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.

The latest update t	ime : 06,06,07 10:11:06	(Update signature de	finitions every 120) minutes)	
The newest version	on : 0.0.7 (Signature defi	nitions updated at 06	/02/23 21:27:41)		
Update signature d	definitions immediately (L	lse TCP port : 80 and	UDP port : 53)	pdate Now Test	
🔽 Enable Anti-Vi	rus (for P2P, M, NetBIO	S)			
[✓ Enable NetBIO	S Alert Notification				
IP Address of	Administrator 192.168.1	1.10			
				ок	Gancel
Set default actio	in of all signatures			OK	Cancel
Set default actio High Risk	m of all signatures Drop 💌	₩ Log	🔽 Alarm	OK (Pass) recommended)	Cancel
Set default actio High Risk Medium Risk	m of all signatures Drop 💌 Drop 💌	년 Log V Log	マ Alarm マ Alarm	([Pass] recommended) ([Pass] recommended)	Cancel
<mark>Set default actio</mark> High Risk Medium Risk Low Risk	n of all signatures Drop 💌 Drop 💌 Pass 💌	다 Log Log Log	교 Alarm 전 Alarm 전 Alarm	([Pass] recommended) ([Pass] recommended) ([Pass] recommended)	Gancel

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*, *Figure 17-4*)

IDESystem Event Alami	_(eixi
He Edit View Tools Persoage Help	
Q2 Q2 VQ 23 × 4 ↔ 23 Reply Reply of Reviewed Revet Dates Next Addresses	
France IIION Dokes Disabar 11.2503 10.25 PM Tex politigin.soft.com.tw Subject: IOPsystem Event Alarm/	
Time Proceed So: P Cod P Event	2
2005-00-11 423451 TC 12 102.050.08023 06.210.03972 1777WARE Meanmain Systems Activity 2005-00-11 423455 TC 12 102.3461.03033 66.10.030972 1777WARE Meanmain Systems Activity 2005-00-11 423455 TC 12 102.3461.03033 66.10.030972 1277WARE Meanmain Systems Activity 2005-00-11 42445 TC 12 102.061.08153 66.10.030972 1277WARE Meanmain Systems Activity 2005-00-11 42445 TC 12 102.061.08153 66.10.030972 1277WARE Meanmain Systems Activity 2005-00-11 42445 TC 12 102.061.08153 66.10.030972 1277WARE Meanmain Systems Activity 2005-00-11 422445 TC 12 102.061.08153 10 102.030972 1277WARE Meanmain Systems Activity 2005-00-11 422445 TC 12 102.0512833 66.034.57225 1277WARE Meanmain Systems Activity 2005-10-11 42245 TC 12 102.046.05033 66.034.57225 1277WARE 1006dFbea.com States 2005-10-11 422457 TC 12 102.046.05033 66.034.57255 1277WARE 1006dFbea.com States	
	크

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 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: [SPY WARE] Metarewards Spyware Activity	Messenger Service	X
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: [SPY WARE] Metarewards Spyware Activity	Messenger from IDPsystem to MANUAL8 on 10/11/2005 (02:25:57PM
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: [SPY WARE] Metarewards Spyware Activity	Warning!!	
Time: 2005-10-11 14:24:45 Source IP: 192.168 189:33 Destination IP: 66:110.189:27 Event: [SPY WARE] Metarewards Spyware Activity	This is an alert message from IDPsystem.	
Source IP: 192.168-189-33 Destination IP: 66-110.189.27 Event: [SPY WARE] Metarewards Spyware Activity	Time: 2005-10-11 14:24:45	
Destination IF: 65.110.189.27 Event: [SPYWARE] Metarewards Spyware Activity	Source IP: 192.168 189.33	
Event: [SPYWARE] Metarewards Spyware Activity	Destination IP 66.110,189.27	
	Event [SPYWARE] Metarewards Spyware Activity	
	OK	

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

Time	Event'-	Bignature Class	interfac-	Stath C -	Victory IP Port -	Action	
2005-10-11 14 24:57	SPVV/ARE] Metarewards Spyware	policy-violation	LAN	192.168.188.33	66.110.189.27.80	×	
2005-10-11 14:24:45	SPYVARE] Melaniswards Spyware	policy-violation	LAN	102468.189.33	66.110.189.27.80	×	
2005-10-11 14 24 39	() SPYWARE Metawards Spyware .	policy-violation	LAN	192,168,189,33	66.110.189.27.80	×	
2005-10-11 14 24 38	C SPYWARE] Metarowards Spyware .	policy-violation	LAN	192 168 189 33	86.110.189.27.80	×	
2005-10-11 14:24:35	SPYWARE] Metarewards Spyware	policy-violation	LAN	192 168 189 33	66.110.189.27.80	×	
2005-10-11 14:24:32	SPVVKARE] Metakewards Spyware .	policy-violation	LAN	192165189.33	66.110.189.27.80	×	
2005-10-11 14 22 45	ATTACK-RESPONSES] 403 Portixed	stenpted-recon	WAN3	64.150.249.6	192 168 189 33 1404	-	
2005-10-11 14:21:57	SPYWARE] GlobaPhon com Divie	trojen-activity	LAN	192 166 189 33	66:194.37.253.60	×	
2005-10-11 14:21:51	SPVWARE; OlobaPhan.com Divie	brown-activity	LAN	19216818933	66.194.37.253.60	×	
2005-10-11 14:21:40	SPVWARE] GlobaPhon.com.Divie	trojen-activity	LAN	192168109.33	68:194:37.253.80	×	

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			4 2		2	Modify
icmp flood			N B		· · · · · · · · · · · · · · · · · · ·	Modify
syn fin					, <u> </u>	Modify
top no flag			0.00			Modify
fin no ack		i i	10 0	Į į		Modify
top land		1				Modify
large icmp		H			11 I	Modify
ip record route						Modify
ip strict arc record route						Modify
ip loose src record route						Modify
invalid url						Modify
winnuke						Modify
bad ip protocol		i l				Modify
portscan			10 0			Modify
http inspect		a l				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).

入侵值测防架特徵接触。2014		
物准务期	補約 前介 北線 第示	秋天
Attack Responses (16)		19-DE
Cl Beckdoor (74)		180
D Bed Traffic (13)		10:00
El Criet (30)		杨度
(100oS(3))		1. Bata
Ci Delettes (165)		0.000 m
(ED34012)		-80
Closs (19)		153
DEvelot (76)		移盘
Offinger (13)		使法
DETP.(70)		150
Dicke (2)		19:01
CIMAP (38)		Hick
Clinto (%)		19:0
CIMISC (56)		15-15
DMdireda (10)		18:0
DM/SQL(D)		10-21
CINERIOS (201)		10.0
CINITP (13)		- 他在
El Oracle (299)		18:0
DP2 (10)		15:3
GBoky (20)		10:0
[]P0P2 (4)		16:31
GR0P3 (27)		180
DPam (21)		12:5
0.690 (76)		移动
Differences (13)		100
QSem(17)		15.0
El Shekole (21)		15:00
CI SMIP (50)		15.2
DSIMP (17)		ilicit.
Ci Service (313)		柳边
030(44)		19.00
[Tribe(13)		特达
CONTRACT)		Hick
DWeb Attacks (46)		15.0
CIVNED COL (349)		150
CiVeb Ciert (18)		制改
Web Colduson (25)		19-11
Civito Frontavas (20)		100
QWeb (5 (115)		19.0
El Web Misc (329)		推动
DWeb HHP (120)		19-2
Contral.		前曲
DOtter (3)		15-21

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*)



Figure 18-3 Intrusion Detection and Prevention Setting Screen



Enable Risk Action Log Aiann Configura Name syn flood Modify 0 ۷ XXX ٧. ¥. udp flood Modify ۷ ۷ ٧ icmp flood ٧ 0 × 4 Modify Y syn fin ¥ O ¥. Modify 1 v top no flag ٧ ٩ 4 ۷ Modify Ŷ fin no ack V. O ø Modify ¥. ¥. Modify top land ¥. 0 4 ٧ ٧ ¥. 0 large icmp 0 ų. ٧ Modily 0 ip record route v Modify 0 ¥ w. Modify ip strict arc record route 0 ¥ 4 ¥ v Modify ip loose src record route ۷ 0 \$ ¥ Y invalid url v 0 2 ¥ ٧ Modify v 0 -Modify winnuke ٧ v bad ip protocol ¥. O -¥ v Modify portscan Monity V Ð × ¥. Y. http inspect Modify Y. ٩ 2 ٧ y

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

Figure 18-4 Anomaly Setting



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*)

Name	Software_O	ack_VVebste (Max. 30 characters, ex	external_mounted_access)
Protocol	FTCP CL	JOP CICMP CIP	
Source Port	0.65535	(Range: 1 - 66535, ex: 80 or 80:8	0)
Destination Port	60.60	(Range: 1 - 65535, ex: 111:112.)	
Risk	High 💌		
Action	Drop 💌	₩ Log	Alarm
Content	cracks	(Max, 50 characte	rs, ex. mount or (5d 6f 75 6e 74()
Advance Option	10		
Non-direction			
Disregard text ca	ise		

Figure 18-5 Custom Setting Screen

特徵名稱	通訊儀定	來源壇	目的堆	围绕	動作	記録	警示	燈	Æ
Software_Crack_Website	TCP	0.65535	80.80	0	×	¥.	(Q)	修改	制能

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	PERMITALL F DENY ALL FWAN1 FWAN2 FWAN3 FWAN4
Traffic Log	Enskle
Statistics	Eneble
IDP	🔽 Enable
Content Blocking	URL Script P2P F IM Download F Upload
Anti-Virus	THTTP / WebMail T 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	Inolique	Configure	Move
Incide_Any	Outoide_Any	ANY.	1	1	Modify Remove Pause	To 1 .

New Entry

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.
 - 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	eriodic report by mail				
Vearly report	Monthly report	Vieckly report	Daily report		
				ок	Cancel
History Report					
C Yearly report	T	2006 💌			
C Monthly report	Γ	2006 💌 06 💌			
C Weekly report	٢	2006 💌 🛛 🖸	4 🛩		
C Daily report	Г	0 💌 00 💌 0000	7 🐨	Send Report	

Multi File Edi	Security Fin t View	wall IDP D Tools Mes	uly Report (sage Help	2065/10/174	
⊈ ∉ Reply	Ge Reply All	NO Forward	Print	X Delete	Previous
From: Date: To: Subject:	noot@nuso October 1 josh@nuso Mulh Secu	ft.com.tw 8, 2005 7:0 ft.com.tw rity Firewall :	5 PM IDP Daily R	eport (2005/	10/17 00
Attach:	-dink De	ily_Report.p	af (18.0 KB)		
					2

Figure 19-2 Receiving the Periodic Report Mail

Figure 19-3 The content of Intrusion Detection and Prevention

Periodic Report	dic report by mail	eso o la				
In Yearly report 1	Monthly report	Vieekly report	Ter Daily report	6	ок	Cancel
History Report						
C Yearly report	E	2006 💌				
C Monthly report	F	2006 👿 06 💌				
Weekly report	F	2005 💌 10 💌 1	6 💌			
C Daily report	F	0 💌 06 💌 0	7 💌	Send Repo	B	

Figure 19-4 History Report Setting Screen

E Molt File Ed	i Security Fin it View ⁻	wall IDP H Fools Mess	alary Weeld age Help	er Beprech (20	
<u>Ø</u> ₽ Reply	De Reply All	M2 Forward	Print	X Delete	Previous **
From: Date: To: Subject: Attach:	mot@nuso October 1 josh@nuso Multi Secu	ft.com.tw 8 , 2005 7:3 ft.com.tw nty Firewall istory_Weekl	19 PM IDP History y_Report.pd	Weekly Rep f (18.6 KB)	art (2005
made	12				×
					<u>z</u>
					6

Figure 19-5 Receiving the History Report E-mail

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)

Figure 19-7 Searching Specific Records Screen

In the Daily Report, click Time to show the Event Detail report. (Figure 19-8)

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.

- **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.

Figure 19-9 Mail Scanning Statistical Charts

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

TITUE	Entre -	TRANSFER LINE AT	and the lot of	Aller will an	Manager of Print in 1	111
NUM, LILLIN DE MALLY	CONTRACTOR Links there and a to the	Continer, Phys., 1910	6.644	Page 100 Feeta	100001-00.44.000	- 34
COLUMN DALLAS	COntraction Contraction Bar	mandation of the party of the	Loss	102 120 100 100	manden and the day	
SOL - LOL D.	Chicago Catter Supervises Ser.	Contract Party and	C.MA	101100-008-00	day and we the law	-2
10.10.10.10.00.01	Contraction to and in the	Line ing de	6.044	1211116-0-1-04	444 102 44 108 104	-0
	The strain and strain and strain	and a state of the state of the	-	AR COLUMN A	And And limit on Links	10
	The starts methods with the start	Castoreland	Contract of		100 100 PML	
ADD OR OTHER DRIVEN AND	Character and the local state	Construction of the second second	L andre	100 100 100 100	and they don the state	- 3
and the set in the last	A CONTRACTOR OF A CONTRACTOR O	Contract of the second	1.044	100 100 100 100	00000 40 00 00	- 3
		Contract of the local	1.001	Call Land Total Lab		-3
NOT THE PARTY NOT THE		and the second second	1.044	CAR I HA CHAR IN		-8
	and the set of the set	and an and a second				-8
COLUMN THE THE NOT DE	A Provide Land of the state of the state	- I - Contraction	· Present		The last two is a last	-8
00810-74116-0036	A Distance of the Postal Postal Postal	and a second		\$141 BR.2 BE 1 RD	TAU THE HIGH STORE DOOL	
1010110-010-010-04	Commery trips from vote the	The Contraction		This be too use	Fed the 9'88 209 2004	~
	The second states from the second state	1000-0001		South # 748 100	131100-00100-001044	
000110110 10 10 38 91	Transic You Found Too Stime	Server assessed	Company of the	210 08 388 100	1980 1885 Add 201 Galler	
contraining his earlies	Contract Value Finance (1007 Filled	and a little of	-	240 Se 100 100	They I and Arley out home:	X
AURT TOTOL FOR WHE FILL	Contraction of the second second second second	Period 1484602	AMPE	2111.006.2081.1245	You and how or search	
pent design als size an	Comment of an Assoc 2500 7008	and a strength	INNE	300-38-21811-30	TNO OR DRIVEN DRIVE	~ ×
EDCLO-DIF HOUSE +	Part of the second second second second	Messolers-ballat	PONER.	041043808	#10.2458.1007.1211.1088	- 60
090-54-60 10 00 10	A Prace service and Passas	patrona galante de protection	-madana	0.0100-300.0	1001100.1001223484	- 40
NULTER OF FROM T	arrace metrosest and system	antenaders anten	1994003	AA110-Jak.0	100100100101464	
000 10-10 10 47 10	and a residence of the second second second	dentation excelsion	Andre	841083488	10110-00110-0012-0-004	
008-10-10 10-07-08	ATTACK (BEIGH SHIEL) SOLF-STREET	allere entities.	(PANIS)	441563888	\$50 LOD 1003 THE 1884	- 40
con the nill her diff load.	Contractor entry-control and diverses.	and the second s	whether a	##190.3#P.0	100100100100100	-
000-141-10 10 47 M	ATTACK MUSIC MUSIC BUT Portnas	among the best control of	www.	84100.00H	the two risks are rear	-
000.10110-10-40-87	ATTACK PROFILED BT CALAR	designation in the liter	-whitee	\$4100.000 N	110 100 100 100 100 100 100 100 100 100	- 40
mail, ratio and an arrise	Contractor preparative projection	(all styles) and (- water	84 (20.999.0	190 100 100 100 100	
100 110-1-0 tol #27-08	COLUMN ADD ADD DOUDED ADD PARAME.	and any data survivo	Market-	des retail cases et	190 190 100 INT 1400-	1.0
001.10.0710.0710.0	A LATTACE ADDRESS OF A LATER	Contraction and the	LANKS.	6-1 CTR 340 F	what A and Jump one under	1
100 - 10 - 10 - 10 - 47 - 10	ATTACK STRATE AND AND AND AND	Control and succession	description of the	And THUR SHOE IS	and the own on home	- 2
COLUMN THE REAL PROPERTY.	ATTACK PROPERTY AND AND AND	and southern and southern	-	All company to	THE R A. LOW CO. LOUGH	- 3
Nor on the line of the	A static metalogramit and house	Control of the local of	-	And store land \$1	dely dana page per sugar	1
and the set of the set of		and and a second second	a constant		about the paper and based	- 1
COLLEG DE LELAS AT		and the second second			190 100,000,000,000	
000.10.11.10.00.00	and a subsection of the second	Party and another	1001010	are reputered	TRO THE COLUMN ST SAME	
000.10-10.10.80.95	A PARTY OF PRIME NOTEST AND POLICIES	Sandora Bess denome	And a second	44.128.348.6	Los ten unit un biente	
000-100-100-000-335	A CONTRACT OF PROPERTY AND PARTICLE	Conceptual Statement	voted	# # 198 - 389 E	The last over the same	- 7
COLUMN HINK OF	The second	percentation of the	POPULA .	88134389.0	The first offer the little	-
Bath DO-Pill Hit all 26	LIFEATTACK PROPOSICELL ROLF HIME	American and an and an and an	199935	PR URB DITH B	132340.100.00.000	
005-1817-8 16 46 28	ATTACK PROPOSICIAL PET FOR LAKE	apprending the off	ANTE .	64188.796.0	TX2 144 101332 web	
105-10-XB 15-45-25	A NUMBER OF STREET, ST	ALL REPORT OF ALL REPORT	unado .	44138.349.9	182350-100,255-494	
005-16-10 10:45:23	CALIFORNIA CONTRACTOR AND ADDRESS	deservation and the	000043	AN COLUMN A	197110-10031-1408	-
005-12-20 10 48:13	CALATTICS ARTICLESS	officer wheel are used	should	66.110.349.0	1921100-1003-001-001	-
101,10,15 15 49-30	CALLER TACK PROPERTY AND TO COME	an a	chaires a	444 1989-2047-8	199 155.540 53 5 465	-
continents stillate en	A TATA TATA AND A PARTY AND A	attendent parter.	the area	en contantes	230-140-140-141-1400	
100.1010.0010.4610	CUPICAR Contant Topoten Salt	tandesetter. itst	CAN.	THE ARE NOT	101.01.46.03.461	1
101010-01010-0012	Chicken town makken impost one limit .	billion imp. Adv.	1,000	180.100.008.005	00.00.46 54 261	×
0001-10110-10146-008	CONTRACTORNAL DISCOURSE AND INCOMENTATION	Transford-Adapt.jean	640	192.188.039	0000.46.84.80.	×
000110-010-00-000	CP STOR FORE Garnet Bandf are first	0.00800148gp.3440	6.001	102180-008.02	TEL 40 AM TO BA	30
005.131.10.10.48.01	Distance lines thank which all	Concernance of	- Panchille	200300-200-1202	102 100 100 225445	×
and the side but was do.	Chargement of the Assess Later will be	100 C 10	al shakes	There is the state	and long time to be to be a	

Figure 19-10 Intrusion Detection and Prevention Daily Records

	IDP Report	Log
🏈 1	he symbols	refer to:

1. 【Action】:

Symbol	♠	Х
Description	Pass	Drop

2. 【Risk】:

Icon	0	· · · 🚺	
Description	High Risk	Medium Risk	Low Risk