Chapter 17

Configure

Instant alerts are issued to the IT administrator by the NUM-MS3000 device upon the inspection of any suspicious packet contents or anomaly traffic flows. In addition, it blocks the packets and warns the IT administrator to prevent the host computer from being attacked by malicious code. In short, the NUS-MS3000 device protects network security, blocks malicious code from entering the network, leaves the internet running smoothly, and ensures information transmission security.

Intrusion Detection and Prevention (IDP), is the standard for NUS-MS3000 to deal with malicious code, being defined as the Intrusion Detection and Prevention setting in this chapter.

【Setting】Terminology:

Intrusion Detection and Prevention setting:

- Intrusion Detection and Prevention will receive automatic updates every 30 minutes, or alternatively, manual updates can be chosen instead. The file's time and version can be shown as well.
- Can detect viruses from unencrypted and uncompressed files.
- Anti-Virus engine, ClamAV, is available for use and offered free of charge.
- The device will warn the IT administrator via E-mail and NetBIOS once a virus is detected.

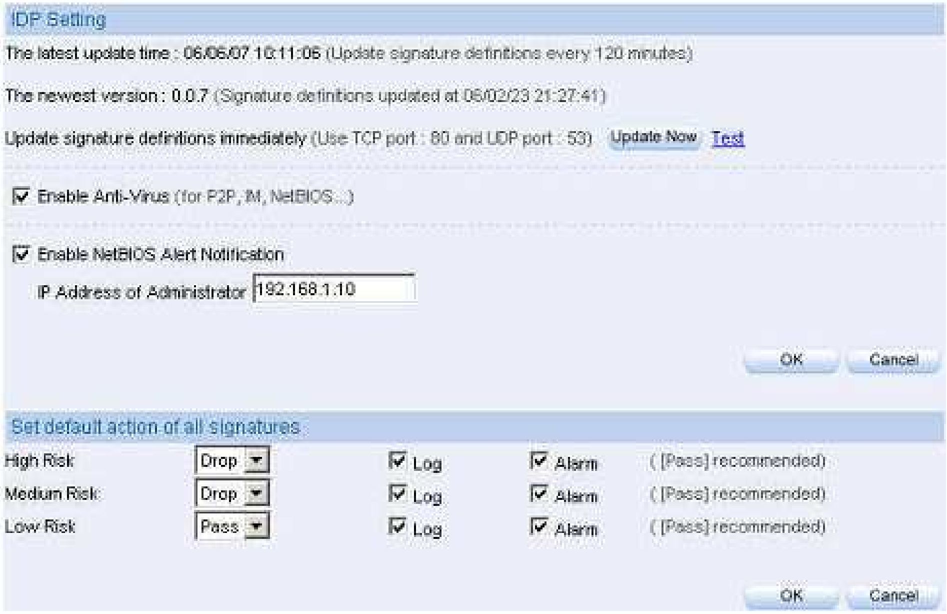
IT administrators can use【Test】function to make sure the device regularly connects to the website for signature updates.

Set default action of all signatures:

- The attacks can be classified into High Risk, Medium Risk and Low Risk. The device will block, log, or provide an alert about the attacks according to their classification.

  - ◆ In the navigation pane, click **System** > **Configure** > **Setting**, check the **Enable E-mail Alert Notification** checkbox:

    1. In the navigation pane, click **IDP > Configure > Setting**, check the **Enable Anti-Virus** checkbox.
    2. Check the **Enable NetBIOS Alert Notification** checkbox.
    3. Enter **192.168.1.10** in the **IP Address of Administrator** field.
    4. Click **OK**.
    5. For **High Risk**, select **Drop,** check the **Log** and the **Alert checkbox**.
    6. For **Medium Risk**, select **Drop**, check the **Log** and the **Alert checkbox**.
    7. For **Low Risk**, select **Pass**, check the **Log** and the **Alert checkbox**.
    8. Click **OK**. ***(Figure 17-1)***
    9. Go to **Policy** and enable the **IDP** function.



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

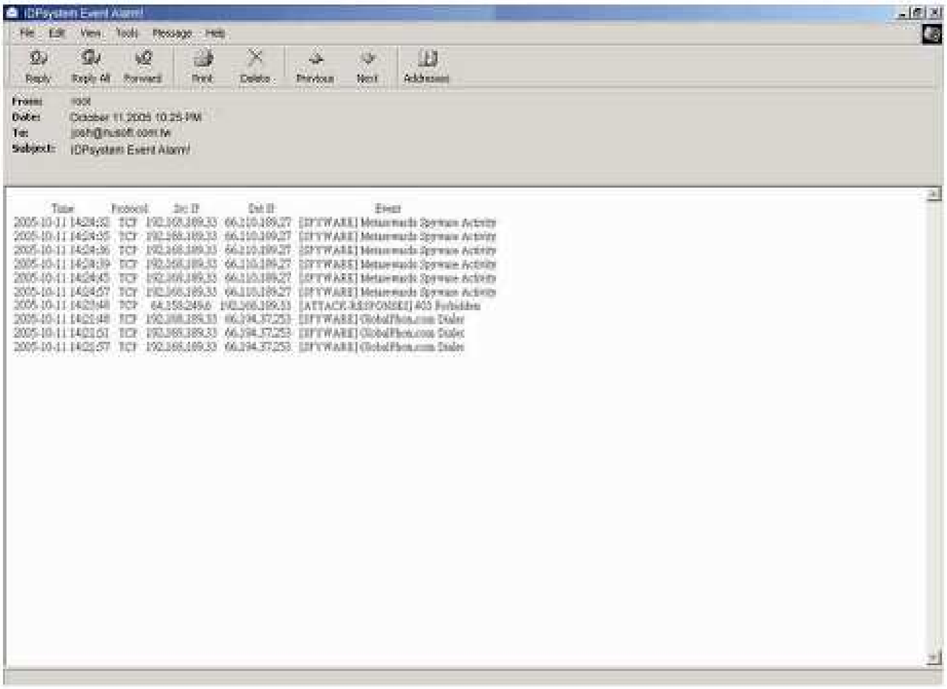
IP Address of Administrator 192.168.1.10

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)

Figure 17-1 Intrusion Detection and Prevention Screen

- Once the attack is detected, the IT administrator would be warned by mail and NetBIOS. Meanwhile, the log would be created in the **IDP report**. ***(Figure 17-2, Figure 17-3, Figure17-4)***

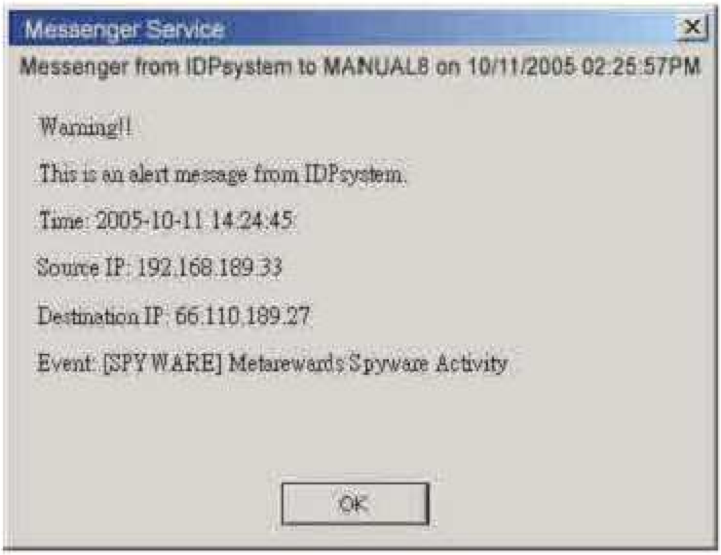


From: root
Date: October 11,2005 10:25 PM
To: josh@nusoft.com.tw
Subject: IDPsystem Event Alarm!

```
      Time          Protocol    Src IP         Dst IP                     Event
2005-10-11 14:24:32   TCP   192.168.189.33  66.110.189.27  [SPYWARE] Metaurmedia Spyware Activity
2005-10-11 14:24:35   TCP   192.168.189.33  66.110.189.27  [SPYWARE] Metaurmedia Spyware Activity
2005-10-11 14:24:36   TCP   192.168.189.33  66.110.189.27  [SPYWARE] Metaurmedia Spyware Activity
2005-10-11 14:24:39   TCP   192.168.189.33  66.110.189.27  [SPYWARE] Metaurmedia Spyware Activity
2005-10-11 14:24:45   TCP   192.168.189.33  66.110.189.27  [SPYWARE] Metaurmedia Spyware Activity
2005-10-11 14:24:57   TCP   192.168.189.33  66.110.189.27  [SPYWARE] Metaurmedia Spyware Activity
2005-10-11 14:23:48   TCP     64.158.249.6  192.168.189.33 [ATTACK-RESPONSES] 403 Forbidden
2005-10-11 14:22:48   TCP   192.168.189.33  66.194.37.253  [SPYWARE] GlobalPhon.com Dialer
2005-10-11 14:22:51   TCP   192.168.189.33  66.194.37.253  [SPYWARE] GlobalPhon.com Dialer
2005-10-11 14:22:57   TCP   192.168.189.33  66.194.37.253  [SPYWARE] GlobalPhon.com Dialer
```

Figure 17-2 Mail the Intrusion Detection and Prevention Alert

Warning mails are sent out only after **Anomaly**, **Pre-defined** and **Custom** are enabled.



Messenger Service

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

Warning!!

This is an alert message from IDPsystem.

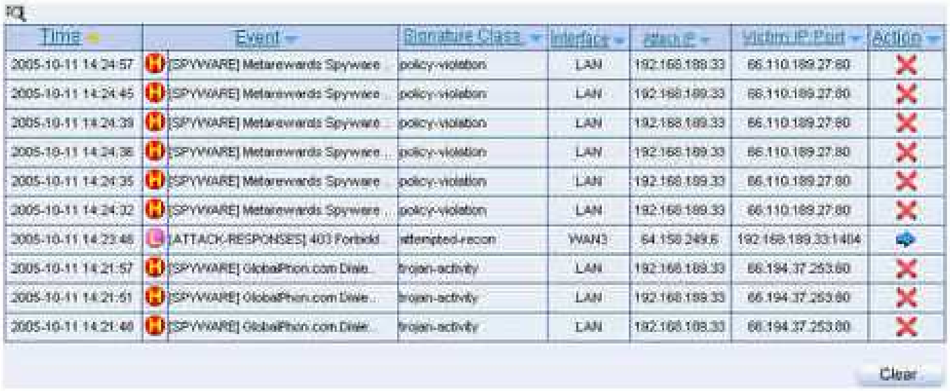
Time: 2005-10-11 14:24:45

Source IP: 192.168.189.33

Destination IP: 66.110.189.27

Event: [SPYWARE] Metarewards Spyware Activity

Figure 17-3 Sending the NetBIOS Alert to the IT Administrator



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 14:23:46	L [ATTACK-RESPONSES] 403 Forbidd...	attempted-recon	WAN3	64.158.249.6	192.168.189.33:1404	➡
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 14:21:46	H [SPYWARE] GlobalPhon.com Diale...	trojan-activity	LAN	192.168.189.33	66.194.37.253:80	✗

Figure 17-4 Intrusion Detection and Prevention Log

The IDP logs will only be created when the corresponding action of logs is are enabled under **IDP > Signature > Anomaly | Pre-defined | Custom**

Chapter 18

Signature Setting

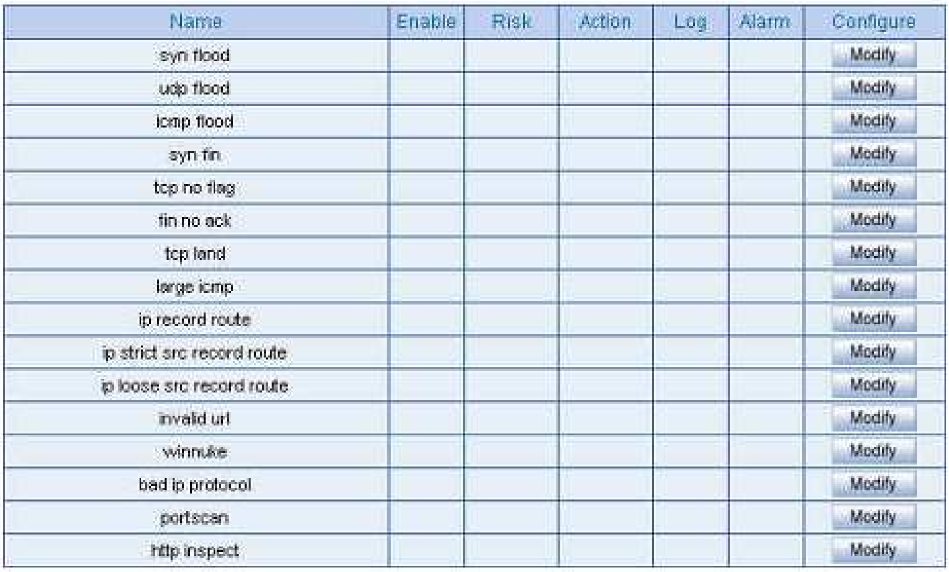
For different attacks, the device provides different solutions, which includes **Anomaly**, **Pre-defined** and **Custom**.

Anomaly will detect and defend against any abnormal packets or anomaly flow using the most up-to-date signature file. **Pre-defined** also detects and defends against anomaly flows using its up-to-date signature file. The signature file cannot be modified or deleted. **Custom** can be designed by the IT administrators according to their needs. **Custom** can detect and defend against the anomaly flow and packets that **Anomaly** and **Pre-defined** were unable to.

【Signature Setting】 terminology:

Anomaly:

- Anomaly can be divided into syn flood, udp flood icmp flood, syn fin, tcp no flag, fin no ack, tcp land, larg icmp, ip record route, ip strict arc record route, ip loose src record route invalid url, winnuke, bad ip protocol, portscan, http inspect and so on. ***(Figure 18-1)***
- According to the IT administrator's needs, specific anomaly flow detecting can be enabled.
- Controls the anomaly flow that is caused by specific packets.
- The action of every signature can be set to pass, block, log or alert.
- Shows the name and risk of a suspected event (anomalous network traffic or activity) as well as the corresponding action (log, alert, pass or drop). It also indicates the protection status (enabled ones are identified with a "check" mark).

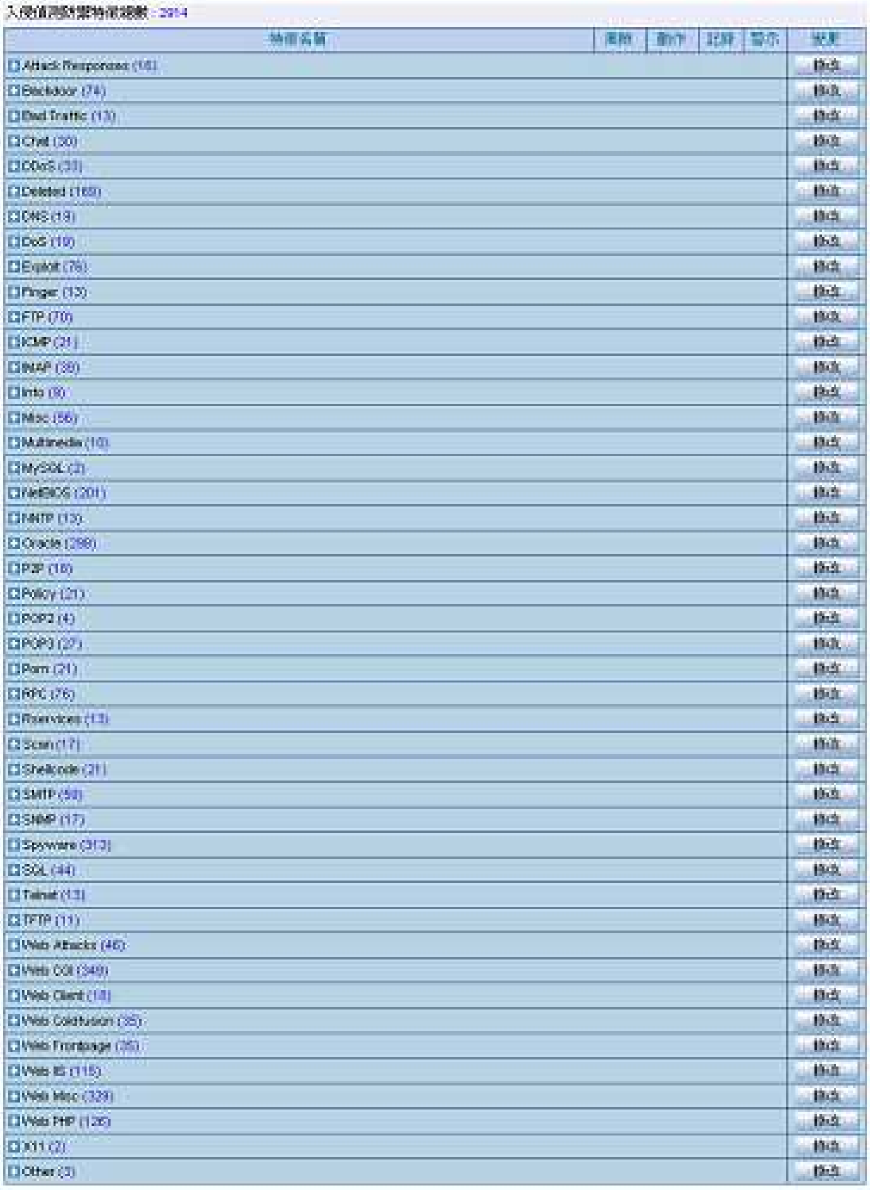


Name	Enable	Risk	Action	Log	Alarm	Configure
syn flood						Modify
udp flood						Modify
icmp flood						Modify
syn fin						Modify
tcp no flag						Modify
fin no ack						Modify
tcp land						Modify
large icmp						Modify
ip record route						Modify
ip strict src record route						Modify
ip loose src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

Figure 18-1 Anomaly Setting Screen

Pre-defined:

- Pre-defined are Attack Responses, Backdoor, Bad Traffic, Chat, DDoS, Delected, 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. Each item contains its signatures. ***(Figure 18-2)***
- Attributes belonging to each specific signature can be changed, such as action, pass, block, log and alert.
- Shows the name and risk of a suspected event (anomalous network traffic or activity) as well as the corresponding action (log, alert, pass or drop). It also indicates the protection status (enabled ones are identified with a “check” mark).



入侵偵測攻擊特徵總數：2914

特徵名稱	開啟	動作	記錄	警示	變更
□ Attack Responses (16)					修改
□ Backdoor (74)					修改
□ Bad Traffic (13)					修改
□ Chat (30)					修改
□ DDoS (33)					修改
□ Deleted (160)					修改
□ DNS (19)					修改
□ DoS (19)					修改
□ Exploit (76)					修改
□ Finger (13)					修改
□ FTP (70)					修改
□ ICMP (21)					修改
□ IMAP (38)					修改
□ Info (8)					修改
□ Misc (56)					修改
□ Multimedia (10)					修改
□ MySQL (2)					修改
□ NetBIOS (201)					修改
□ NNTP (13)					修改
□ Oracle (298)					修改
□ P2P (16)					修改
□ Policy (21)					修改
□ POP2 (4)					修改
□ POP3 (27)					修改
□ Porn (21)					修改
□ RPC (76)					修改
□ Rservices (13)					修改
□ Scan (17)					修改
□ Shellcode (21)					修改
□ SMTP (50)					修改
□ SNMP (17)					修改
□ Spyware (313)					修改
□ SQL (44)					修改
□ Telnet (13)					修改
□ TFTP (11)					修改
□ Web Attacks (46)					修改
□ Web CGI (349)					修改
□ Web Client (18)					修改
□ Web Coldfusion (35)					修改
□ Web Frontpage (35)					修改
□ Web IIS (115)					修改
□ Web Misc (329)					修改
□ Web PHP (126)					修改
□ X11 (2)					修改
□ Other (3)					修改

Figure 18-2 Pre-defined Setting Screen

In the settings of **configure**, any setting related to **pre-defined** would take action against any threats. According to the requirements of the IT administrator, the action that the signature adapts to each attack can be configured.

Name:

- For the IT administrator to name the signatures.

Protocol:

- For setting the required detection and protection, there are TCP, UDP, ICMP and IP.

Source Port:

- The port of the computer that sent the attacks. (range 0~65535)

Destination Port:

- The port of the computer that is being attacked. (range 0~65535)

Risk:

- Define the risk level of the packets.

Action:

- The applied action on the packets.

Content:

- Setting the content of the packets.

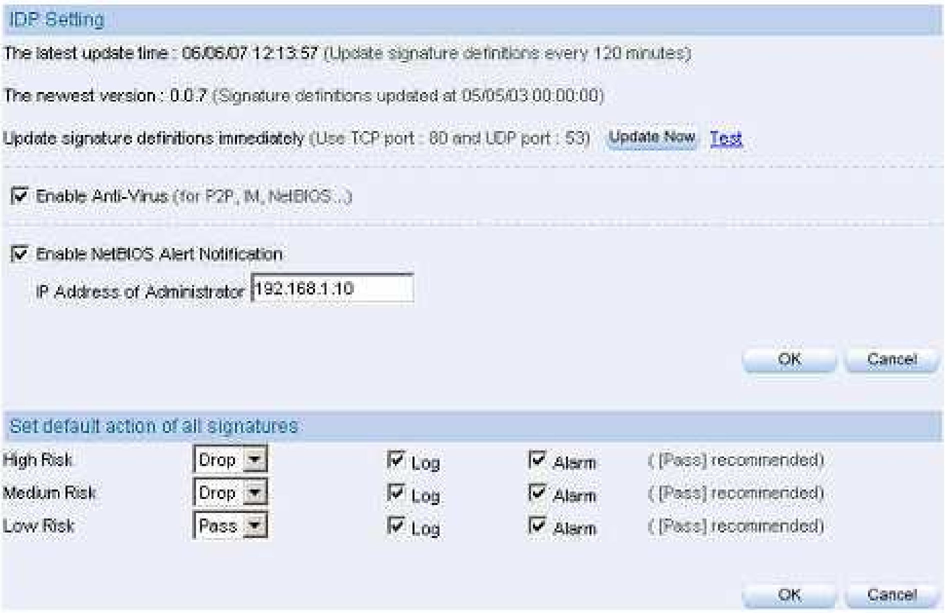
Advanced option:

- **Non-direction:** Filter the packages according to their direction i.e. Inbound or Outbound.
- **Disregard text case:** Determines if the device is case sensitive to the packet contents.

Signature Example

To Detect Anomaly Flows and Abnormal Packets, Using the Pre-defined and Custom Settings for Detecting and Defending against the Attack

Step 1. Click **Configure** > Setting, add the following settings: ***(Figure 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

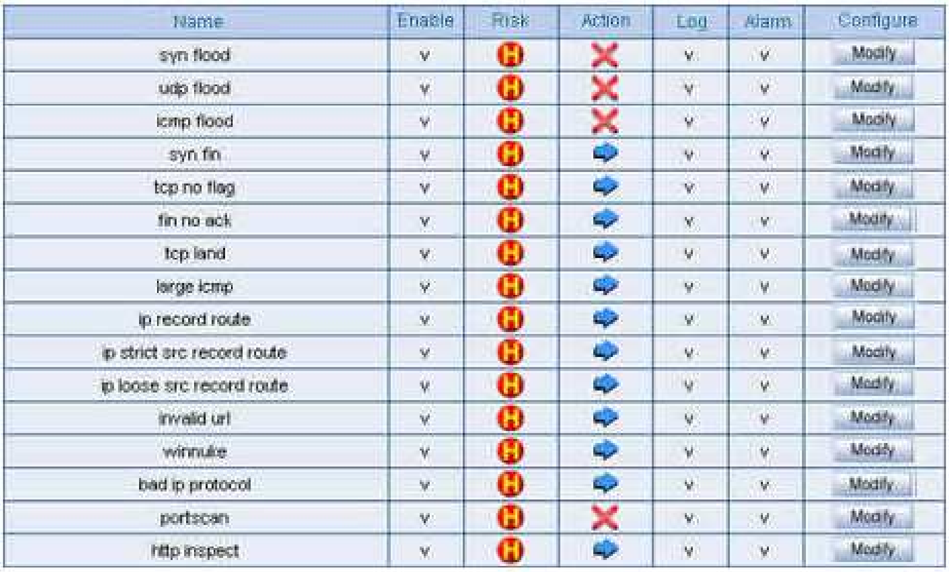
High Risk	Drop	☑ Log	☑ Alarm	([Pass] recommended)
Medium Risk	Drop	☑ Log	☑ Alarm	([Pass] recommended)
Low Risk	Pass	☑ Log	☑ Alarm	([Pass] recommended)

OK Cancel

Figure 18-3 Intrusion Detection and Prevention Setting Screen

Signature Example

Step 2. Click **IDP** > **Signature** > **Anomaly** and add the following settings ***(Figure 18-4)***



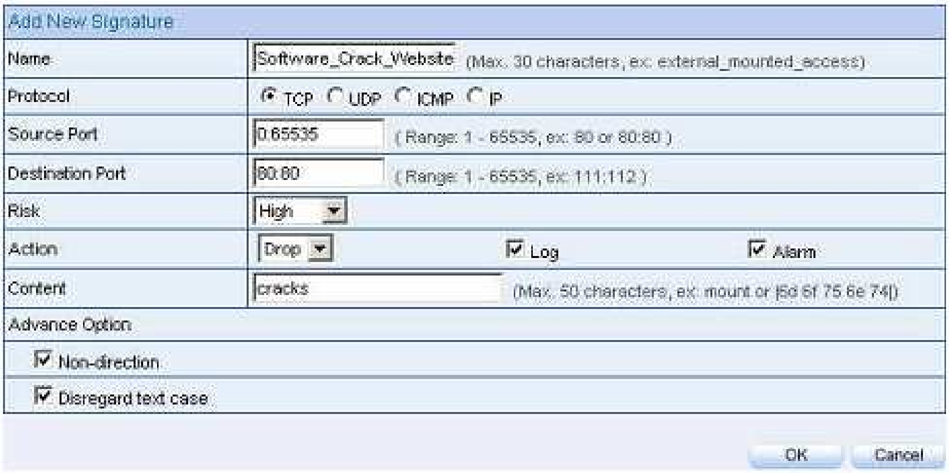
Name	Enable	Risk	Action	Log	Alarm	Configure
syn flood	v	H	✕	v	v	Modify
udp flood	v	H	✕	v	v	Modify
icmp flood	v	H	✕	v	v	Modify
syn fin	v	H	➡	v	v	Modify
tcp no flag	v	H	➡	v	v	Modify
fin no ack	v	H	➡	v	v	Modify
tcp land	v	H	➡	v	v	Modify
large icmp	v	H	➡	v	v	Modify
ip record route	v	H	➡	v	v	Modify
ip strict 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

Figure 18-4 Anomaly Setting

Signature Example

Step 3. Click IDP > Signature > Custom, Click New Entry. ***(Figure 18-5)***

- Enter Software_Crack_Website in the **Name** field.
- Tick **TCP** in the **Protocol** selection.
- Enter 0:65535 in the **Source Port** field.
  Enter 80:80 in the **Destination Port** field.
- From the **Risk** drop-down list select **High**
- Enter cracks in the **Content** field
- Tick the **Non-direction** and **Disregard text case** checkbox in the **Advance Option** selection. ***(Figure 18-6)***



Add New Signature

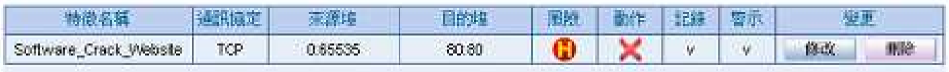
Name	Software_Crack_Website (Max. 30 characters, ex: external_mounted_access)
Protocol	● TCP ○ UDP ○ ICMP ○ IP
Source Port	0:65535 (Range: 1 - 65535, ex: 80 or 80:80)
Destination Port	80:80 (Range: 1 - 65535, ex: 111:112)
Risk	High
Action	Drop ☑ Log ☑ Alarm
Content	cracks (Max. 50 characters, ex: mount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

Advance Option

☑ Non-direction

☑ Disregard text case

Figure 18-5 Custom Setting Screen



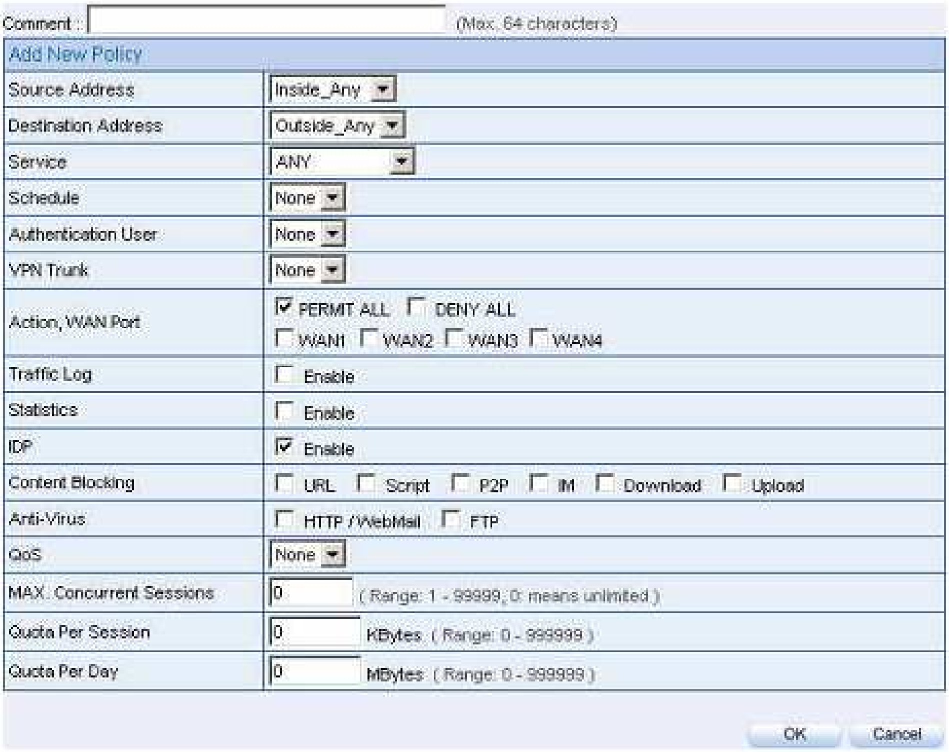
特徵名稱	通訊協定	來源埠	目的埠	風險	動作	記錄	警示	變更
Software_Crack_Website	TCP	0:65535	80:80	H	✗	v	v	修改 刪除

Figure 18-6 Custom Setting Complete

Complete the **Content** field with plaintext (a desired word string) or a corresponding hexadecimal ASCII code. For example, “cracks” is represented by |63 72 61 63 6b 73| in the hexadecimal system.

Signature Example

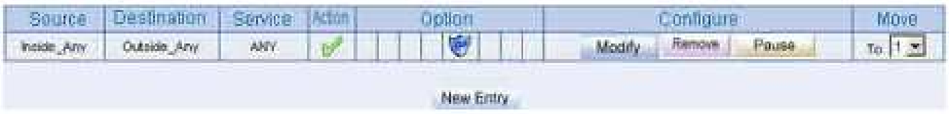
Step 4. Click **Policy** > **Outgoing**, and Click **OK** *(Figure 18-7, Figure 18-8)*



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)

Figure 18-7 Intrusion Detection and Prevention Setting



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

Figure 18-8 Intrusion Detection and Prevention Settings Complete

Chapter 19

Intrusion and Prevention Reports

NUS-MS3000 organizes the logs of Intrusion Detection and Prevention into daily records, providing enterprises with an easier way to know the network security.

Intrusion and Prevention Reports is introduced in detail in this section:

【Setting】terminology:

Periodic Report:

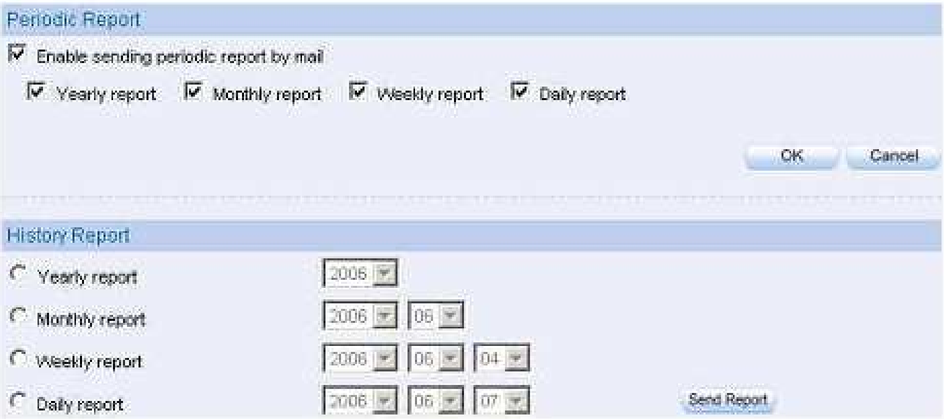
- Can produce and send the reports to the IT administrator according to the nominated time.

History Report:

- Can create reports on a specified date and can then e-mail it to the IT administrator.
    - Click **System** > **Configure** > **Setting**, Check the **Enable E-mail Alert Notification** checkbox. Add the following settings in the IDP report.
        1. To enable **Periodic Report** function, click **IDP** > **IDP Report** > **Setting**, and check the **Yearly Report**, **Monthly Report**, **Weekly Report** and **Daily Report** checkbox.
        2. Click **OK**.***(Figure 19-1)***
        3. The NUS-MS3000 sends the statistic report to the IT administrator at the specific time. ***(Figure 19-2, Figure 19-3)***
        4. For setting the **History Report**, click **IDP** > **IDP Report** > **Setting**, enter the date that you want to receive the reports ***(Figure 19-4)***
        5. Click **Send Report**.
        6. The device will send the reports to the IT administrator instantly. ***(Figure 19-5, Figure 19-6)***

Periodic Report:

1. Yearly Report: Creates the report at 00.00 hours on January 1st.
2. Monthly Report: Creates the report at 00.00 hours on the first day of the month.
3. Weekly Report: Creates the report at 00.00 hours on the first day of the week.
4. Daily Report: Creates the report at 00.00 hours everyday.



Periodic Report

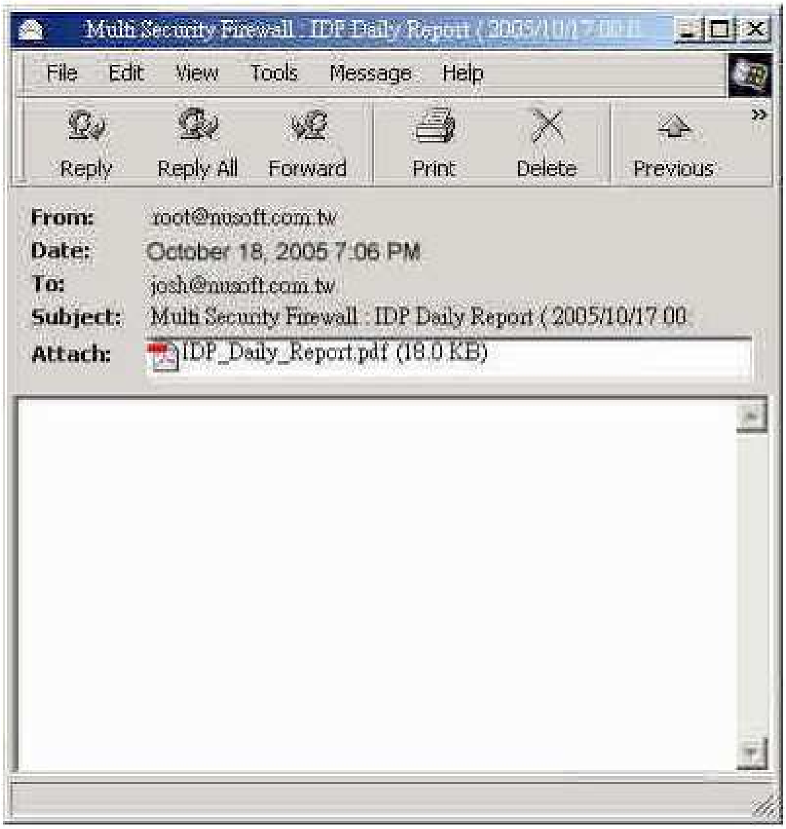
☑ Enable sending periodic report by mail

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

History Report

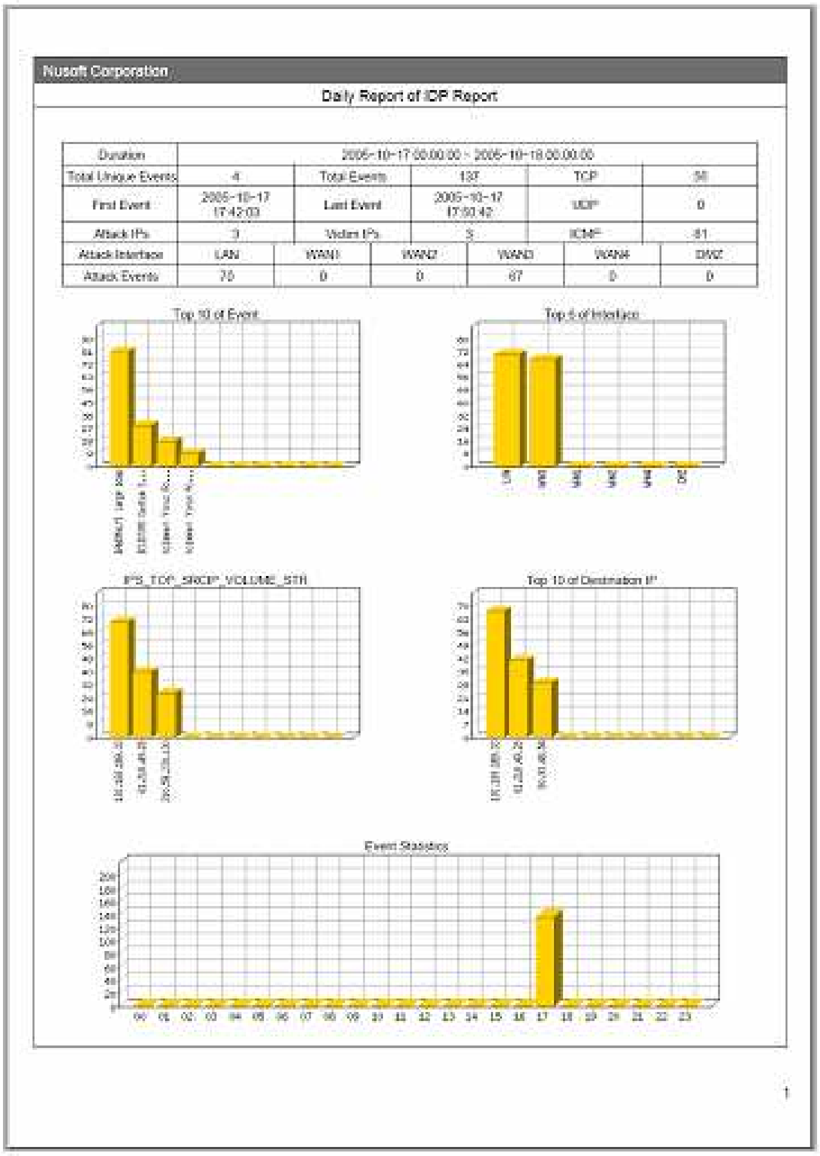
○ Yearly report	2006		
○ Monthly report	2006	06	
○ Weekly report	2006	06	04
○ Daily report	2006	06	07

Figure 19-1 Periodic Report Setting Screen



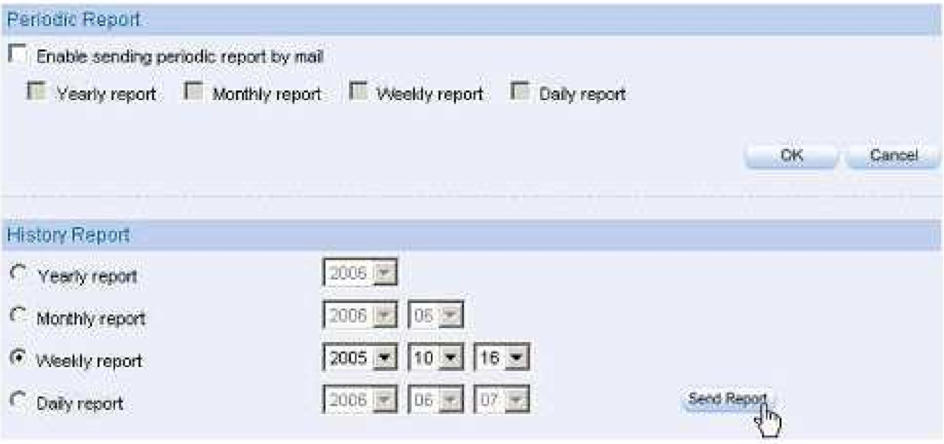
From: root@nusoft.com.tw
Date: October 18, 2005 7:06 PM
To: josh@nusoft.com.tw
Subject: Multi Security Firewall : IDP Daily Report (2005/10/17 00
Attach: IDP_Daily_Report.pdf (18.0 KB)

Figure 19-2 Receiving the Periodic Report Mail



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

Figure 19-3 The content of Intrusion Detection and Prevention



Periodic Report

☐ Enable sending periodic report by mail

☐ Yearly report ☐ Monthly report ☐ Weekly report ☐ Daily report

History Report

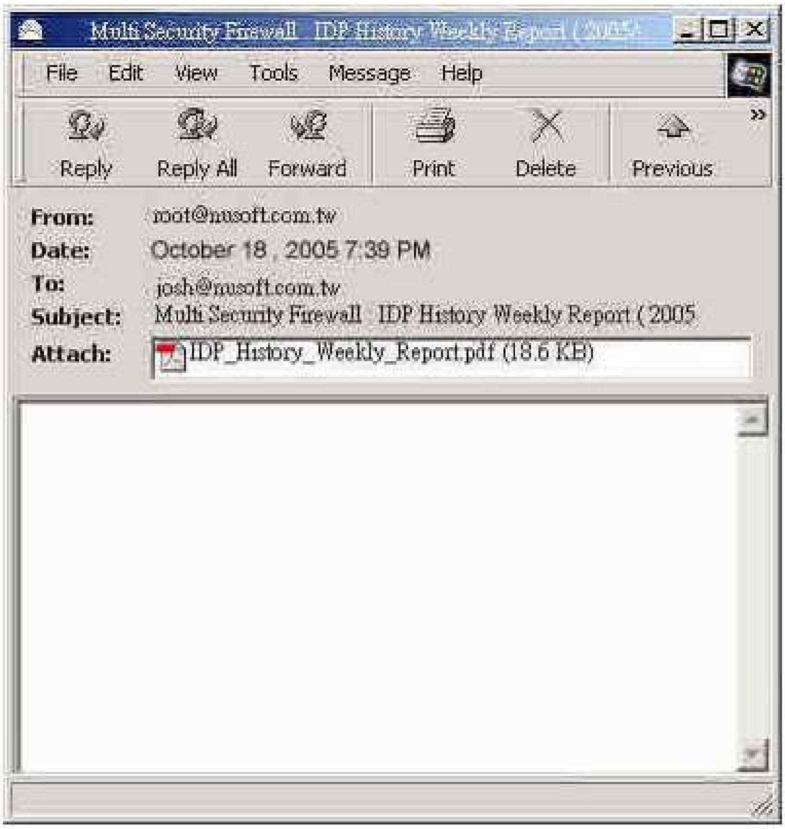
○ Yearly report 2006

○ Monthly report 2006 06

● Weekly report 2005 10 16

○ Daily report 2006 06 07

Figure 19-4 History Report Setting Screen



Multi Security Firewall IDP History Weekly Report (2005

From: root@nusoft.com.tw

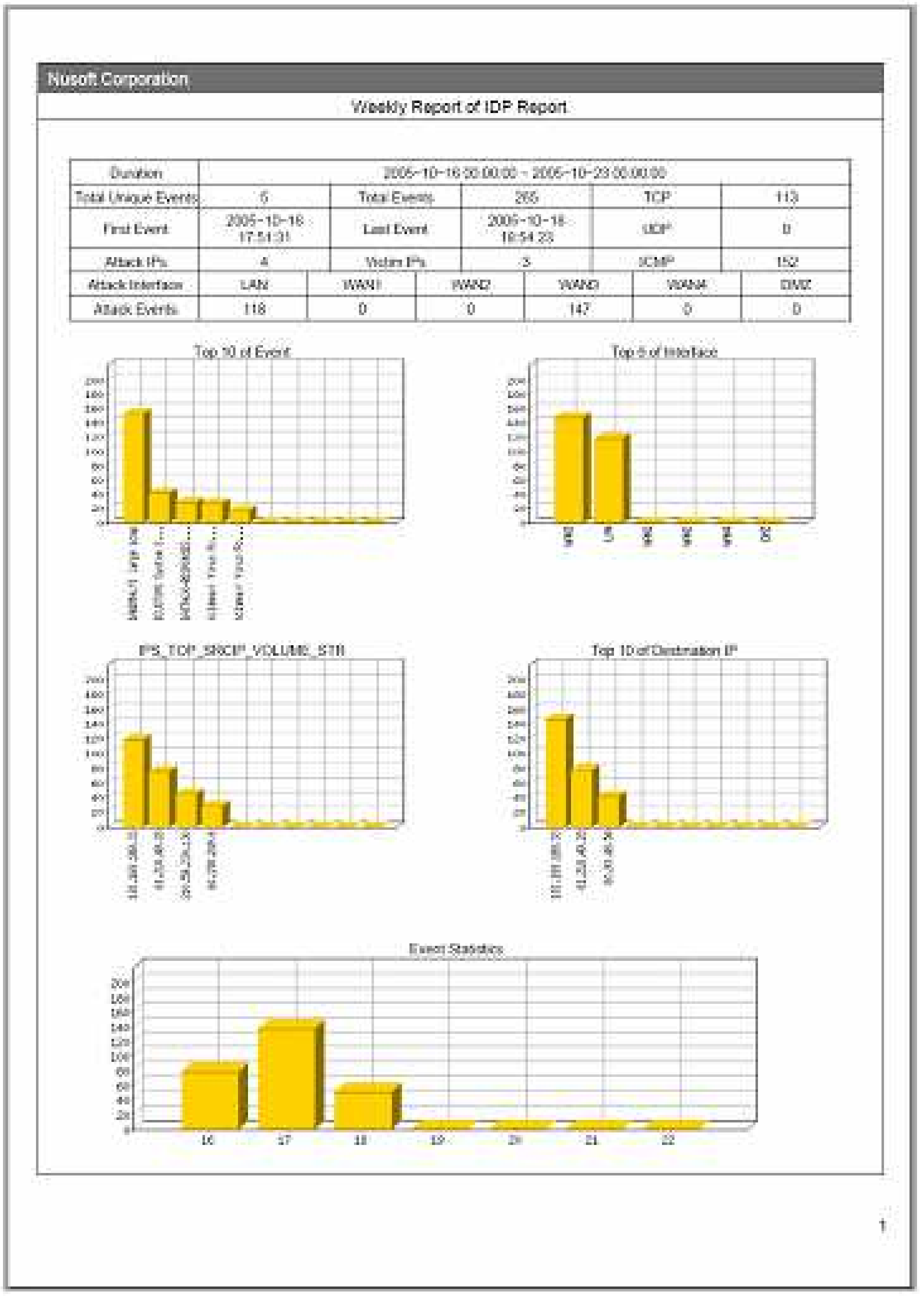
Date: October 18 , 2005 7:39 PM

To: josh@nusoft.com.tw

Subject: Multi Security Firewall IDP History Weekly Report (2005

Attach: IDP_History_Weekly_Report.pdf (18.6 KB)

Figure 19-5 Receiving the History Report E-mail



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

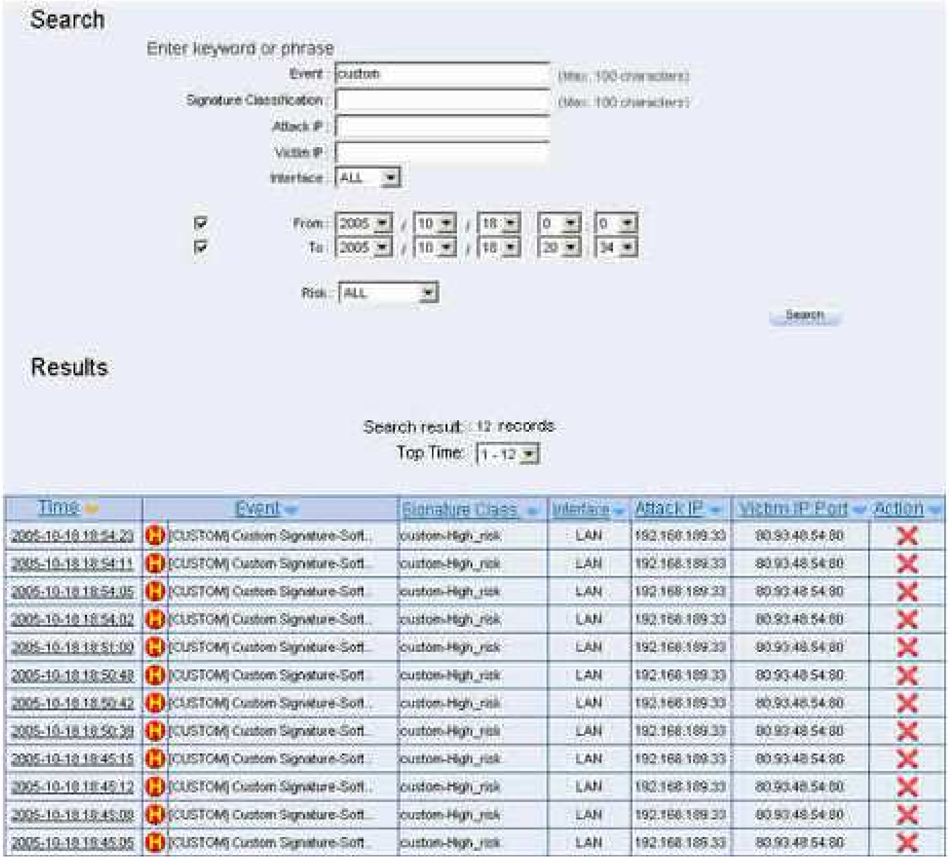
Figure 19-6 History Report of Intrusion Detection and Prevention

Intrusion Prevention report would be sent as a PDF attachment to the IT administrator.

【Daily Report】Terminology:

Search:

- The IT administrator can search the records in the NUS-MS3000 device according to keywords or the abnormal packets, signature, source IP addresses, destination IP addresses, interface, date, danger and so on.
  - Adding the following setting:
    1. Enter the keywords related to the abnormal packets or attacks in the **Event** field.
    2. From the **Interface** drop-down list, choose **ALL**.
    3. Enable and set the time interval to search for records.
    4. From the **Risk** drop-down list, choose **ALL**.
    5. Click **Search**. ***(Figure 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

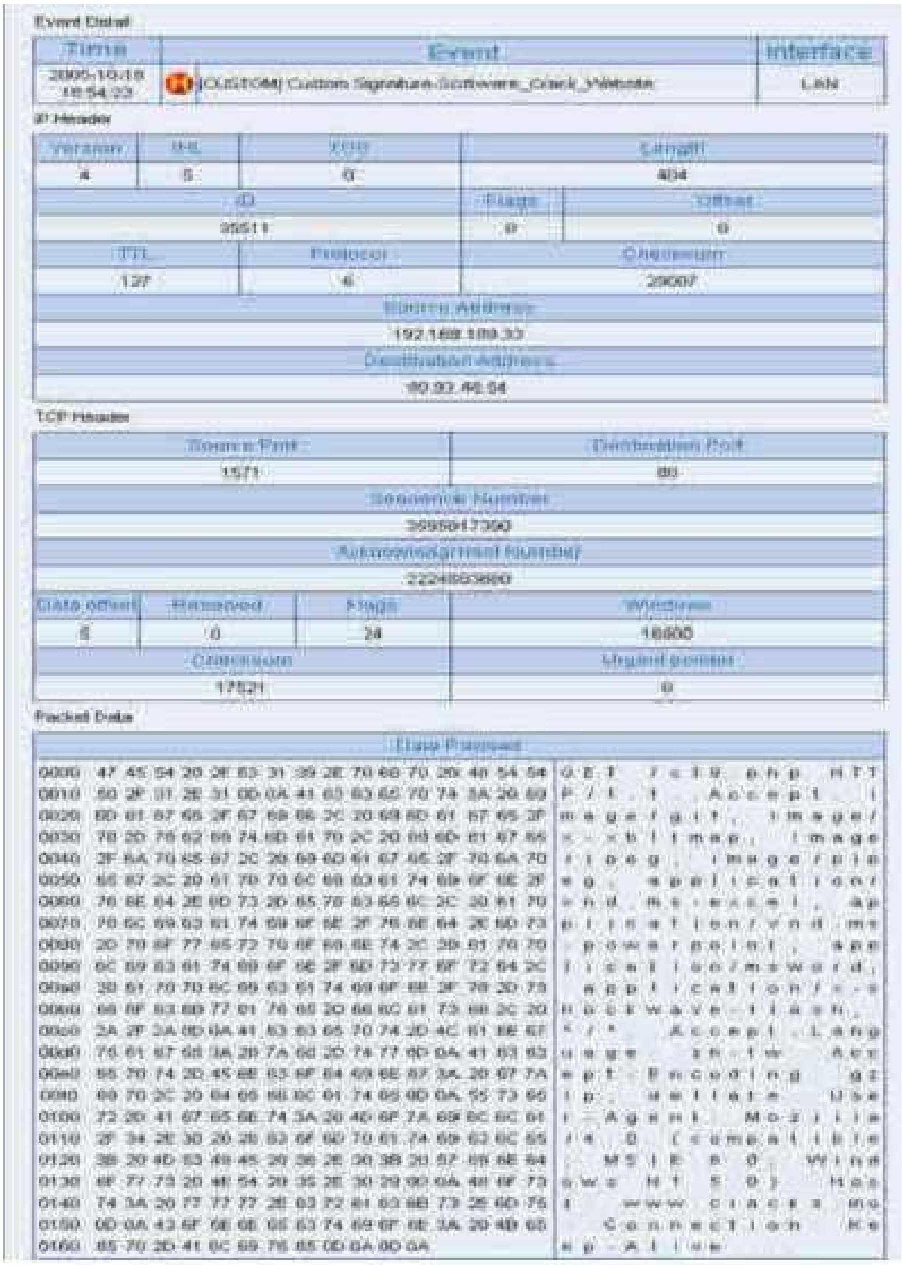
Search result : 12 records

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 18:50:38	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	✗

Figure 19-7 Searching Specific Records Screen

In the **Daily Report**, click **Time** to show the **Event Detail** report. ***(Figure 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
80.93.46.54

TCP Header

Source Port	Destination Port
1571	80

Sequence Number
3695917390

Acknowledgment Number
2224663880

Data offset	Reserved	Flags	Window
5	0	24	16600

Checksum	Urgent pointer
17521	0

Packet Data

Copy Payload

```
0000  47 45 54 20 2F 63 31 39 2E 70 68 70 20 48 54 54   G E T   / c 1 9 . p h p   H T T
0010  50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 69   P / 1 . 1     A c c e p t :   i
0020  6D 61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65 2F   m a g e / g i f ,   i m a g e /
0030  78 2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67 65   x - x b i t m a p ,   i m a g e
0040  2F 6A 70 65 67 2C 20 69 6D 61 67 65 2F 70 6A 70   / j p e g ,   i m a g e / p j p
0050  65 67 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F   e g ,   a p p l i c a t i o n /
0060  76 6E 64 2E 6D 73 2D 65 78 63 65 6C 2C 20 61 70   v n d . m s - e x c e l ,   a p
0070  70 6C 69 63 61 74 69 6F 6E 2F 76 6E 64 2E 6D 73   p l i c a t i o n / v n d . m s
0080  2D 70 6F 77 65 72 70 6F 69 6E 74 2C 20 61 70 70   - p o w e r p o i n t ,   a p p
0090  6C 69 63 61 74 69 6F 6E 2F 6D 73 77 6F 72 64 2C   l i c a t i o n / m s w o r d ,
00a0  20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 73     a p p l i c a t i o n / x - s
00b0  68 6F 63 6B 77 61 76 65 2D 66 6C 61 73 68 2C 20   h o c k w a v e - f l a s h ,
00c0  2A 2F 2A 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67   * / *     A c c e p t - L a n g
00d0  75 61 67 65 3A 20 7A 68 2D 74 77 0D 0A 41 63 63   u a g e :   z h - t w     A c c
00e0  65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A   e p t - E n c o d i n g :   g z
00f0  69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 55 73 65   i p ,   d e f l a t e     U s e
0100  72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61   r - A g e n t :   M o z i l l a
0110  2F 34 2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65   / 4 . 0   ( c o m p a t i b l e
0120  3B 20 4D 53 49 45 20 36 2E 30 3B 20 57 69 6E 64   ;   M S I E   6 . 0 ;   W i n d
0130  6F 77 73 20 4E 54 20 35 2E 30 29 0D 0A 48 6F 73   o w s   N T   5 . 0 )     H o s
0140  74 3A 20 77 77 77 2E 63 72 61 63 6B 73 2E 6D 75   t :   w w w . c r a c k s . m u
0150  0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65       C o n n e c t i o n :   K e
0160  65 70 2D 41 6C 69 76 65 0D 0A 0D 0A               e p - A l i v e
```

Figure 19-8 Event Detail Report

The order of Daily Report can be listed by the time, event, signature class, interface, attack IP address, victim IP address, victim IP port and action.

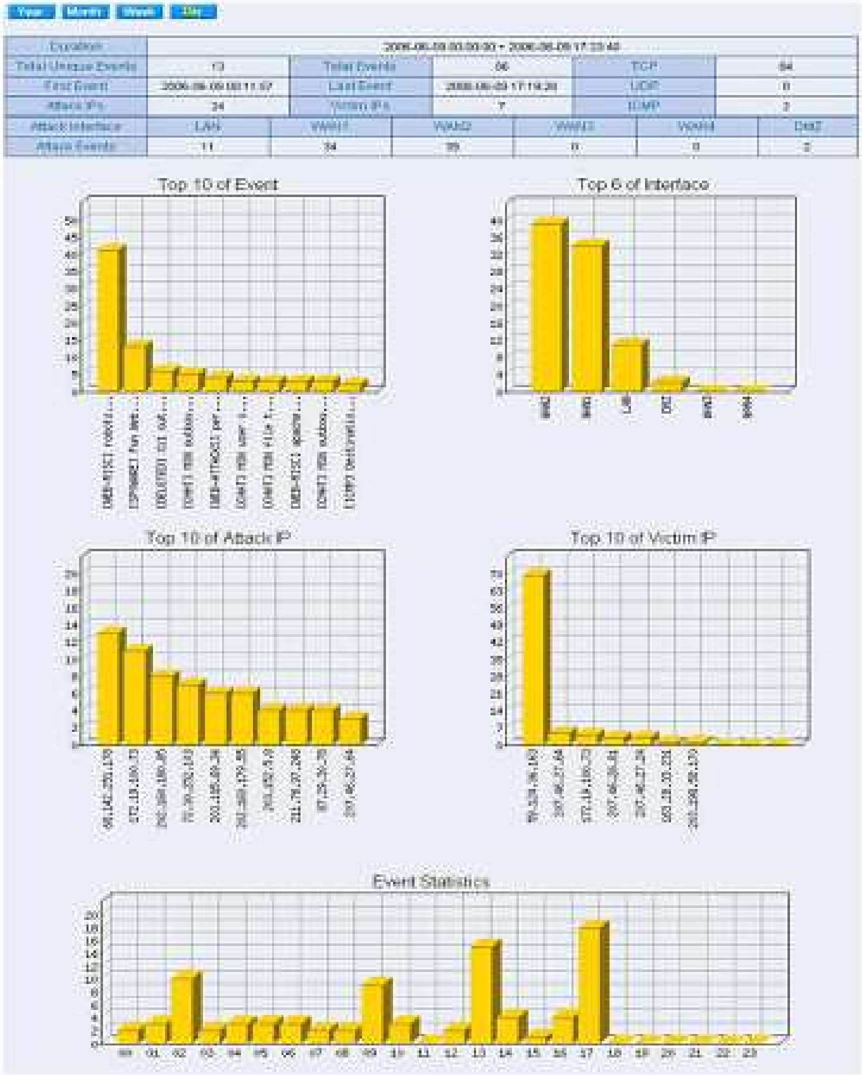
IDP Report Statistics

Step 1. To see the Intrusion Detection and Prevention report, click **ICP** > **IDP Report** > **Statistics**.

Step 2. There are **Year**, **Month**, **Week** and **Day** on the upper left corner. Click **Day** to see the Daily report, click **Week** to see the Weekly report, click **Month** to see the Monthly report, click **Year** to see the Yearly report.

Step 3. Intrusion Detection and Prevention report ***(Figure 19-9)***

- **Y-axis** indicates the amount of abnormal packets and signature of identified attacks.
- **X-axis** indicates the 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 17:19:20	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

Figure 19-9 Mail Scanning Statistical Charts

IDP Report Statistics

Step 1. To see the handling status of Intrusion Detection and Prevention, click **IDP** > **IDP Reports** > **Log**. *(Figure 19-10)*

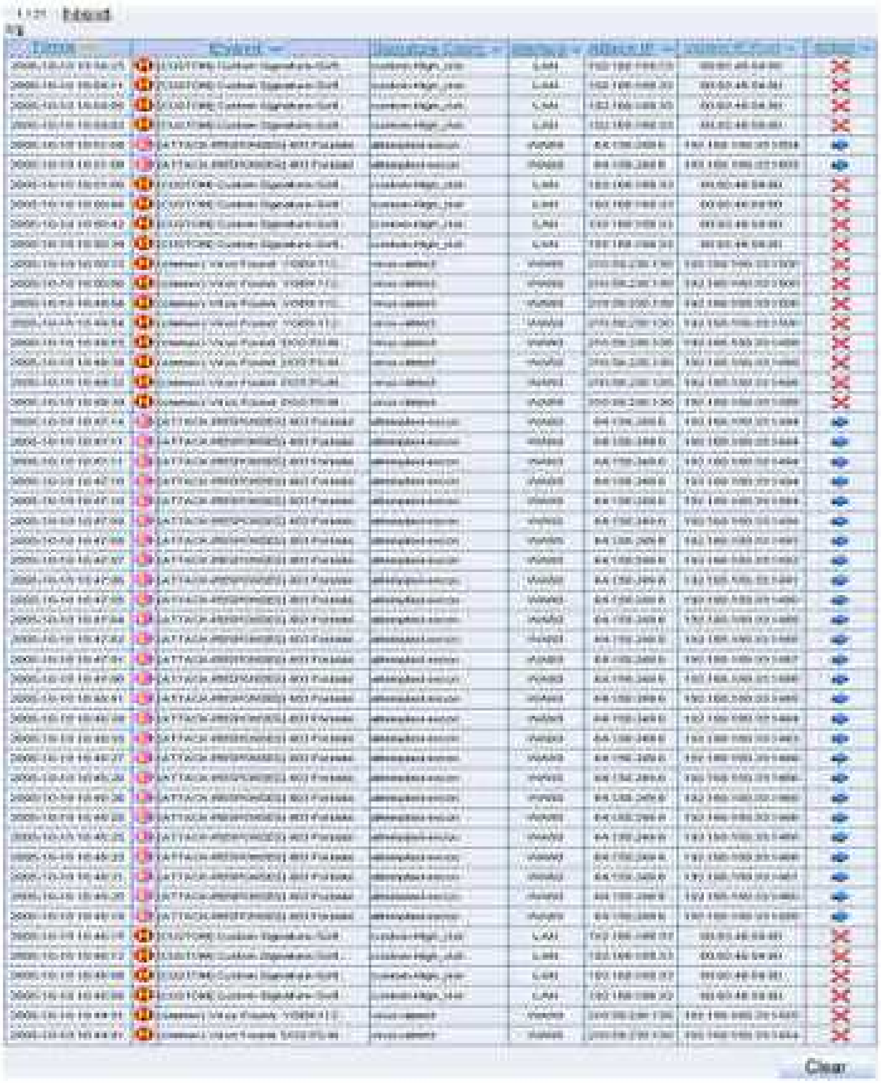
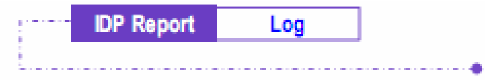


Figure 19-10 Intrusion Detection and Prevention Daily Records

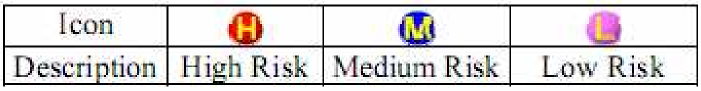


The symbols refer to:

1.【Action】:

Symbol	➡	✖
Description	Pass	Drop

2.【Risk】:



Icon	H	M	L
Description	High Risk	Medium Risk	Low Risk