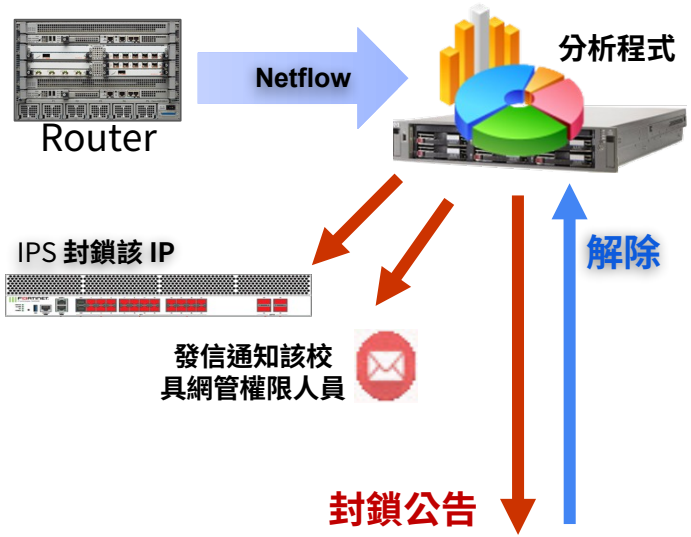
Netflow 流量分析封鎖機制

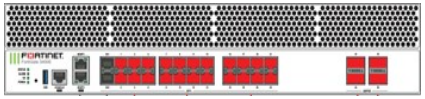
編號	名稱	已登錄服務之 IP flow 門檻值	未登錄服務之 IP flow 門檻值
1	SMTP-OVERFLOW	登記 SMTP 1000	100
2	SCAN-PORT-137-138-139	100	100
3	SCAN-PORT-445	100	100
4	SCAN-PORT-1434	100	100
5	MSBLAST	5000	1000
6	SCAN-PORT-SSH	500	200
7	企圖登入教網主機	9	9
8	IRC-BOTNET	X	X
9	SSLVPN10443	X	X
10	OVERFLOW	30000	5000



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

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]Sality.Botnet	1	2024-05-23 07:06:58
[IPS]Malware.Sinkhole	3	2024-05-23 02:07:26

臺中市政府教育局
Education Bureau, Taichung City Government

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= 5

dstintfrole= "undefined"

臺中市政府教育局
Education Bureau, Taichung City Government

Ncloud 查找

臺中市政府教育局
Education Bureau, Taichung City Government

查找結果