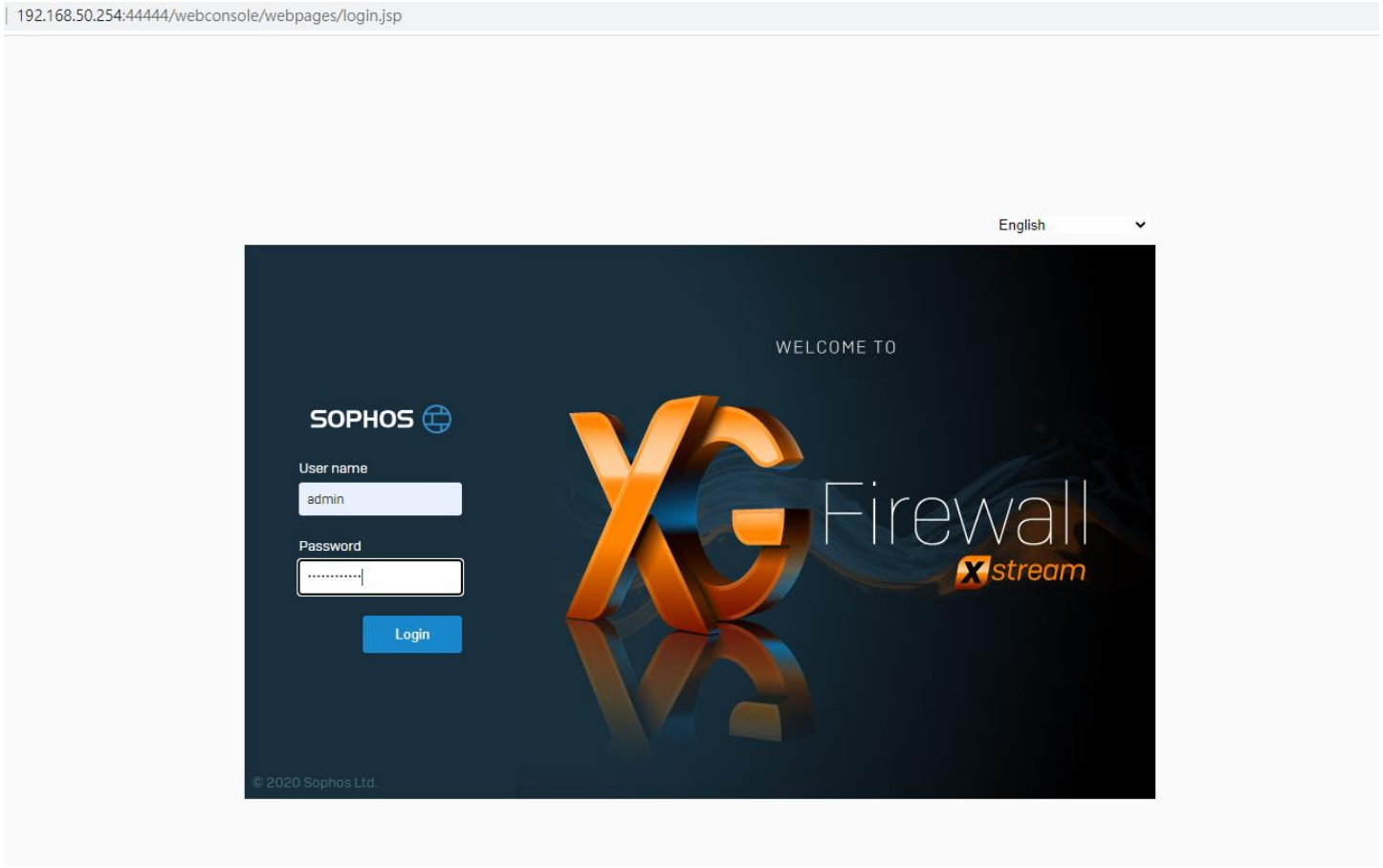
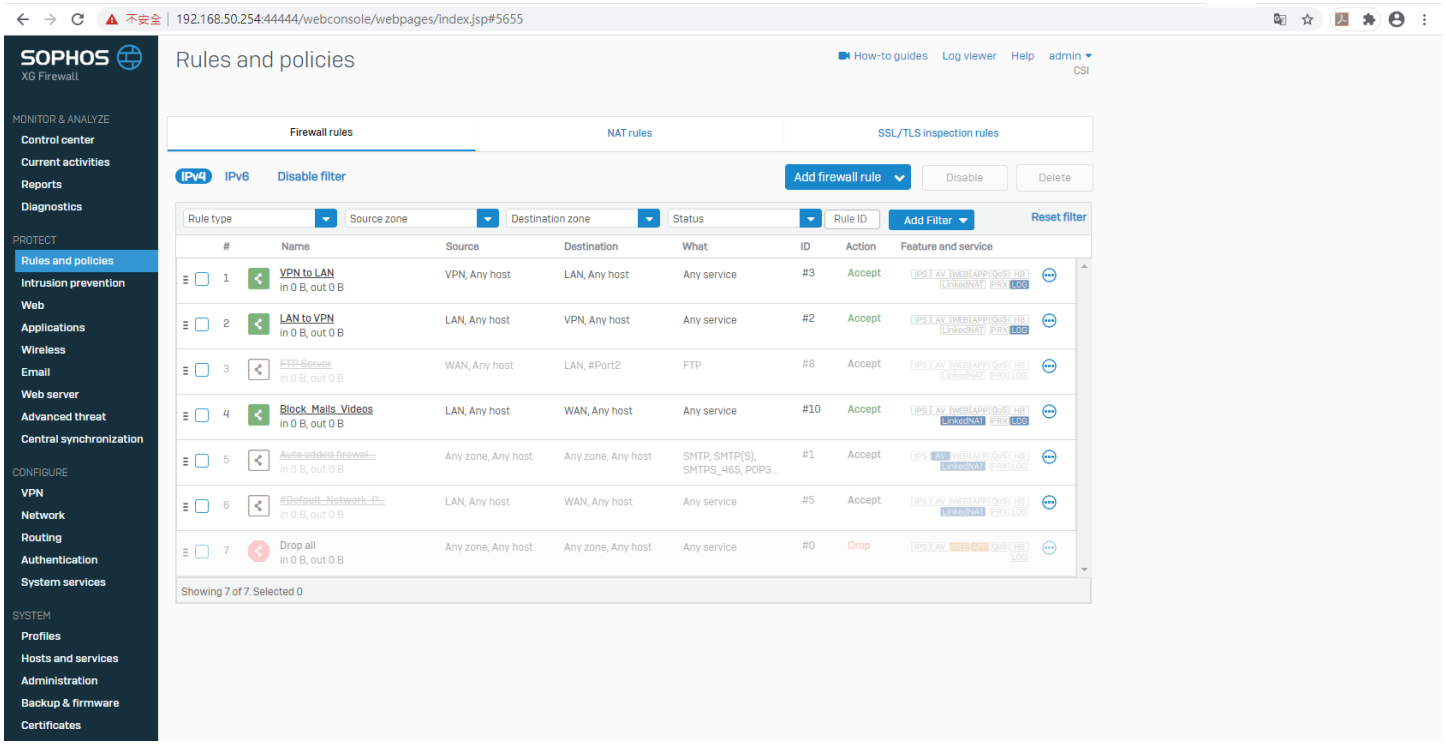
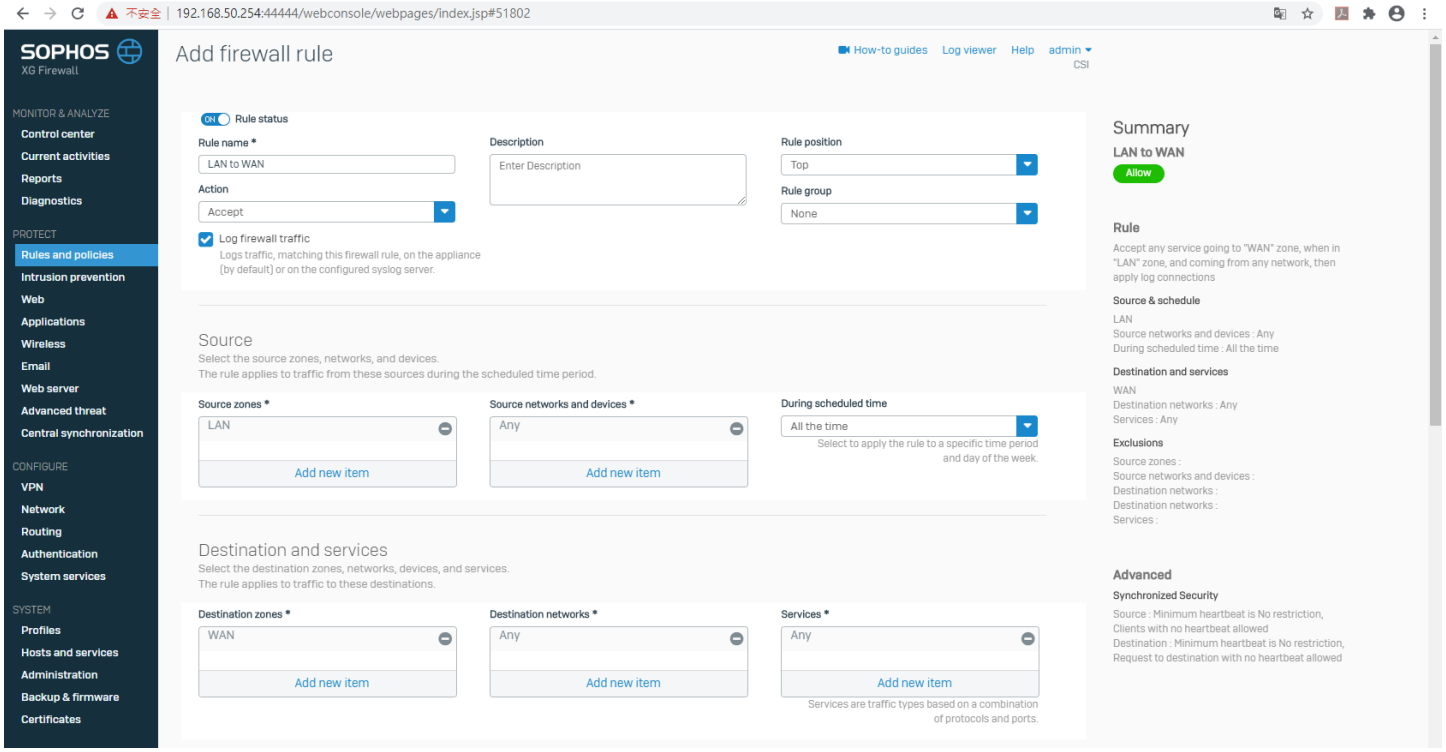
SOPHOS SW-18.0.1_MR-1-Build396.SFW-396



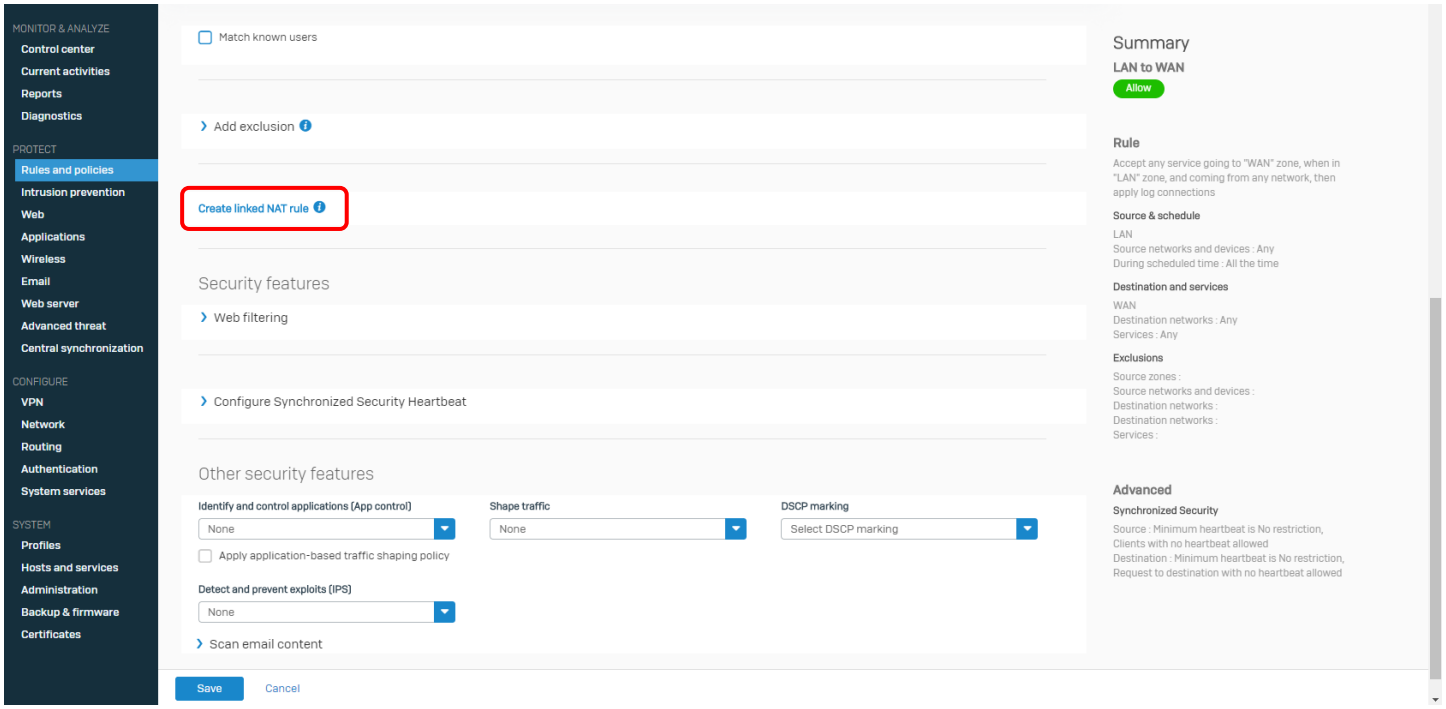
比較重要的就是 Rules 跟 Network 介面的設定，Rules 基本上比較常用到 Firewall rules 跟 NAT rules 頁面，



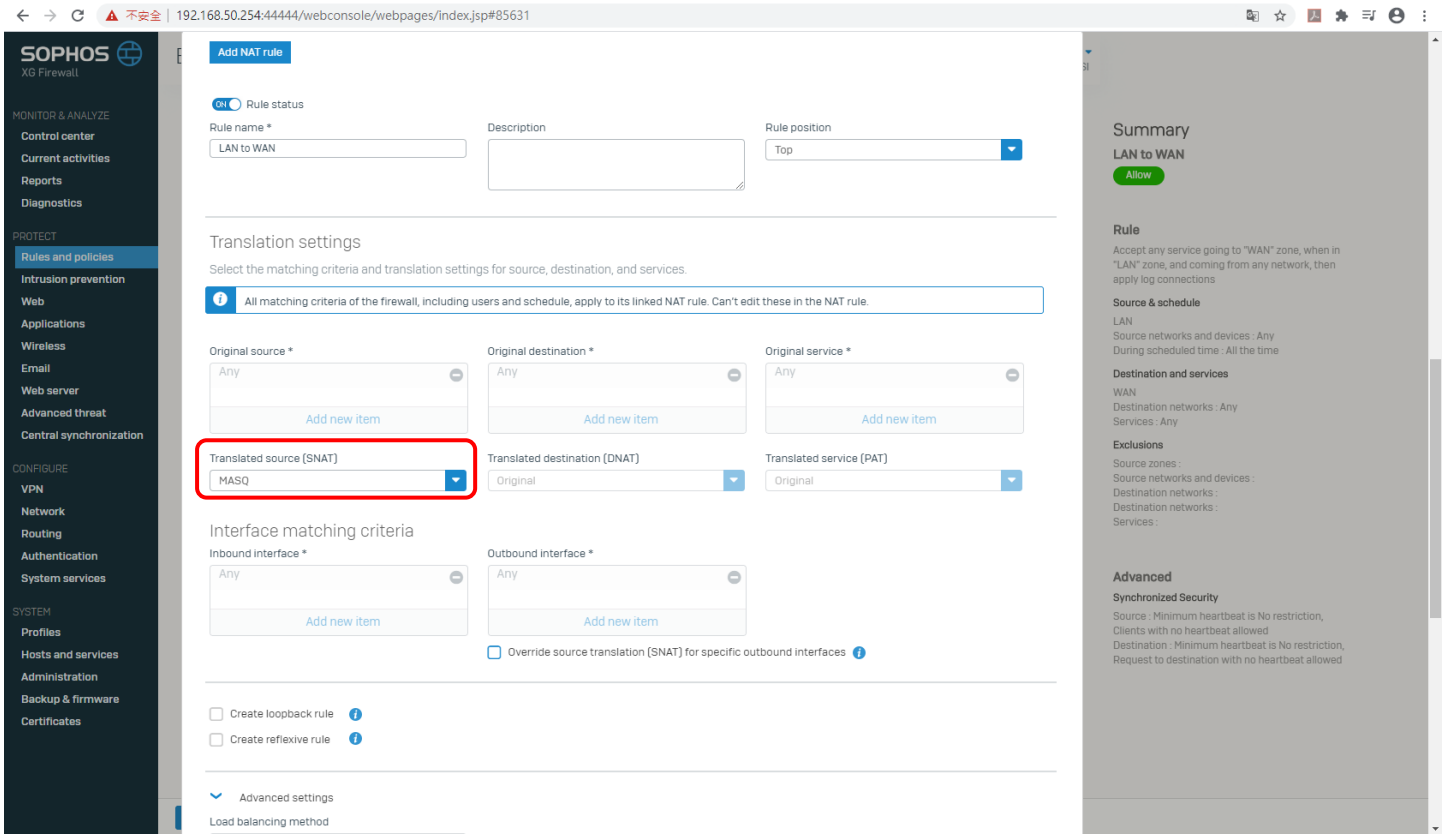
試著新增一般 LAN to WAN 方向，上半部設定沒有太大的問題



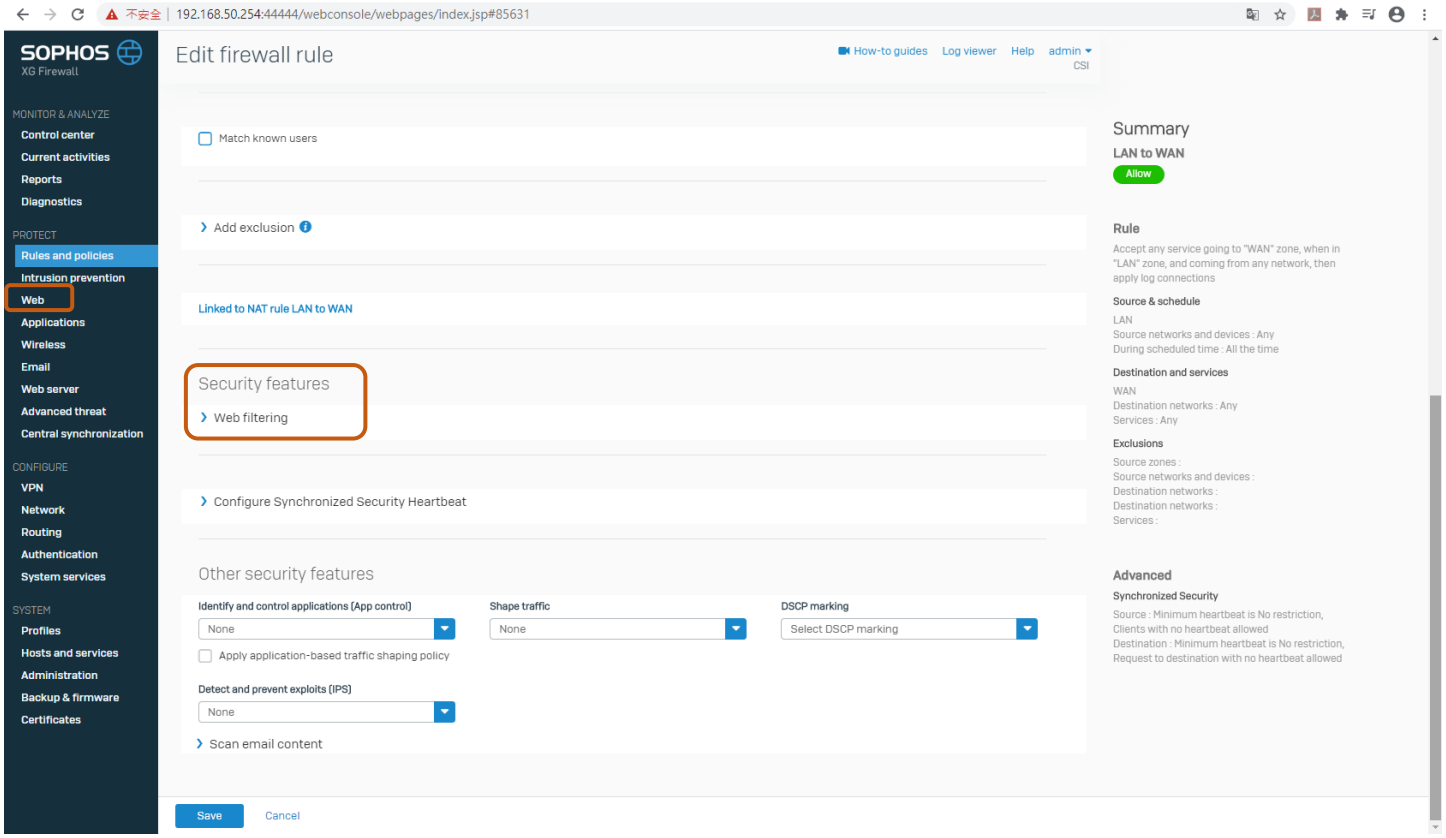
但是下半部有個需要注意的地方，Create Linked NAT rule 裡面還需要設定，點擊它，



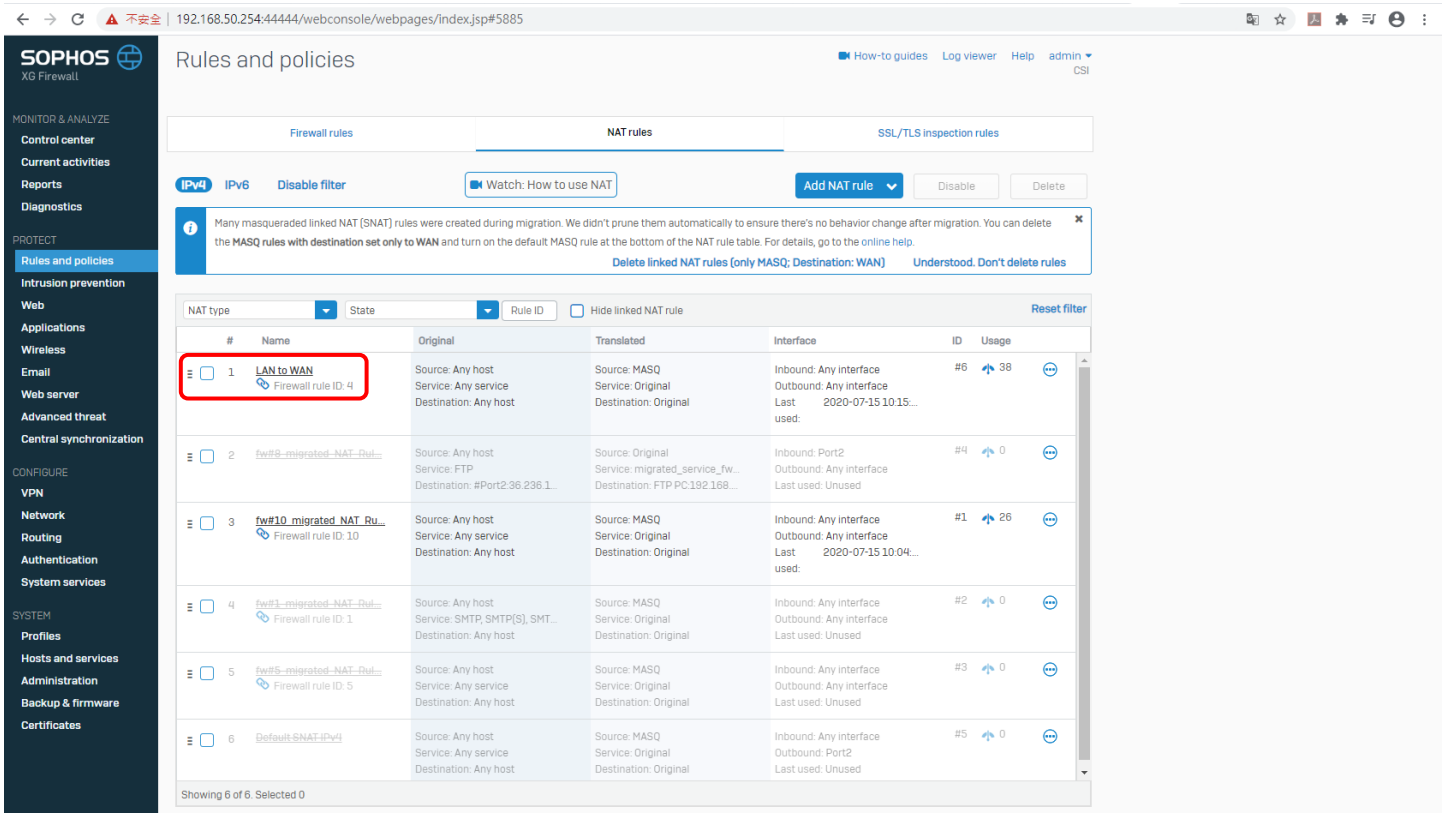
會出現新視窗，SNAT 要選擇 MASQ，接著按 Save，



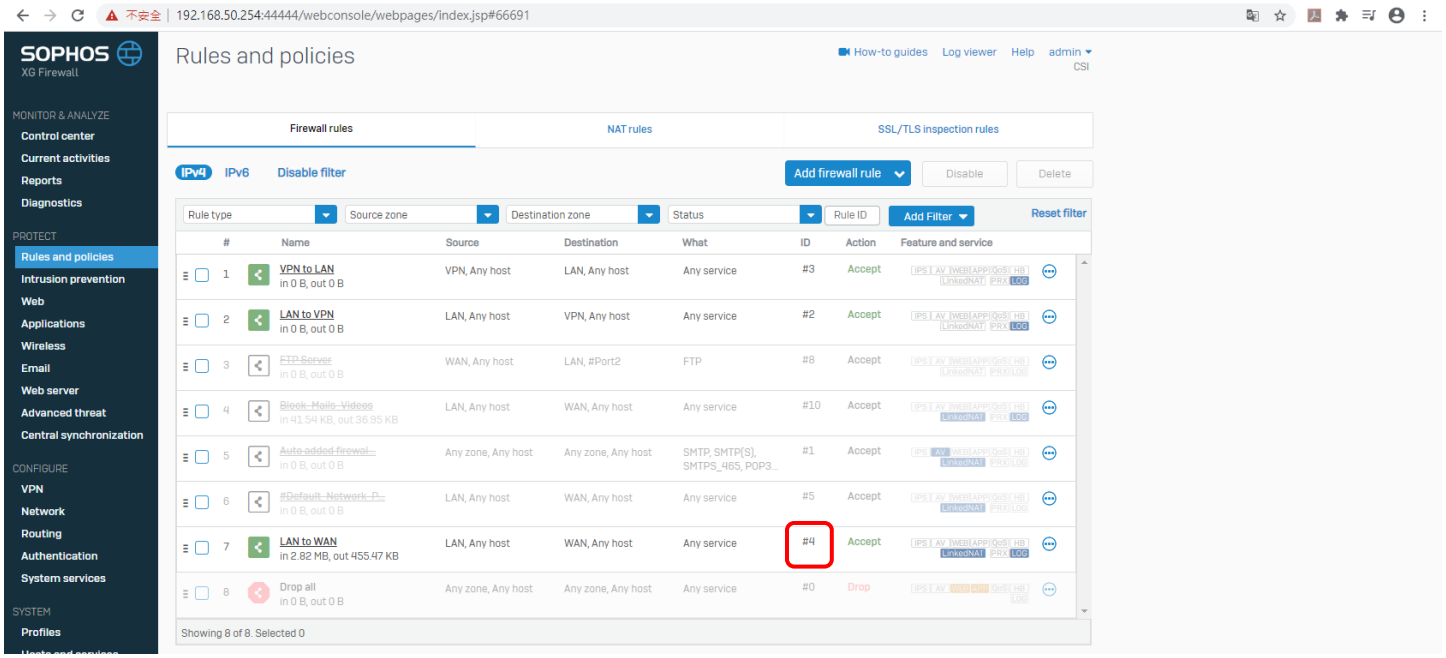
回到這畫面後再按 Save，這樣就能上網了，如果有網頁限制(譬如禁止上 Yahoo 網站)，就需要用到 Web Filtering 的地方，前提還是要到 Web 項目先做一些篩選，



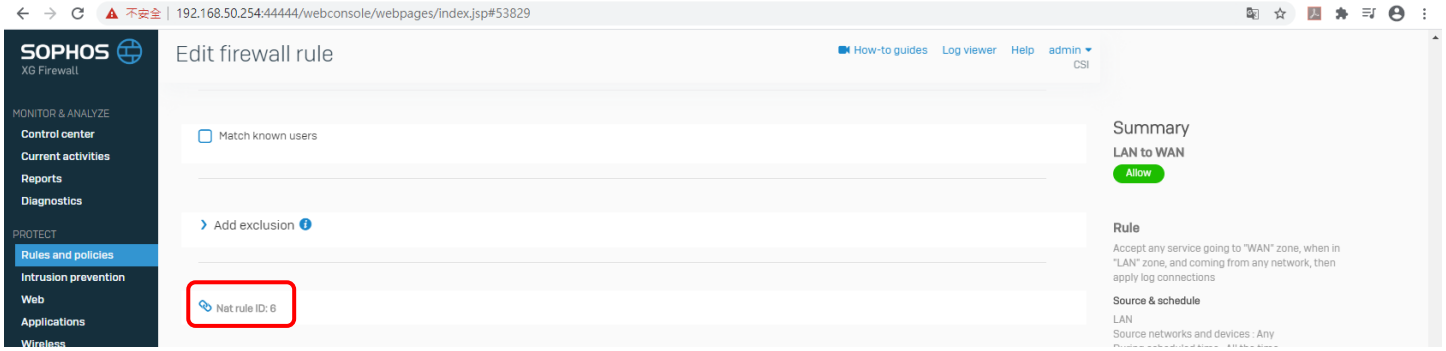
到 NAT rules 頁面會看到一條 LAN to WAN 就是剛剛新增的該規則下方有個 Firewall rule ID：4



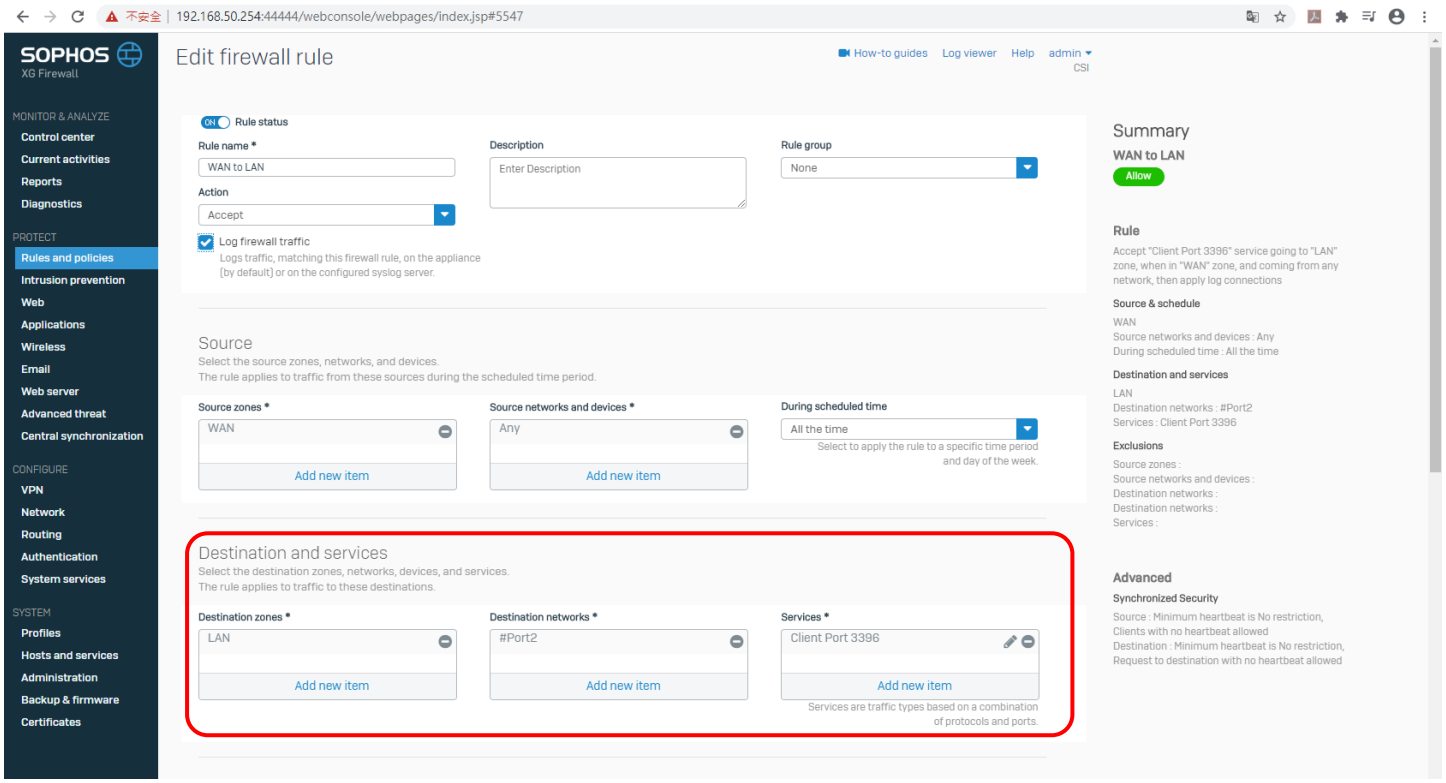
剛好就是對應 LAN to WAN，



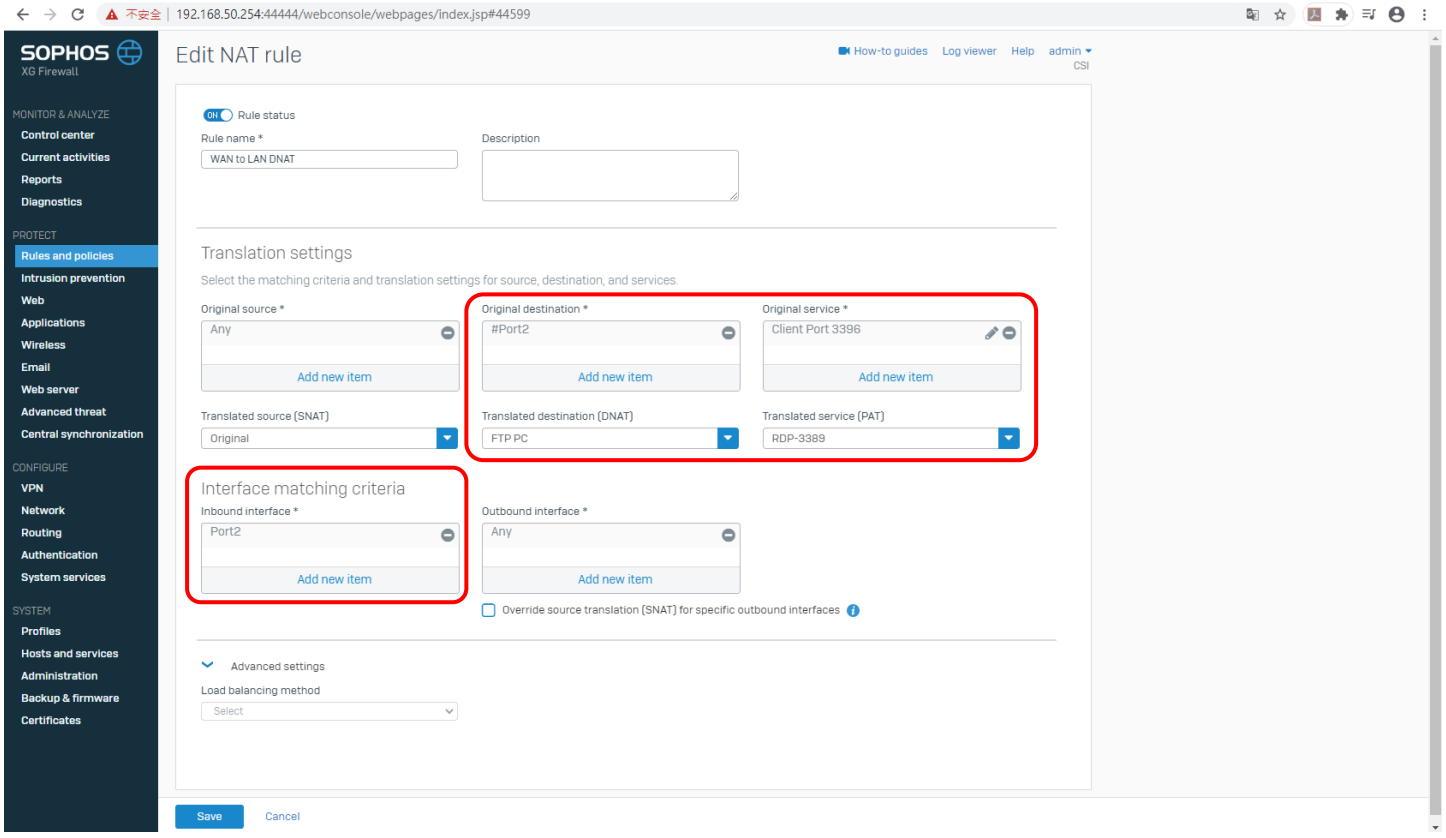
而且一旦新增是無法替換 NAT rules 的，LAN to WAN 是套 NAT rule ID：6，



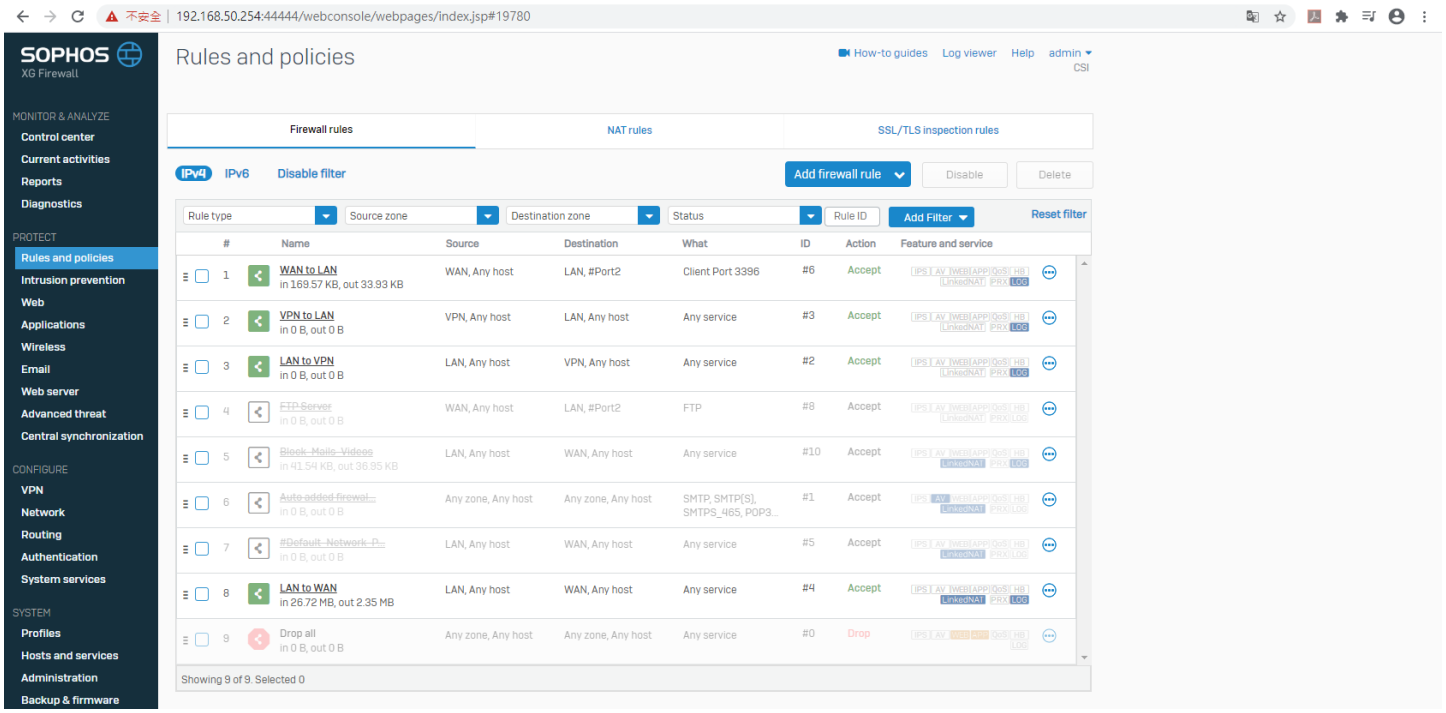
接著是一樣很重要的 WAN to LAN 設定，先在 Firewall rules 頁面，新增 WAN to LAN 規則，注意 Destination zones 選 LAN，但 Destination Networks 還是選 WAN IP，使用的 Port 為 3396。
這邊覺得這次的 v.18 版本把 Firewall 明確分成外內兩道牆(Firewall rule 頁面跟 NAT rule 頁面)，這樣內外要分別設定。



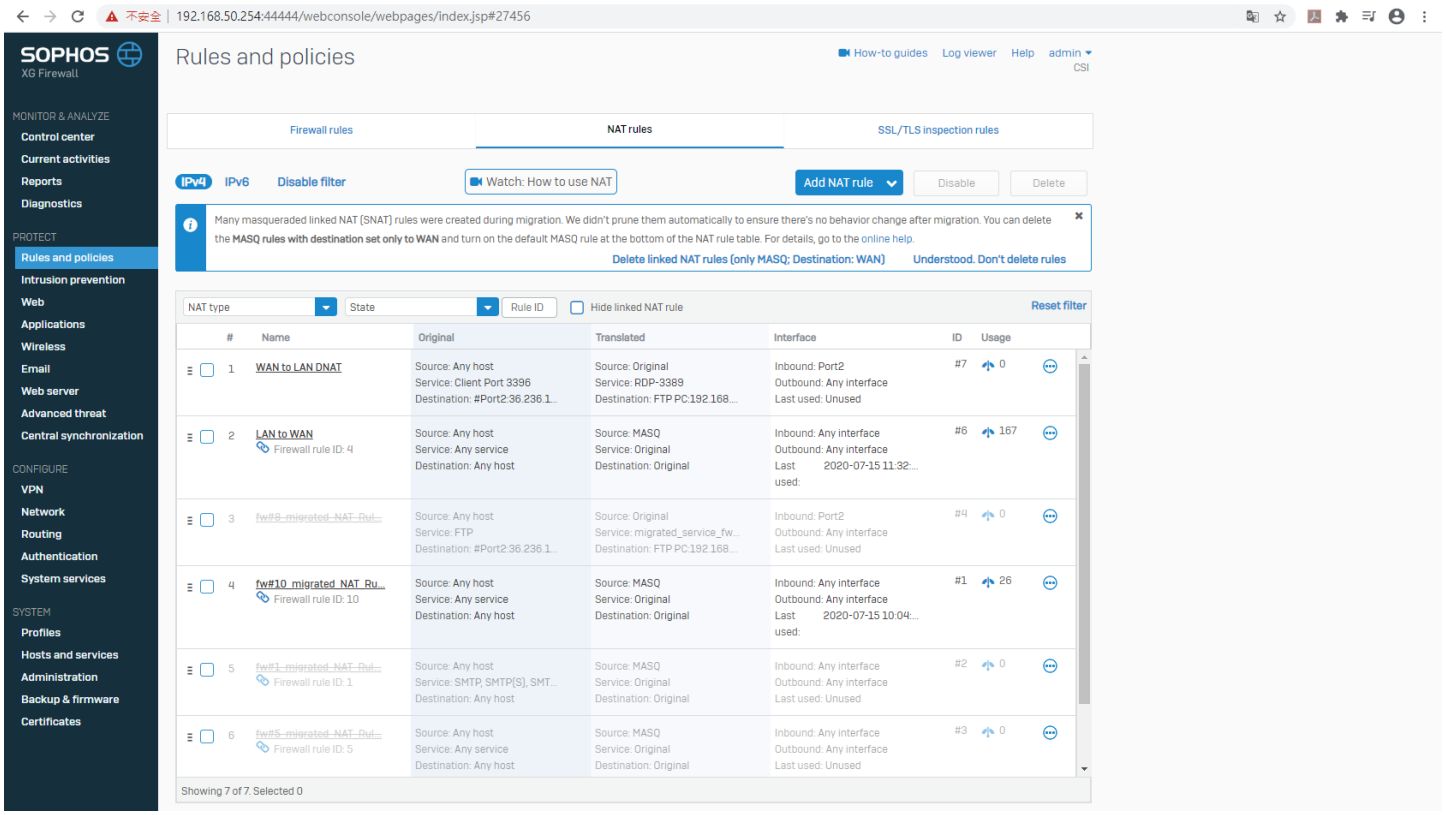
接著到 NAT rules 新增設定 DNAT，如下圖填寫資料，這樣就能用遠端桌面功能登入 FTP PC 了。



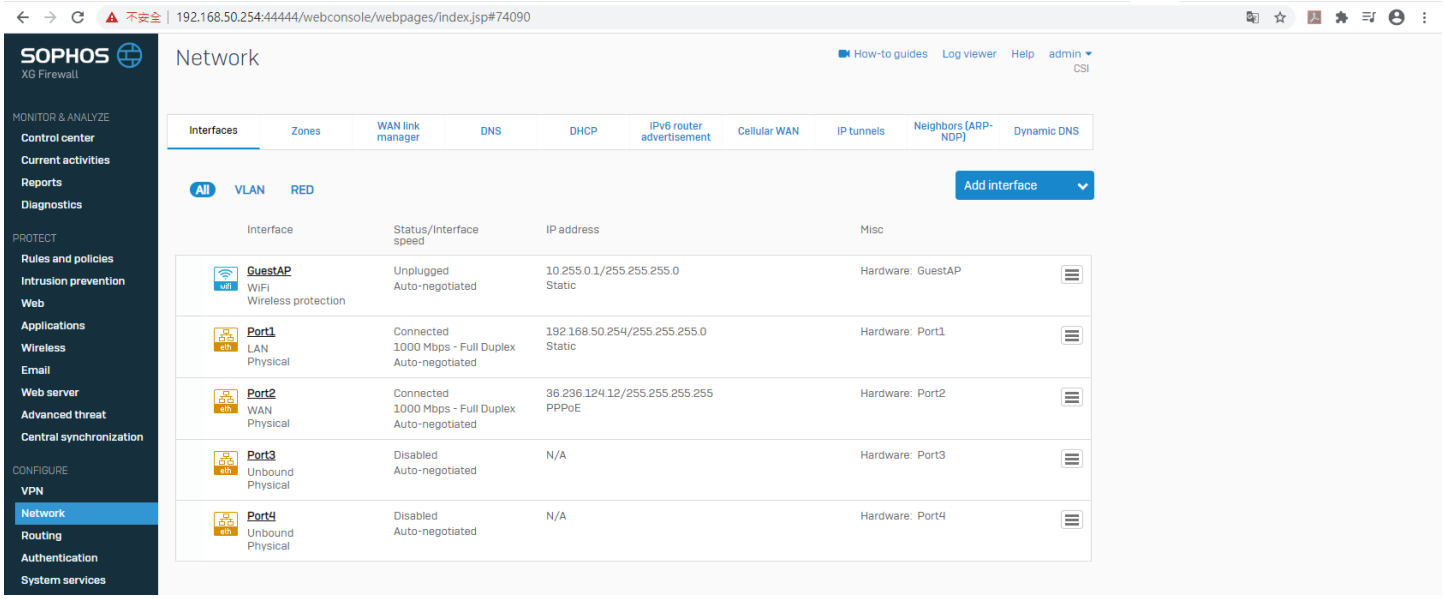
新增完 LAN to WAN 跟 WAN to LAN 規則後的 Firewall rules 畫面，



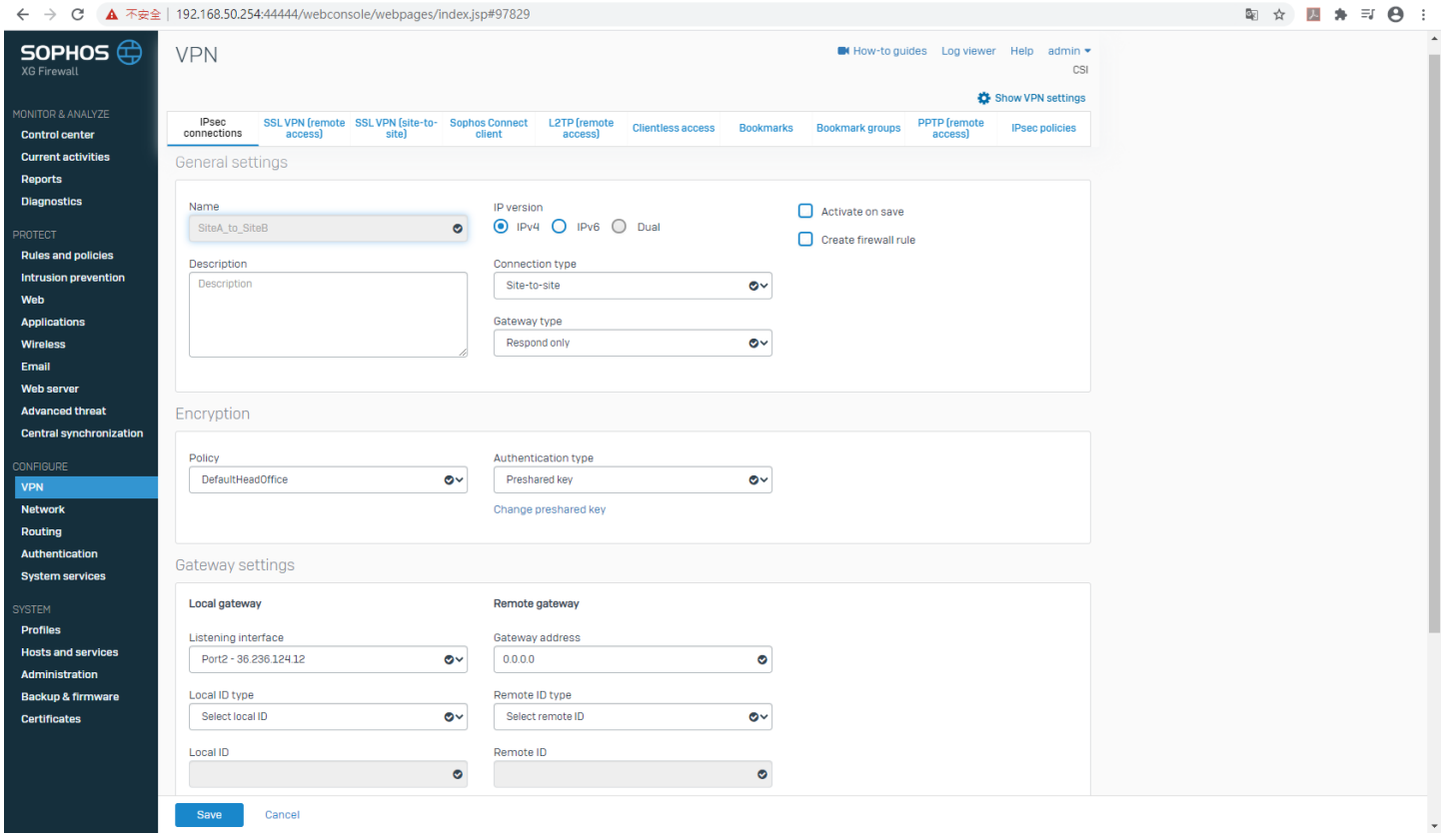
新增完 LAN to WAN 跟 WAN to LAN 規則後的 NAT rules 畫面



Network 介面沒多大改動，



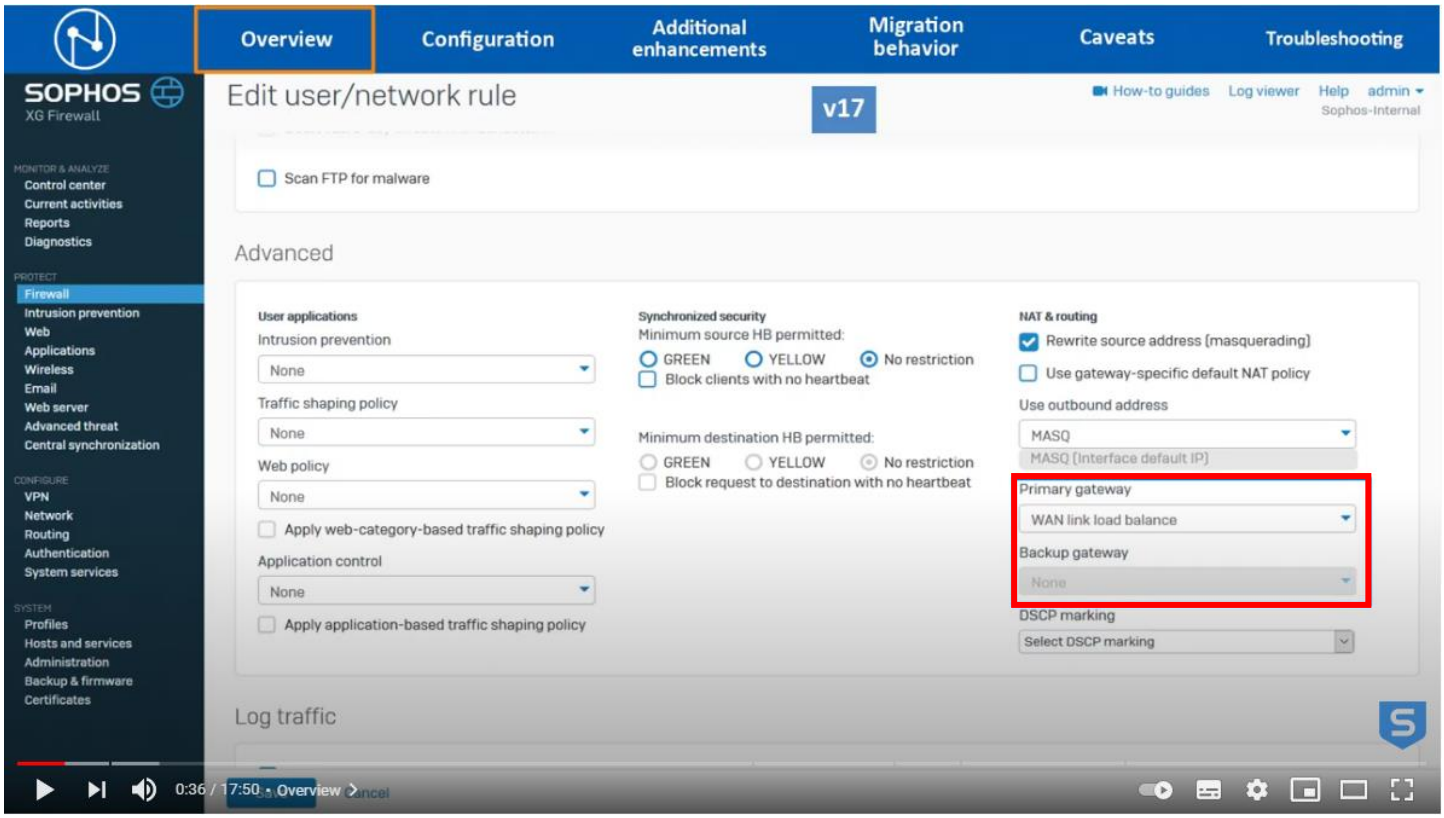
IPsec VPN 也沒改變，



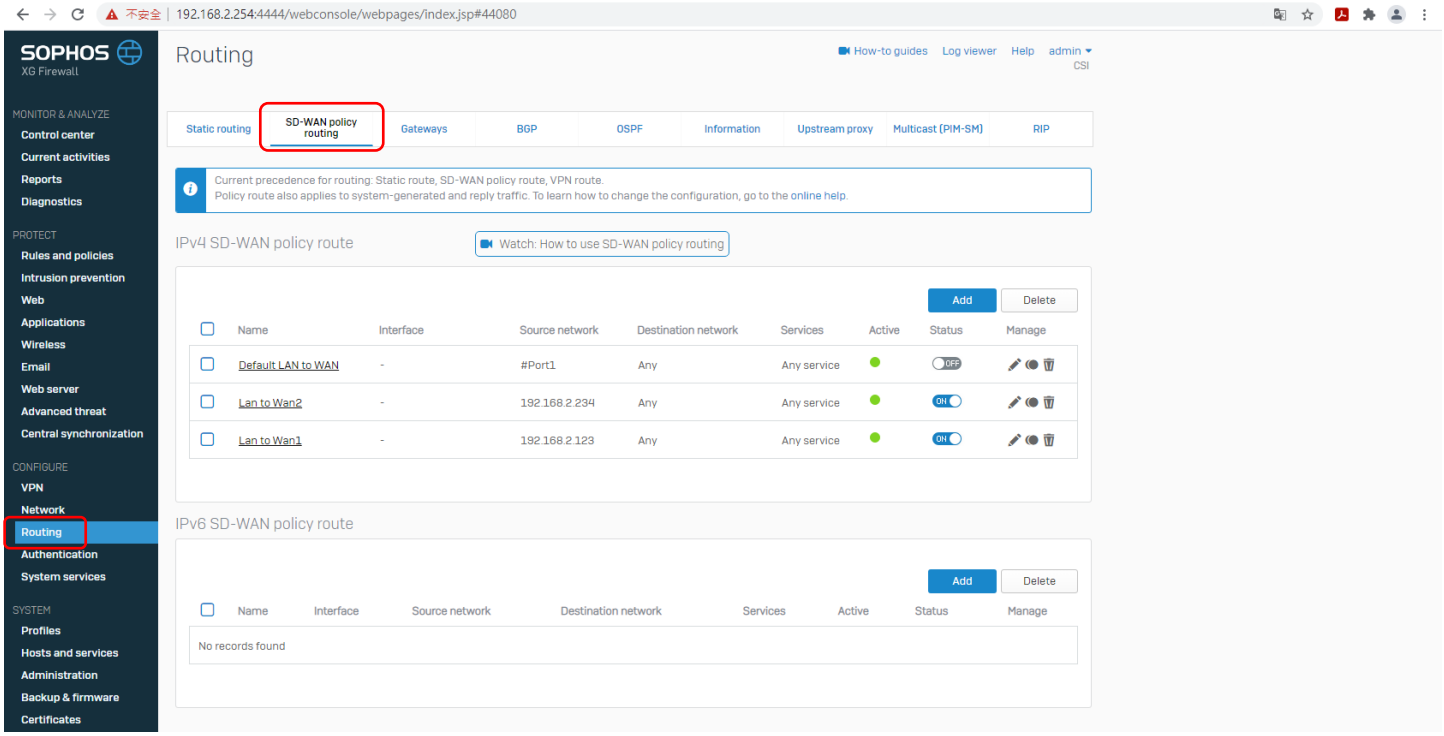
基本上大概就是 Rules and policies(原本的 Firewall)的設定要慢慢摸索，

==========2021.6.16==========

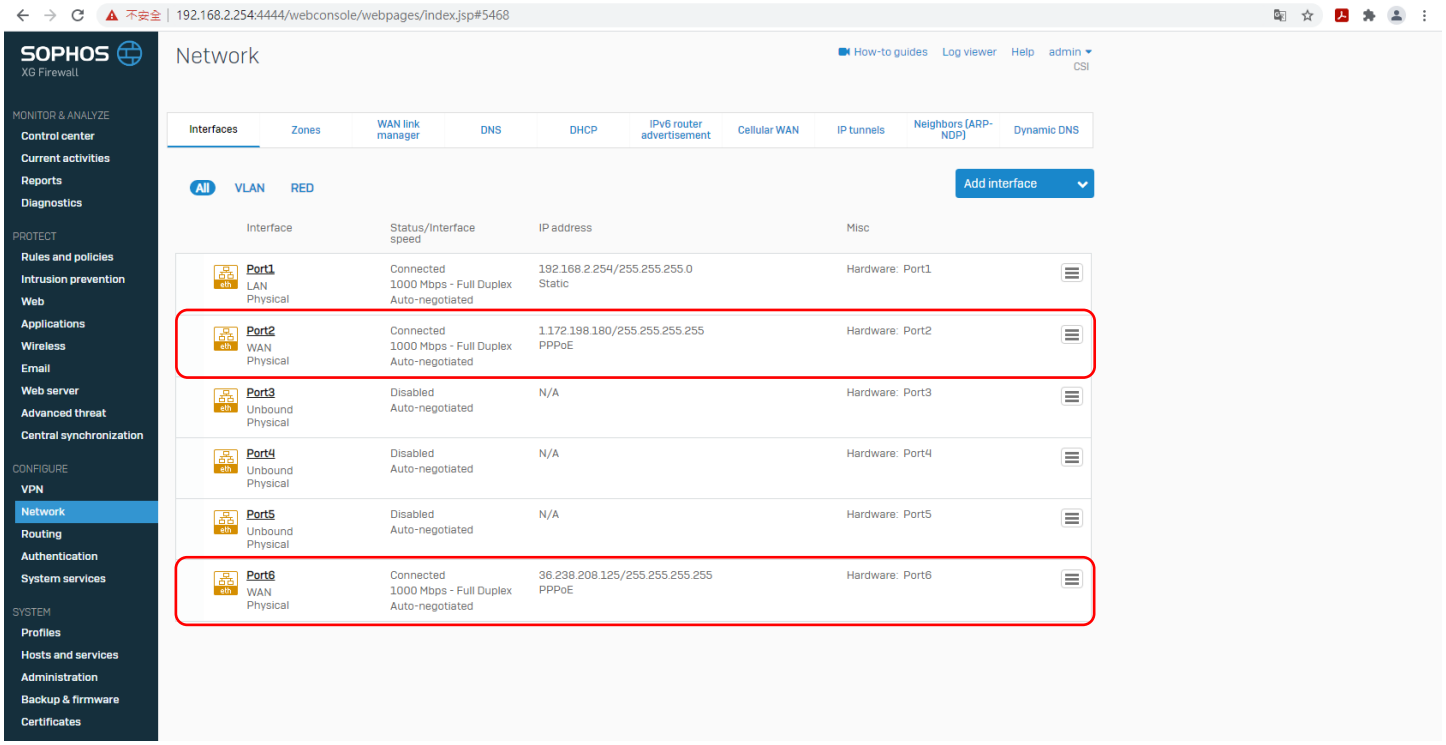
v18 有個項目跟 v17 非常不一樣，Primary gateway 跟 Backup gateway 要到其他地方設定，參考影片：
https://www.youtube.com/watch?v=TolZsFNbBuM，



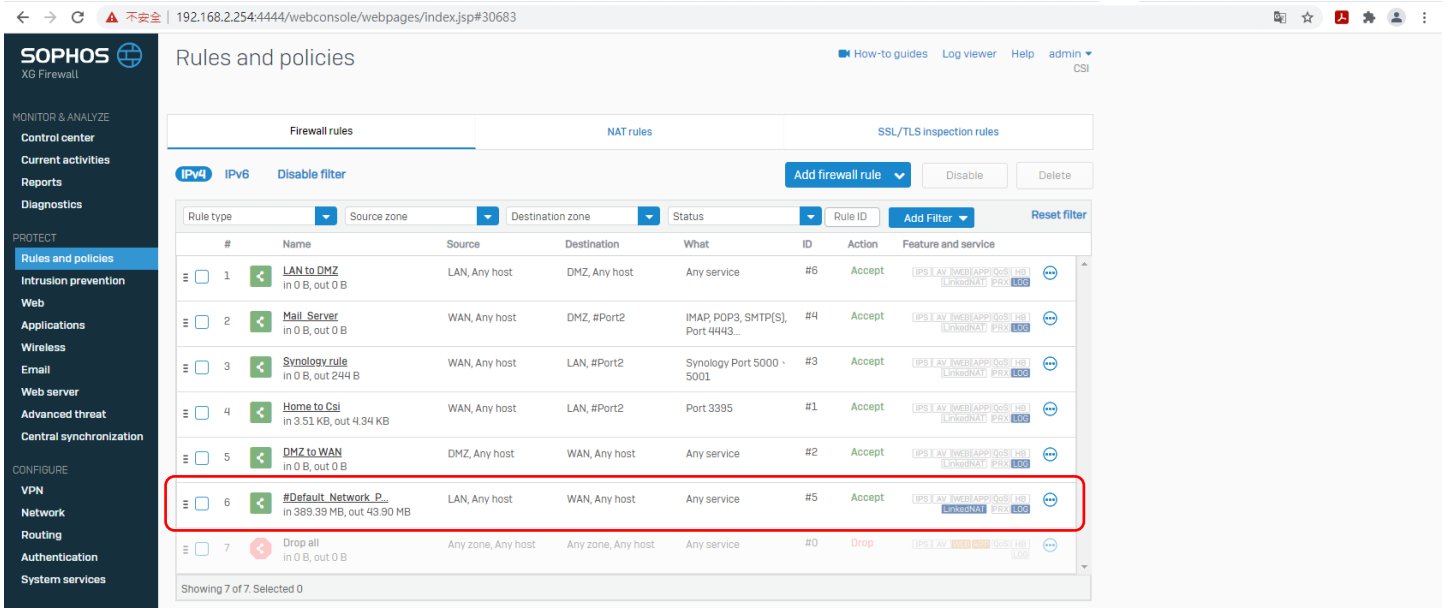
v18 要到 Routing 項目中的 SD-WAN policy routing 新增 IPv4 SD-WAN policy route，



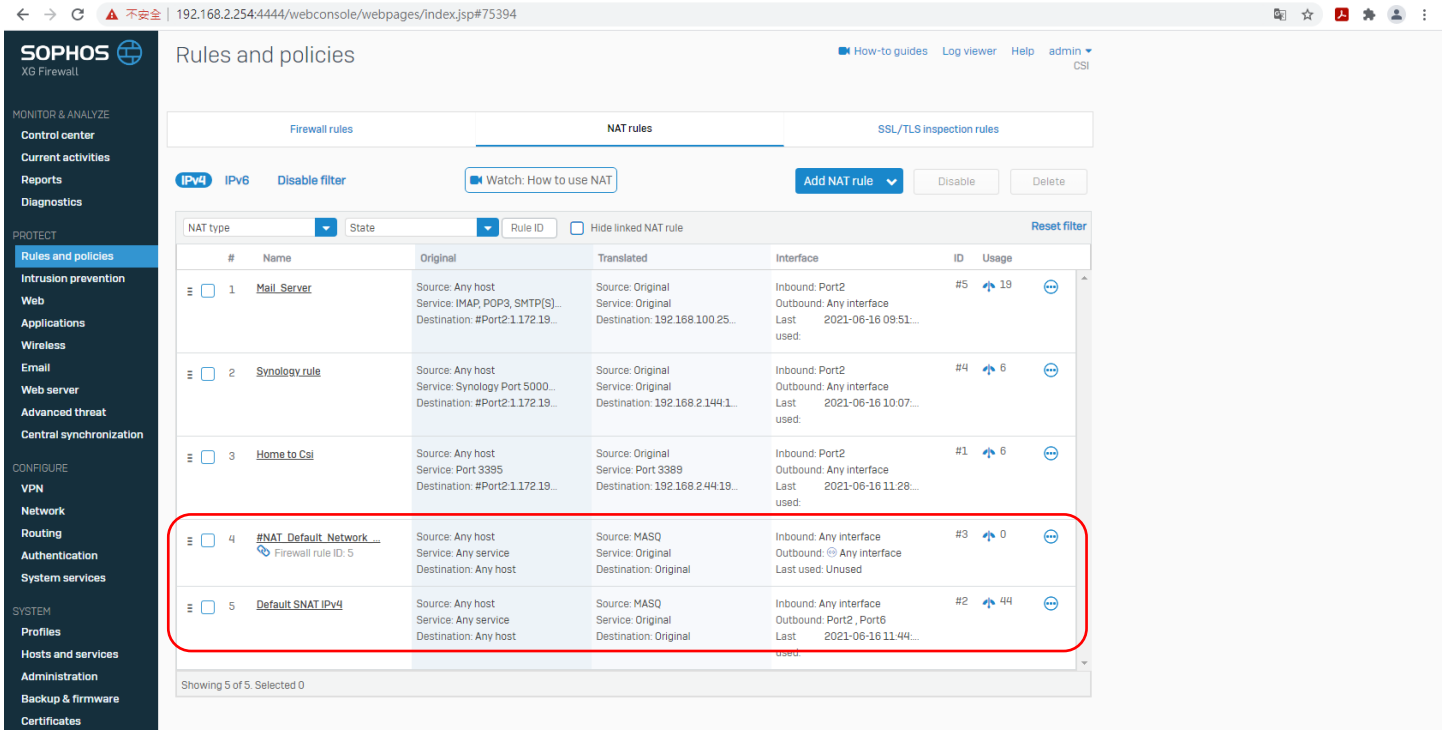
這邊做個小測試，準備兩個 WAN port(下圖中的 Port 2、6)，因為照影片中這樣設定，是不是不用設定 NAT rule 也能連上外網，



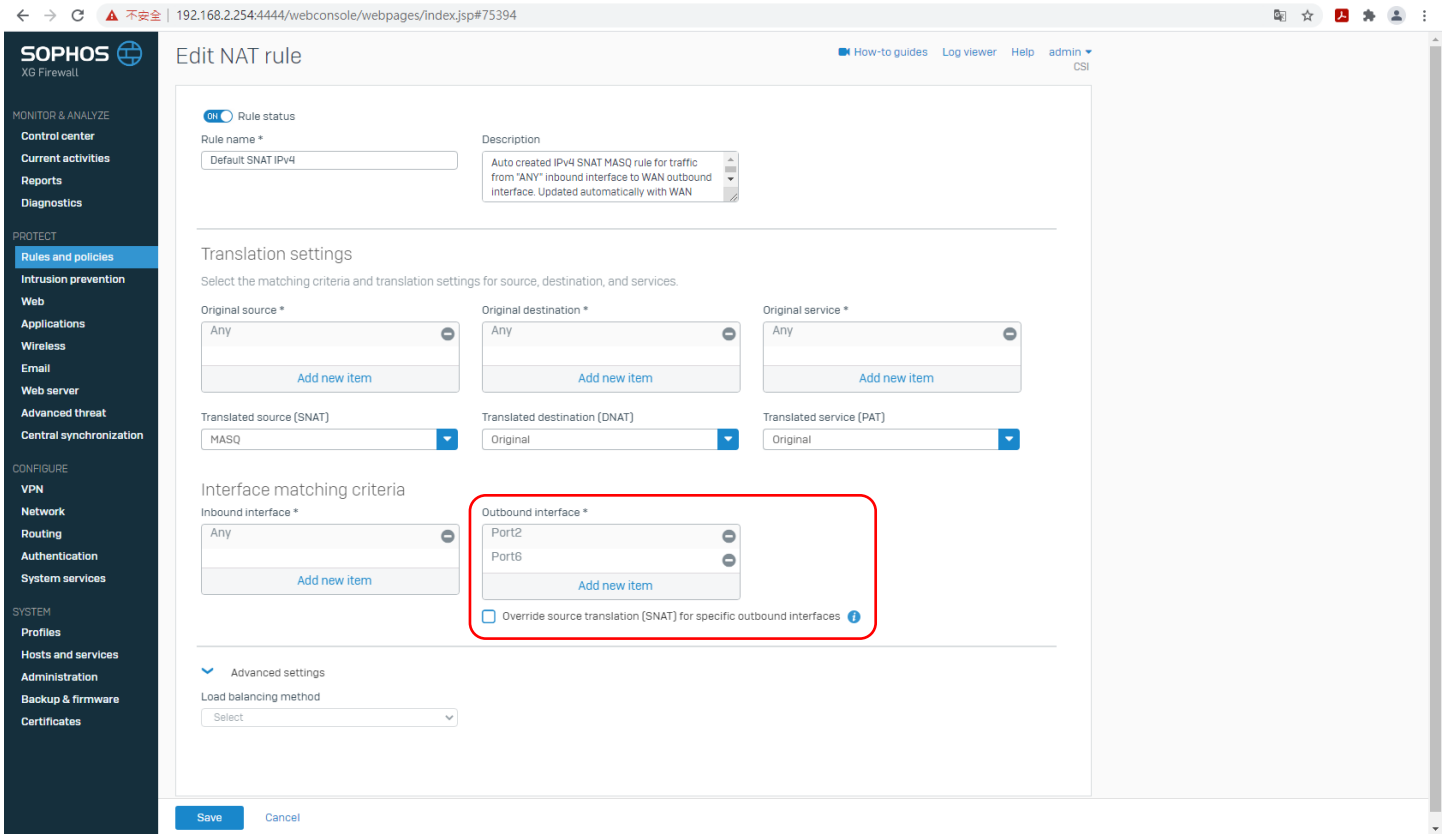
Firewall rule 當然有個 LAN to WAN(下圖中的#Default_Network_Policy)的規則，該 Firewall rule ID：5，



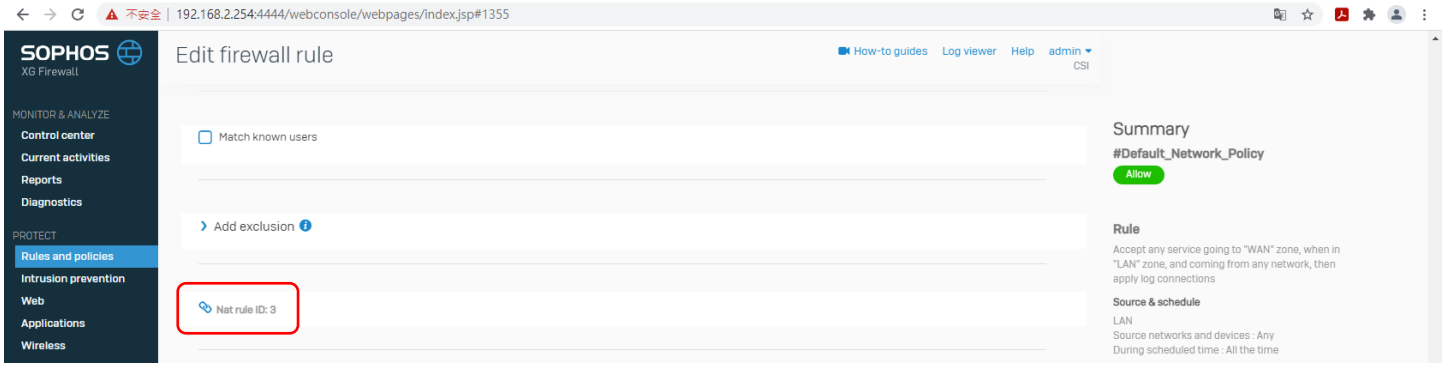
Firewall rule 要連到外網基本上需要搭配 NAT rule，而下圖中可以給#Default_Network_Policy 配合的 NAT rule 有 Default SNAT IPv4 跟#NAT_Default_Network_Policy，

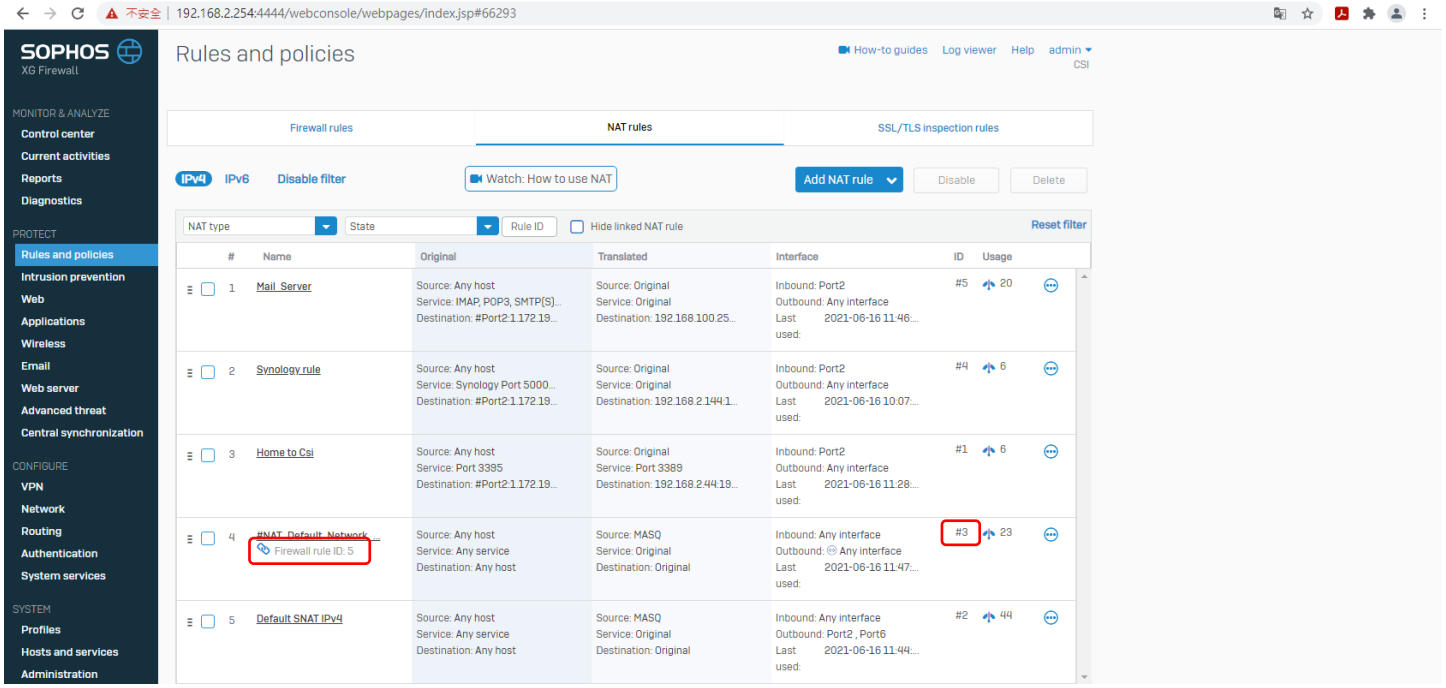


Default SNAT IPv4 是預設的 NAT rule，安裝好 v18 就會自動生成，而且它的 Outbound interface 可以手動調整(其實只要在 Network 新增 WAN port 系統都會幫忙加入新的 Port)，

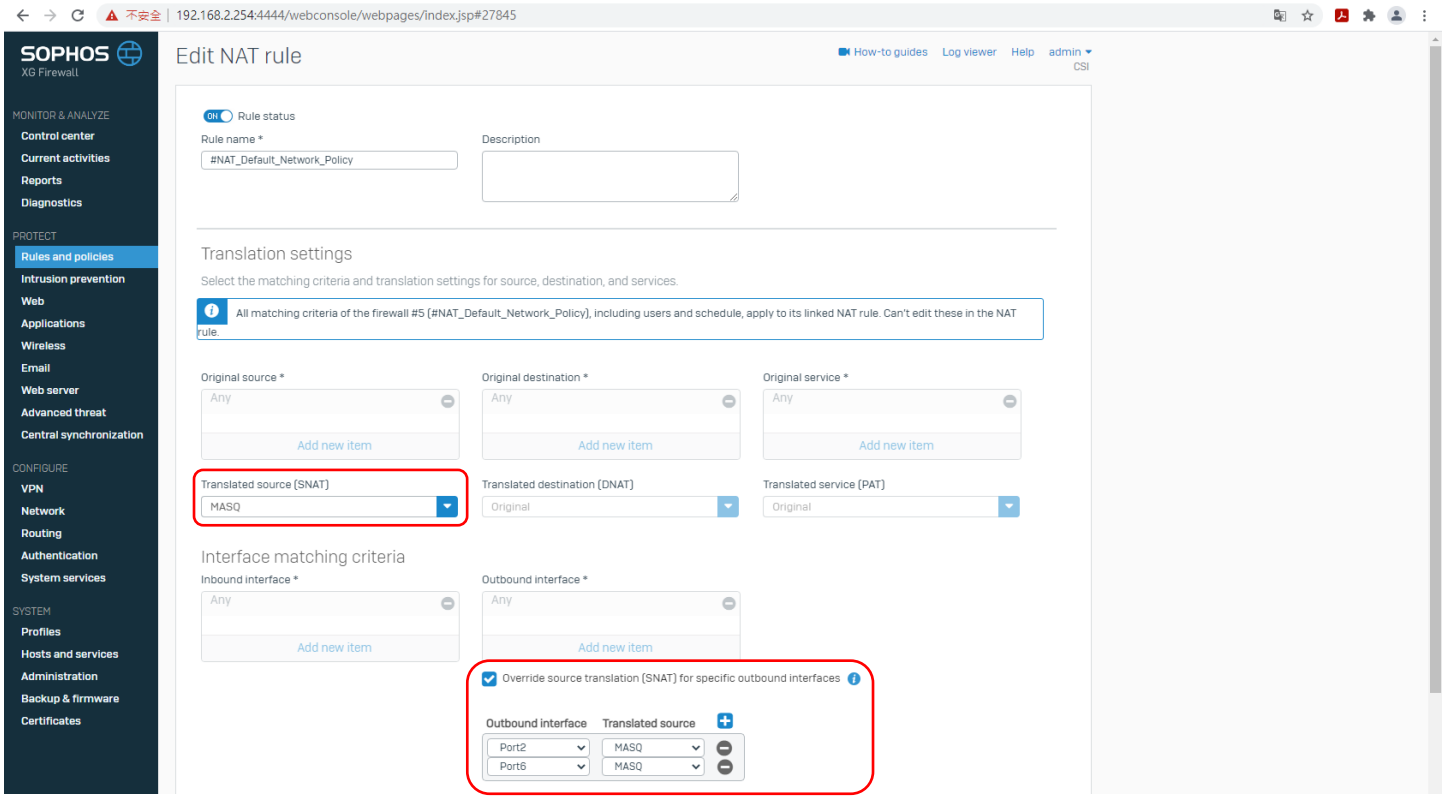


接著是#NAT_Default_Network_Policy，這條 NAT rule 是在 Firewall rule 的#Default_Network_Policy 裡新增的，所以會註明是哪條 Firewall rule 的，(在最後面的測試中結論**這步驟不需要做**)

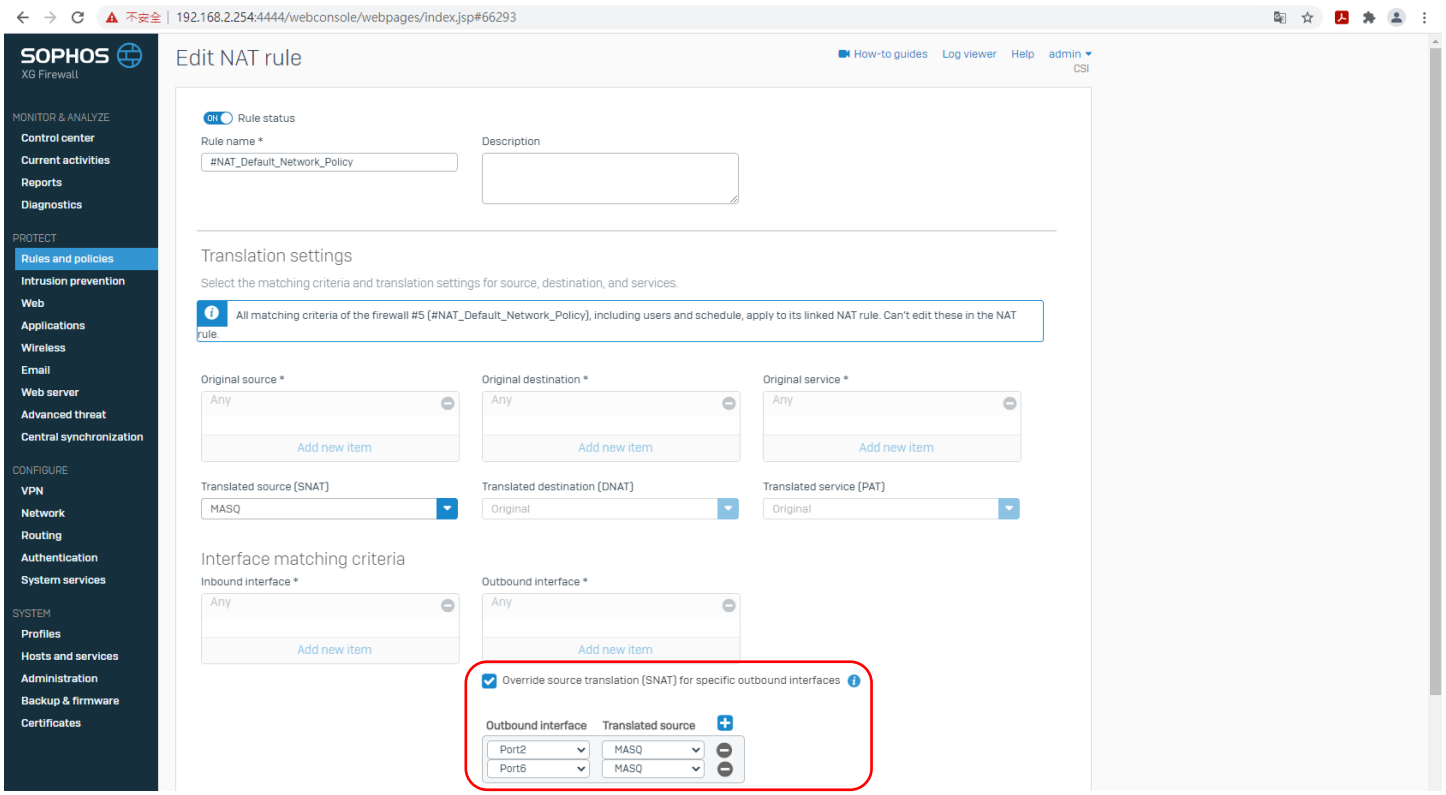




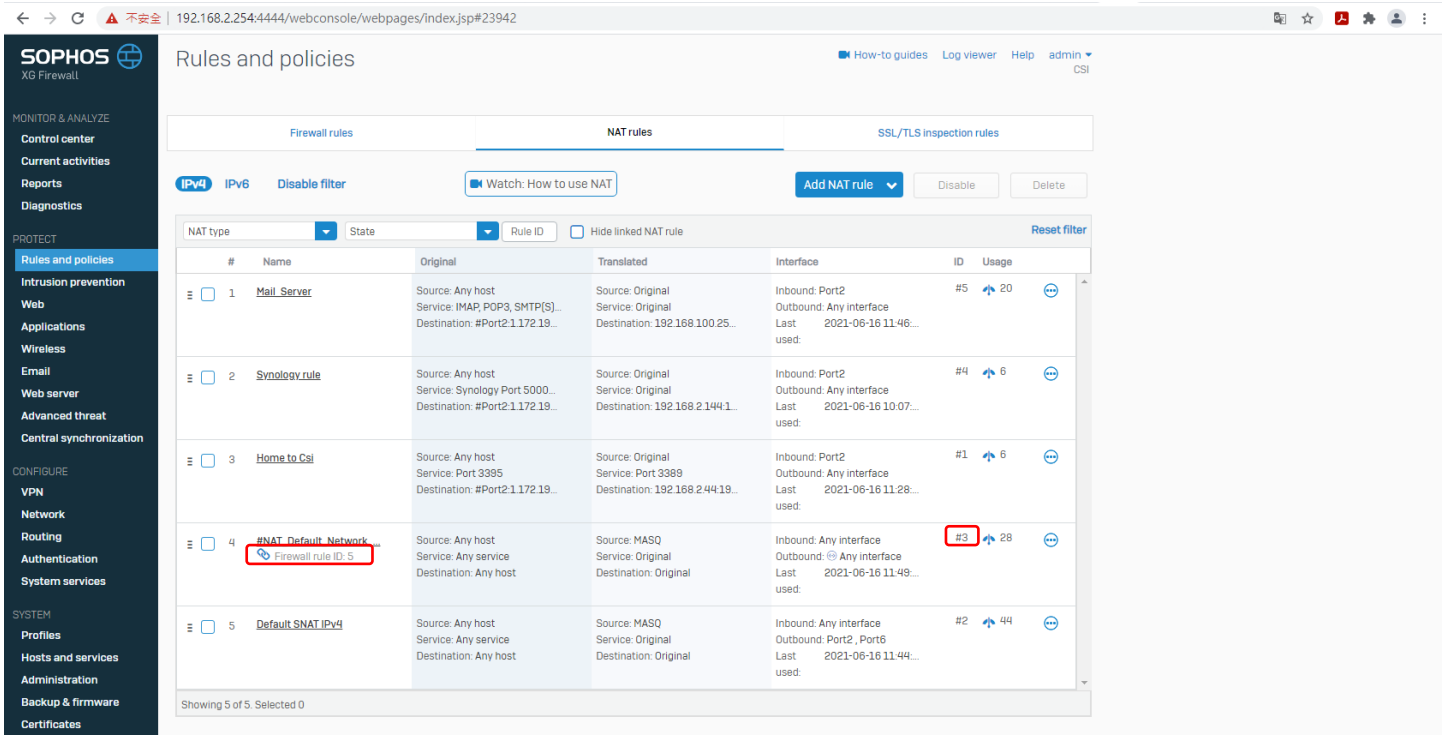
而如果 NAT rule 是在 Firewall rule 裡新增的，基本上能修改的地方不多，只有紅框所匡列的地方可以設定，(在最後面的測試中結論**這步驟不需要做**)



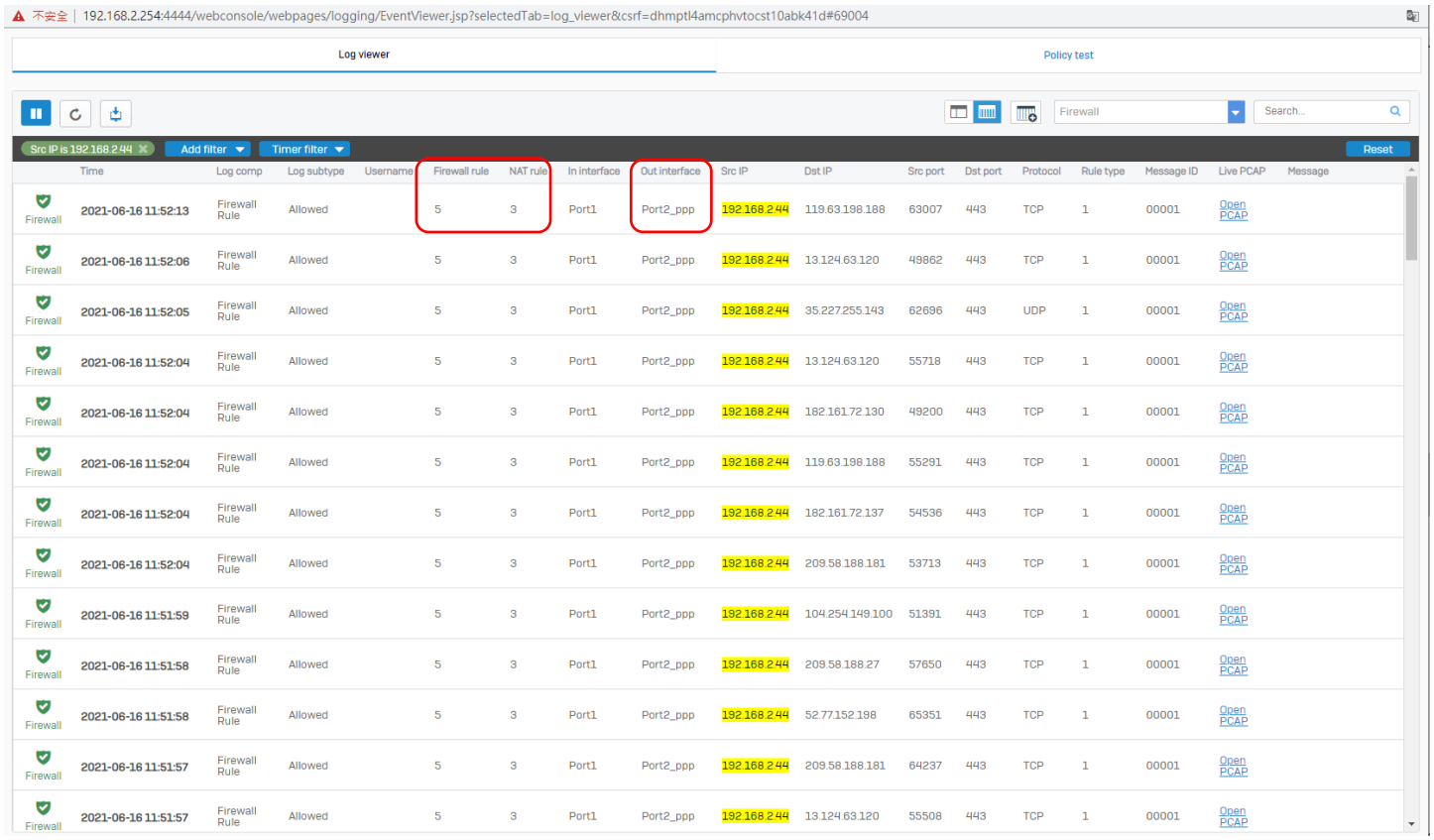
如果只有一條 WAN Port 的話基本上所有 LAN to WAN 相關的 Firewall rule 只要搭配 Default SNAT IPv4 這條預設的 NAT rule 即可；但如果是有兩個 WAN Port，然後限定哪個 LAN 是走哪條 WAN Port 就要在 Firewall rule 裡面新增 NAT rule，而要指定從哪條出去就要勾選 Override source translation (SNAT) for specific outbound interfaces，然後選好 WAN port，可以多個 WAN port，(在最後面的測試中結論**這步驟不需要做**)



這邊就讓#Default_Network_Policy(Firewall rule ID: 5)搭配#NAT_Default_Network_Policy(NAT rule ID: 3)，然後去查看 Log viewer，

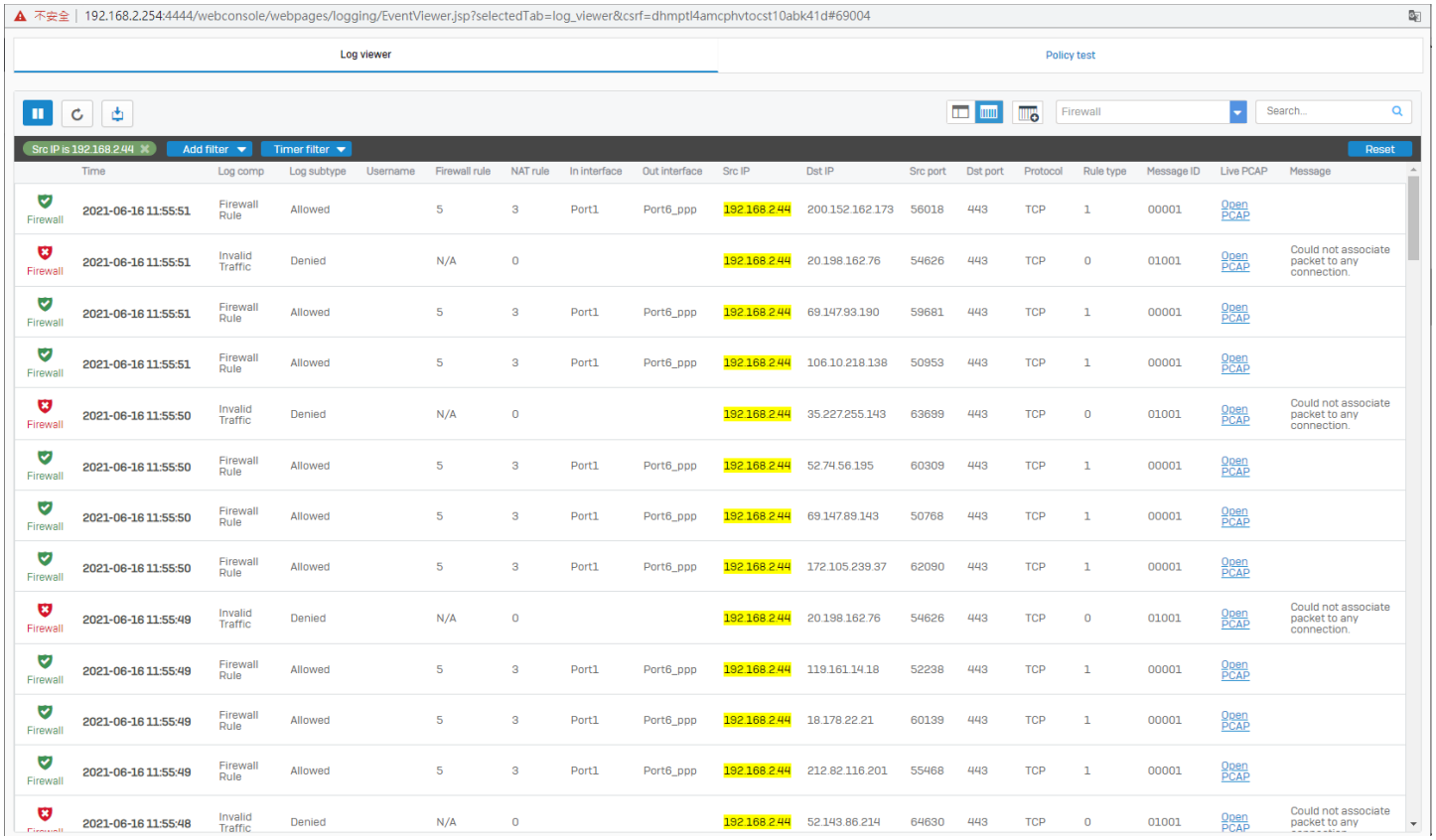


有一台 PC(192.168.2.44)在上網，從 Log viewer 中可以看出該 PC 使用 Firewall rule ID: 5 跟 NAT rule ID: 3，走 Port 2 的 WAN 逛網頁，



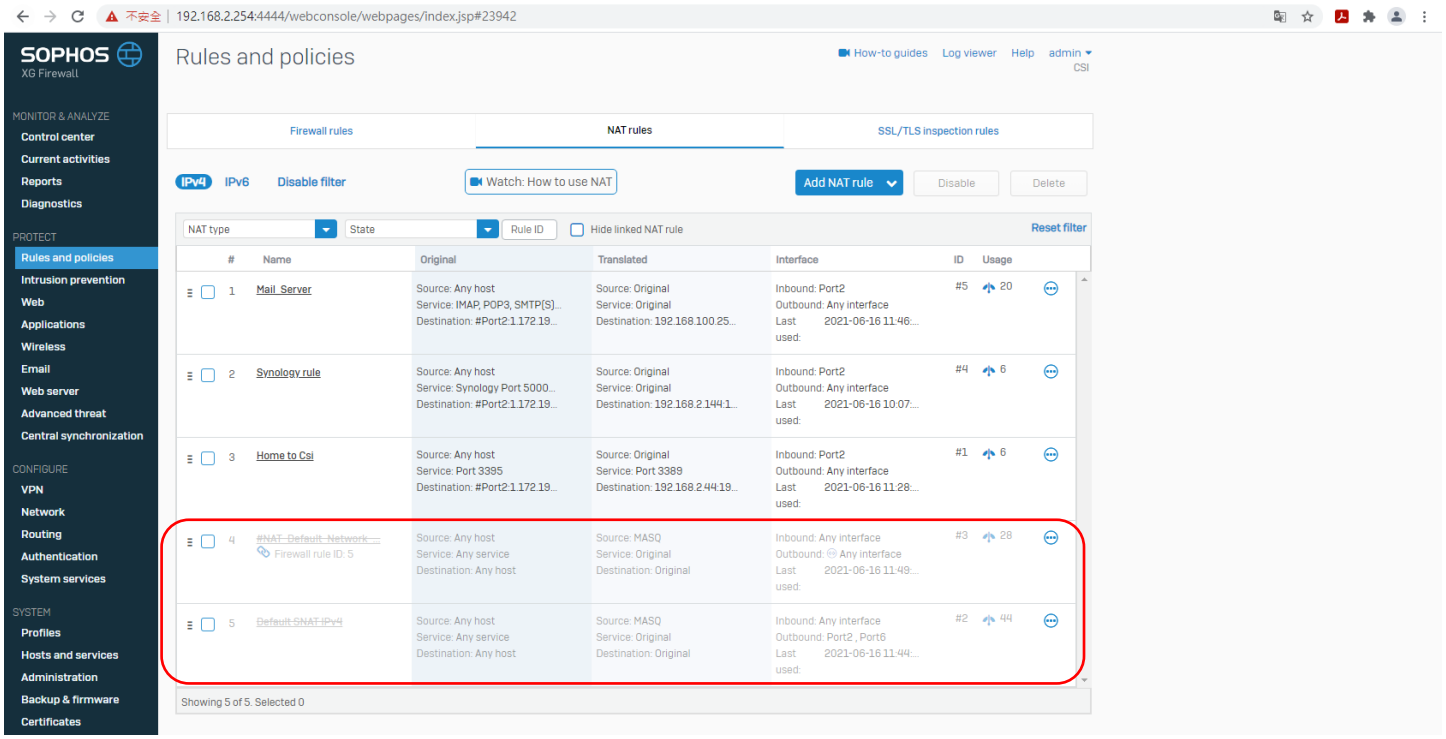
Time	Log comp	Log subtype	Username	Firewall rule	NAT rule	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Message ID	Live PCAP	Message
2021-06-16 11:52:13	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	119.63.198.188	63007	443	TCP	1	00001	Open PCAP	
2021-06-16 11:52:06	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	13.124.63.120	49862	443	TCP	1	00001	Open PCAP	
2021-06-16 11:52:05	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	35.227.255.143	62696	443	UDP	1	00001	Open PCAP	
2021-06-16 11:52:04	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	13.124.63.120	55718	443	TCP	1	00001	Open PCAP	
2021-06-16 11:52:04	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	182.161.72.130	49200	443	TCP	1	00001	Open PCAP	
2021-06-16 11:52:04	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	119.63.198.188	55291	443	TCP	1	00001	Open PCAP	
2021-06-16 11:52:04	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	182.161.72.137	54536	443	TCP	1	00001	Open PCAP	
2021-06-16 11:52:04	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	209.58.188.181	53713	443	TCP	1	00001	Open PCAP	
2021-06-16 11:51:59	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	104.254.149.100	51391	443	TCP	1	00001	Open PCAP	
2021-06-16 11:51:58	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	209.58.188.27	57650	443	TCP	1	00001	Open PCAP	
2021-06-16 11:51:58	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	52.77.152.198	65351	443	TCP	1	00001	Open PCAP	
2021-06-16 11:51:57	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	209.58.188.181	64237	443	TCP	1	00001	Open PCAP	
2021-06-16 11:51:57	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	13.124.63.120	55508	443	TCP	1	00001	Open PCAP	

把 Port 2 的 WAN 孔線拔掉，看 PC 會不會改連 Port 6 的 WAN，是可以的。

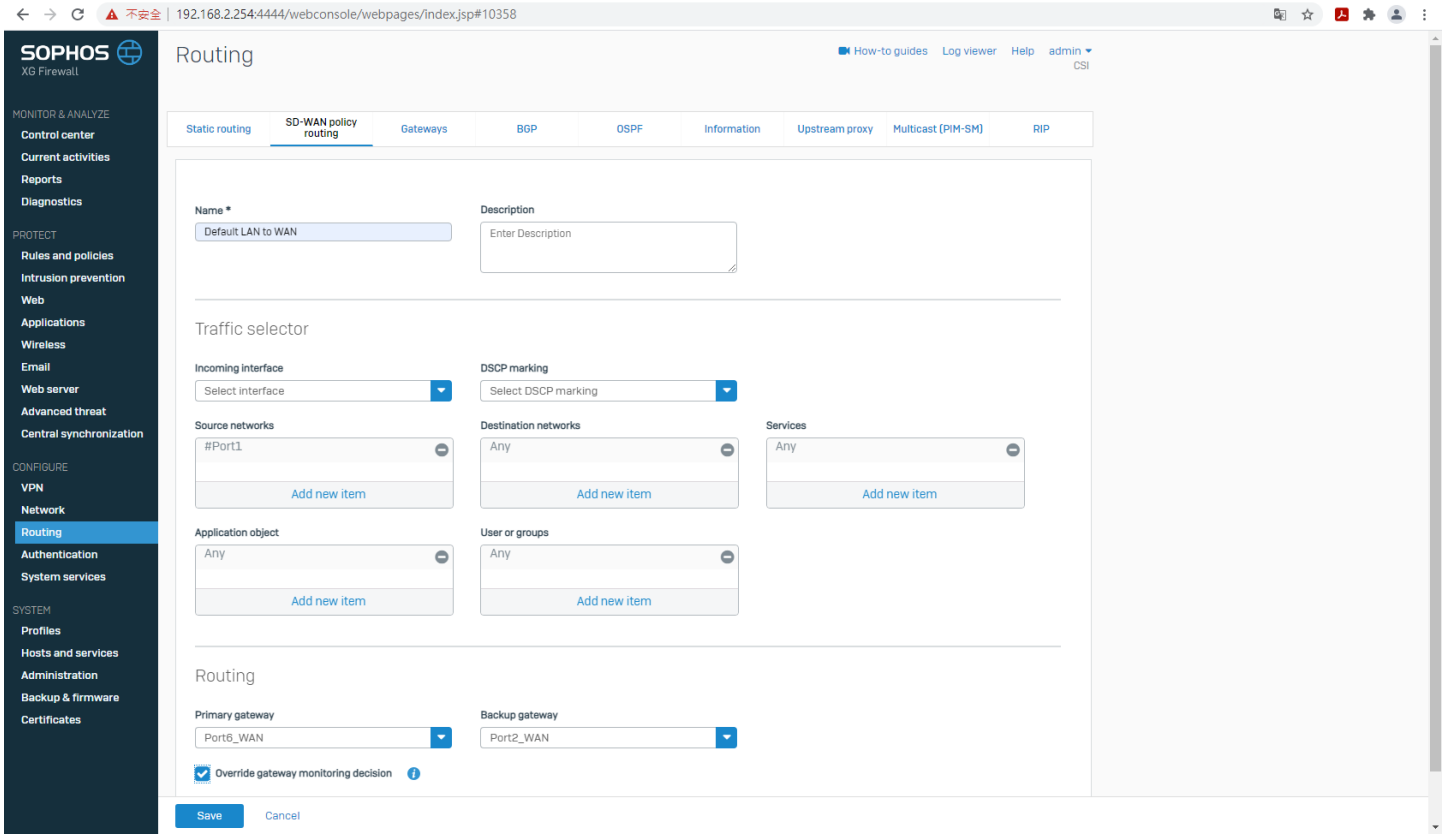


Time	Log comp	Log subtype	Username	Firewall rule	NAT rule	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Message ID	Live PCAP	Message
2021-06-16 11:55:51	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	200.152.162.173	56018	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:51	Invalid Traffic	Denied		N/A	0			192.168.2.44	20.198.162.76	54626	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 11:55:51	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	69.147.93.190	59681	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:51	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	106.10.218.138	50953	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:50	Invalid Traffic	Denied		N/A	0			192.168.2.44	35.227.255.143	63699	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 11:55:50	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	52.74.56.195	60309	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:50	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	69.147.89.143	50768	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:50	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	172.105.239.37	62090	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:49	Invalid Traffic	Denied		N/A	0			192.168.2.44	20.198.162.76	54626	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 11:55:49	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	119.161.14.18	52238	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:49	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	18.178.22.21	60139	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:49	Firewall Rule	Allowed		5	3	Port1	Port6_ppp	192.168.2.44	212.82.116.201	55468	443	TCP	1	00001	Open PCAP	
2021-06-16 11:55:48	Invalid Traffic	Denied		N/A	0			192.168.2.44	52.143.86.214	64630	443	TCP	0	01001	Open PCAP	Could not associate packet to any

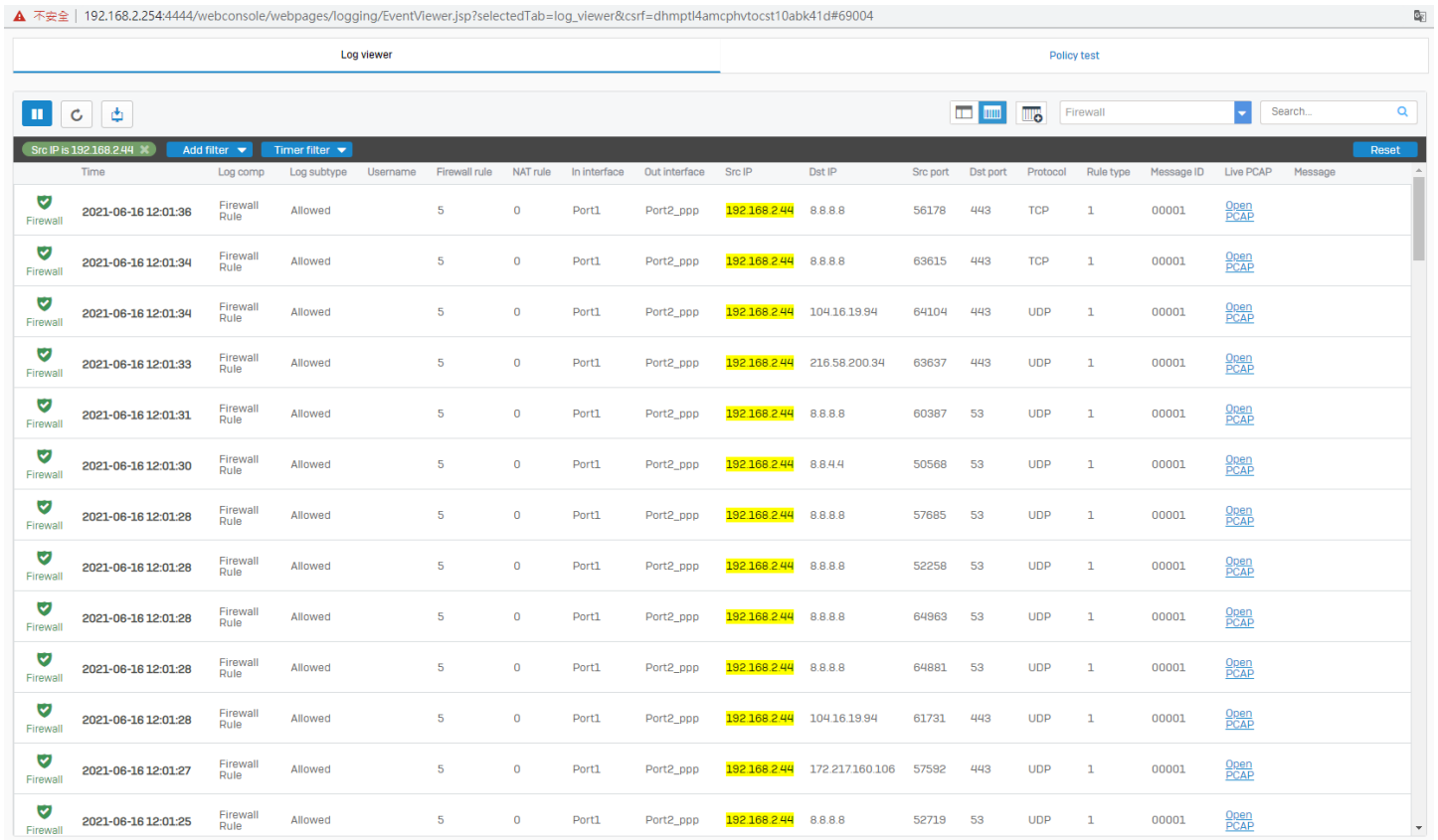
回到正題，關掉 NAT rule 只設定 SD-WAN policy route 看能不能上網，



SD-WAN policy route 的設定內容，#Port 1(LAN zone)，Primary gateway 選 Port6_WAN，

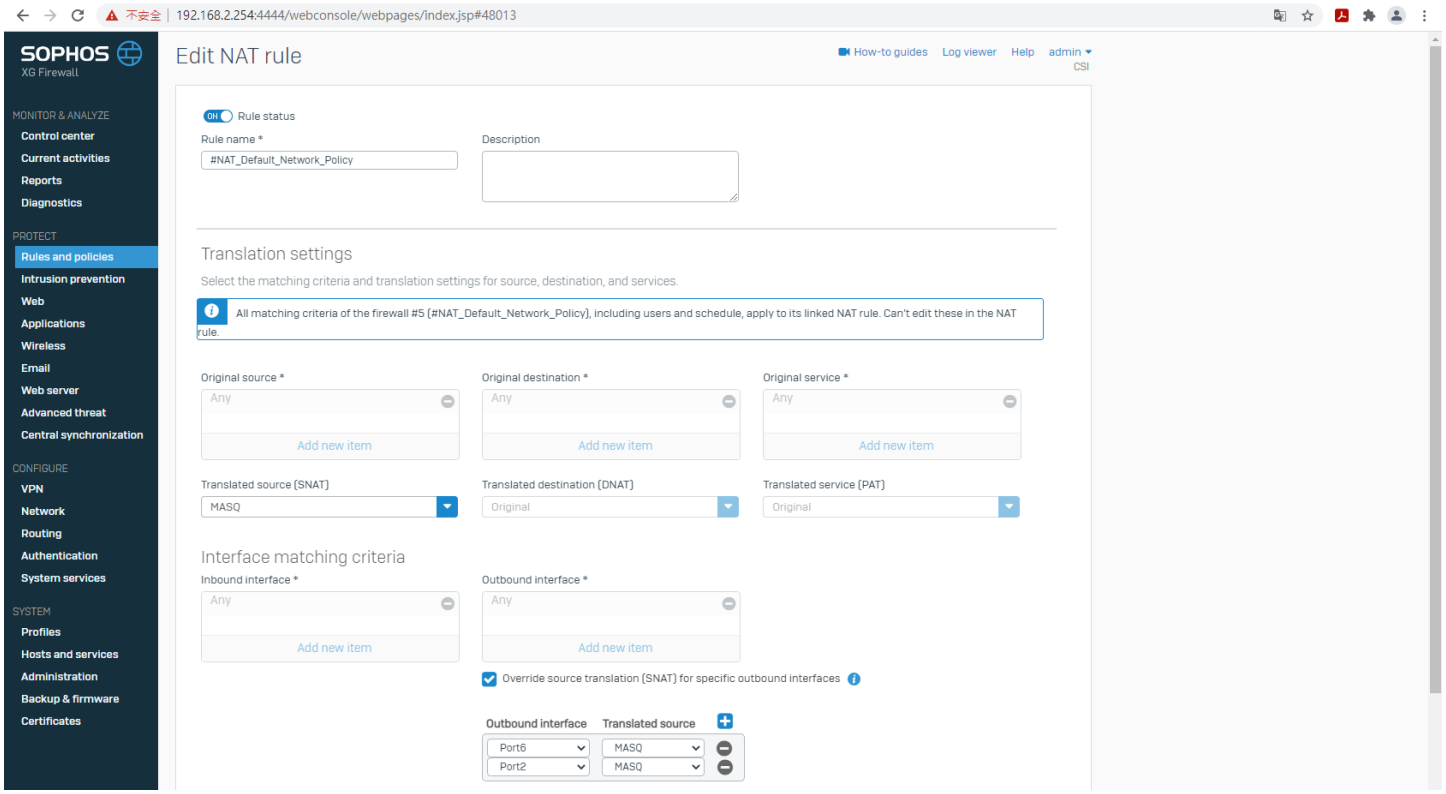


查看 Log viewer，因為沒有經過 NAT rule，只設定 SD-WAN policy route 是無法上網的，不過上圖中 Primary Gateway 明明是選 Port 6，Log viewer 卻還是顯示經過 Port2，

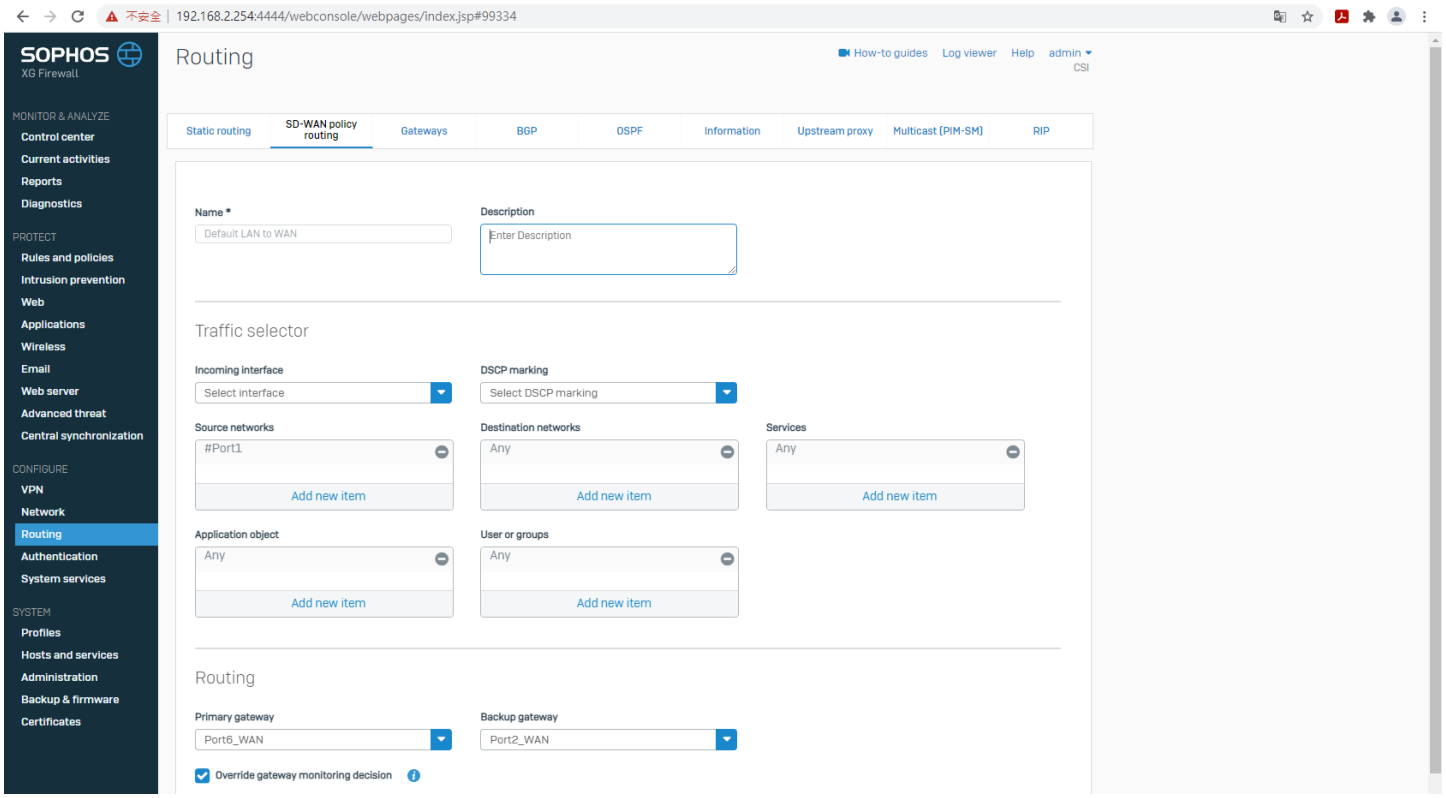


Time	Log comp	Log subtype	Username	Firewall rule	NAT rule	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Message ID	Live PCAP	Message
2021-06-16 12:01:36	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	56178	443	TCP	1	00001	Open PCAP	
2021-06-16 12:01:34	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	63615	443	TCP	1	00001	Open PCAP	
2021-06-16 12:01:34	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	104.16.19.94	64104	443	UDP	1	00001	Open PCAP	
2021-06-16 12:01:33	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	216.58.200.34	63637	443	UDP	1	00001	Open PCAP	
2021-06-16 12:01:31	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	60387	53	UDP	1	00001	Open PCAP	
2021-06-16 12:01:30	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.4.4	50568	53	UDP	1	00001	Open PCAP	
2021-06-16 12:01:28	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	57685	53	UDP	1	00001	Open PCAP	
2021-06-16 12:01:28	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	52258	53	UDP	1	00001	Open PCAP	
2021-06-16 12:01:28	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	64963	53	UDP	1	00001	Open PCAP	
2021-06-16 12:01:28	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	64881	53	UDP	1	00001	Open PCAP	
2021-06-16 12:01:28	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	104.16.19.94	61731	443	UDP	1	00001	Open PCAP	
2021-06-16 12:01:27	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	172.217.160.106	57592	443	UDP	1	00001	Open PCAP	
2021-06-16 12:01:25	Firewall Rule	Allowed		5	0	Port1	Port2_ppp	192.168.2.44	8.8.8.8	52719	53	UDP	1	00001	Open PCAP	

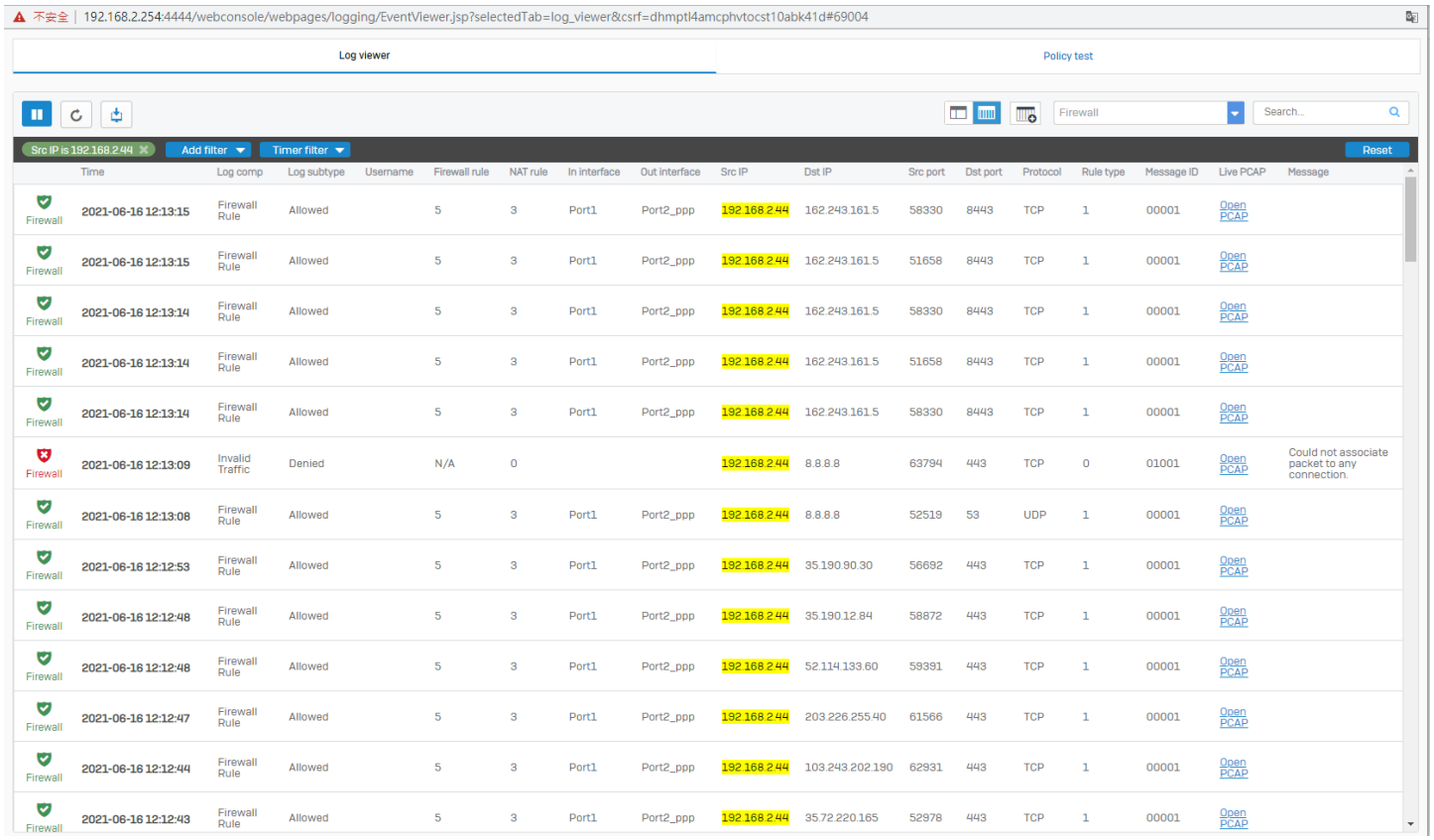
這邊打算再測試 WAN Gateway 的順序，想把 Port6 當主要閘道(Primary Gateway)，NAT rule 的 #NAT_Default_Network_Policy 打開，outbound interfaces 先 Port6 再 Port2，(在最後面的測試中結論**這步驟不需要做**)



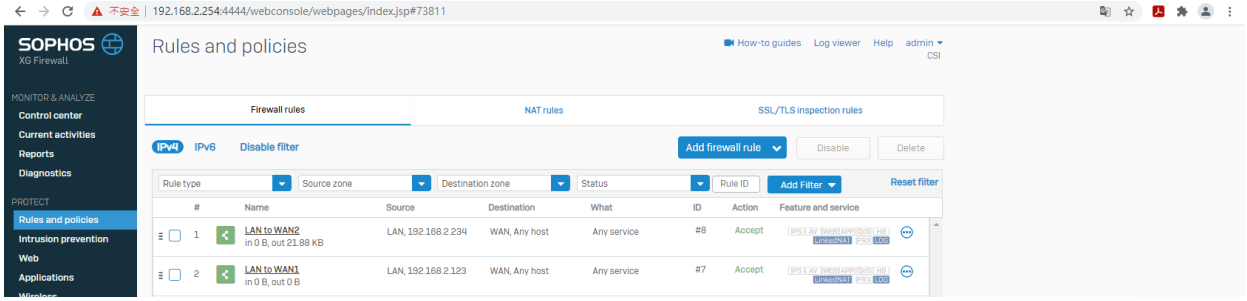
SD-WAN policy route 也是先 Port6 再 Port2，

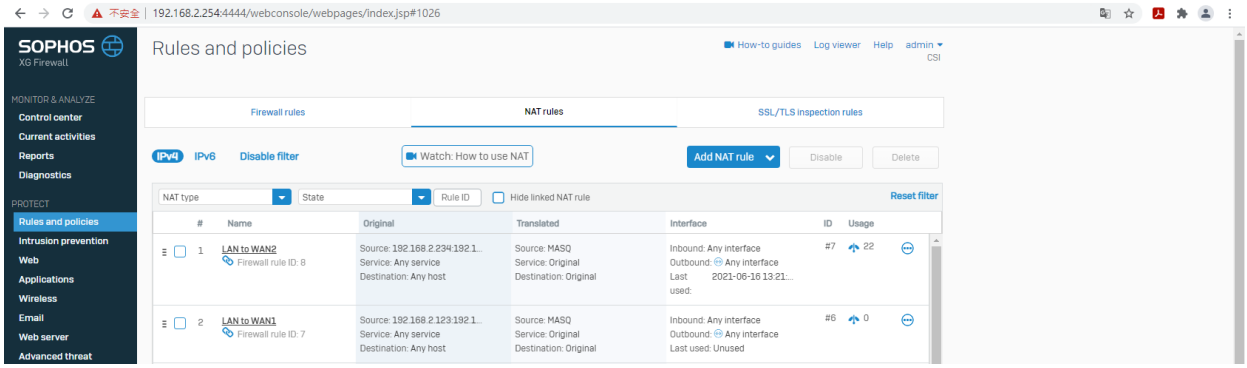


這樣設定沒有效果，

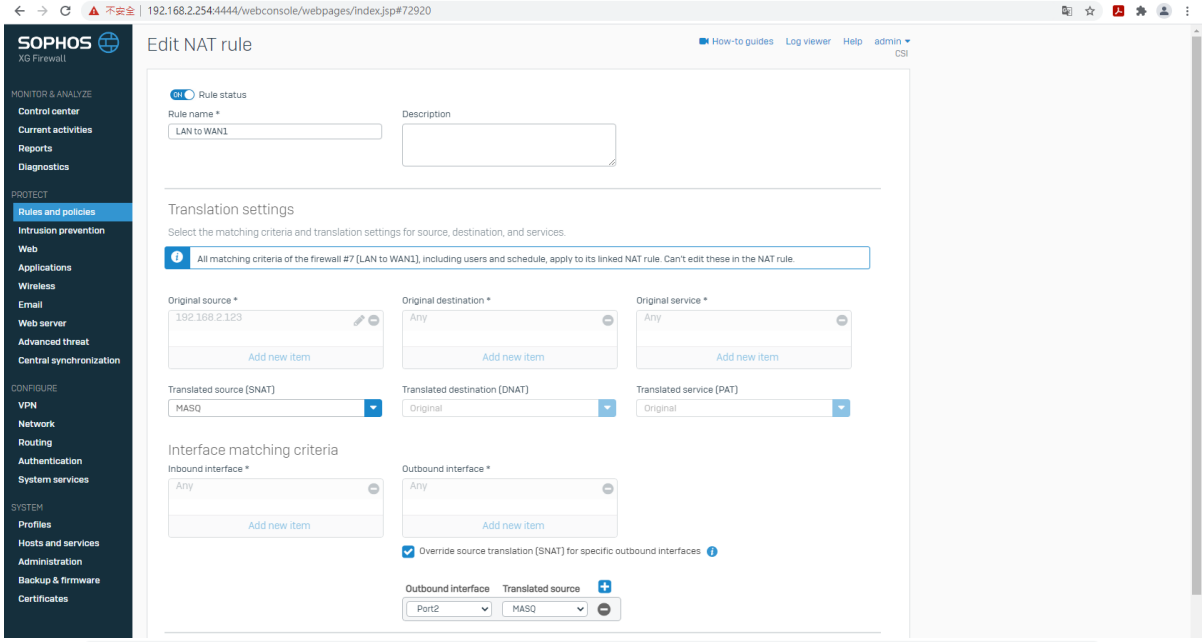


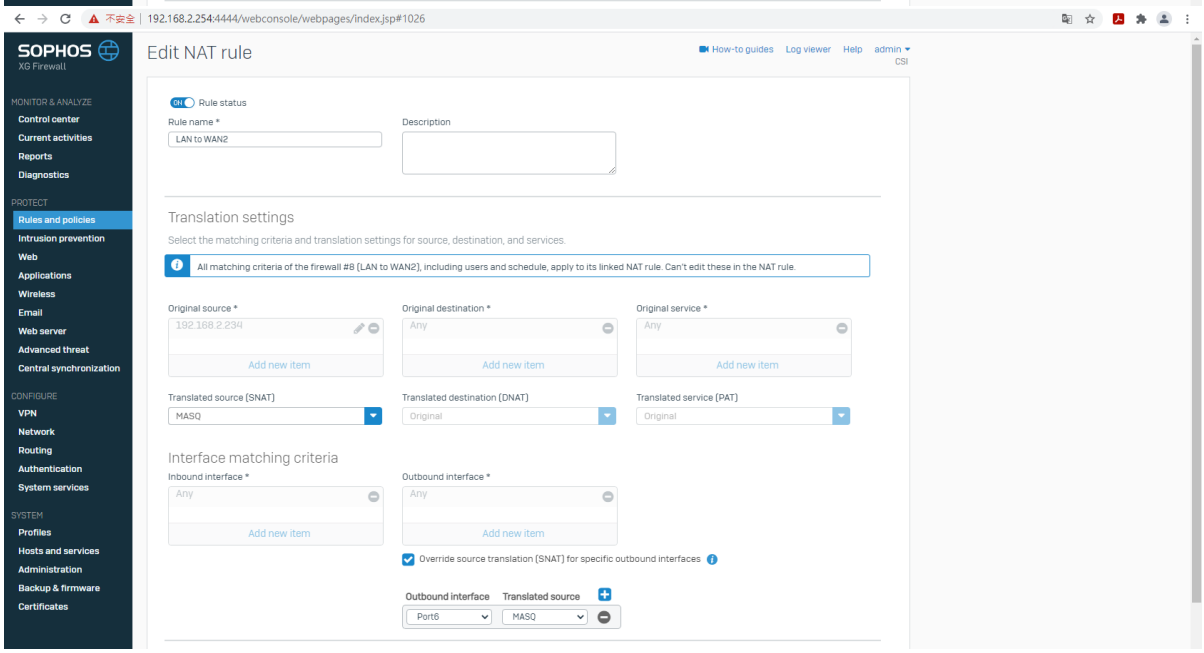
這邊再繼續做測試，LAN 192.168.2.123 走 Port2_WAN 出去；LAN 192.168.2.234 走 Port6_WAN 出去，



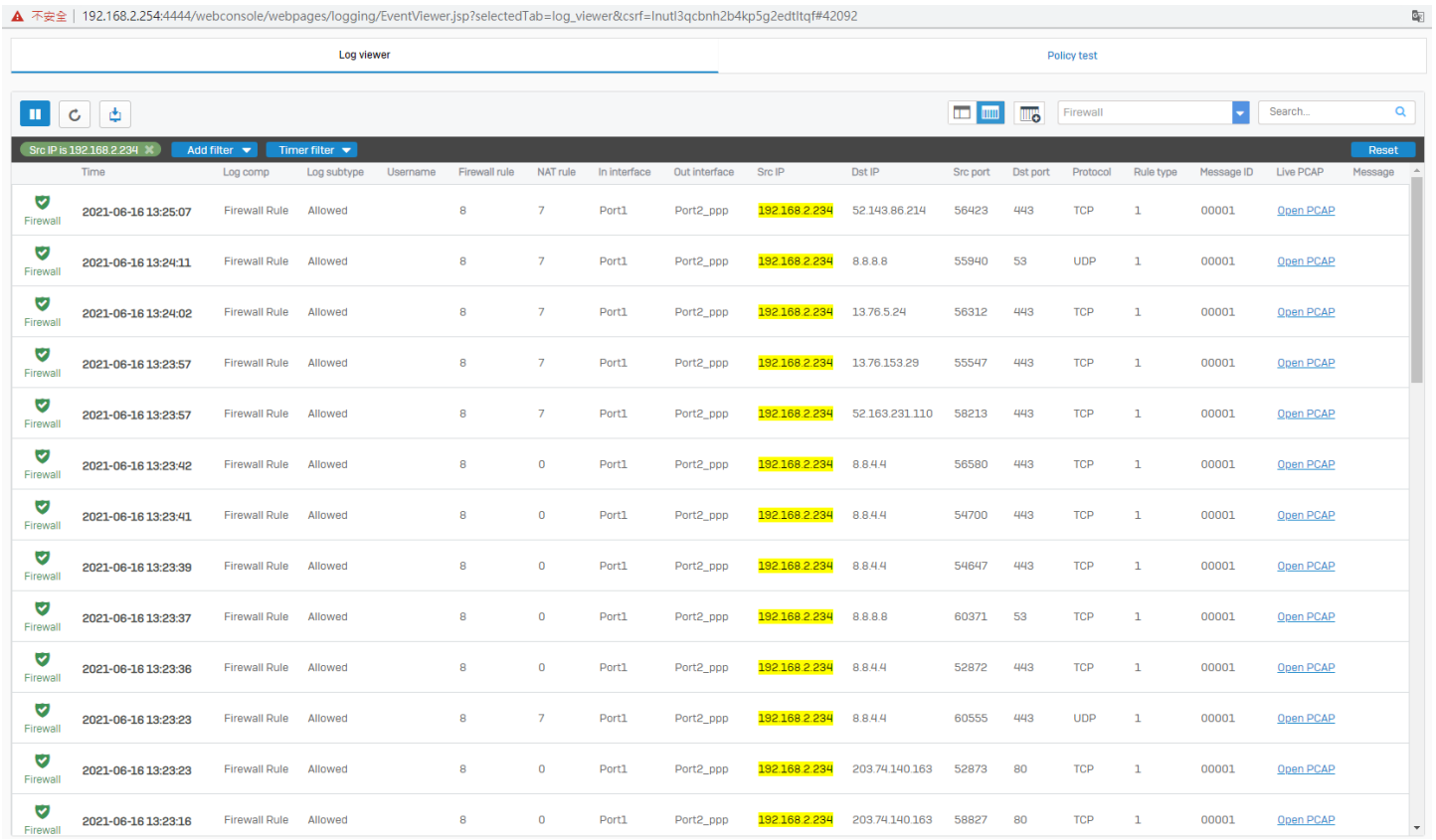


(因為後面的結論，其實不需要在 Firewall rule 裡新增 NAT rule，)

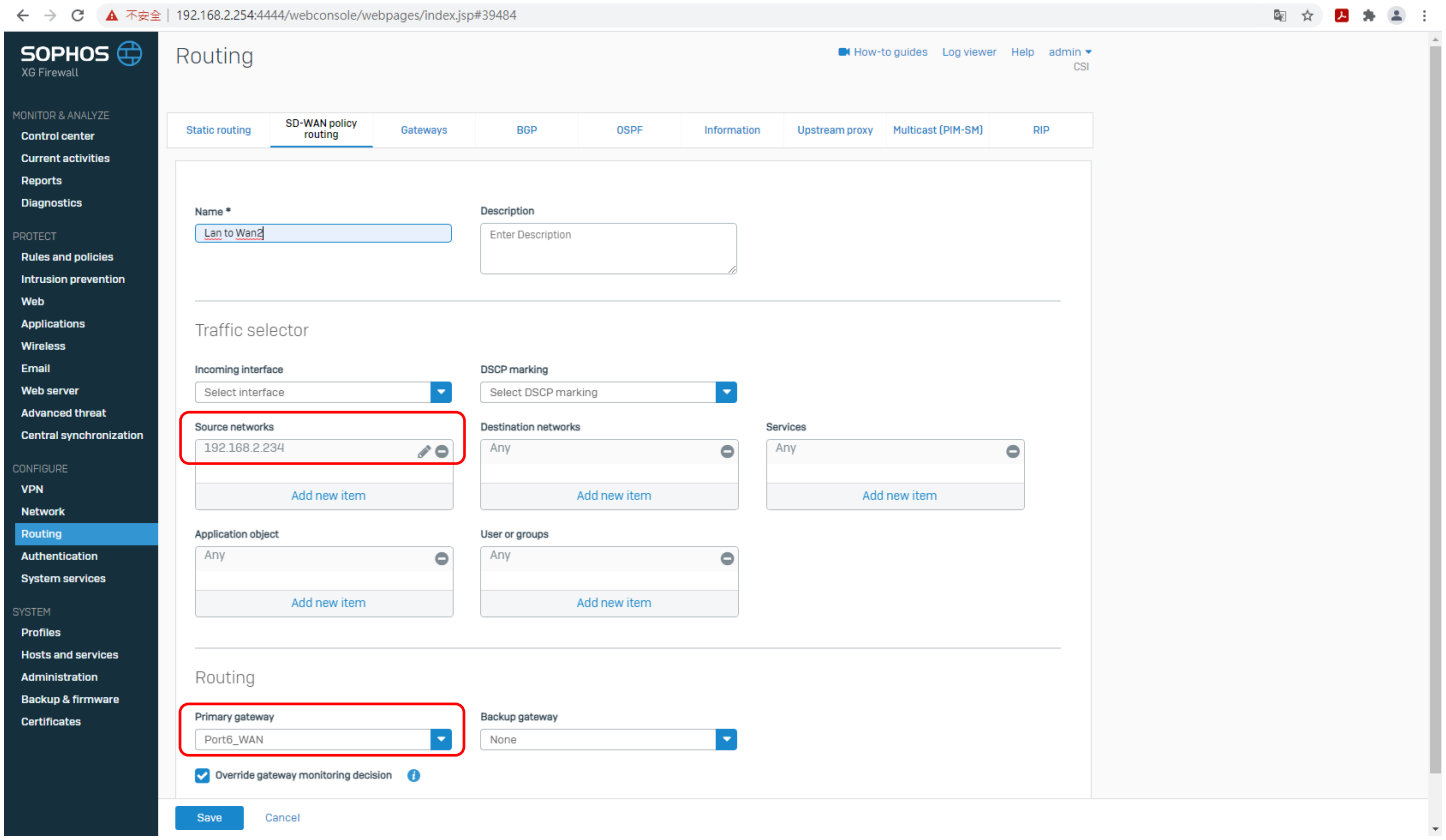




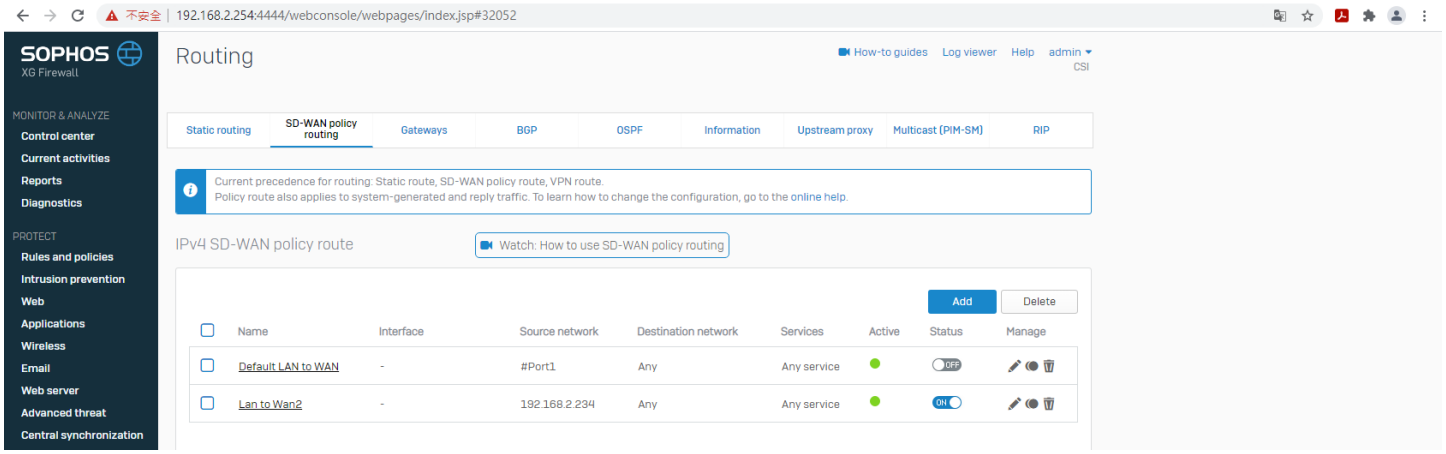
還沒設定 SD-WAN policy route，先查看 Log viewer，192.168.2.234 應該要走 Port6，但還是走 Port2，



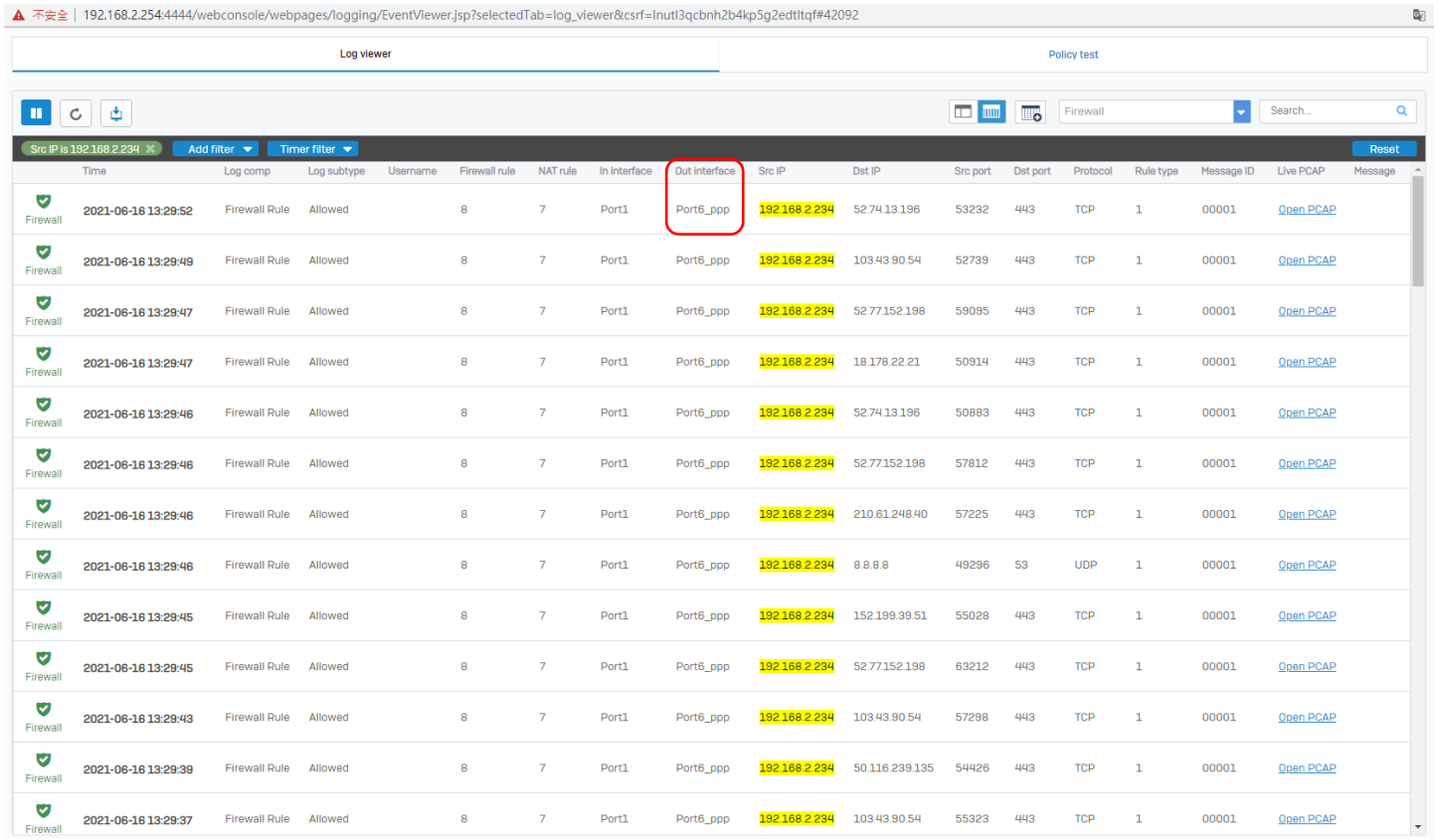
去 SD-WAN policy route 設定 LAN to WAN2，非常直白就是 192.168.2.234 要走 Port6_WAN，



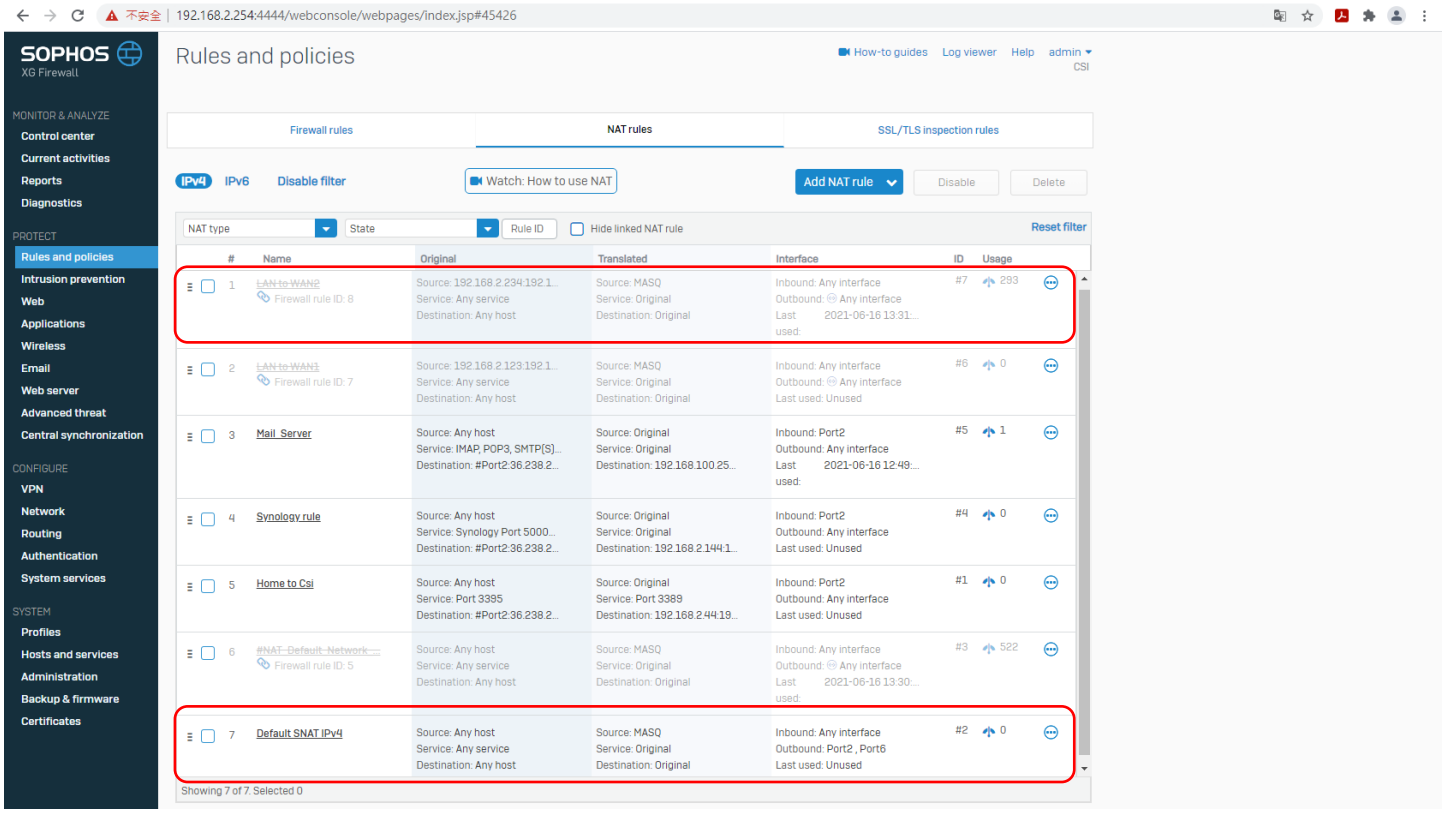
新增完成，



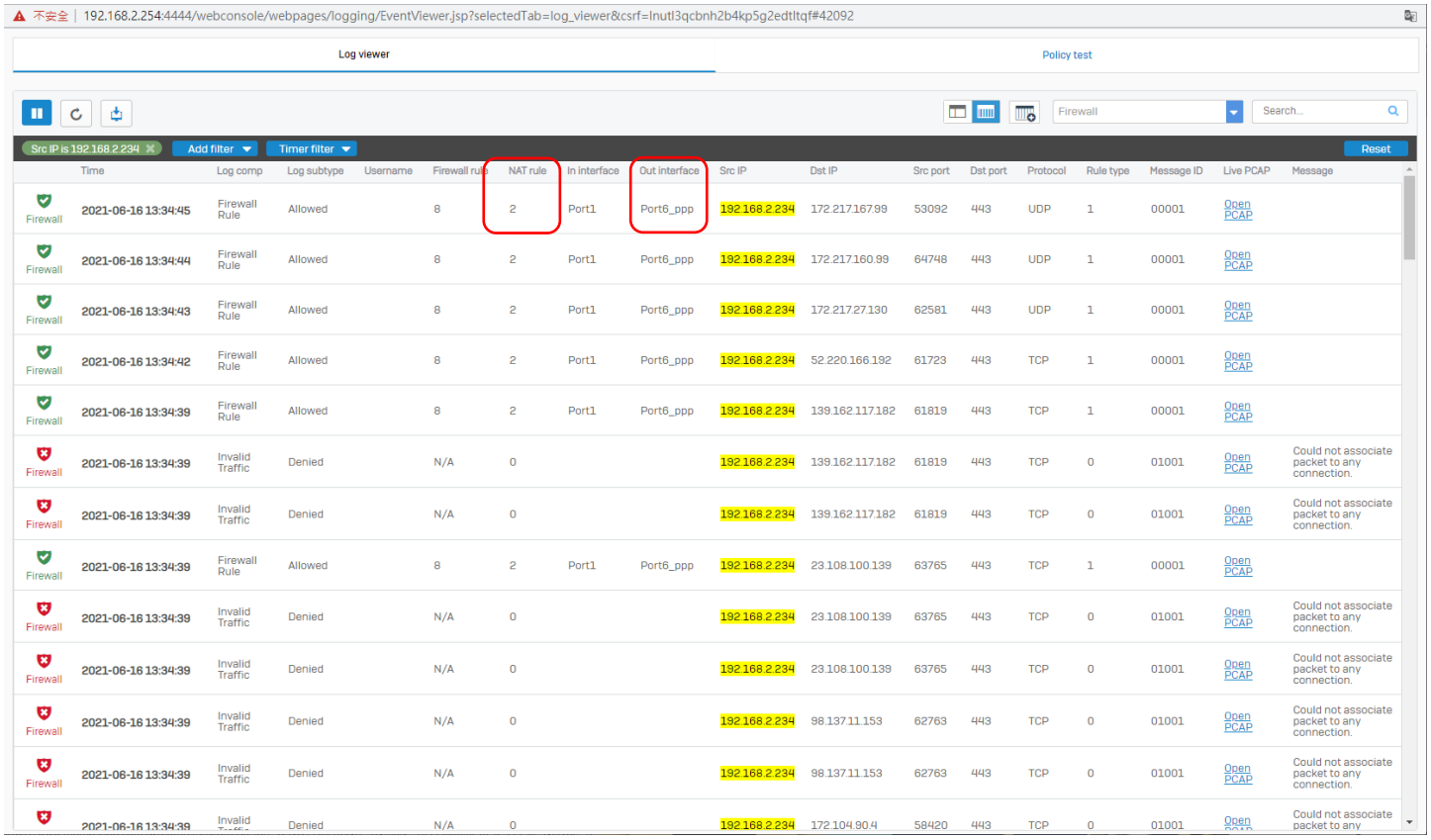
有作用，192.168.2.234 從 Port6_WAN 出去，



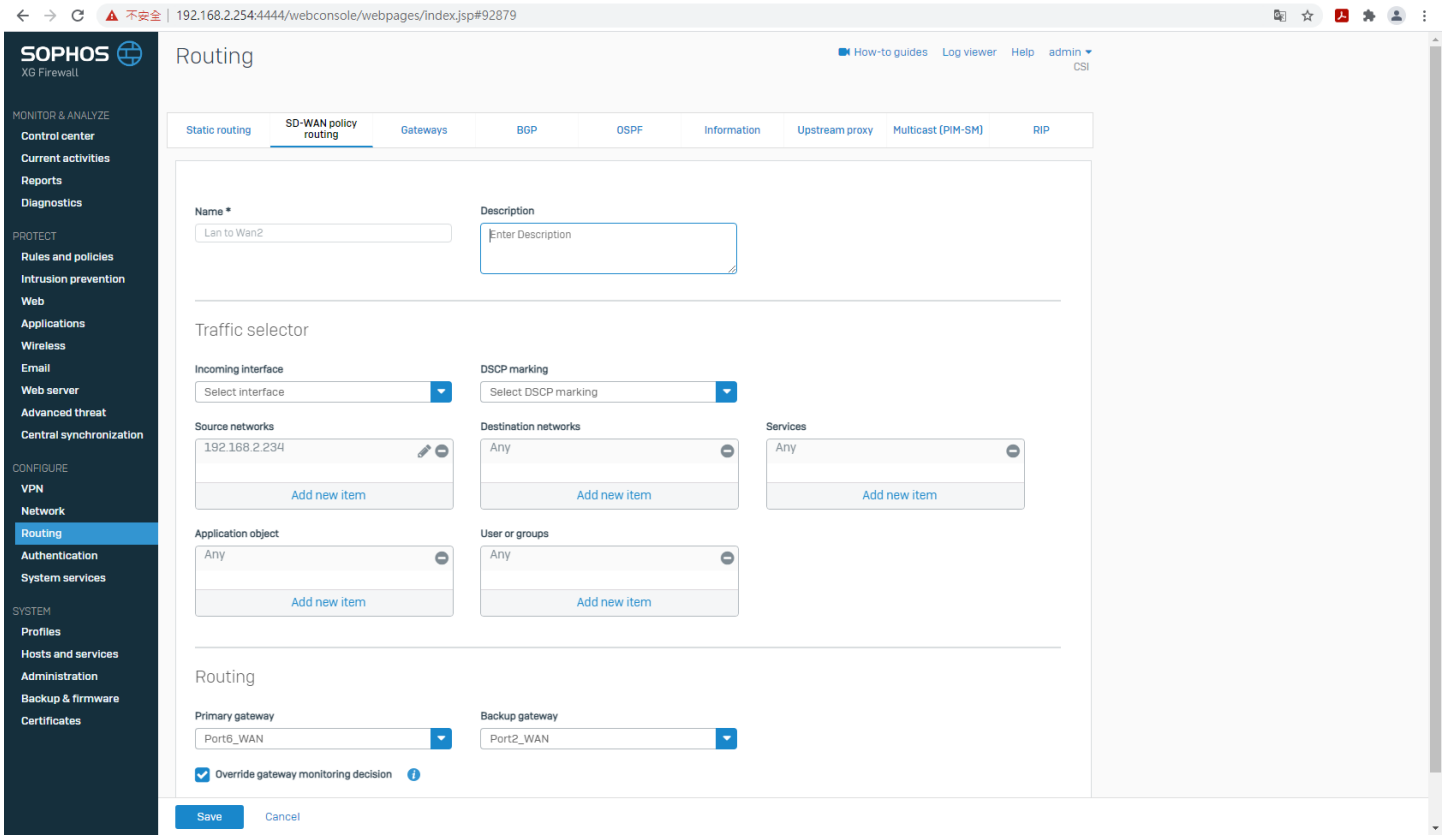
竟然這樣我們把 NAT rule ID：7 關閉，只用預設的 Default SNAT IPv4 試試，



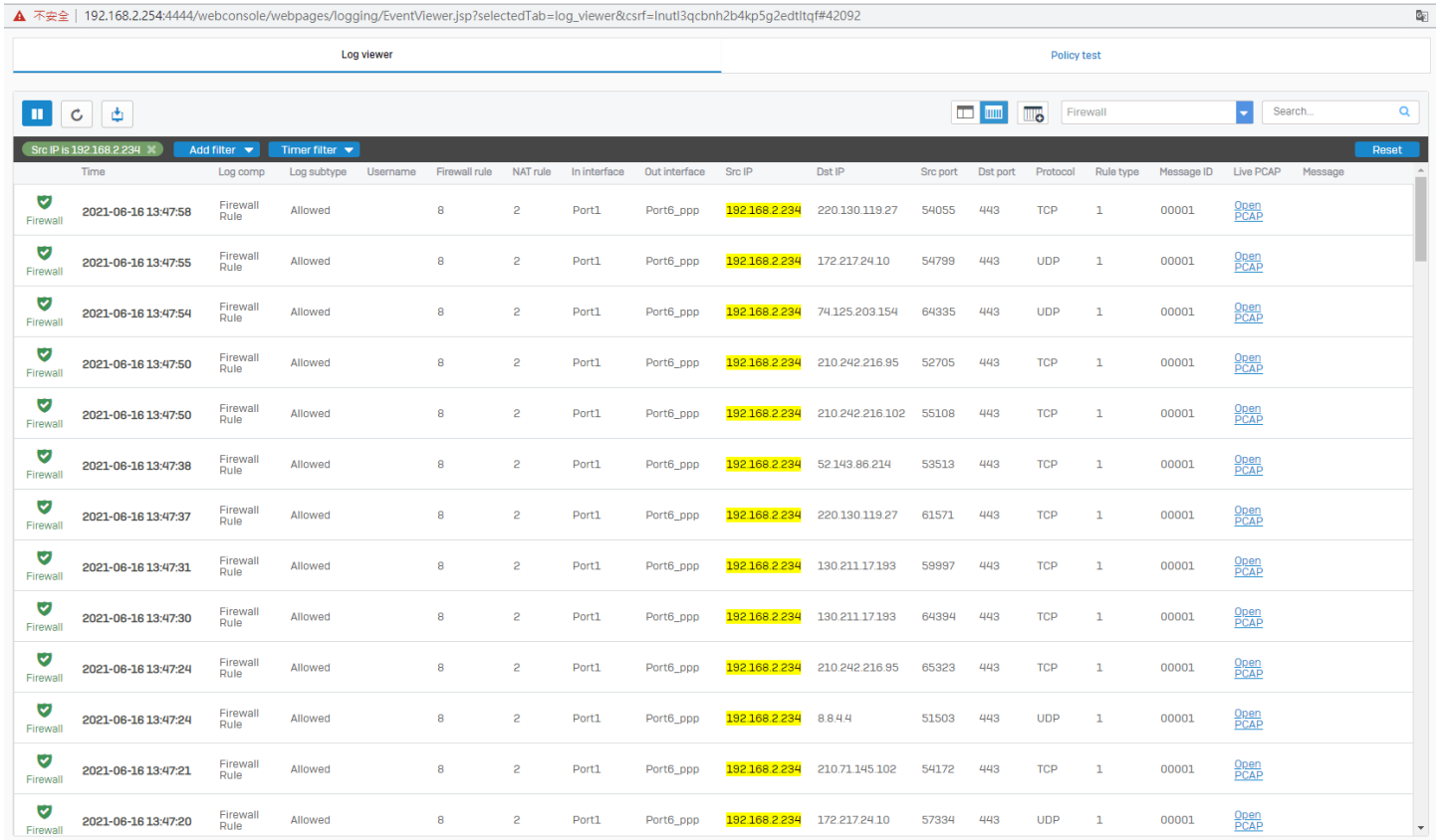
可以看出就算 Firewall rule 裡新增的 NAT rule 關掉用預設的 Default SNAT IPv4 也是能走 Port 6_WAN，



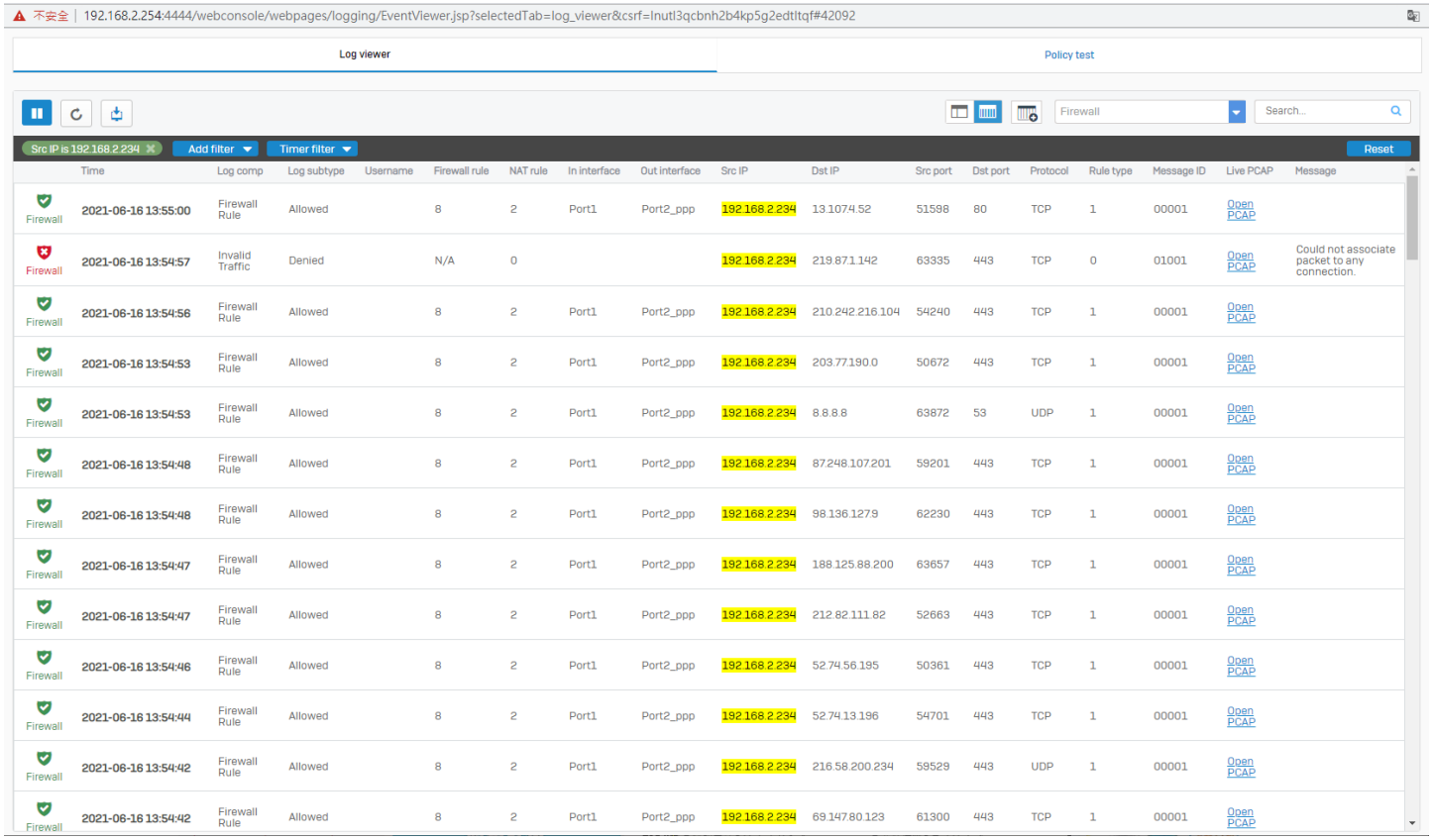
再進階一點設定，總要給 192.168.2.234 如果是 Port6_WAN 斷線，Port2_WAN 要接替上去，



依舊 Port6_WAN 優先，接下來要把 Port6_WAN 的網路線拔掉，照理說 192.168.2.234 會改從 Port2_WAN 出去，

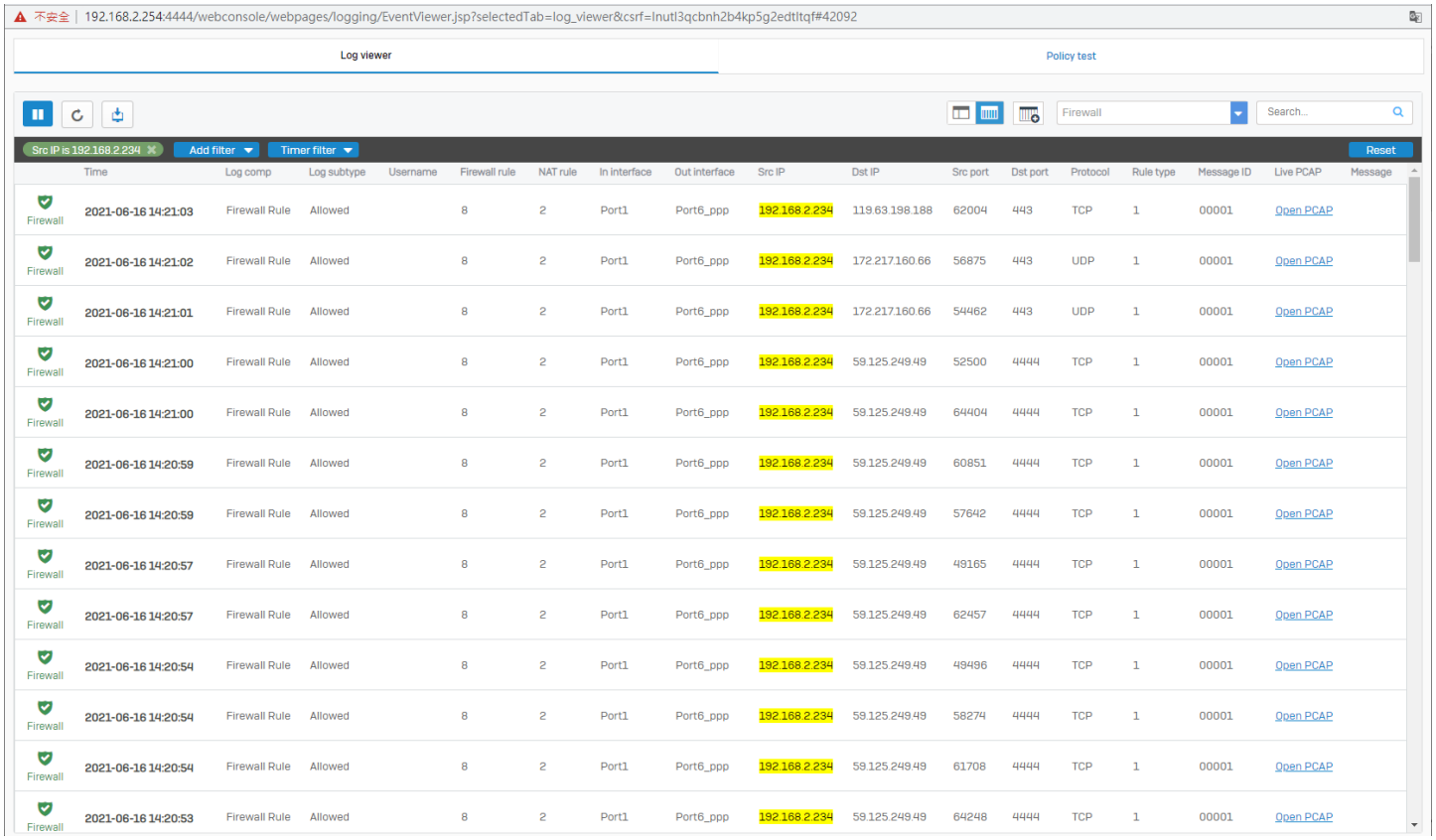


確實流量改從 Port2_WAN 出去，但可能因為是 PPPoE 的 WAN 所以有斷線差不多 3 分鐘，



Time	Log comp	Log subtype	Username	Firewall rule	NAT rule	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Message ID	Live PCAP	Message
2021-06-16 13:55:00	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	13.107.4.52	51598	80	TCP	1	00001	Open PCAP	
2021-06-16 13:54:57	Invalid Traffic	Denied		N/A	0			192.168.2.234	219.87.1.142	63335	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 13:54:56	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	210.242.216.104	54240	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:53	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	203.77.190.0	50672	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:53	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	8.8.8.8	63872	53	UDP	1	00001	Open PCAP	
2021-06-16 13:54:48	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	87.248.107.201	59201	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:48	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	98.136.127.9	62230	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:47	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	188.125.88.200	63657	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:47	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	212.82.111.82	52663	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:46	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	52.74.56.195	50361	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:44	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	52.74.13.196	54701	443	TCP	1	00001	Open PCAP	
2021-06-16 13:54:42	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	216.58.200.234	59529	443	UDP	1	00001	Open PCAP	
2021-06-16 13:54:42	Firewall Rule	Allowed		8	2	Port1	Port2_ppp	192.168.2.234	69.147.80.123	61300	443	TCP	1	00001	Open PCAP	

接上 Port6_WAN 也主動導回了，



Time	Log comp	Log subtype	Username	Firewall rule	NAT rule	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Message ID	Live PCAP	Message
2021-06-16 14:21:03	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	119.63.198.188	62004	443	TCP	1	00001	Open PCAP	
2021-06-16 14:21:02	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	172.217.160.66	56875	443	UDP	1	00001	Open PCAP	
2021-06-16 14:21:01	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	172.217.160.66	54462	443	UDP	1	00001	Open PCAP	
2021-06-16 14:21:00	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	52500	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:21:00	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	64404	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:59	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	60851	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:59	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	57642	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:57	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	49165	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:57	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	62457	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:54	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	49496	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:54	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	58274	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:54	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	61708	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:53	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.249.49	64248	4444	TCP	1	00001	Open PCAP	

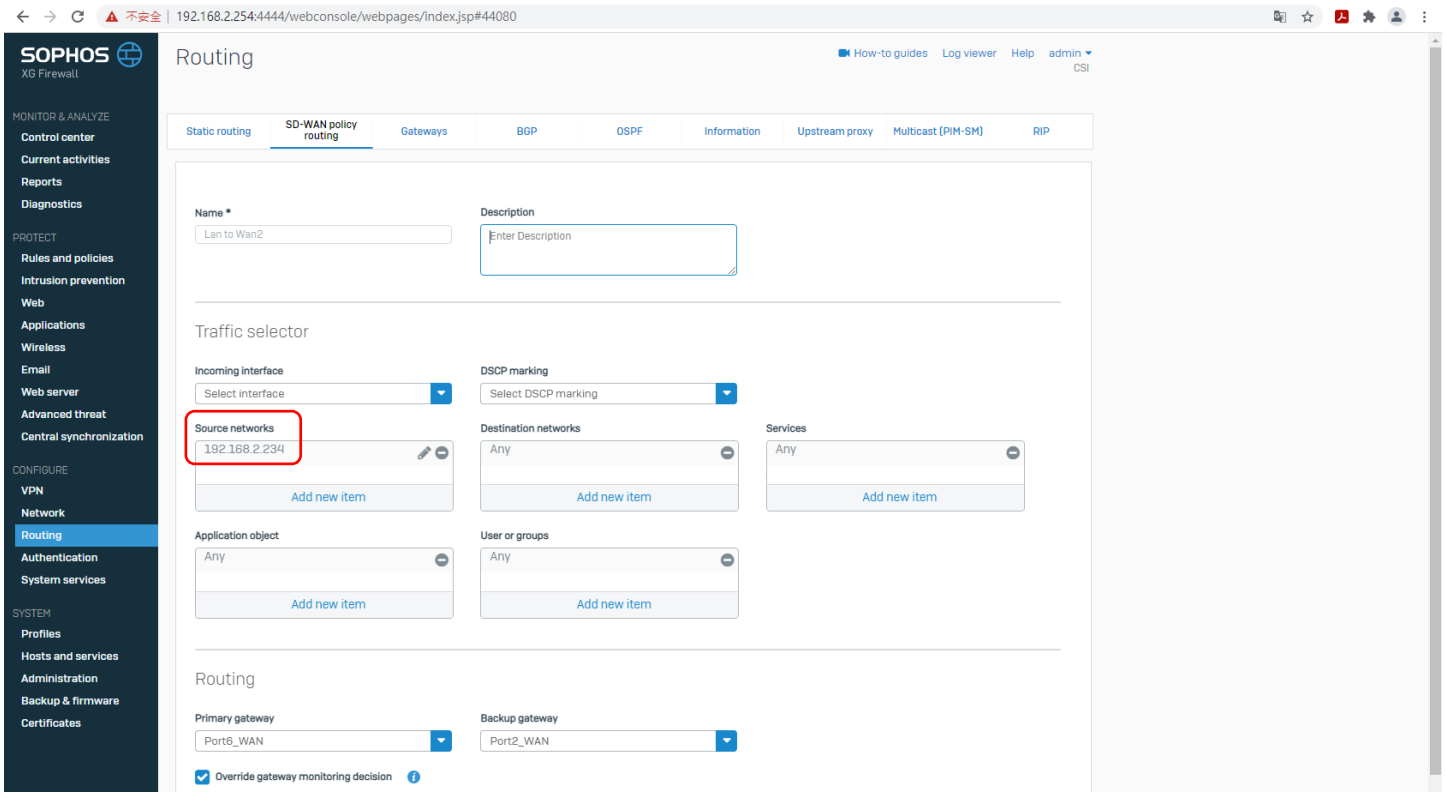
這邊總結一下該如何設定才會導向正確的 WAN port，

注意事項：

1.基本上 LAN to WAN 相關的 NAT rule 用預設的 Default SNAT IPv4 即可。

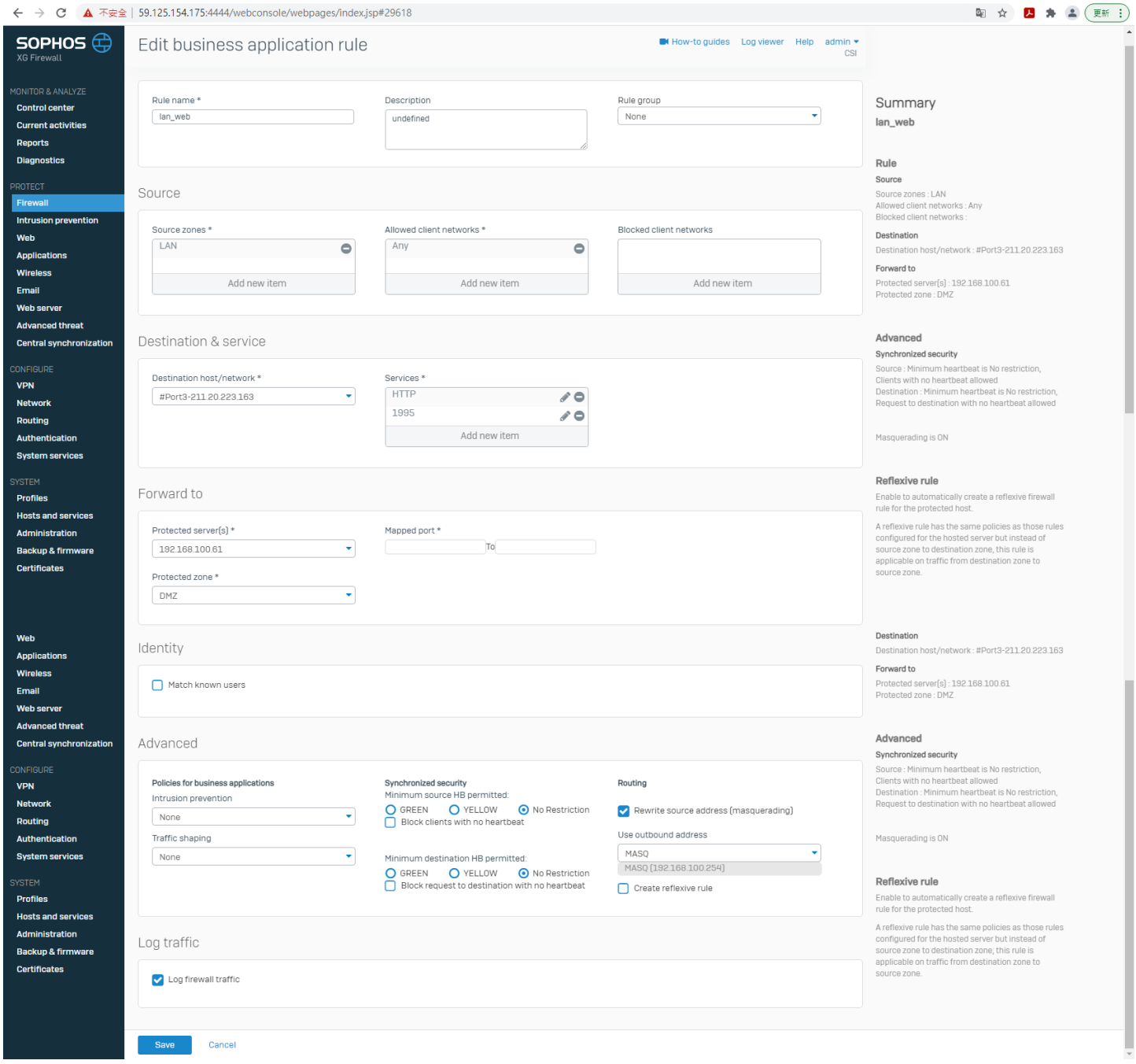
2. SD-WAN policy route 的 Source networks 選用#Port1 一定是以最前方網孔的 WAN 優先，譬如 WAN 有 Port2 跟 Port6，如果選#Port1 一定會以 Port2_WAN 優先出去，即使 Primary gateway 選了 Port6 也是如此，**這點非常重要**。

3.只有 Source networks 在選定 address IP(譬如 192.168.2.234/32)，Primary gateway 跟 Backup gateway 的優先功能才會發揮作用。

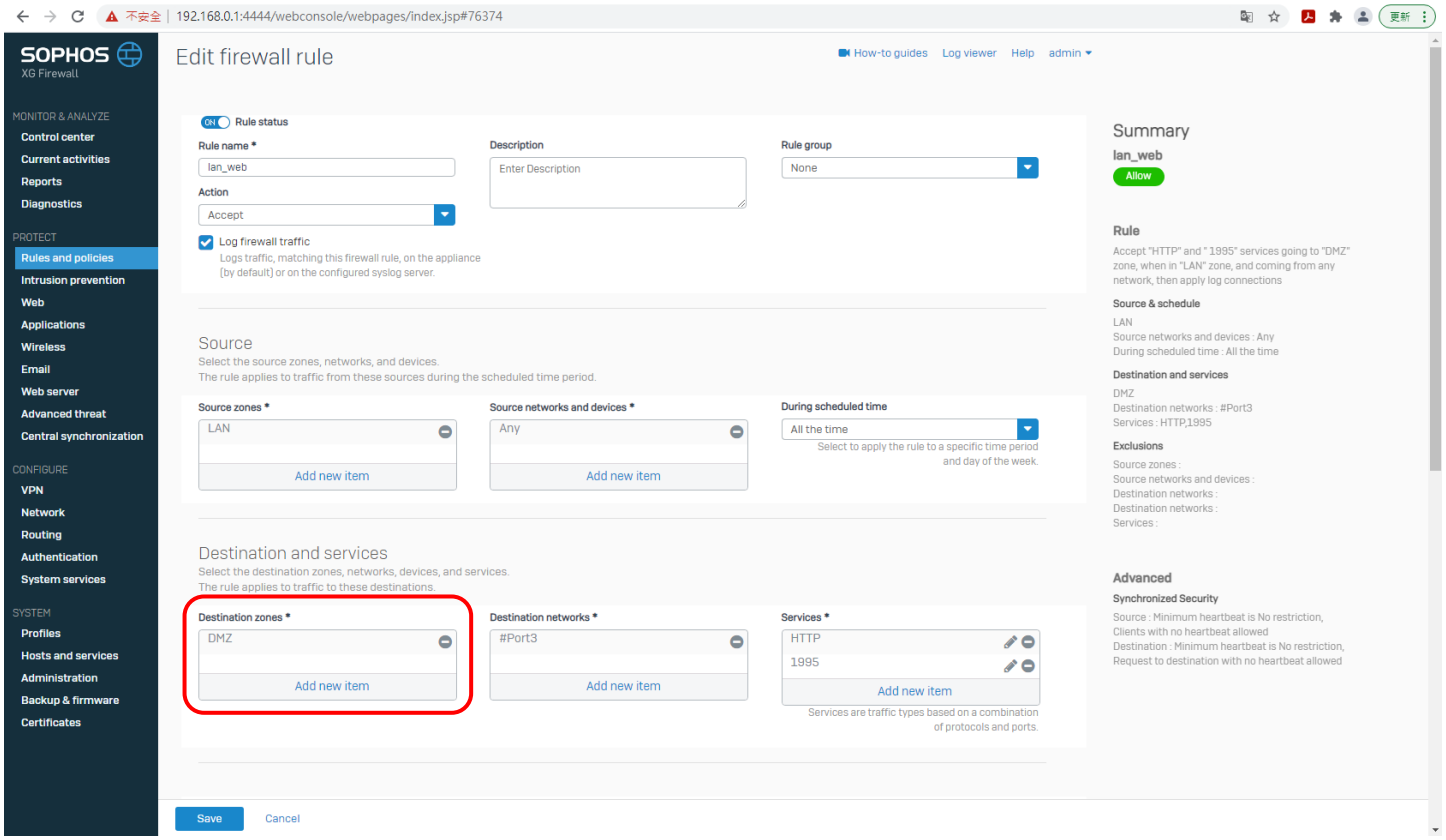


==========2021.6.18(這邊的內容被第 26 頁之後修正)==========

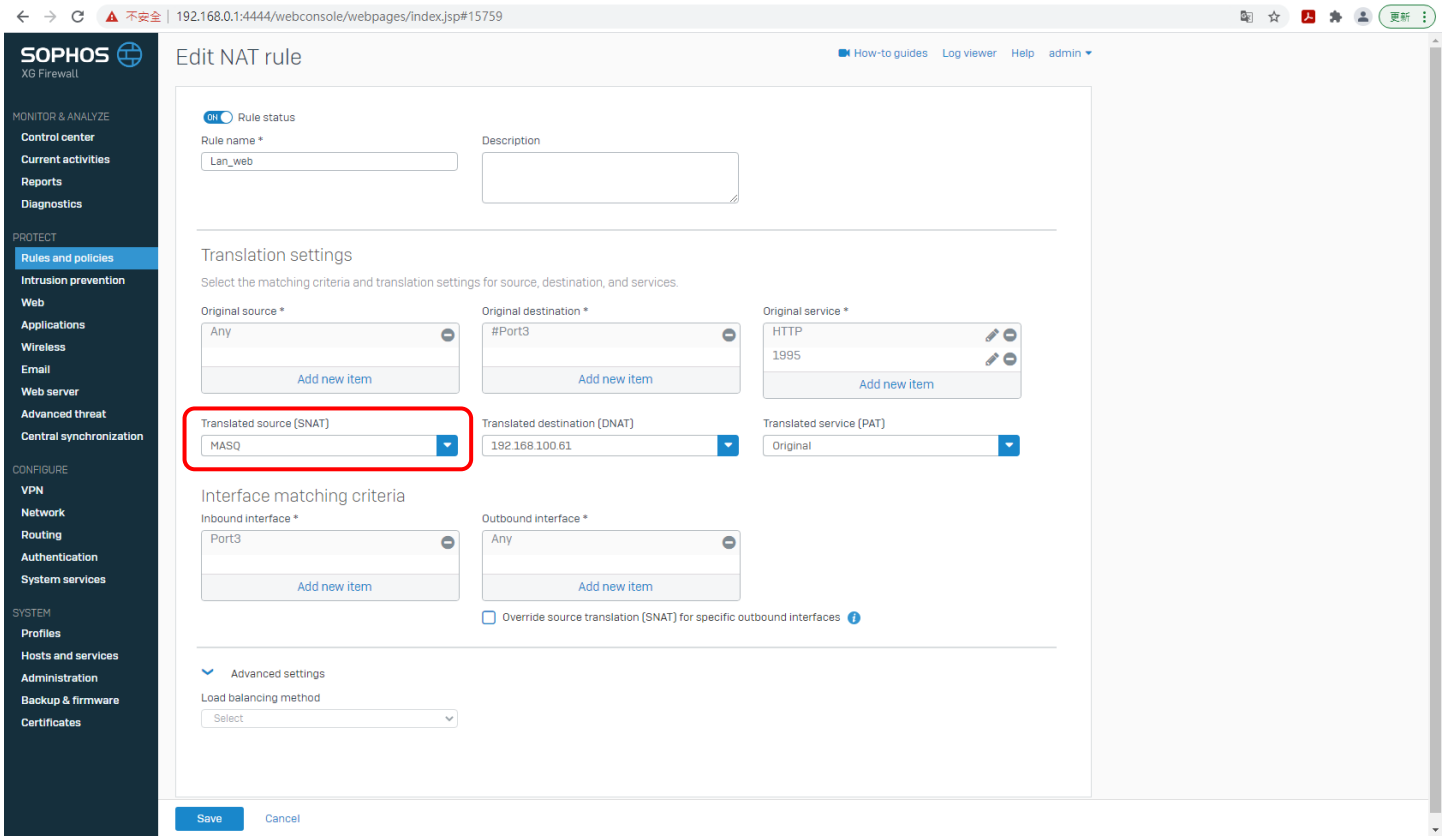
發現 LAN to WAN to DMZ 的防火牆規則在 v18 不太確定怎麼設定，所以這邊先記錄一下，先放上 v17 是怎樣設定的，



以上 v17 是那樣設定，v18 我是這樣設定，這一頁不確定的地方是 Destination zones 這欄位，因為 v17 沒有這一欄位，但按照 LAN to WAN 跟 WAN to DMZ 官方討論區有人分享的設定內容(網址：https://community.sophos.com/sophos-xg-firewall/f/recommended-reads/121919/how-to-configure-firewall-rule-and-nat-rule-on-sophos-xg-v18)，我把 Destination zones 選擇 DMZ，



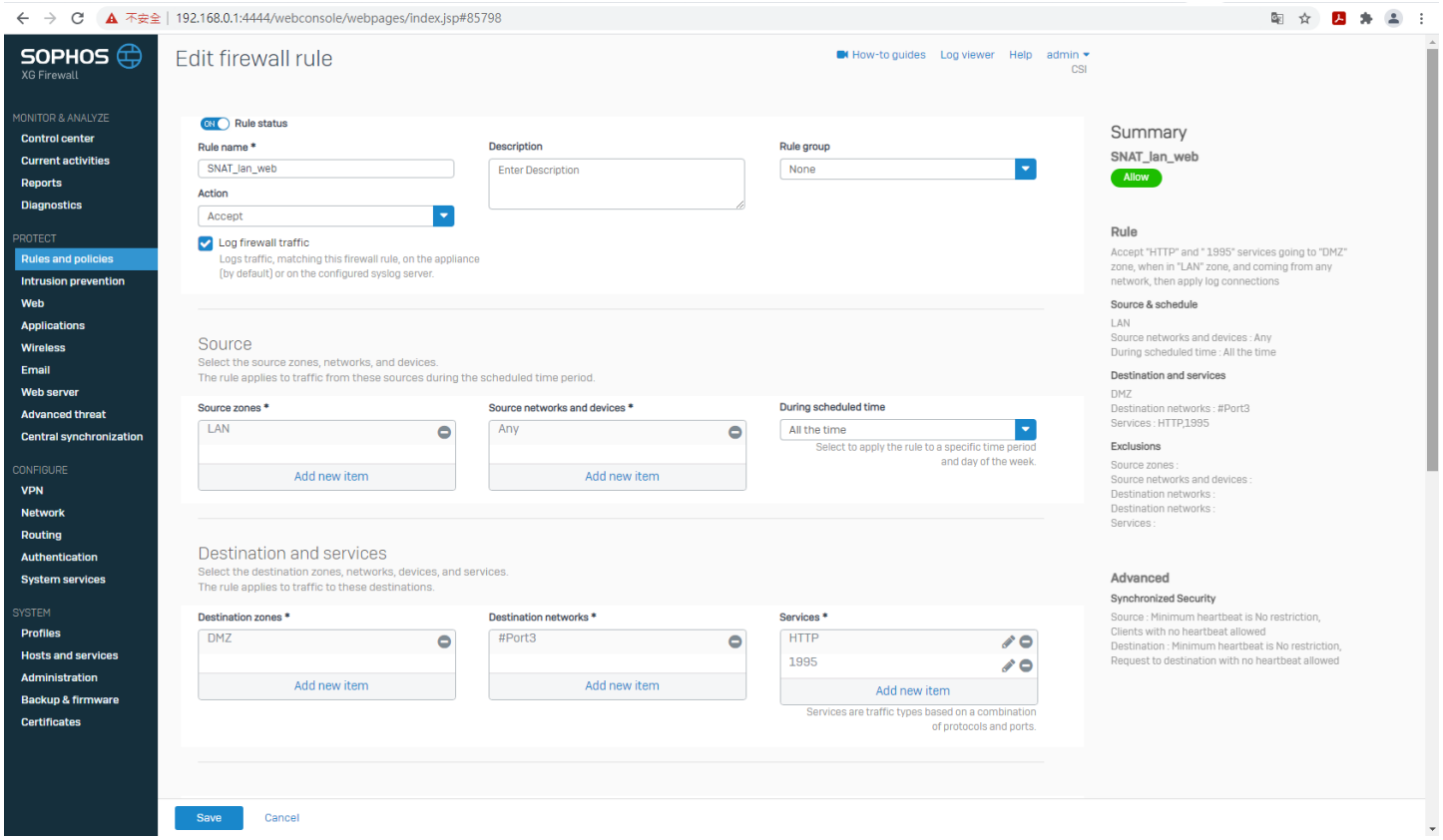
接下來是 NAT rule 這邊，基本上 Original destination 選哪個 Inbound interface 就會選一樣的，所以這邊都是 Port3，另外比較特別的是 Translated source 選了 MASQ(一般都選 Original)，Outbound interface 有考慮要不要選 Port4(DMZ zone)，可是官方討論區那人分享一句話"Outbound interface" is configured to Port1, the DNAT rule won't match inbound HTTPS traffic arriving Port2.”大致是說如果 Outbound interface 只選 Port1 的話，那 HTTPS 的流量就不能依靠 Port2 通過，所以這邊還是保持基本上的設定選 Any 了。



==========2021.6.29 更新==========

LAN to WAN to LAN(or DMZ)，其實這是 SNAT 的概念(然後平常 WAN to LAN 的是 DNAT 概念)，LAN to WAN 也是 SNAT 概念，
官方 SNAT(LAN to WAN to LAN(or DMZ))的設定內容，參考網址：https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/learningContents/CreatingSNATRule.html，不過最後沒有使用這個設定，

最後用 v17.5.15 升到 v18.0.5 知道 LAN to WAN to LAN(or DMZ)的 SNAT 的設定方式，這邊用生命線的來作範例，防火牆規則基本上沒有問題，



重要的是 NAT 規則的設定，重點有兩個地方：Inbound interface 要選 Port1(LAN)，Translated source (SNAT)選 MASQ，基本上釐清了 SNAT(LAN to WAN to DMZ<or LAN>)的設定問題了。