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 \rightarrow Configure \rightarrow 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 ti	me : 06/06/07 10:11:06	(Update signature de	finitions every 120) minutes)	
The newest versio	n : 0.0.7 (Signature defi	nitions updated at 06	/02/23 21:27:41)		
Update signature d	efinitions immediately (L	lse TCP port : 80 and	UDP port : 53)	pdate Now Test	
Enable Anti-Vir	rus (for P2P, IM, NetBIO	S)			
Finable NetBIO	S Alert Notification				
IP Address of	Administrator 192.168.	1.10			
				OK	Cancel
				- OK	Guilder
Set default actio	n of all signatures				
High Risk	Drop 💌	✓ Log	🔽 Alarm	([Pass] recommended	0
Medium Risk	Drop 💌	🔽 Log	🔽 Alarm	([Pass] recommended	Ð.
Low Risk	Pass 💌	I Log	🔽 Alarm	([Pass] recommended	i)
				ок	Cancel

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** \rightarrow **IDP Report**. (*Fig. 17-2, Fig. 17-3, Fig. 17-4*)

le Edit View Tools Mr	ssage Help		
21 21 12		◆ 団	
Reply Reply All Forward	Print Delete Previous	Next Addresses	
im: root			
te: October 11.2005 10	25 PM		
josn@nusoft.com.t	N Taireal		
iprayatem Event P	larini		
Time Instand	Out 10 Part 12	Enint	
5-10-11 14:24:32 TCF 192	168,189,33 66,110,189,27 [SPYWAR	Metazewards Spyware Activity	
5-10-11 14:24:35 TCF 192	168.189.33 66.110.189.27 [SPYWARE	Metarewards Spyware Activity	
5-10-11 14:24:56 TCP 192	168.189.33 66.110.189.27 [SPYWARE	Metazewarda Spyware Activity	
5-10-11 14:24:45 TCF 192	168,189,33 66,110,189,27 [SFYWART	Metalewards Spyware Activity Metalewards Spyware Activity	
5-10-11 14:24:57 TCF 192	168,189,33 66,110,189,27 [SPYWARF	Metazewards Spyware Activity	
5-10-11 14:23:48 TCF 64	158.249.6 192.168.189.33 [ATTACK-	ESPONSES] 403 Forbidden	
05-10-11 14:21:56 TCF 192	168,189,33,66,194,37,253, [SPTWARE	GlobalPhon.com Dialer	
5-10-11 14:21:57 TCF 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 Service	×
Messenger from IDPsystem to MANUAL8 on 10/11/2005 0	2:25:57PM
Waming!!	
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	
OK	
OK	

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

<u>Time</u>		Event -	Signature Class	Interface -	Bttank IE -	Victim IP Part -	Action
2005-10-11 14:24:57	C	[SPYWARE] Metarewards Spyware	policy-violation	LAN	192.168.189.33	66,110,189,27:80	×
2005-10-11 14:24:45	0	(SPYWARE) Metarewards Spyware .	policy-violation	LAN	192.168.189.33	66.110.189.27:80	×
2005-10-11 14:24:39	0	SPYWARE] Metarewards Spyware	policy-violation	LAN	192.168 189.33	66.110.189.27:60	×
2005-10-11 14:24:36	0	SPYWARE] Metarewards Spyware	policy-violation	LAN	192.168.189.33	66.110.189.27.80	×
2005-10-11 14:24:35	0	SPYWARE] Metarewards Spyware	policy-violation	LAN	192.168 189.33	66.110.189.27:60	×
2805-10-11 14:24:32	0	SPYWARE] Metarewards Spyware .	policy-violation	LAN.	192.168.189.33	66.110.189.27.80	X
2005-10-11 14:23:48	0	(ATTACK-RESPONSES) 483 Forbidd	attempted-recon	WANE	64 158 249.6	192 168 189 33 1484	-
2005-10-11 14:21:57	Ø	(SPYVVARE) GlobalPhon.com Diale	trojan-activity	LAN	192 168 189 33	66.194.37.253.60	×
2005-10-11 14:21:51	0	[SPYVVARE] GlobaPhon.com Diale.	trojan-activity	LAN	192 168 189 33	66.194.37.253.80	×
2005-10-11 14:21:48	0	[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.

<u>Signature</u>

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
tep no flag						Modify
fin no ack						Modify
tcp land						Modify
large icmp)			Modify
ip record route						Modify
ip strict src record route			0			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.

Name Risk Attor Log Math Configure 2 Back Responses (6). Modify Modify Modify 2 Back Traffe (13) Modify Modify Modify 2 Dock (13) Modify Modify Modify 2 Dock (169) Modify Modify Modify 2 Dock (16) Modify Modify Modify 2 Dock (16) Modify Modify Modify 2 Modify (2) Modify Modify Modify 2 Modify (3) Modify Modify Modify 2 Port (16) Modify Modify Modify 2 Pord (6) Modify	Total IDP Signatures Number : 2916					
Cathles Responses (16).MediayDelection (75)MediayCathle (13)MediayCathle (13)MediayDobles (13)MediayDobles (169)MediayDobles (169)MediayCathle (169)MediayCathle (169)MediayCathle (169)MediayCathle (169)MediayCathle (169)MediayCathle (160)MediayCathle (160)MediayCathle (161)MediayCathle (162)MediayCathle (163)MediayCathle (163)MediayCathle (163)MediayCathle (163)MediayCathle (163)MediayCathle (163)MediayCathle (163)MediayCathle (163)Mediay <trr>Cathle (163)Mediay<t< th=""><th>Name</th><th>Risk</th><th>Action</th><th>Log</th><th>Alarm</th><th>Configure</th></t<></trr>	Name	Risk	Action	Log	Alarm	Configure
Binktor (75)MediaBinktraffs (3)MediaDobat (31)MediaDobat (32)MediaDobat (35)MediaDobat (36)MediaDobat (36)MediaDobat (36)MediaDobat (36)MediaDobat (36)MediaDobat (36)MediaDobat (36)MediaDobat (37)MediaDobat (3	Attack Responses (16)					Modify
Bat ratic (13)ModiyChat (31)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (31)ModiyChot (31)ModiyChot (31)ModiyChot (31)ModiyChot (31)ModiyChot (31)ModiyChot (31)ModiyChot (31)ModiyChot (31)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (32)ModiyChot (33)ModiyChot (34)ModiyChot (35)ModiyChot (35)ModiyChot (35)ModiyChot (35)ModiyChot (35)ModiyChot (35) <t< td=""><td>Backdoor (75)</td><td></td><td></td><td></td><td></td><td>Modify</td></t<>	Backdoor (75)					Modify
CharlMediaCDDS3 (33)MediaCDDS3 (33)MediaCDDS3 (18)MediaCDS3 (19)MediaCDS3 (19)MediaCEpplot (76)MediaCEpplot (76)MediaCEPP (70)MediaCDMP (21)MediaCMMP (30)MediaCMMS (30)MediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMediaPropicitificMedia <td>Bad Traffic (13)</td> <td></td> <td></td> <td></td> <td></td> <td>Modify</td>	Bad Traffic (13)					Modify
CDDS(33)ModilyDbelded(189)ModilyDbS(13)ModilyDbS(16)ModilyDbS(17)ModilyDbS(17)ModilyDbS(17)ModilyDbS(17)ModilyCDDS(17)ModilyDbS(15)ModilyDbS(15)ModilyDbS(15)ModilyDbS(15)ModilyDbS(15)ModilyDbS(15)ModilyDbS(15)ModilyDbS(15)Modily<	Chat (31)					Modify
Deleted (169)ModifyDNS (19)ModifyDSG (19)ModifyExplot (76)ModifyExplot (76)ModifyPTP (70)ModifyDNS (19)ModifyDNS (20)ModifyDNS (56)ModifyMultinois (10)ModifyModify (21)ModifyModify (21)ModifyMultinois (10)ModifyDNS (56)ModifyModify (21)ModifyDNS (22)ModifyOracle (280)ModifyDNS (13)ModifyDNS (13)ModifyDPOP2 (1)ModifyDPOP2 (1)ModifyDPOP2 (1)ModifyDPOP2 (1)ModifyDPOP3 (77)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifyDYME (13)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifySoan (17)ModifyDYME (13)ModifyDYME (13)ModifyDYME (13)ModifyUMB Aback (16)ModifyUMB	DDoS (33)					Modify
DNS (19)ModifyDDS (19)ModifyDExplat (76)ModifyFTP (70)ModifyCMP (21)ModifyCMP (20)ModifyCMP (20)ModifyCMM (20)ModifyCM (20)<	Deleted (169)					Modify
Dos(%)MontyC Explot (76)MontyC Finger (13)MontyC Finger (13)MontyC MAP (21)MontyC MAP (30)MontyC Mont (30)MontyC Matter (30)MontyC Pope (37)MontyC Pope (37)MontyC Pope (37)MontyC Pope (30)MontyC Soan (17)MontyC Shart (33)MontyC Shart (33)MontyC Shart (33)MontyC Shart (34)MontyC Shart (35)MontyC Shart (35)MontyC Shart (35)MontyC Monty (35)MontyC Mon	DNS (19)					Modify
Ekpatr(%)ModingEkpatr(%)ModingFIP (70)ModingCMAP (3)ModingInfor (9)ModingInfor (5)ModingMutack (6)ModingMutack (6)ModingCMAP (3)ModingMutack (2)ModingCMAP (3)ModingCMAP (3) <td>DoS (19)</td> <td></td> <td></td> <td></td> <td></td> <td>Modify</td>	DoS (19)					Modify
IP reprMedingIP FP (70)MedingIP (71)MedingIP (72)MedingIP (72)Meding	CExplot (76)					Modify
IP F70;ModeDKMP (2)ModeDKMP (3)ModeDinto (3)ModeModeModeDinto (5)ModeMutimedia (10)ModeDinto (50)ModeDinto (50)ModeDinto (28)ModeDinto (28)ModeDinto (29)ModeDinto (29)ModeDinto (29)ModeDinto (20)ModeDinto (20)Mode <td>C Finger (13)</td> <td></td> <td></td> <td></td> <td></td> <td>Modify</td>	C Finger (13)					Modify
CMAP (2)ModityCMAP (3)ModityCMAP (3)Modi	G FTP (70)					Modify
IMAP (39)ModilyIMAP (39)ModilyIMAP (30)ModilyIMAP (30)	CICMP (21)					Modify
Inits (9)ModifyI Mics (56)ModifyMuttinedis (10)ModifyI MySoL (2)ModifyI MySoL (20)ModifyI NHENOS (20)ModifyO Nate (28)ModifyO Pape (18)ModifyP Pape (16)ModifyP Pape (24)ModifyP Pope (24)ModifyP Pope (24)ModifyP Pope (27)ModifyR Bervices (13)ModifySean (17)ModifySean (17)ModifyStaff (75)ModifyStaff (75)ModifyWeb Kock (86)ModifyWeb Kock (76)ModifyWeb Kock (76)Mod	CIMAP (39)					Modify
I Masc (56)ModityC Muthredia (10)ModityC Muthredia (10)ModityC Muthredia (20)ModityC Muthredia (20)ModityC Macle (288)ModityC Macle (288)ModityC Pacle (288)ModityC Pacle (288)ModityC Pacle (289)ModityC Pacle (289)ModityC Pacle (289)ModityC Pacle (289)ModityC Pacle (289)ModityC Pacle (280)ModityC Pacle (281)ModityC Pacle (281)ModityC Pacle (281)ModityC Recruces (13)ModityC Sheltoche (21)ModityC Het (13) <t< td=""><td>Cinto (9)</td><td></td><td></td><td></td><td></td><td>Modify</td></t<>	Cinto (9)					Modify
I Mutimedia (10)MedityCM/SQL (2)MedityCM/SQL (2)MeditySCAN (17)MeditySCAN (17)MeditySCAN (17)MeditySMMP (17)MeditySMMP (17)MeditySMMP (13)MeditySSMMP (13)MedityCM/SQL (2)MedityCM/SQL (2)MedityCM/SQL (2)MeditySMMP (13)MedityCM/SQL (2)MedityCM/SQL (2)	C Misc (56)					Modify
Impsol (2)MedityInvestions (201)MedityInvestions (202)MedityInvestions (202)Me	C Multimedia (10)					Modify
INHEBIOS (201)ModifyINNTP (13)ModifyOracle (288)ModifyOP2P (18)ModifyIPOR2 (21)ModifyIPOR2 (27)ModifyIPOR2 (28)ModifyIPOR2 (28)ModifyIPOR	MySQL (2)					Modify
INNTP (13) Medity Oracle (286) Medity DP2P (18) Medity DPOR2 (21) Medity DPOR2 (21) Medity DPOR2 (21) Medity DPOR2 (27) Medity DPOR3 (27) Medity DPOR3 (27) Medity RPC (76) Medity CRPC (76) Medity State (13) Medity DState (21) Medity State (17) Medity State (17) Medity State (17) Medity State (17) Medity State (21) Medity State (21) Medity State (21) Medity State (17) Medity State (18) Medity State (18) Medity </td <td>C NetBIOS (201)</td> <td></td> <td></td> <td></td> <td></td> <td>Modify</td>	C NetBIOS (201)					Modify
D'oracle (298) Modify D'P2P (16) Modify D'POP2 (16) Modify D'POP2 (21) Modify D'POP2 (27) Modify D'POR2 (27) Modify D'POR2 (27) Modify D'POR2 (27) Modify D'POR (21) Modify C'POR (21) Modify D'POR2 (27) Modify C'POR2 (27) Modify C'Son (17) Modify C'Son (17) Modify C'Son (21) Modify C'Son (21) Modify C'Son (21) Modify C'Son (21) Modify C'Hor (13) Modify C'Hor (25) <td>CINNTP (13)</td> <td></td> <td></td> <td></td> <td></td> <td>Modify</td>	CINNTP (13)					Modify
DP2P(18) Modify DPolicy (21) Modify DPOP2 (4) Modify DPOP3 (27) Modify DStation (21) Modify DStation (23) Modify DVeb Califusion (35) Modify DVeb Califusion (35) Modify DVeb Statis (15) Modify <tr< td=""><td>Q Oracle (298)</td><td></td><td></td><td></td><td></td><td>Modify</td></tr<>	Q Oracle (298)					Modify
Delicy (21) Modify DPOR2 (4) Modify DPOR2 (4) Modify DPOR2 (27) Modify DPorn (21) Modify DRPC (75) Modify C RScrüces (13) Modify D Scan (17) Modify D Scan (17) Modify D Scan (17) Modify D Shellcode (21) Modify D Shell Code (31) Modify D Shell Code (34) Modify D Web Col (34) Modify D Web Col (34) Modify	CIP2P (18)					Modify
DiPOP2 (4) Modify DiPOP3 (27) Modify Displaced (21) Modify Displaced (31) Modify Displaced (34) Modify Diveb Calify (23) Modify Diveb Calify (25) Modify Diveb Frontpage (35) <td>C Policy (21)</td> <td></td> <td></td> <td></td> <td></td> <td>Modify</td>	C Policy (21)					Modify
DPOP3 (27) Modily DPOR (21) Modily DPOR (21) Modily DPOR (21) Modily DPOR (25) Modily DRec (76) Modily DRec (76) Modily DScen (17) Modily DScen (17) Modily DScen (17) Modily DStatiote (21) Modily DSMP (59) Modily DSMP (17) Modily DSMP (17) Modily DSVMP (313) Modily DSQL (44) Modily DSQL (44) Modily DTFTP (11) Modily DVMeb CGl (349) Modily DVMeb CGl (349) Modily DVMeb Claint (18) Modily DVMeb Claint (18) Modily DVMeb Claint (18) Modily DVMeb Claint (18) Modily DVMeb IS (115) Modily DVMeb Misc (329) Modily DVMeb Misc (329) Modily DVMeb Misc (329) Modily	CIPOP2 (4)					Modify
Depen (21) Modify R RPC (76) Modify R Services (13) Modify D Sen (17) Modify D Sen (17) Modify D Sen (17) Modify D Shellcode (21) Modify D Shellcode (33) Modify D SolL (44) Modify D SolL (44) Modify D Web Attacks (45) Modify D Web Calif (18) Modify D Web Calif (18) Modify D Web Calif (18) Modify D Web Calif (15) Modify D Web Calif (15) Modify	CIPOP3 (27)					Modify
DIRPC (76) Modify Rservices (13) Modify Discon (17) Modify Discon (17) Modify Discon (17) Modify Discon (21) Modify Divebs Cient (18) Modify Diveb Dis (115) Mo	C Porn (21)					Modify
Cli Rservices (13) Modify Cl Scan (17) Modify Cl Scan (17) Modify Cl Scan (21) Modify Cl SMIP (58) Modify Cl SMIP (58) Modify SIMMP (17) Modify Cl SNMP (17) Modify Cl SQL (44) Modify Cl SQL (44) Modify Cl Telhet (13) Modify Cl Telhet (13) Modify Cl Velo Attracks (46) Modify Cl Velo Attracks (46) Modify Cl Velo Colert (18) Modify Cl Velo Mac (329)	CRPC (76)					Modify
Scan (17) Modify Shellcode (21) Modify Shellcode (21) Modify ShftP (59) Modify Spyware (313) Modify O Solt (44) Modify O Teihet (13) Modify I TFIP (11) Modify O Web CGI (349) Modify O Web CGI (349) Modify O Web Celldrusion (35) Modify O Web Celldrusion (35) Modify O Web Celldrusion (35) Modify O Web S (115) Modify O Web IS (115) Modify O Web IS (125) Modify O Web PHP (126) Modify O Web (322) Modify O Web (3) Modify O Wher (3) Modify	CRservices (13)					Modify
Shellcode (21) Modify SMTP (59) Modify SMRP (17) Modify Spyware (313) Modify Spyware (313) Modify SIL (44) Modify Teinet (13) Modify TFTP (11) Modify Web CGI (349) Modify Web CGI (349) Modify Web CGI (349) Modify Web CGI (35) Modify Web Clant (18) Modify Web Clant (18) Modify Web Clant (18) Modify Web Prontpage (35) Modify Web Prontpage (35) Modify Web Prify (125) Modify Web Prify (126) Modify Web Prify (126) Modify With (2) Modify With (3) Modify	🖸 Scan (17)					Modify
SMTP (5S) Modify SSMTP (5S) Modify SSMMP (17) Modify Spyware (313) Modify SSL (44) Modify SSL (44) Modify There (13) Modify There (13) Modify THE (14) Modify Web Attacks (46) Modify Web Cold (349) Modify Web Cold (349) Modify Web Cold (35) Modify Web Cold (35) Modify Web Strontpage (35) Modify Web Mack (329) Modify Modify Modify Web Mack (329) Modify Modify Modify Modify Modify Modify Modify	Shellcode (21)					Modify
D SNMP (17) Modify D Spyware (313) Modify D SQL (44) Modify D Solut (44) Modify D Teinet (13) Modify D Teinet (13) Modify D Teinet (13) Modify D Web Attacks (46) Modify D Web Cold (349) Modify D Web Cold (35) Modify D Web S (115) Modify D Web Masc (329) Modify D Web Masc (329) Modify D Web Masc (329) Modify D Web PHP (126) Modify D X11 (2) Modify D Other (3) Modify	SMTP (59)					Modify
Dispyware (313) Modify Dispyware (313) Modify Dispyware (313) Modify Dispymare (314) Modify Diveb Call (349) Modify Diveb Call (18) Modify Diveb Call (18) Modify Diveb Call (18) Modify Diveb Call (15) Modify Diveb Call (15) Modify Diveb IS (115) Modify Diveb IS (125) Modify Diveb Mac (329) Modify Diveb Mac (329) Modify Diveb Mac (32) Modify Divel (2) Modify	SNMP (17)					Modify
SQL (44) Modify ITelhet (13) Modify ITFIP (11) Modify ITFIP (11) Modify IVVeb Attracks (46) Modify IVVeb Cold (349) Modify IVVeb Cold (18) Modify IVVeb IS (115) Modify IVVeb Misc (329) Modify IVVeb Misc (329) Modify IVVeb IS (112) Modify IVVeb IS (12) Modify IVVeb IS (12) Modify	C Spyware (313)					Modify
Teinet (13) Modify CTFTP (11) Modify CTVeb Attacks (46) Modify CVMeb CGI (349) Modify CVMeb CGI (35) Modify CVMeb IS (15) Modify CVMeb IS (15) Modify CVMeb IS (15) Modify CVMeb IS (229) Modify CVMeb PHP (126) Modify CVX11 (2) Modify CVX11 (2) Modify	CI SQL (44)					Modify
LTFTP (11) Modify UVeb Attacks (46) Modify UVeb CGI (349) Modify UVeb Client (18) Modify UVeb Frontpage (35) Modify UVeb IS (115) Modify UVeb Misc (329) Modify UVeb PHP (126) Modify UX11 (2) Modify Other (3) Modify	Teinet (13)					Modify
Web Attacks (45) Modify Web CGI (349) Modify Web Client (18) Modify Web Colditusion (35) Modify Web Frontpage (35) Modify Web IS (115) Modify Web Misc (329) Modify Web Misc (329) Modify Web PHP (126) Modify X11 (2) Modify Other (3) Modify	C TETP (11)					Modify
Web C8 (349) Modify Web Client (18) Modify Web Colditation (35) Modify Web Frontpage (35) Modify Web IS (115) Modify Web Misc (329) Modify Web Misc (329) Modify Web PHP (126) Modify X11 (2) Modify Other (3) Modify	Web Attacks (46)					Modify.
Web Ctent (18) Modify Web Colditusion (35) Modify Web Frontpage (35) Modify Web IS (115) Modify Web Misc (328) Modify Web Misc (326) Modify Web Misc (326) Modify Web PHP (126) Modify X11 (2) Modify Other (3) Modify	Web CGI (349)					Modify
Web Coldfusion (35) Modify Q Web Frontpage (35) Modify Q Web IS (115) Modify Q Web IS (125) Modify Q Web IS (126) Modify Q Web PHP (126) Modify Q Web (22) Modify Q Web (12) Modify Q Web (12) Modify Q Web (12) Modify Q Web (23) Modify	QWeb Client (18)					Modify
Web Frontpage (35) Modify ©Web IIS (115) Modify ©Web IIS (125) Modify ©Web PHP (126) Modify ©Web PHP (126) Modify ©X11 (2) Modify © Other (3) Modify	Web Coldfusion (35)					Modify
Web IS (115) Modify Web Misc (329) Modify Web PHP (126) Modify IX11 (2) Modify Other (3) Modify	OVVeb Frontpage (35)					Modify
Web Misc (329) Modify VVeb PHP (126) Modify I X11 (2) Modify Other (3) Modify	Web IS (115)					Modify
Web PHP (126) Modify X11 (2) Modify Other (3) Modify	Web Misc (329)					Modify
■ X11 (2) Modify ■ Other (3) Modify	Vveb PHP (126)					Modify
Other (3) Modify	DX11 (2)					Modify
	Other (3)					Modify

Fig. 18-2 The pre-defined setting

Solution Configure \rightarrow 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 : $0 \sim 65535$).

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.

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

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

The latest update t	time : 06/06/07 12:13:57	(Update signature de	finitions every 120) minutes)		
The newest version	on : 0.0.7 (Signature det	initions updated at 05/	05/03 00:00:00)			
Update signature c	definitions immediately (I	Jse TCP port : 80 and	UDP port : 53)	pdate Now Tes	L.	
Enable Anti-Vi	irus (for P2P, IM, NetBIO	S)				
Enable NetBIO	S Alert Notification					
IP Address of	Administrator 192.168	1.10				
					ок	Cancel
Set default actio	on of all signatures					
Set default actic High Risk	on of all signatures	🔽 Log	₽ Alarm	([Pass]rec	ommended)	
Set default actic High Risk Medium Risk	on of all signatures Drop 💌 Drop 💌	I⊽ Log I⊽ Log	IZ Alarm IZ Alarm	([Pass] rec ([Pass] rec	ommended) ommended)	
<mark>Set default actic</mark> High Risk Medium Risk Low Risk	Drop 💌 Drop 💌 Drop 💌 Pass 💌	도 Log 도 Log 도 Log	I⊄ Alarm I⊄ Alarm I⊄ Alarm	([Pass] rec ([Pass] rec ([Pass] rec	ommended) ommended) ommended)	

Fig. 18-3 The IDP configure setting

Name	Enable	Risk	Action	Log	Marm	Configure
syn flood	v	0	×	y.	v	Modify
udp flood	Y.	0	×	¥.	Y	Modify
icmp flood	Ŷ	0	X	¥.	V.	Modify
syn fin	Y	0	-	Ŷ	v	Modify
top no flag	v	0	-	-¥.	V.	Modify
fin no ack	v v	0	-	¥.	×	Modify
top land	y .	0	-	¥.	¥.	Modify
large icmp	- V	0	-	Y	Y	Modify
ip record route	v	٢	-	SV/	v	Modify
ip strict src record route	¥	0	۵		v	Modify
ip loose src record route	9	0	-	*	v	Modify
invalid url	v	0	-	¥.	¥	Modify
winnuke	v	0	-		Y	Modify
bad ip protocol	v	0	-	v	v	Modify
portscan	v	0	×	(V .)	v	Modify
http inspect	v	0	-	Y	V.	Modify

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

Fig. 18-4 The anomaly setting

Signature Example

Step3 In **Signature** \rightarrow **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)

Name	Software_Crack_Website (Max. 30 characters, ex: external_mounted_access)				
Protocol	C TCP C				
Source Port	0:65535 (Range: 1 - 65535, ex: 60 or 80:80)				
Destination Port	80:80	(Range: 1 - 65535, (ex: 111:112)		
Risk	High 💌	Í.			
Action	Drop 💌	🔽 Lo	g	🔽 Alarm	
Content	cracks	(Max	. 50 characte	rs, 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	Cont	igure
Software_Crack_Website	TCP	0:65535	80:80	0	×	Y	v	Modify	Remove
			New Entry						

Fig. 18-6 Complete the custom setting

ASCII code . (For example : cracks can be transfer to |63 72 61 63 6b 73|).

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

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any 💌
Service	ANY
Schedule	None 💌
Authentication User	None 💌
VPN Trunk	None 💌
Action, WAN Port	
Traffic Log	Enable
Statistics	Enable
IDP	🔽 Enable
Content Blocking	URL C Script C P2P C IM C Download C 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	MBytes (Range: 0 - 999999)

Fig. 18-7 The IDP setting in policy

Source	Destination	Service	Action	Option		Configure	0	Move
Inside_Any	Outside_Any	ANY	6		Modify	Remove	Pause	To 1
				New Entry				

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 \rightarrow Configure \rightarrow 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.

 $\ensuremath{\text{2.Monthly report}}$: 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 p	eriodic report by mail					
Vearly report	Monthly report	Veekly report	Daily report			
				9	ок	Cancel
History Report						
C Yearly report	ſ	2006 💌				
C Monthly report	[2006 🛒 06 🛒				
C Weekly report	ſ	2006 🗾 06 🛒 0	4 💌			
C Daily report	ſ	2006 💌 🛛 💽 🛛	7 💌	Send Report	1	

Fig. 19-1 The periodic report setting

S Mult	Security Fin it View	wall IDP D Tools Mes	aly Report (sage Help	2005/10/171	
<u>Ω</u> ₽ Reply	ي Reply All	MQ Forward	Print	X Delete	Previous 3
From: Date: To: Subject: Attach:	root@nuso October 1 josh@nuso Multi Secu TDP_De	ft.com.tw 8, 2005 7:0 ft.com.tw rity Firewall ily_Report.p	5 PM IDP Deily R If (18.0 KB)	eport (2005/	10/17 00.
					2

Fig. 19-2 Receive the periodic report



Daily Report of IDP Report

Duration		2005-10-17 00:00:00 ~ 2005-10-18 00:00:00						
Total Unique Events	4	4 Total Events 137		37		TCP	56	
First Event	2005-10-17 17:42:03	Last Eve	ent	2005- 17:5	-10-17 50:42		UDP	0
Attack IPs	3	Victim IF	°s		3		ICMP	81
Attack Interface	LAN	WAN1	V	VAN2	WAN	3	WAN4	DMZ
Attack Events	70	0		0	67		0	0



IPS_TOP_SRCIP_VOLUME_STR







Fig. 19-3 The IDP report content

Periodic Report		0
Enable sending periodic re	eport by mail	
T Yearly report T Mc	onthly report 📕 Weekly report 📕 Daily repo	ort
History Report		
C Yearly report	2006 💌	
C Monthly report	2006 🛃 06 🛒	
• Weekly report	2005 💌 10 💌 16 💌	
C Daily report	2006 💌 06 💌 07 💌	Send Report

Fig. 19-4 The history report setting

🔿 Multi	Security Fin	swall IDP H	istory Weekly	r Bepland (20	us pio l×
File Edi	t View	Tools Mes	sage Help		1
Qa	<u>⊈</u> ∂	WD Econycord	Delet	X	- Arrow Arro
From: Date: To: Subject: Attach:	not@nuso October 1 josh@nusc Multi Secu	ft.com.tw 8 , 2005 7:: ft.com.tw nity Firewall istory_Week	39 PM IDP History y_Report pd:	Weekly Rep f (18.6 KB)	ort (2005
					1
					1

Fig. 19-5 Receive the history report



Weekly Report of IDP Report

Duration		2005-10-16 00:00:00 ~ 2005-10-23 00:00:00						
Total Unique Events	5 Total Events			2	65		TCP	113
First Event	2005-10-16 17:51:31	Last Eve	ent	2005- 18:5	-10-18 54:23		UDP	0
Attack IPs	4	Victim If	^o s		3		ICMP	152
Attack Interface	LAN	WAN1	V	VAN2	WAN	3	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)



Fig.	19-7	То	search	the	specific	record
------	------	----	--------	-----	----------	--------

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

TITIT	.a.		and the second second		Ball Baller Control
7005.10.10			amit:	Contraction of the second s	fritterrino;a
18:54:23	C tousrompo	autom Signature S	ionware_dri	nck_Webster	E.MSI
D Hendete			100		
Vension)	11-42	1099		\$240(4 11)	
- 2	97	0		404	
	100		Filter	10 Million	11
	95511		0	0	
000		FROM SOL		Cham-um	
12	6	(6)	1	29007	
		History	Audennin		
		192.16	0 189 33		
		Constitute	onodross	-	
		-90.9	2 40 54		
		1,994,00	8.993.09C		
1.147 F1804064					
	Toging Prin			Treating/uni Port	1
	1571			60	
		200000	on Plennton		
		⇒995	817390		
		Automounde	ermeit Norm	iner.	
		.7224	103000		
liate offeri	#Removed	F 1992		Windows	
.6	0	24		16900	
	Cristellsorn	12		Efrigant polition	
	12521			Ű.	
Southeast Plantas	0.24211				
HIGHINE CHIMA		(Trans)	C HOLD BE		
0000 47 65	54 20 08 65 24	99 JE 70 68 70 J	0 40 54 54	ART VATE	0.0.0.017
0010 50 29	31 2E 31 0D UA	41 63 63 65 70 7	4 34 26 69	P/1 1 A0	cept
0020 60 61	87 65 2F 67 69	66 2C 20 69 8D 6	1 67 65 27	mage/ait.	1. 10. 10. 10. 10
0000 78 20	70 62 69 74 60	61 70 2C 20 60 6	0 61 67 65	K - × B I m e p	Imag
0040 2F 64	70 65 67 2C 20	69 60 61 67 65 2	F 70 GA 20	11000,110	000/0/0)
0050 46 87	20 20 61 70 70	6C 00 03 61 74 0	0.66 66 29	* g , * p p l i	0.01100
0080 76 8E	04 2E 0D 73 2D	65 78 83 66 60 2	C 20.61 70	# n.d. m.e + e x	57 J
0070 70 60	09 03 01 74 DB	DE DE 27 76 DE 0	0.61 20 20	p I I C M T I C M	ryna m
0000 60 69	03 61 74 69 65	68 OF 60 73 77 6	E 72 64 20	Licelient	
00a0 20 61	70 70 80 69 63	61 74 69 6F 8E 2	F 78 20 75	a oplicet	Ion/
0000 66 6F	63.60 77.01 76	65 20 66 60 B1 7	3 68 20 20	no o i wave.	110.00.
0060 2A 2F	2A 0D 6A 41 63	63 65 70 74 20 4	C 61 8E 87	× / × Ac.c.s	01-1.00
0000 75.65	67 65 BA 20 7A	68 30 74 77 00 0	A 41 67 63	11 0 g e - 1 H -	1 10 10.0
0060 85 70	74 2D 45 6E 63	EF 64 69 6E 87 3	A 201 67 7A	ept - Encod	10.0 0
0040 00 70	25 20 04 05 66	BC 01 74 65 00 0	A 55 73 65	Ip: della	1.4 0.5
0100 72 20	41 67 65 66 74	3A 20 40 6F 7A 6	0 00 00 01	Ageni	MOZILI
0120 38-20	40 53 49 45 20	Se de 70 01, (4 6	2 66 66 69	MSIE	0 101
0130 6F 77	73 20 41 54 20	35 28 30 29 00 0	A 40 0F 75	OWENT E	0 1 10
0140 74 DA	20 77 77 77 28	63 72 61 63 6E 7	3 3E 6D 75	E www.or	
01/00 00-04	43 6F 6E 6E 6E	63 74 69 6F 6E 3	A 20 40 65	Connect	Lon R
and the second				and the set of the set	

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.



- **Step1** In **IDP Report** \rightarrow **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.

-- IDP Report Statistics

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

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

Horizontal ordinate : Time .



Fig. 19-9 The IDP statistics

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

Litter Litter Description Litter Description Litter District of the second of the secon	13						
DBMD-101101004 Charles Wast 2005 0000 Control of Section 2000 000000000 Control of Section 200000000000		Logard	Annual Martin Class.	COLOR T	sumation and	Warmer III mud ++ 1	States -
DepoN:04.01 Binker, 1 Charlon Binker, 200 DepoN:04.02 Binker, 200 Sector 200 Se	2005;10:10:54:23	Cast Comp Cluster Supervise Soft	cutterp right and	EAN!	110210030000	1025148.54 10	×
D005 010 010000 D1000000000000000000000000000000000000	2005-10-10 10:54.11	CUOTON) Custom Signature Soft	manderin Hilger, ymar	Lint	102100100.33	00.93 48.54.00	×
Description Current Processor Current Processor <th< td=""><td>2005-50-10 18:54:05</td><td>COSTON Conton September South</td><td>constorn #Bgin_cost</td><td>Link.</td><td>10210030030</td><td>00.93.48.54.80</td><td>×</td></th<>	2005-50-10 18:54:05	COSTON Conton September South	constorn #Bgin_cost	Link.	10210030030	00.93.48.54.80	×
3000, 1	poor lists in the second	O Plant OND Caston Signature 2008	CUBBON PROP. Man.	6,000	102164.184.35	AND AN DRIVE	×
0000100000000000000000000000000000000	2020-10-10 10:01:00	ATTACH-INDICATED 401 Forjakt	attementation -	SHAWAY	44.110-249-0	130-180-100-05-1404	-
D005 CONTROL CONTROL Signature Signature Sold Control Signature Sold Control Signature Signature Sold Control Signature Signature Sold Control Signature Signature Sold Control Signature Sold <thcontrol signature="" sold<="" th=""> Control Signat</thcontrol>	2006/10/318 10:02:00	CATTACECHICKARDEEL-403 Forball	alteraphent-inicial	(IN(ADED	041032458.0	4103 FEB.100.023500	AD-
D005010111100142 CV21000102000000000000000000000000000000	2005-10-10 10:01:00	COSt Coll Caston Signature Sel	contract proprietable	Links'	103.168.108.05	00.00 48 54 00	×
Store Control (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	2005/10/10 10:00:66	COSTON Culture Superiore Galt	content-bidgs.gtm	Linty.	10210810833	00'00 40 54 50	×
Scholar 11 11 121 20 Color Color QL current ' 1000 ' Trans' ' 10000 ' 10000 ' 1000 ' 1000 ' 1000 ' 1000 ' 1000 ' 10000 ' 1000 ' 10	2008-10-18 18 50-42	Decourterell Custom Sagneture-Built	CONICEPERSONNEL	LAN-	1982 180 2118 23	0030.48.54.00	×
D001-01010020 Image: Commed Vote Found VORE 11: How and the image: Vote Found VORE 11	2000-10-18 18 88 20	COSTON) Custom Signahire-Soft	compression and	LIN	10010810833	00 83 48 54 88	×
School 10-10 11 0000 Bit Damacy Yorke France Yorke 112 State and the state of	2005-10-11110-0020	Dataman Street and Store 115	intersonation f	- Noterr	210 14.230 130	103 100 100 33 1000	×
Bits Control Control <thcontrol< th=""> <thcontrol< th=""> <thcont< td=""><td>2000-10-10 10 00:00</td><td>Comment) Veral Found, VODI 112</td><td>(Star Inning)</td><td>1000045</td><td>110 11 230 170</td><td>100,180,480,223500</td><td>×</td></thcont<></thcontrol<></thcontrol<>	2000-10-10 10 00:00	Comment) Veral Found, VODI 112	(Star Inning)	1000045	110 11 230 170	100,180,480,223500	×
Statistic Statistic <t< td=""><td>2005-16-18 Ho 48-55</td><td>O COMMAND VILLE FOUND VOIDA THE</td><td>ineque-dierent</td><td>Whites</td><td>210 19 200 120</td><td>100/100/109/337500</td><td>**</td></t<>	2005-16-18 Ho 48-55	O COMMAND VILLE FOUND VOIDA THE	ineque-dierent	Whites	210 19 200 120	100/100/109/337500	**
Sec. 16. 11 10 00000 Commany Your Fund Cool Dial How Mand You Page 210 000 20000 100 100 00000 100 100 00000 100 100 00000 100 100 00000 100 0000000 100 0000000 100 0000000 100 00000000000 100 0000000000000000000000000000000000	2005-10-11 49-54	Dichemer's Veril Pount VOER 135	www.iiitect.	- www.wa	UNIV 54 J WY 120-	192188468 8825584	×
S205:15:15:11 16:34:53 0: xmassey Your Prace DOS Pract resumand 100/00 100.18:10:10:14:14 Xmm S205:16:11 16:34:15 0: xmassey Your Prace DOS Pract resumand 100/00 100.18:10:10:14:14 Xmm S205:16:11 16:34:15 0: xmm 0: xmm Xmm 100.18:10:10:10:10:10:10:10:10:10:10:10:10:10:	2005-10-10-10-49-55	Containey's Value Foreids (ICO Munit	Invise inner!	///////	210 == 200:100	102/100 103 351400	×
Data Description Description <thdescription< th=""> <thde< td=""><td>2005-50-18 18 49-59</td><td>Distantion's Virus Fisans DOZ PD-M</td><td>barres manuel</td><td>Celliner.</td><td>110 m 2 10 1 10</td><td>100-100-100-031-000</td><td>1</td></thde<></thdescription<>	2005-50-18 18 49-59	Distantion's Virus Fisans DOZ PD-M	barres manuel	Celliner.	110 m 2 10 1 10	100-100-100-031-000	1
Status Control Control <th< td=""><td>manufaction telland</td><td>Contractory's United Franker 2023 Dillar</td><td>owner things</td><td>incases.</td><td>UTO 108 2181 100</td><td>100.088.180.011440</td><td>1</td></th<>	manufaction telland	Contractory's United Franker 2023 Dillar	owner things	incases.	UTO 108 2181 100	100.088.180.011440	1
2005 10.01 01 02 44 0 04778/04 02576/2051 400 Faithed deceder-wood 90465 04 100.000 100.010.010.01.0144 0 2005 10.01 01 04.71 11 0 14774/04 02576/2051 400 Faithed deceder-wood 90465 04 100.000 100.0100.010.01.0144 0 2005 10.01 01 04.71 11 0 14774/04 02576/2051 400 Faithed deceder-wood 90465 04 100.000 100.0100.0101.0144 0 2005 10.01 01 04.71 11 0 14774/04 02576/2051 400 Faithed deceder-wood 90465 04 100.000 100.0100.0101.0144 0 2005 10.01 01 04 70 01 0 14774/04 02501/0400 Faithed deceder-wood 90465 04 100.000 100.0100.01144 0 2005 10.01 01 04 70 01 0 14774/04 02501/0400 Faithed deceder-wood 90465 04 100.000 100.0100.0100.0100.0100.0100.	2025-10-18 18 49-29	Constant Virial Found DOG INLAS	Interior content :	(MAN)	100 10 200 100	190.088-009.053480	2
BODD -10 - 10 - 10 - 27 - 11 ATTACX-Influence (IIII) - 400 - Protease and advanced amount Invalued amount <td>D005-10-10 10 x7244</td> <td>CONTRACTOR AREAN AND TANKING AND TANKING</td> <td>attendent wegen</td> <td>WARD</td> <td>641082458</td> <td>100.140.170.0223.884</td> <td>ada</td>	D005-10-10 10 x7244	CONTRACTOR AREAN AND TANKING AND TANKING	attendent wegen	WARD	641082458	100.140.170.0223.884	ada
S000.10.1111.11.01.02.0 GL ATTACA-MILLINGCODI GL DI Oraca. mendes-second MARGE AL-100_ARE 100.100.100.12.1.148 GL S000.10.111.11.01.01.01 GL ATTACA-MILLINGCODI GL DI Oraca. mendes-second MARGE AL-100_ARE 100.100.100.12.1.148 GL ATTACA-MILLINGCODI GL DI Oraca. mendes-second MARGE AL-100_ARE 100.100.100.12.1.148 GL ATTACA-MILLINGCODI GL ATTACA-MILLINGCODI GL ATTACA mendes-second MARGE AL-100_ARE 100.100.100.12.1.148 GL ATTACA-MILLINGCODI GL ATTACA <t< td=""><td>2005-10-10 10 47-11</td><td>ATTACH SHUDDEDING AND Postant</td><td>attempted arrows</td><td>WARES</td><td>64350.249.6</td><td>102108-100-331494</td><td>-</td></t<>	2005-10-10 10 47-11	ATTACH SHUDDEDING AND Postant	attempted arrows	WARES	64350.249.6	102108-100-331494	-
Store 1G 11 11 14 7/10 Part ACC HINE SCORED and Contract mercediter (Herorit Woods 64.116.2481 100.100 TID 10.1498 100.100 TID 10.1498 2005 1D-111 TID 47 00 Part ACC HINE SCORED and Contract Mercediter (Herorit Woods 64.116.2489.0 100.100 TID 10.1498 Part ACC 2005 1D-111 TID 47 00 Part ACC HINE SCORED and Contract Mercediter (Herorit Woods 64.116.248.0 100.100 TID 10.1198 Part ACC 2005 1D-111 TID 47 00 Part ACC HINE SCORED and Contract Mercediter (Herorit Woods 64.116.248.0 100.100 TID 10.1198 Part ACC 2005 1D-111 TID 47 00 Part ACC HINE SCORED and Contract Mercediter (Herorit Woods 64.116.248.0 100.100 TID 10.1184 Part ACC 2005 1D-111 HA 70 Part ACC HINE SCORED and Contract Mercediter (Herorit Woods 64.116.248.0 100.100 TID 10.1487 Part ACC 2005 1D-111 HA 70 Part ACC HINE SCORED and Contract Mercediter (Herorit Woods 64.116.248.0 100.100 TID 10.1487 Part ACC 2005 1D-111 HA 70 Part ACC HINE SCORED and Contract Mercediter (Herorit Woods 64.116.248.0 100.100 T	2005-10-10 10:02:11	ARTICLE STREET AND FORDER	among double or company	mahit	041100.349.0	100.100.100.0011484	10
SSS: 10-19 TE 471 0 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.0 102 190 H00 J11444 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.0 100 J40.00 J11444 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.00 100 J40.00 J103.00 J40.00 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.00 100 J40.00 J40.00 J21.400 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.00 100 J40.00 J40.00 J21.400 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.00 100 J40.00 J40.00 J11400 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.00 J40.00 J11400 Image: ATTACCA INTERPORTED (ADD Formation interregeneration) WMARE 64 190 J40.00	2006-10-111147-10	ATTACH MULTEROSTI 401 College	divergiteit ann dit	Westers	641150 24118	10233007802803404	-
2005-10-1011014709 247TACM INTERCALLED 400 Formal Interageneration Index 44 195-245.0 100.100.100.000.021491 2005-10-10110470 247TACM INTERCEDED 40.0 Formal Interageneration 190.005 64.155-245.0 100.100.000.021491 1 2005-10-101470 247TACM INTERCEDED 40.0 Formal Interageneration 190.005 64.155-245.0 100.100.000.021491 1 2005-10-101470 247TACM INTERCEDED 40.0 Formal Interageneration 190.005 64.155-245.0 100.100.000.051444 1 2005-10-101477 247ACM Interaction Interaction 190.000 104.100.000.051444 100.100.000.051444 1 100.100.000.051444 1 100.100.000.01444 100.100.000.01447 1 <td>2005-30-10 10 47 10</td> <td>ATTACH MISHON INC. 403 Fortant</td> <td>allowed and a second</td> <td>Valadata</td> <td>44-11003494.8</td> <td>122 198 199 20 1994</td> <td>-</td>	2005-30-10 10 47 10	ATTACH MISHON INC. 403 Fortant	allowed and a second	Valadata	44-11003494.8	122 198 199 20 1994	-
Security 10 Contract of the Arrow of the Ar	2005.30.10104/09	Stattach Printing and Format	affects for Campber	weekee	64.150.383.0	100 740 740 33 1404	-
IDSD: 15:10 INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) 2005: 15:10 INTRACK ARE INTRODUCED (402 / 011ml) 2005: 15:10 INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) 2005: 15:10 INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) 2005: 15:10 INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) 2005: 15:10 INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (402 / 011ml) INTRACK ARE INTRODUCED (400 / 011ml) INTRACK ARE INTRODUCED (40	2005-20-10 10 47-00	ATTACK PROPERTY AND FORTHALL	mena mala and do	(Investors)	64155.369.0	102 100 100 10 10 100	-
S200-11/-11/11.81.47-06 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.180.405.31.344 S S200-11/-11/11.47-01 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.180.405.31.344 S S200-11/-11/11.47.01 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.180.405.31.344 S S200-11/-11/11.47.01 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.180.400.05.348 S S200-11/-11/11.47.01 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.180.00.03.348 S S200-11/-11/11.47.01 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.100.00.03.3146 S S200-11/-11/11.47.01 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.100.00.03.3146 S S200-11/-11/11.47.01 S-ATTACM-MINIMPORTS (S) BUT Formal attemption-modely VAAVA 64.150.248.6 102.100.010.32.1486 S S200	1000-10-10-10-45-02	a tatta a month and ant fortake	all second se	ALC: N	64 (100 (24) 0	100 400 400 33 1407	-
Biologics (6, 519, 19, 87,00) CATTACCH HIGHONE (2) attr Formal Biologics (6, 519, 19, 87,00) CATTACCH HIGHONE (2) attr Formal Biologics (6, 519, 19, 87,00) CATTACCH HIGHONE (2) attr Formal Biologics (6, 519, 19, 87,00) CATTACCH HIGHONE (2) attr Formal Biologics (6, 519, 19, 87,00) CATTACCH HIGHONE (2) attr Formal Biologics (6, 519, 19, 87,00) CATTACCH HIGHONE (2) attr Formal Biologics (7, 70, 19, 19, 19, 19, 19, 19, 19, 19, 19, 19	Shared Annual and a subst	ATTAIN MENTION AND A STREET	and the second second	LANGAGE	an free place	100 100 100 10 1400	- 2
Sector 16:10:10:14:47-04 ATTA S2: 40000/CPUED1 400 Format History MAT ecco Workpit 44:176:246.00 10:10:00:10:01:01:01:01:01:01:01:01:01:0	2005 10 10 10 10 17 05	A TRACK MULTINGERSTRY AND SOLUME	and and and another	10000044	Ad one place	100 100 100 00 100 100	-
School (1) School	Seed of he he ar ar			- Landard	A CONTRACTOR	Marrison April 1991 1 400	
2005-10-10 11.8 47.0 47.1752-4400000000000000000000000000000000000	and down to station		and in the local states of the	and and a	404-150-240-0	Alex dam and the same	
Construction Construction<	2020 10:10 10:47:02	A TRACK MUSICAL STREET	and the state of t	141403	A4.100.240.0	192 188 189 189 149	-
2000-10-10 10 40 41 0) 417 A2A/4000 Discrete Discrete 000 Flattere immediate function 004400 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0 100,100,214.00 44,100,248.0<	Sector and the sector		and the second se	(Tripleta)	64.108.2488	And American and the state	
Automatical and the second s	2006-10-11118-02-00	A TIA PUBLICADE OF POLICE	and the second second	animala l		THE AGE AND ADD ADD	-
2000-10-11 10 41/20 2017 ACX-000002021 400 Portaxi anteraction control VAND	2000-30-10 10:40 01	A TTACAL AND INCOME IN A COPPORT	and the second second	anonpep	04/350/249/0	100 100 100 00 1405	
2000-10-11 10 2001-10-11	3005-10-11118-00	TALLACSI SUBSIDIERE ST STD A OLDER		INVISIO INVISIO	*** 1101.04% ()	100,100,000,000,000,000	19
2000-10-11110-01228 INTERCONDUCTORING ADDITIONAL INTERCONDUCTORING VOLUME 64-150-240.00 TEXTRETORING INTERCONDUCTORING 2000-10-11110-01228 INTERCONDUCTORING INTERCONDUCTORING INTERCONDUCTORING VOLUME 64-150-240.00 TEXTRETORING INTERCONDUCTORING INTERCONDUCTORING <td< td=""><td>2008/10/18 18 48:35</td><td>ALL VOID ALL VOID ALL</td><td>Internation (Internation (International)</td><td>WIND</td><td>64158.2498</td><td>100.000 000 000 000 000</td><td></td></td<>	2008/10/18 18 48:35	ALL VOID ALL	Internation (Internation (International)	WIND	64158.2498	100.000 000 000 000 000	
2000-10-10 10 40 20 •••••••••••••••••••••••••	2005-10-10 10 49-27	ATTACH MISHCAPIES 303 Portage	Pages Annual Annual	- VOAHD	64.100.249-8	122-130 105-321400	
accord (a) (119 (1197)) accord (a) (11	2000-10-10-10-01-20	A LACK MUSICAL DI ACA PARAM	10000000000000000	POURS	441563460	1001000000000000000	-
2000-10-10 10 40 22 INTERCENTION CONSTRUCTION AND CONSTRUCTION OF CONSTRUCTUCUCUCUCUCUCUCUCUCUCUCUCUCUUCUUCUCUCUUCUUCUUCUUCUC	2000-10-18 18 48:20	A strain a sector of the secto	1000011001-100000	(NOADE)	#4.155.249.0	102160303321860	
2000-10-10 18 49/23 CP14114-Interference (VALUE) Memory Interference (VALUE) VALUE	2008-10-18 16 49 25	ATTACH MEMORSEST 403 Portaki	When a fail the or	100013	64/(55.249.0	192,100,103,331,400	-
2000, 10: 10: 10: 40: 22 (a) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI DI NALEZ) (b) ATTACK - MUSINGACCU (ALI POLINAL MININGACON (ALI POLINAL	2000-10-10 18 41/25	ATTAL IN PROPOSED IN AD FORMAL	appending-incore	(convis	64 150 J49 6	192160405.351466	-
2005-10-10 10 44/22 23/3177-22-48039/64/2013 407 Format Internation 96045 64.126-2484 102.186.100.00.01.144 • 2005-10-10 10 44/22 23/3177-22-48039/64/2013 107 Format Internationance 96045 64.126-2484 102.186.100.00.1444 • 2005-10-10 10 46/20 23/3177-22-48039/64/2013 107 Format Internationance 96045 64.126-2484 102.186.100.00.1444 • 2005-10-10 10 46/20 23/3177-22-48039/64/20130 Format Internationance 96045 64.126-2484 102.186.100.00.1444 • 2005-10-10 10 46/20 23/3176-22-48039 custom resp. (internationance) 96045 64.126-2484 102.186.188.23 00.0148.44.48 • 2005-10-10 10 46/20 23/3176-22-48039 custom resp. (internationance) Custom resp. (internationance) Custom resp. (internationance) 00.0148.188.23 00.0148.44.48 • 2005-10-10 10 46/20 20/317640 Custom Resp. (internationance) Custom re	1005-15-10 10 45 23	ATTACALIBUSICATION AND FOLIAM	haberraded-record	9101/143	64/155.249 B	107.100.103.33.1408	-
2005-10-10-10-00-00 2007-17-00-00000000000000000000000000000	2005-14-18-16-44:25	ATTACK RUSPONSEST AND FORMAL	immitted ancon	14/14/3	64150.249.6	192 166 109 39 1464	-
2005-10-11 10 4E 10 CP A T ACO-RESERVATES ADD FORMAL ADD FO	2005,10.1818.00.00	A TRACK MUNICIPALITY ADD FORMAN	Manual Angel	INCAPPS	84.1252.349.8	192100.100.353.440	
2005-10-17.114.41-9 COTTORI Quarker Signature Suff. Autom High, 218. CAV Tip 100.10023 00.012.40.54.00 X 2005-10-17.114.41-9 COTTORI Quarker Signature Suff. custom High, 218. Lake Tip 100.100.103.3 60.00.40.54.00 X 2005-10-17.114.41-91 COTTORI Quarker Signature Suff. custom High, 218. Lake Tip 100.100.103.3 60.00.40.54.00 X 2005-10-17.114.41-91 COTTORI Quarker Signature Suff. custom High, 218. Lake Tip 100.100.103.3 60.00.46.54.00 X 2005-10-17.114.41-91 COTTORI Quarker Signature Suff. custom High, 218. Lake Tip 100.100.103.3 60.00.46.54.00 X 2005-10-17.114.41-91 Of 100.017.000 Quarker Signature Suff. custom High, 218. Lake Tip 100.100.100.20 X 2005-10-111.114.41-91 Of 100.00.0100 High Annex Vol(01.111 onus makest Volds 200.010.21.010 X 2005-10-111.144.41 Of 100.00.0100 High Annex Vol(01.111 onus makest Volds 200.010.21.010 X 2005-10-111.144.41 Of 100.00.0100 High Annex Vol(01.111 onus makest Volds	2005-10/18 18 48 18	ATTACACHISICATESI NO FORMAL	alterigiani eecon	UNION BID	64-103(2498-8)	100.188-100-323.468	-
2005-00-10-10-01/2 COT CMR Control Reportant flow Automotivege unit Lake 102.000-103.3 00.00-40.54.00 XXX 2005-00-10-10-01/2 COT CMR Control Reportant flow Control CMR Control Reportant flow Control CMR Control Reportant flow XXX 102.100.100.23 00.00-40.54.00 XXX 2005-10-10-10-01/2 COT CMR Control Reportant flow Control CMR Control Reportant flow Control CMR Control Reportant flow XXX XXX 102.100.100.23 00.00-40.54.00 XXX 2005-10-10-10-01/2 COT CMR Control Reportant flow Control CMR Control Reportant flow Control CMR Control Reportant flow XXX XXXX XXXX XXXX	2005-10-18 18 45 18	COSTONI Custom Operature Surf	Roution #age, plat	DOM:	192300.000233	60.97.48.54.88	×
3005-10 (1)	2008-40-1010-4032	CUSTON Computition Signature Sign	anustration angen under	L.008.	103.168.109.33	60.50 40 54 EU	×
2005-10-10-01-04 QP (CO) FORQ Customer Signatures from Contem Figs. plan CAP (32-160-200-22) 00-07-48 tot 00 X 2005-10-10-10-04-01 QP (CO) FORQ Customer Signatures from Annual statement VADAD (32-160-200-22) 00-07-48 tot 00 X 2005-10-10-10-04-01 QP (CO) FORQUE V/ORDER From Child Fill Annual statement VADAD (30-02-20)-120 Tes: 160-100-30-148.00 X 2005-10-10-10-04-041 QP (CO) FORQUE V/ORDER From Child Fill Annual statement VADAD (20-02-22)(-1.00) Tes: 160-100-30-148.00 X	2005/10/1718 46:08	COSTON) Cutton Suppliere Soft	CONTON PAGE, 110	6.009	102.108.108.32	00.00.46.64.00	×
2006-10-10-14-01 (1) (4-01 (1) (2009)	2006/10/18 18 48:05	CODTONE Custom Signature (Suit	COMMITTERS, 200	EAH	19216030833	00.00/48/00/00	×
2006 A D. M. M. M. M. M. Martin College Contract Coll (Coll College Co	2005-30-10 10 44 01	Distantian's Visital Found, VOEN 111	-statistict -	-Venid	100 TB 230 130	102 100 100 30 1465	×
	2000-10-1010-044-01	Constraints & States & constant, Delite 1951-56		Notars	20038230.000	100.100.100.33140+	×

Clear.

Fig. 19-10 The IDP log



1.Action:

Icon		\times
Description	Pass	Drop

2.Risk :

Icon	6	0	
Description	High Risk	Medium Risk	Low Risk

_ . _ . _ . _

4