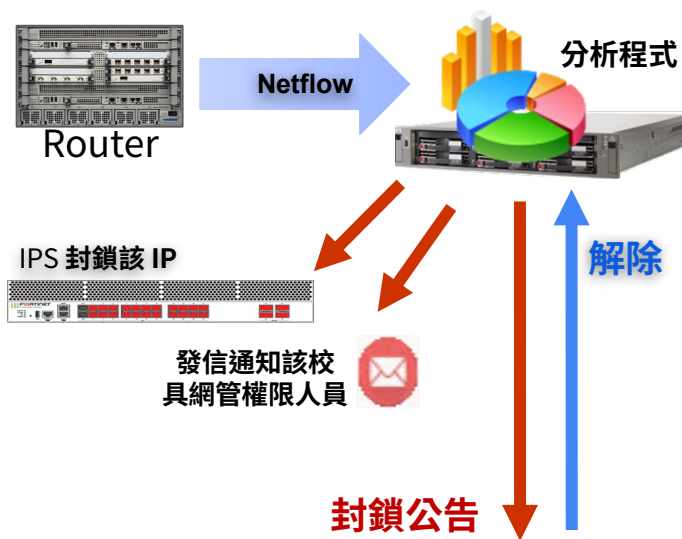


Netflow 流量分析封鎖機制

編號	名稱	已登錄服務之 IP flow 門檻值	未登錄服務之 IP flow 門檻值
1	SMTP-OVERFLOW	登記 SMTP 1000	100
2	SCAN-PORT-137-138-139	100	100
3	SCAN-PORT-445	100	100
4	SCAN-PORT-1434	100	100
5	MSBLAST	5000	1000
6	SCAN-PORT-SSH	500	200
7	企圖登入教網主機	9	9
8	IRC-BOTNET	X	X
9	SSLVPN10443	X	X
10	OVERFLOW	30000	5000

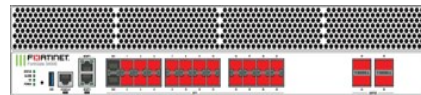


解決問題後，再至教育服務網→網路管理專區
 →網路管理系統解除封鎖
 ※ 具網管權限人員，使用公務帳號解除

序	學校名稱	限制IP	限制型態	流量	發現時間	距今	管理
1	臺中市立第一高級中學	192.168.1.1	[IPS]Malware.Sinkhole	1	2024-05-15 19:34:23	0.54	解除
2	臺中市立第一高級中學	192.168.1.72	[IPS]Malware.Sinkhole	10	2024-05-15 15:32:24	0.71	解除
3	臺中市立第一高級中學	219.141.1.1	SCAN-PORT-445	22647	2024-05-15 11:12:18	0.89	解除

進階防護 -IPS 封鎖機制

	偵測時間段	發現異常行為時
已登錄服務之 IP	AM 00:00~AM 06:00 及 PM 20:00~PM 24:00	立即封鎖該 IP ，並發通知信。
	AM 06:01 ~ PM 19:59	系統先記錄該 IP 的異常行為， 不立即進行封鎖 。當日晚上八點，封鎖該 IP ，並發信通知。
未登錄服務之 IP	全日 24 小時	立即封鎖該 IP ，並發通知信。



IPS

日誌資料



分析程式

限制型態	流量	發現時間
[IPS]Salinity.Botnet	1	2024-05-23 07:06:58
[IPS]Malware.Sinkhole	3	2024-05-23 02:07:26

通知信範例

網管人員 老師:
您好! <<此為系統自動發信, 請勿直接回覆此信>>
貴單位 IP=1
被偵測出符合特徵之異常連線封包傳送, 為不影響網路正常運作, 故暫停此IP上網權利。
限制型態: [IPS]Stealc.Botnet
發現時間: 2024- 1 :6
參考資料: <http://www.fortinet.com/ids/VID54535>
煩請予以檢查並消除流量異常的問題後至教育服務網 <https://service.tc.edu.tw/network/network-netflow> 解除限制。

若有問題, 可連絡 資網中心網路機電組 協助處理。
臺中市資網中心 網路機電組 TEL: 04-23952340 nc.net@tc.edu.tw

IPS log message
profile= "Main-IPS"
crlevel= "high"
date= 2024-05
hostname= "5"
policyid= 319
subtype= "ips"
url= "/129edec4272dc2c8.php"
pri= 185
proto= 6
dstip= 9 5
dstintrole= "undefined"
ref= "<http://www.fortinet.com/ids/VID54535>"

Ncloud 查找

3

網管人員 老師:
您好! <<此為系統自動發信, 請勿直接回覆此信>>
貴單位 IP=1
被偵測出符合特徵之異常連線封包傳送, 為不影響網路正常運作, 故暫停此IP上網權利。
限制型態: [IPS]Stealc.Botnet
發現時間: 2024- 1 :6
參考資料: <http://www.fortinet.com/ids/V>
煩請予以檢查並消除流量異常的問題後
若有問題, 可連絡 資網中心網路機
臺中市資網中心 網

IPS log message
profile= "Main-IPS"
crlevel= "high"
date= 2024-05
hostname= "5"
policyid= 319
subtype= "ips"
url= "/129edec427dc2c8.php"
pri= 185
proto= 6
dstip= 9 5
dstintfrole= "undefined"

5

1 事件查詢

2 Syslog

4 選擇【學校防火牆】及【FortiGate-3401E-IPS】

5 將【dstip】設定為目的 IP

3 建議設前後 5 分鐘

模擬畫面

Home / 事件 / 事件查詢

事件查詢

+ 查詢條件 田 進階條件 刷新 歷史記錄 啟動查詢

報表製作依據

設備 事件關鍵字

IP 過濾 IP 過濾 - 來源 IP IP 過濾 - 目的 IP

Port 過濾

動態欄位顯示: /

查詢條件

請選擇查詢條件

起始時間 2024/05/21 18:50:00

結束時間 2024/05/22 18:50:00

OK

查找結果

事件查詢

自動更新

OFF

+ 查詢條件

田 進階條件

↺ 重新輸入

📜 歷史記錄

🔍 啟動查詢

報表製作依據

☒ Syslog

☐ Flow

查詢時間區段

☐ 選擇時間區段

5分鐘內

☐ 過去

☒ 起迄時間

2024/

動態欄位顯示: Auto

設備: 國小 - fortigate 100F [140. .254], 國小 - FortiGate-3401E-IPS] ✕

目的 IP: 34.218.204.173 ✕

查詢條件

請選擇查詢條件

資料時間範圍: 2024/ 總筆數: 3

時間	設備	等級	事件	來源 IP	目的 IP	來源 Po	目的 Po	來源 IP 名稱	目的 IP 名稱	來源區	目的區	動作	Hit	事件型	協定	Bytes	Pac	NAT 來源 IP	NAT 來源 Po	流入介面	流出介面	Policy	Session ID	Source	來源 MAC
2024-11-14 14:11:00	fortigate 100F	Notice		192.168.1.2	34.218.204.173	50008	80		Amazon	(其他)	US (美國)	Permit	1	traffic	TCP	367/216	4/4	140.239.139.50008				254		1	4C:81:04
2024-11-14 14:11:00	FortiGate-3401E-IPS	Notice		140.239.139.1	34.218.204.173	50008	80		Amazon	TW (臺灣)	US (美國)	Permit	1	traffic	TCP	303/164	3/3		-			148		8 1	
2024-11-14 14:11:00	FortiGate-3401E-IPS	High	attack=Malware.Sir hostname=mobiles attackid=46581. backdoor: Malware Sinkhole	140.239.139.1	34.218.204.173	50008	80		Amazon	TW (臺灣)	US (美國)	Permit	1	ips	TCP	0	0		-			148		8 1	

可疑設備