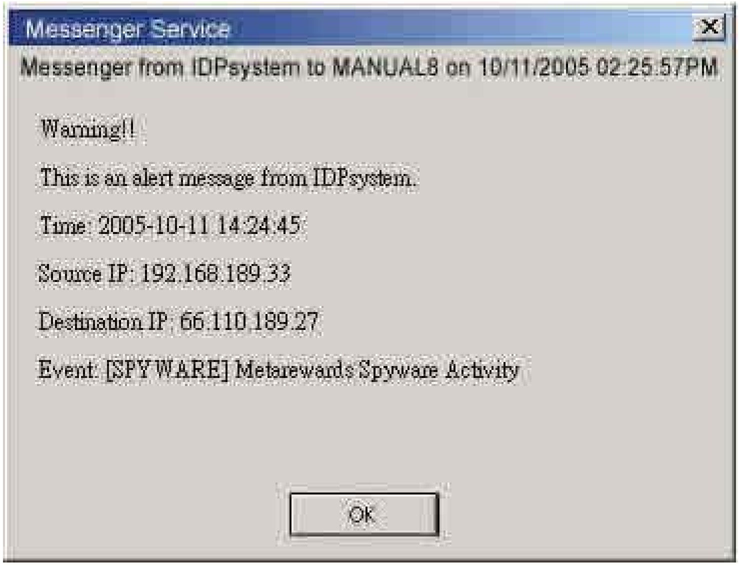


From: root
Date: October 11,2005 10:25 PM
To: josh@nusoft.com.tw
Subject: IDPsystem Event Alarm!

```
      Time          Protocol    Src IP         Dst IP                  Event
2005-10-11 14:24:32  TCP  192.168.189.33  66.110.189.27  [SPYWARE] Metarewards Spyware Activity
2005-10-11 14:24:35  TCP  192.168.189.33  66.110.189.27  [SPYWARE] Metarewards Spyware Activity
2005-10-11 14:24:36  TCP  192.168.189.33  66.110.189.27  [SPYWARE] Metarewards Spyware Activity
2005-10-11 14:24:39  TCP  192.168.189.33  66.110.189.27  [SPYWARE] Metarewards Spyware Activity
2005-10-11 14:24:45  TCP  192.168.189.33  66.110.189.27  [SPYWARE] Metarewards Spyware Activity
2005-10-11 14:24:57  TCP  192.168.189.33  66.110.189.27  [SPYWARE] Metarewards Spyware Activity
2005-10-11 14:23:48  TCP    64.158.249.6  192.168.189.33 [ATTACK-RESPONSES] 403 Forbidden
2005-10-11 14:21:48  TCP  192.168.189.33  66.194.37.253  [SPYWARE] GlobalPhon.com Dialer
2005-10-11 14:21:51  TCP  192.168.189.33  66.194.37.253  [SPYWARE] GlobalPhon.com Dialer
2005-10-11 14:21:57  TCP  192.168.189.33  66.194.37.253  [SPYWARE] GlobalPhon.com Dialer
```

Fig. 17-2 Send the IDP notification

The MIS engineer must enable the alarm function to send mail notification in Anomaly , Pre-defined and Custom .



Messenger from IDPsystem to MANUAL8 on 10/11/2005 02:25:57PM

Warning!!

This is an alert message from IDPsystem.

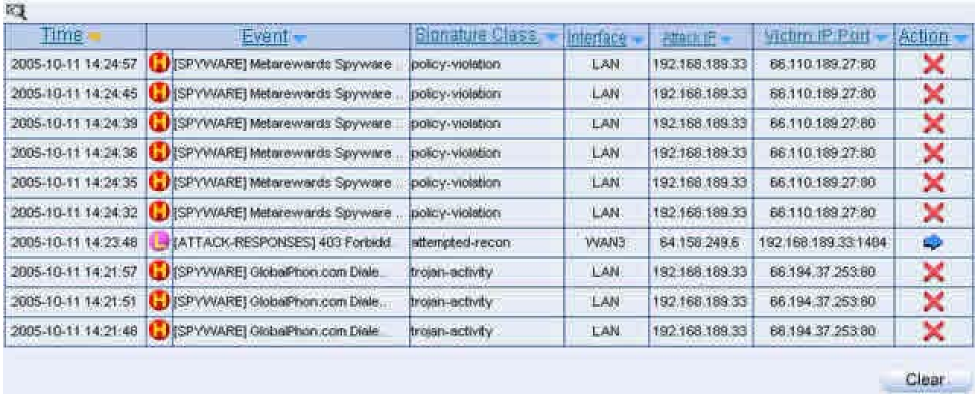
Time: 2005-10-11 14:24:45

Source IP: 192.168.189.33

Destination IP: 66.110.189.27

Event: [SPYWARE] Metarewards Spyware Activity

Fig. 17-3 Send the NetBIOS notification to MIS engineer



Time	Event	Signature Class	Interface	Attack IP	Victim IP:Port	Action
2005-10-11 14:24:57	H [SPYWARE] Metarewards Spyware	policy-violation	LAN	192.168.189.33	66.110.189.27:80	✗
2005-10-11 14:24:45	H [SPYWARE] Metarewards Spyware ...	policy-violation	LAN	192.168.189.33	66.110.189.27:80	✗
2005-10-11 14:24:39	H [SPYWARE] Metarewards Spyware	policy-violation	LAN	192.168.189.33	66.110.189.27:80	✗
2005-10-11 14:24:36	H [SPYWARE] Metarewards Spyware ...	policy-violation	LAN	192.168.189.33	66.110.189.27:80	✗
2005-10-11 14:24:35	H [SPYWARE] Metarewards Spyware	policy-violation	LAN	192.168.189.33	66.110.189.27:80	✗
2005-10-11 14:24:32	H [SPYWARE] Metarewards Spyware ...	policy-violation	LAN	192.168.189.33	66.110.189.27:80	✗
2005-10-11 14:23:48	L [ATTACK-RESPONSES] 403 Forbidd	attempted-recon	WAN3	64.158.249.6	192.168.189.33:1484	➡
2005-10-11 14:21:57	H [SPYWARE] GlobalPhon.com Diale...	trojan-activity	LAN	192.168.189.33	66.194.37.253:80	✗
2005-10-11 14:21:51	H [SPYWARE] GlobalPhon.com Diale...	trojan-activity	LAN	192.168.189.33	66.194.37.253:80	✗
2005-10-11 14:21:48	H [SPYWARE] GlobalPhon.com Diale...	trojan-activity	LAN	192.168.189.33	66.194.37.253:80	✗

Fig. 17-4 The IDP Log

The MIS engineer must enable the Log function in Anomaly , Pre-defined and Custom , in order to result the IDP log.

Signature

The SG-1000 can provide the correspond comparison rules included **Anomaly** , **Pre-defined** and **Custom** according to different attack types.

The **Anomaly** can detect and prevent the anomaly flow and packets via the signature updating. The **Pre-defined** can also detect and prevent the intrusion through the signature updating. Both the anomaly and pre-defined signatures can not be deleted or modified . The **Custom** can detect the other internet attacks, anomaly flow packets except the original **Anomaly** and **Pre-defined** detection according to the user demand .

Signature

Anomaly

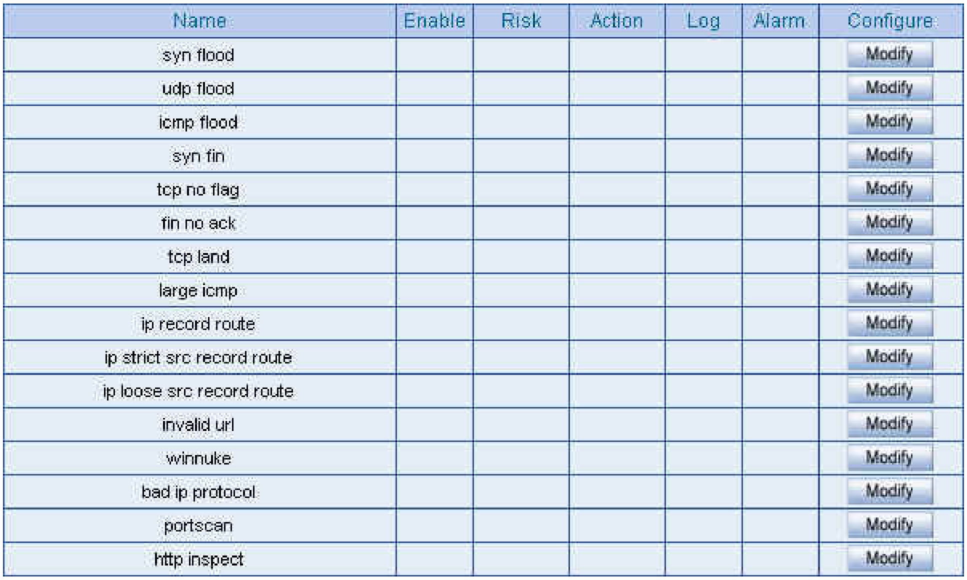
It includes the syn flood, udp flood, icmp flood, syn fin, tcp no flag, fin no ack, tcp land, larg icmp, ip record route, ip strict src record route, ip loose src record route, invalid url, winnuke, bad ip protocol, portscan and http inspect , such Anomaly detection signatures. (*Fig. 18-1*)

User can enable the anomaly packets signature to detect , depends on the user demand .

User can manage the specific anomaly flow packets.

User can modify the action of pass , drop , log or alarm.

The SG-1000 can display all the anomaly detection signature attribute of name , enable , risk , action , log and alarm.

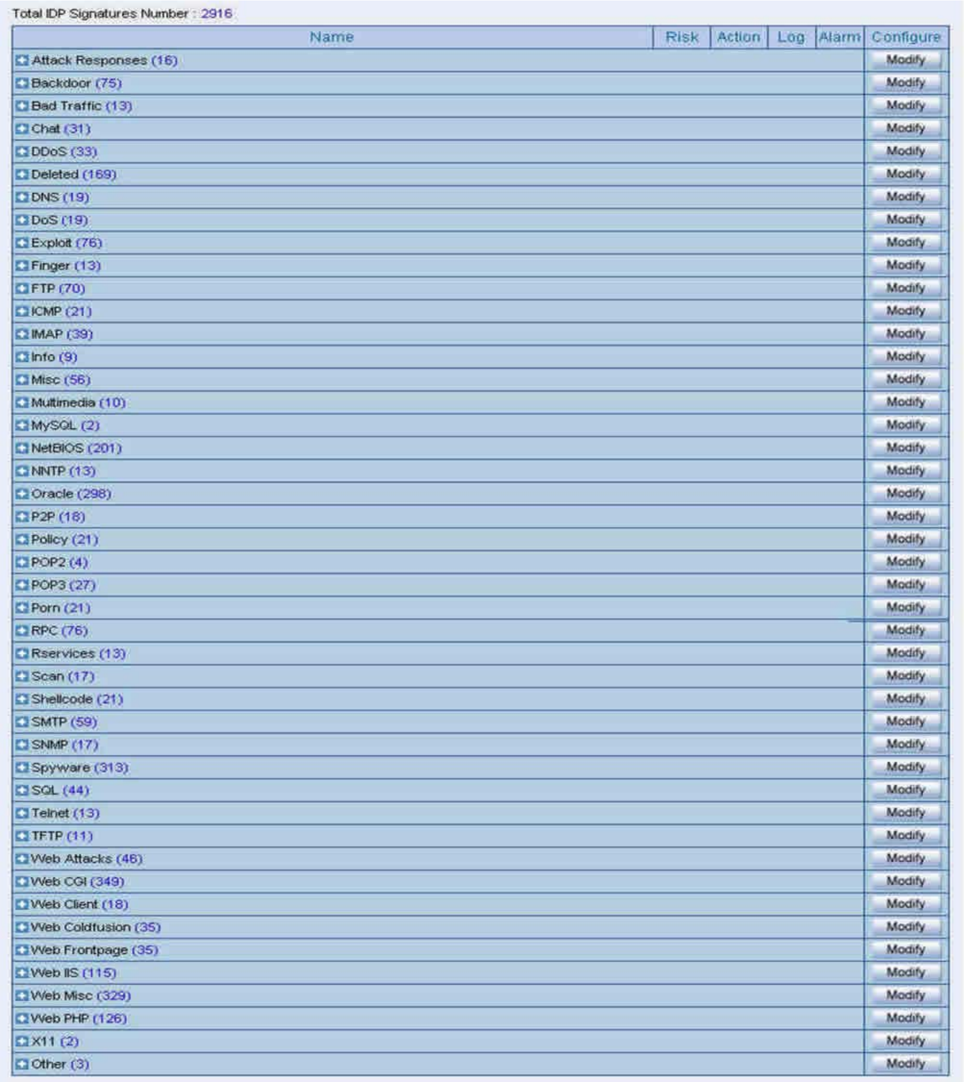


Name	Enable	Risk	Action	Log	Alarm	Configure
syn flood						Modify
udp flood						Modify
icmp flood						Modify
syn fin						Modify
tcp no flag						Modify
fin no ack						Modify
tcp land						Modify
large icmp						Modify
ip record route						Modify
ip strict src record route						Modify
ip loose src record route						Modify
invalid url						Modify
winnuke						Modify
bad ip protocol						Modify
portscan						Modify
http inspect						Modify

Fig. 18-1 The anomaly signature setting

Pre-defined

„ It includes the Attack Responses, Backdoor, Bad Traffic, Chat, DDoS, Deleted, DNS, DoS, Exploit, Finger, FTP, ICMP, IMAP, Info, Misc, Multimedia, MySQL, NetBIOS, NNTP, Oracle, P2P, Policy, POP2, POP3, Porn, RPC, Rservices, Scan, Sellcode, SMTP, SNMP, Spyware, SQL, Telnet, TFTP, Web Acctacks, Web CGI, Web Client, Web Coldfusion, Web Frontpage, Web IIS, Web Misc, Web PHP and X11. On the other hand , every types included its attack signature. （***Fig. 18-2***） User can modify the signature action of pass , drop , log or alarm in every types . The SG-1000 can display all the attack signature attribute of name , risk , action , log and alarm.



Total IDP Signatures Number : 2916

Name	Risk	Action	Log	Alarm	Configure
Attack Responses (16)					Modify
Backdoor (75)					Modify
Bad Traffic (13)					Modify
Chat (31)					Modify
DDoS (33)					Modify
Deleted (169)					Modify
DNS (19)					Modify
DoS (19)					Modify
Exploit (76)					Modify
Finger (13)					Modify
FTP (70)					Modify
ICMP (21)					Modify
IMAP (39)					Modify
Info (9)					Modify
Misc (56)					Modify
Multimedia (10)					Modify
MySQL (2)					Modify
NetBIOS (201)					Modify
NNTP (13)					Modify
Oracle (298)					Modify
P2P (18)					Modify
Policy (21)					Modify
POP2 (4)					Modify
POP3 (27)					Modify
Porn (21)					Modify
RPC (76)					Modify
Rservices (13)					Modify
Scan (17)					Modify
Shellcode (21)					Modify
SMTP (59)					Modify
SNMP (17)					Modify
Spyware (313)					Modify
SQL (44)					Modify
Telnet (13)					Modify
TFTP (11)					Modify
Web Attacks (46)					Modify
Web CGI (349)					Modify
Web Client (18)					Modify
Web Coldfusion (35)					Modify
Web Frontpage (35)					Modify
Web IIS (115)					Modify
Web Misc (329)					Modify
Web PHP (126)					Modify
X11 (2)					Modify
Other (3)					Modify

Fig. 18-2 The pre-defined setting

In Configure → Setting , the SG-1000 will access the default action of risk setting when the user modify the Pre-defined . User can modify the action of every signature depends on the user demand after the IDP configuration.

Name

The MIS engineer can define the signature name.

Protocol

The detection and prevention protocol setting includes TCP , UDP, ICMP and IP.

Source Port

To set the attack PC port.（Range :0~65535）.

Destination Port

To set the attacked (victim) PC port.（Range : 0~65535）.

Risk

To define the threats of attack packets.

Action

The action of attack packets.

Content

To set the attack packets content.

Advance Option

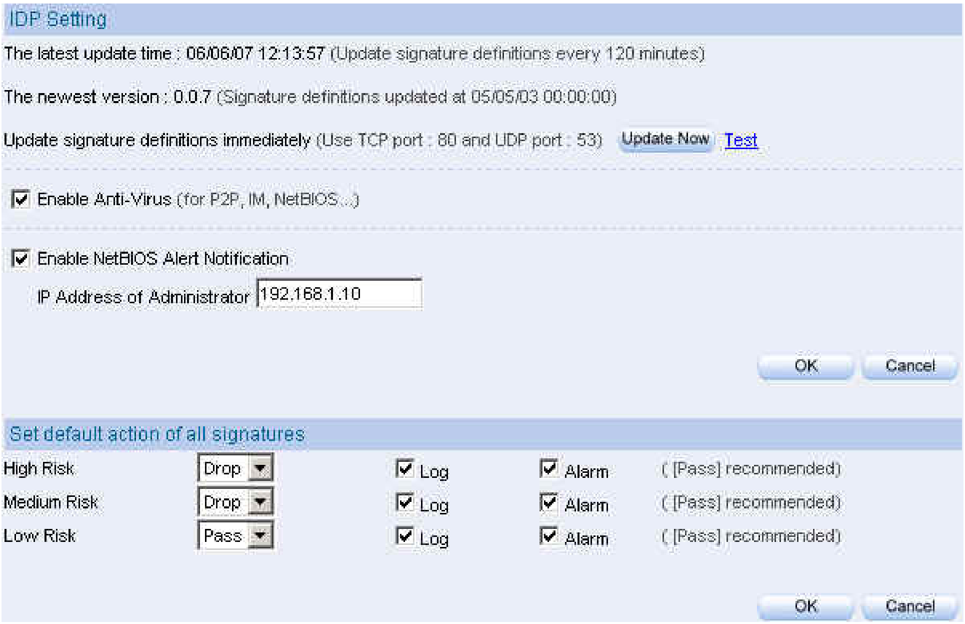
It can filter the inbound and outbound attack packets.

The user can choose to process the packets filtering according to the text case in signatures contents.

Signature Example

To detect the anomaly flow and packets with the custom and pre-defined settings , in order to detect and prevent the intrusion.

Step1 In **Configure → Setting** , add the following settings： (***Fig. 18-3***)



IDP Setting

The latest update time : 06/06/07 12:13:57 (Update signature definitions every 120 minutes)

The newest version : 0.0.7 (Signature definitions updated at 05/05/03 00:00:00)

Update signature definitions immediately (Use TCP port : 80 and UDP port : 53) Update Now Test

☑ Enable Anti-Virus (for P2P, IM, NetBIOS ...)

☑ Enable NetBIOS Alert Notification

IP Address of Administrator 192.168.1.10

OK Cancel

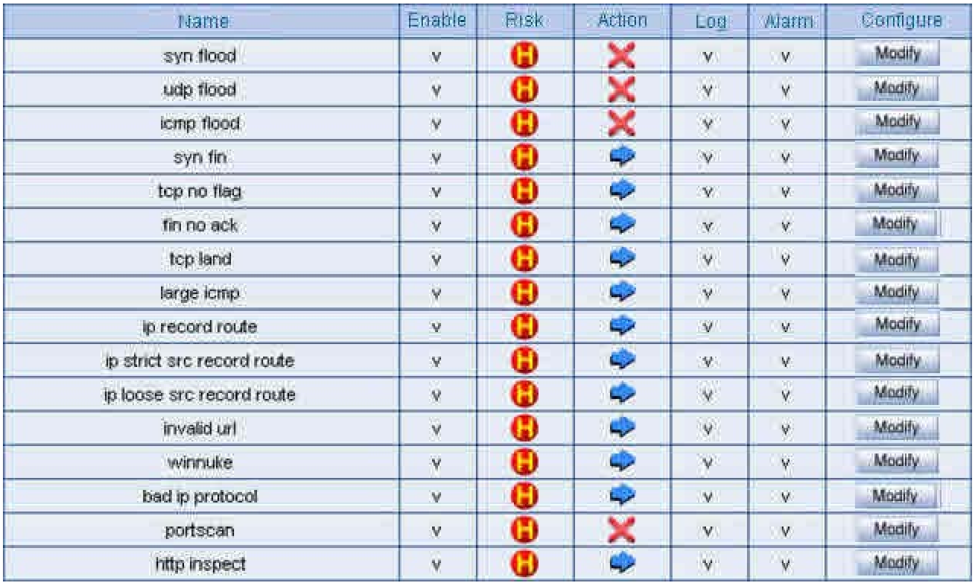
Set default action of all signatures

High Risk	Drop	☑ Log	☑ Alarm	([Pass] recommended)
Medium Risk	Drop	☑ Log	☑ Alarm	([Pass] recommended)
Low Risk	Pass	☑ Log	☑ Alarm	([Pass] recommended)

OK Cancel

Fig. 18-3 The IDP configure setting

Step2 In **Signature → Anomaly** , add the following settings：（***Fig. 18-4***）



Name	Enable	Risk	Action	Log	Alarm	Configure
syn flood	v	H	✗	v	v	Modify
udp flood	v	H	✗	v	v	Modify
icmp flood	v	H	✗	v	v	Modify
syn fin	v	H	➡	v	v	Modify
tcp no flag	v	H	➡	v	v	Modify
fin no ack	v	H	➡	v	v	Modify
tcp land	v	H	➡	v	v	Modify
large icmp	v	H	➡	v	v	Modify
ip record route	v	H	➡	v	v	Modify
ip strict src record route	v	H	➡	v	v	Modify
ip loose src record route	v	H	➡	v	v	Modify
invalid url	v	H	➡	v	v	Modify
winnuke	v	H	➡	v	v	Modify
bad ip protocol	v	H	➡	v	v	Modify
portscan	v	H	✗	v	v	Modify
http inspect	v	H	➡	v	v	Modify

Fig. 18-4 The anomaly setting

Signature Example

Step3 In **Signature → Custom** , add the following setting：

Click **New Entry**.（*Fig. 18-5*）

Name, enter Software_Crack_Website.

Protocol, select TCP.

Source Port, enter 0:65535.

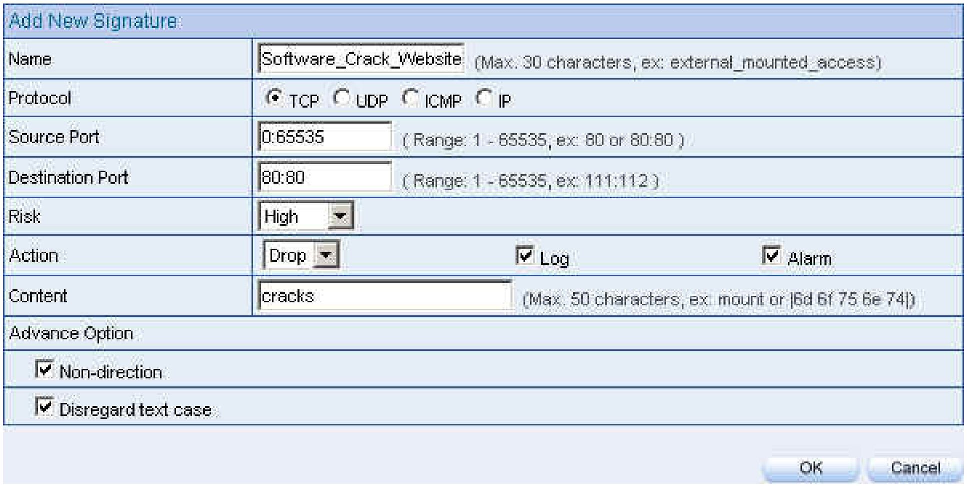
Destination Port, enter 80:80.

Risk, select High.

Action, select Drop, Log and Alarm.

Content, enter cracks.

Advance Option, select Non-direction and Disregard text case.（*Fig. 18-6*）



Add New Signature

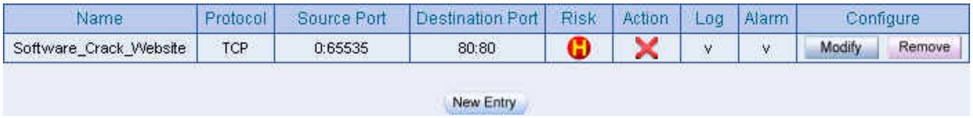
Name	Software_Crack_Website (Max. 30 characters, ex: external_mounted_access)
Protocol	● TCP ○ UDP ○ ICMP ○ IP
Source Port	0:65535 (Range: 1 - 65535, ex: 80 or 80:80)
Destination Port	80:80 (Range: 1 - 65535, ex: 111:112)
Risk	High
Action	Drop ☑ Log ☑ Alarm
Content	cracks (Max. 50 characters, ex: mount or |6d 6f 75 6e 74|)

Advance Option

☑ Non-direction

☑ Disregard text case

Fig. 18-5 The custom setting



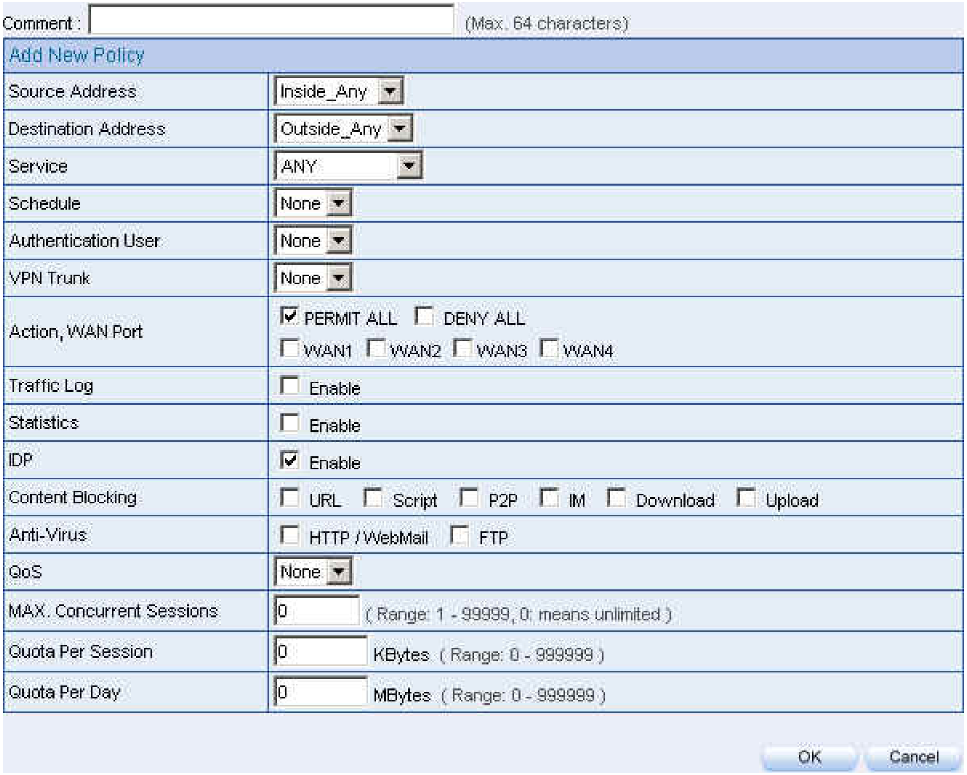
Name	Protocol	Source Port	Destination Port	Risk	Action	Log	Alarm	Configure
Software_Crack_Website	TCP	0:65535	80:80	H	✗	v	v	Modify Remove

Fig. 18-6 Complete the custom setting

In Content , the MIS engineer can enter the string to detect or transfer it to the 16 carries ASCII code . (For example ：cracks can be transfer to |63 72 61 63 6b 73|) .

Signature Example

Step4 In **Policy → Outgoing** , add the new policy and enable **IDP**：（*Fig. 18-7*、*Fig. 18-8*）

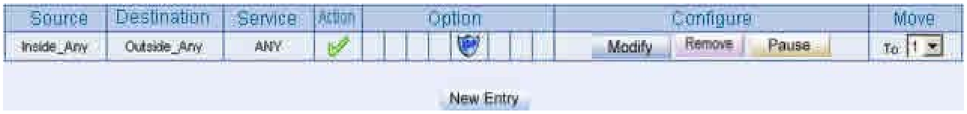


Comment : (Max. 64 characters)

Add New Policy

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	☑ PERMIT ALL □ DENY ALL □ WAN1 □ WAN2 □ WAN3 □ WAN4
Traffic Log	□ Enable
Statistics	□ Enable
IDP	☑ Enable
Content Blocking	□ URL □ Script □ P2P □ IM □ Download □ Upload
Anti-Virus	□ HTTP / WebMail □ FTP
QoS	None
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)

Fig. 18-7 The IDP setting in policy



Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	IDP	Modify Remove Pause	To 1

Fig. 18-8 Complete the IDP setting in policy

IDP Report

The SG-1000 can display the IDP record by statistics and log. So that the enterprises can easily know the whole network status.

In this Chapter , we will make the introduction of **IDP Report**.

Setting

Periodic Report

It can send the period report to recipient according to the selected date.

History Report

It can send the history report according to the assigned date.

In **System → Configure → Setting** , enable **E-mail Alert Notification** . On the other hand , add the following settings in **IDP Report :**

1. **Enable sending period report by mail , select Yearly report ,Monthly report , Weekly report , Daily report .**
2. Click **OK .** (***Fig. 19-1***)
3. When the time arrived , the SG-1000 will send the report to recipient . (***Fig. 19-2, Fig. 19-3***)
4. In **History Report** , select the date to send the report. (***Fig. 19-4***)
5. Click **Send Report .**
6. It will send the related report to the user. (***Fig. 19-5, Fig. 19-6***)

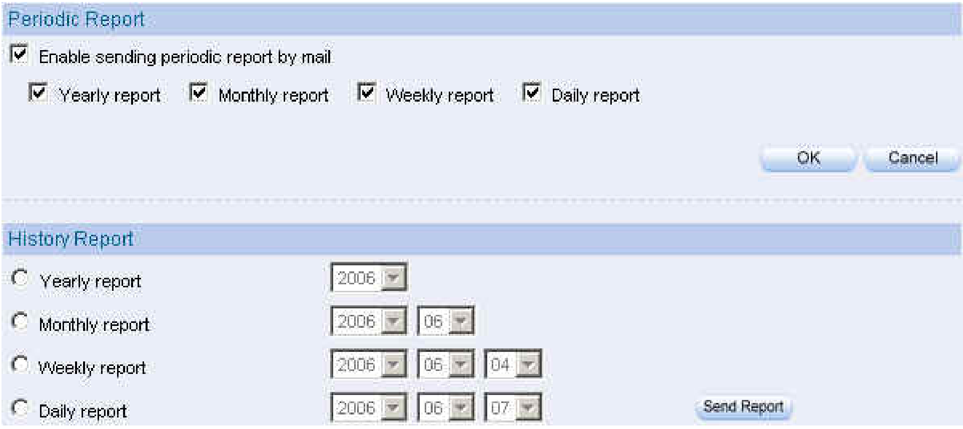
The periodic report will result in the following date:

1.Yearly report ; It results in 00:00 AM , January first , Yearly.

2.Monthly report : It results in 00:00 AM , first day , Monthly .

3.Weekly report : It results in 00:00 AM , first day , Weekly .

4.Daily report : It results in 00:00, Daily.



Periodic Report

☑ Enable sending periodic report by mail

☑ Yearly report ☑ Monthly report ☑ Weekly report ☑ Daily report

History Report

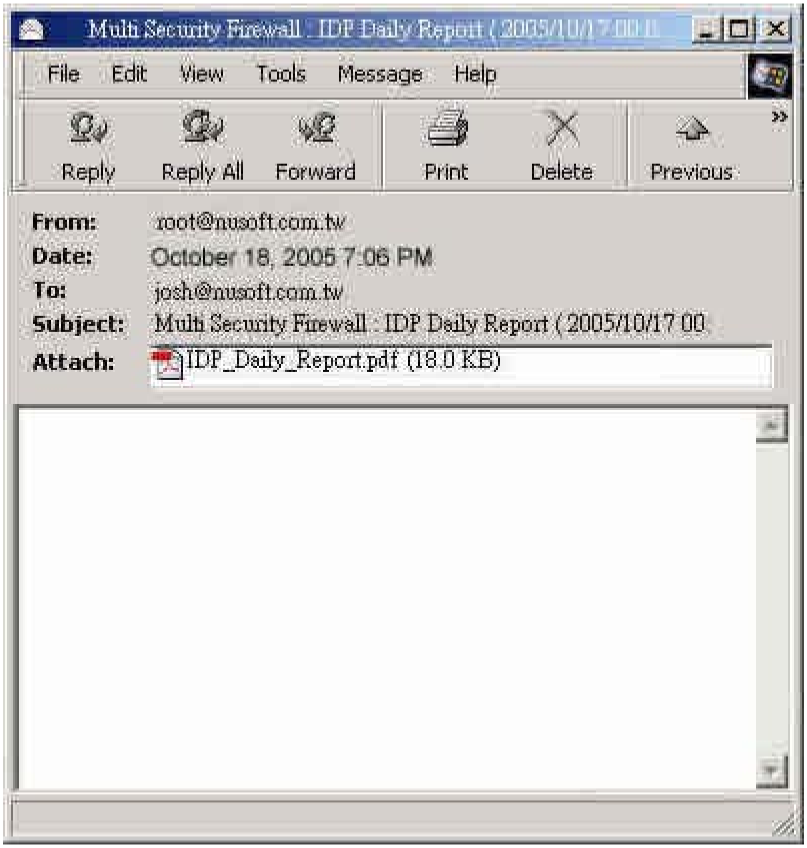
○ Yearly report 2006

○ Monthly report 2006 06

○ Weekly report 2006 06 04

○ Daily report 2006 06 07

Fig. 19-1 The periodic report setting



From: root@nusoft.com.tw

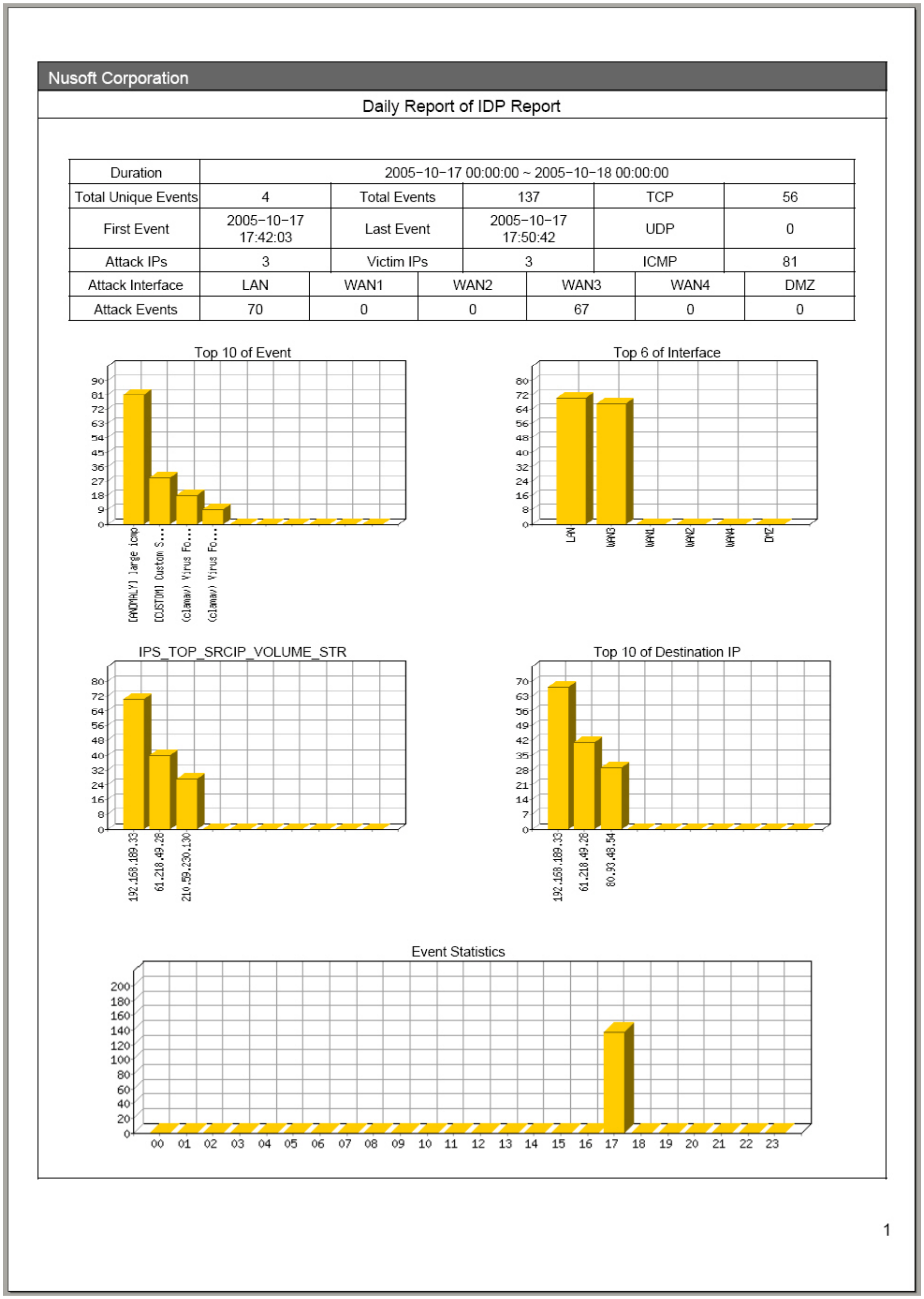
Date: October 18, 2005 7:06 PM

To: josh@nusoft.com.tw

Subject: Multi Security Firewall : IDP Daily Report (2005/10/17 00

Attach: IDP_Daily_Report.pdf (18.0 KB)

Fig. 19-2 Receive the periodic report



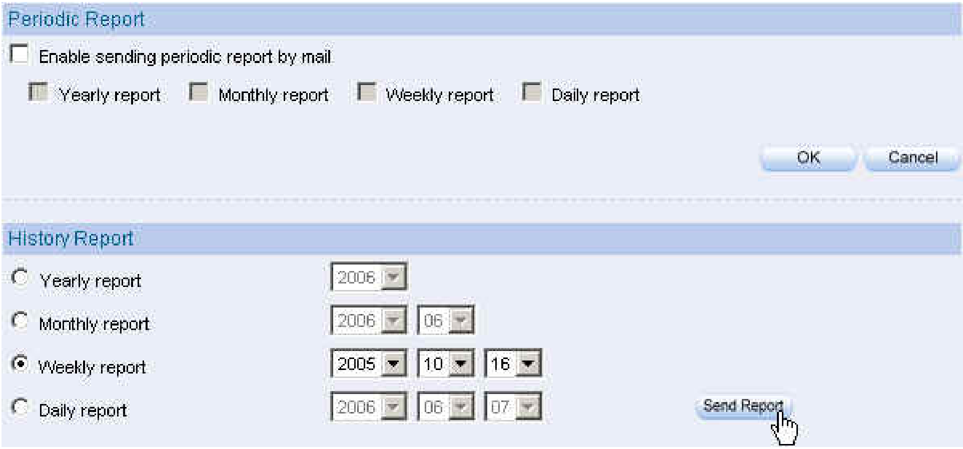
Nusoft Corporation

Daily Report of IDP Report

Duration	2005−10−17 00:00:00 ~ 2005−10−18 00:00:00				
Total Unique Events	4	Total Events	137	TCP	56
First Event	2005−10−17 17:42:03	Last Event	2005−10−17 17:50:42	UDP	0
Attack IPs	3	Victim IPs	3	ICMP	81

Attack Interface	LAN	WAN1	WAN2	WAN3	WAN4	DMZ
Attack Events	70	0	0	67	0	0

Fig. 19-3 The IDP report content



Periodic Report

□ Enable sending periodic report by mail

□ Yearly report □ Monthly report □ Weekly report □ Daily report

History Report

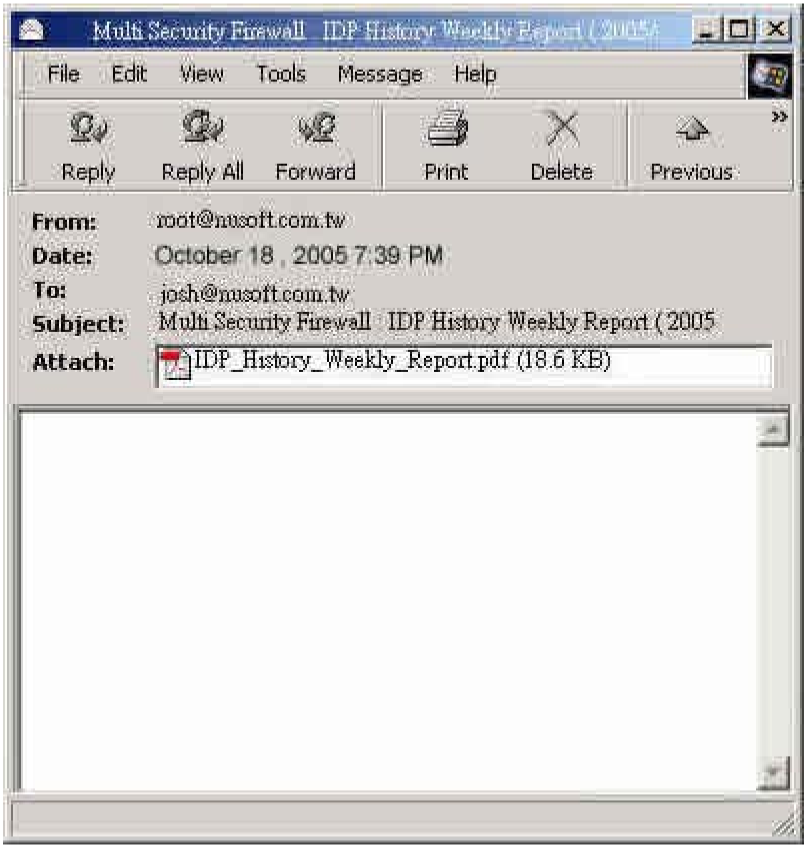
○ Yearly report 2006

○ Monthly report 2006 06

● Weekly report 2005 10 16

○ Daily report 2006 06 07

Fig. 19-4 The history report setting



Multi Security Firewall IDP History Weekly Report (2005/

From: root@nusoft.com.tw

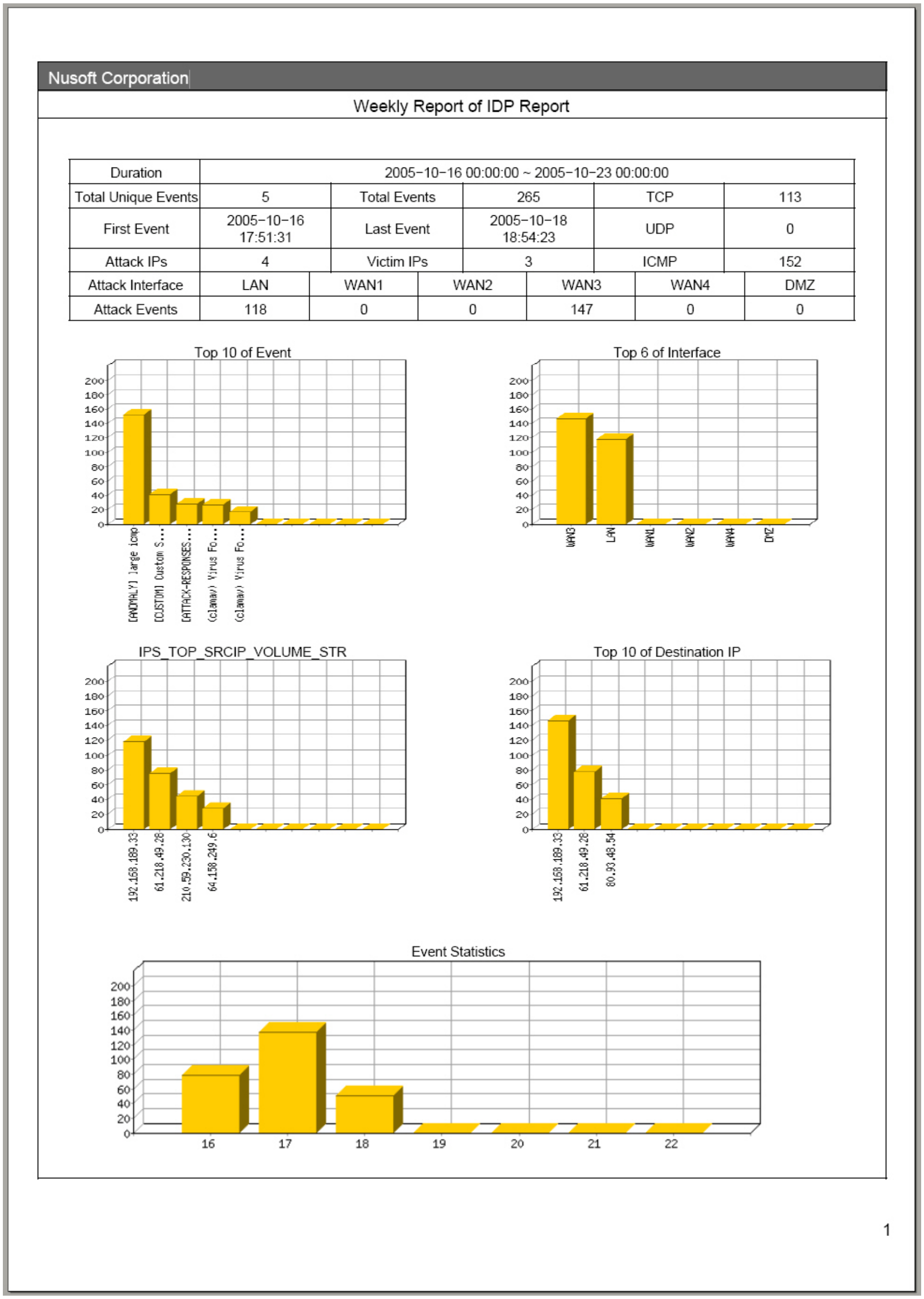
Date: October 18 , 2005 7:39 PM

To: josh@nusoft.com.tw

Subject: Multi Security Firewall IDP History Weekly Report (2005

Attach: IDP_History_Weekly_Report.pdf (18.6 KB)

Fig. 19-5 Receive the history report



Nusoft Corporation

Weekly Report of IDP Report

Duration	2005-10-16 00:00:00 ~ 2005-10-23 00:00:00				
Total Unique Events	5	Total Events	265	TCP	113
First Event	2005-10-16 17:51:31	Last Event	2005-10-18 18:54:23	UDP	0
Attack IPs	4	Victim IPs	3	ICMP	152

Attack Interface	LAN	WAN1	WAN2	WAN3	WAN4	DMZ
Attack Events	118	0	0	147	0	0

Fig. 19-6 The history report content

The IDP report will attached as PDF format to send to the recipient.

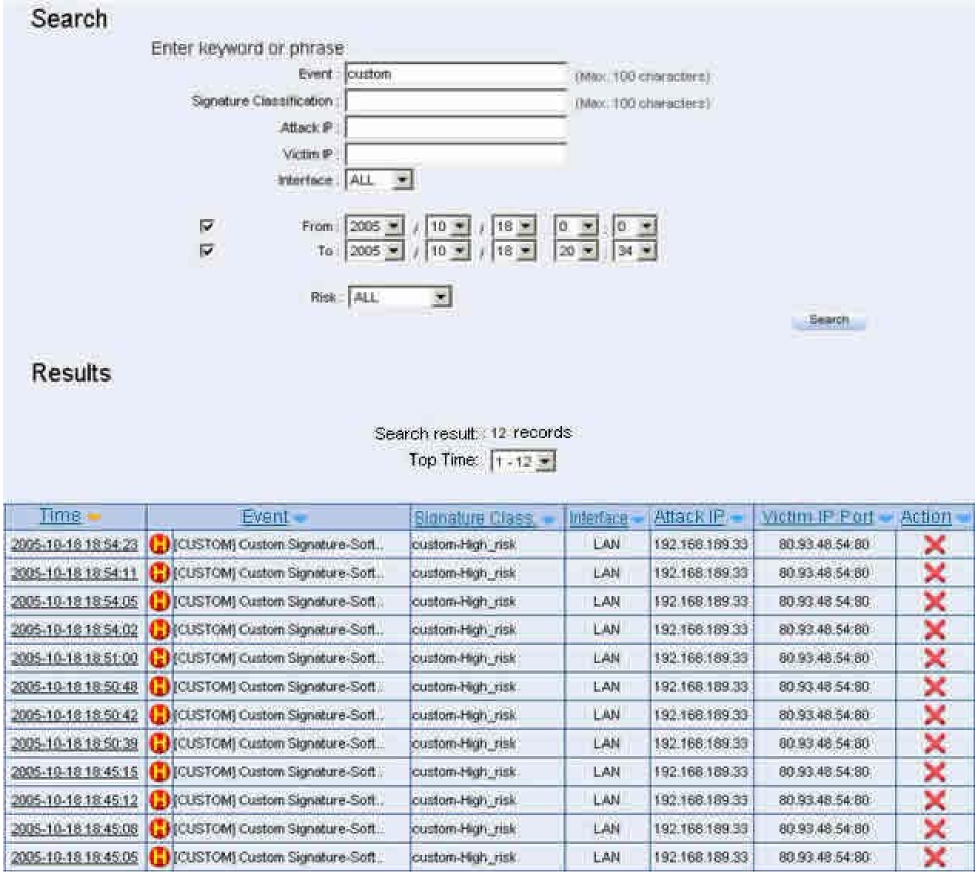
Log

Search

The SG-1000 can search the records correspond to the condition depends on the Event , Signature Classification , Attack IP , Victim IP , Interface , Date and Risk .

Add the following settings：

1. **Event** , enter the keyword of anomaly and attack packets events.
2. **Interface** , select ALL .
3. Select **after this date and before this date** , in order to search the record in date period .
4. **Risk** , select ALL .
5. Click **Search**. (***Fig. 19-7***)



Search

Enter keyword or phrase

Event : custom (Max. 100 characters)

Signature Classification : (Max. 100 characters)

Attack IP :

Victim IP :

Interface : ALL

☑ From : 2005 / 10 / 18 0 : 0

☑ To : 2005 / 10 / 18 20 : 34

Risk : ALL

Results

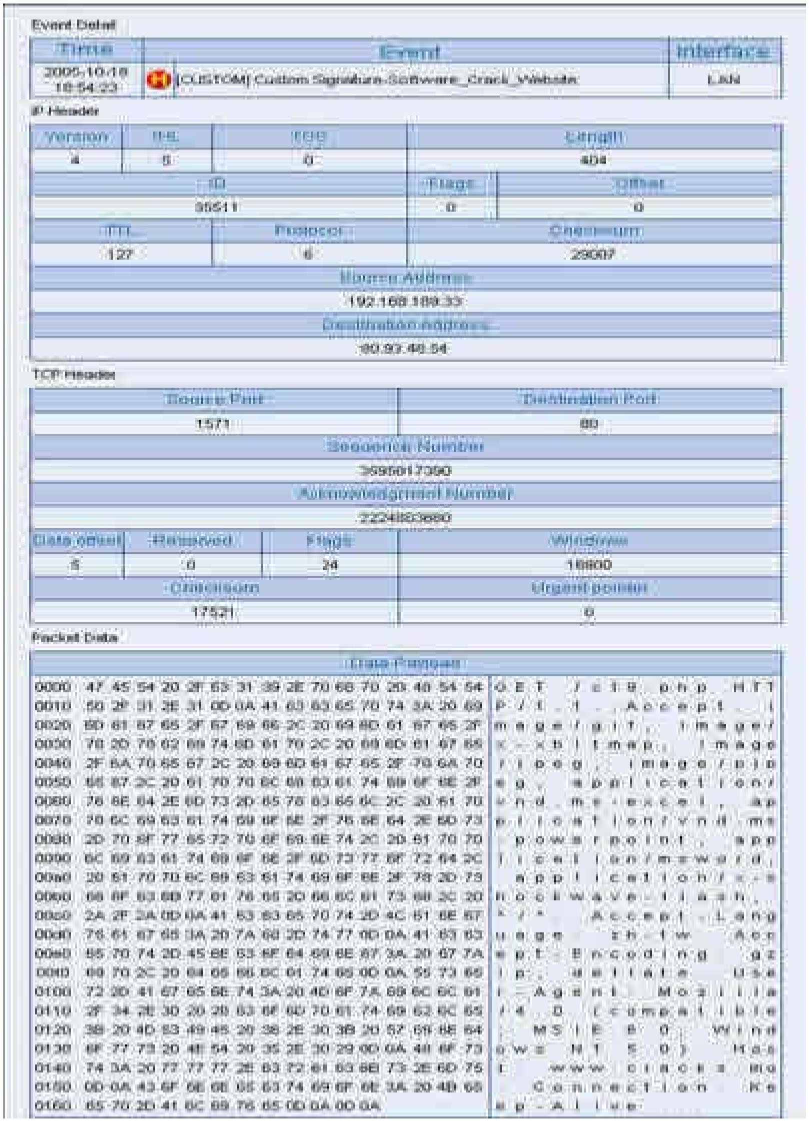
Search result: 12 records

Top Time: 1 - 12

Time	Event	Signature Class	Interface	Attack IP	Victim IP:Port	Action
2005-10-18 18:54:23	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:54:11	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:54:05	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:54:02	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:51:00	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:50:48	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:50:42	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:50:39	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:45:15	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:45:12	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:45:08	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗
2005-10-18 18:45:05	H [CUSTOM] Custom Signature-Soft...	custom-High_risk	LAN	192.168.189.33	80.93.48.54:80	✗

Fig. 19-7 To search the specific record

In **Log → Search ,** click Time link , then it shows the **Event Detail** . (***Fig. 19-8***)



Event Detail

Time	Event	Interface
2005-10-18 18:54:23	[CUSTOM] Custom Signature-Software_Crack_Website	LAN

IP Header

Version	IHL	TOS	Length
4	5	0	404

ID	Flags	Offset
35511	0	0

TTL	Protocol	Checksum
127	6	29007

Source Address
192.168.189.33

Destination Address
80.93.48.54

TCP Header

Source Port	Destination Port
1571	80

Sequence Number
3595917390

Acknowledgment Number
2224803880

Data offset	Reserved	Flags	Window
5	0	24	16800

Checksum	Urgent pointer
17521	0

Packet Data

Data Payload

```
0000  47 45 54 20 2F 63 31 39 2E 70 68 70 20 48 54 54   GET /c19.php HTT
0010  50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 69   P/1.1..Accept: i
0020  6D 61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65 2F   mage/gif, image/
0030  78 2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67 65   x-xbitmap, image
0040  2F 6A 70 65 67 2C 20 69 6D 61 67 65 2F 70 6A 70   /jpeg, image/pjp
0050  65 67 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F   eg, application/
0060  76 6E 64 2E 6D 73 2D 65 78 63 65 6C 2C 20 61 70   vnd.ms-excel, ap
0070  70 6C 69 63 61 74 69 6F 6E 2F 76 6E 64 2E 6D 73   plication/vnd.ms
0080  2D 70 6F 77 65 72 70 6F 69 6E 74 2C 20 61 70 70   -powerpoint, app
0090  6C 69 63 61 74 69 6F 6E 2F 6D 73 77 6F 72 64 2C   lication/msword,
00a0  20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 73    application/x-s
00b0  68 6F 63 6B 77 61 76 65 2D 66 6C 61 73 68 2C 20   hockwave-flash, 
00c0  2A 2F 2A 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67   */*..Accept-Lang
00d0  75 61 67 65 3A 20 7A 68 2D 74 77 0D 0A 41 63 63   uage: zh-tw..Acc
00e0  65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A   ept-Encoding: gz
00f0  69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 55 73 65   ip, deflate..Use
0100  72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61   r-Agent: Mozilla
0110  2F 34 2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65   /4.0 (compatible
0120  3B 20 4D 53 49 45 20 36 2E 30 3B 20 57 69 6E 64   ; MSIE 6.0; Wind
0130  6F 77 73 20 4E 54 20 35 2E 30 29 0D 0A 48 6F 73   ows NT 5.0)..Hos
0140  74 3A 20 77 77 77 2E 63 72 61 63 6B 73 2E 6D 75   t: www.cracks.mu
0150  0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65   ..Connection: Ke
0160  65 70 2D 41 6C 69 76 65 0D 0A 0D 0A               ep-Alive....
```

Fig. 19-8 The event detail

✎In Log, the SG-1000 can make the sorting by Time , Event , Signature Classification , Interface , Attack IP , Victim IP Port and Action.

IDP Report Statistics

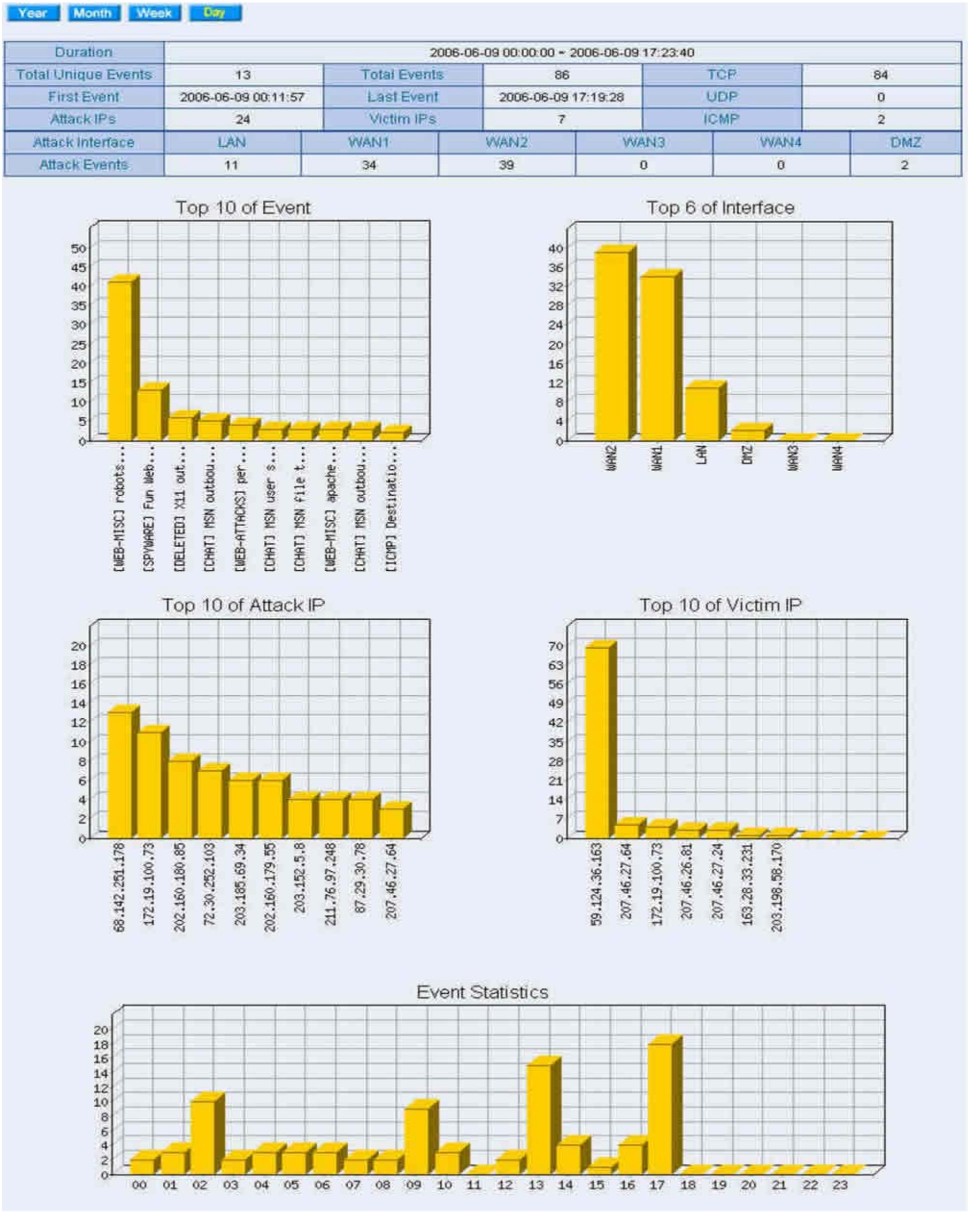
Step1 In **IDP Report → Statistics** , it shows the scanned mail statistics report in SG-1000.

Step2 In **Statistics** , click **Day** , to view the daily report . Click **Week** , to view the Weekly report . Click **Month** , to view the Monthly report . Click **Year** , to view the Yearly report .

Step3 The IDP Statistics . (*Fig. 19-9*)

Ordinate：The amount signatures of detected anomaly packets and attacks.

Horizontal ordinate：Time .



Duration	2006-06-09 00:00:00 ~ 2006-06-09 17:23:40				
Total Unique Events	13	Total Events	86	TCP	84
First Event	2006-06-09 00:11:57	Last Event	2006-06-09 17:19:28	UDP	0
Attack IPs	24	Victim IPs	7	ICMP	2

Attack Interface	LAN	WAN1	WAN2	WAN3	WAN4	DMZ
Attack Events	11	34	39	0	0	2

Fig. 19-9 The IDP statistics

IDP Report | Log

Step1 In **IDP Report → Log** , it shows the IDP status in SG-1000. （*Fig. 19-10*）

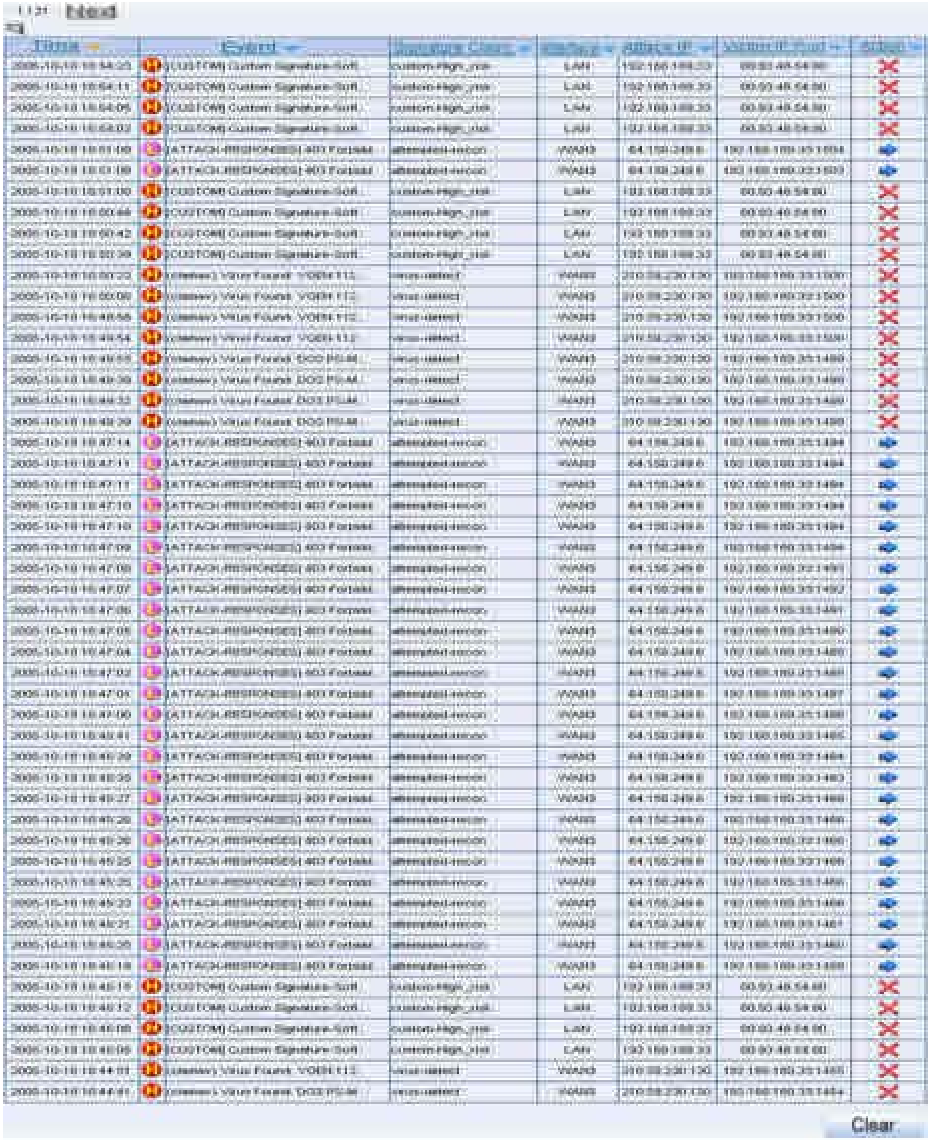


Fig. 19-10 The IDP log

IDP Report | Log

The icon description in Log：

1.Action：

Icon	➡	✕
Description	Pass	Drop

2.Risk：

Icon	H	M	L
Description	High Risk	Medium Risk	Low Risk