

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，

192.168.50.254:44444/webconsole/webpages/index.jsp#5655

Rules and policies

How-to guides Log viewer Help admin

Firewall rules NAT rules SSL/TLS inspection rules

IPV4 IPV6 Disable filter Add firewall rule Disable Delete

Rule type	Source zone	Destination zone	Status	Rule ID	Add Filter	Reset filter
1	VPN to LAN in 0 B, out 0 B	LAN, Any host	Any service	#3	Accept	...
2	LAN to VPN in 0 B, out 0 B	VPN, Any host	Any service	#2	Accept	...
3	FTP Server in 0 B, out 0 B	LAN, #Port2	FTP	#8	Accept	...
4	Block Mails_Videos in 0 B, out 0 B	LAN, Any host	Any service	#10	Accept	...
5	Auto-added firewall... in 0 B, out 0 B	Any zone, Any host	SMTP, SMTP(S), SMTPS_465, POP3...	#1	Accept	...
6	#Default_Network_P... in 0 B, out 0 B	LAN, Any host	Any service	#5	Accept	...
7	Drop all in 0 B, out 0 B	Any zone, Any host	Any service	#0	Drop	...

Showing 7 of 7. Selected 0

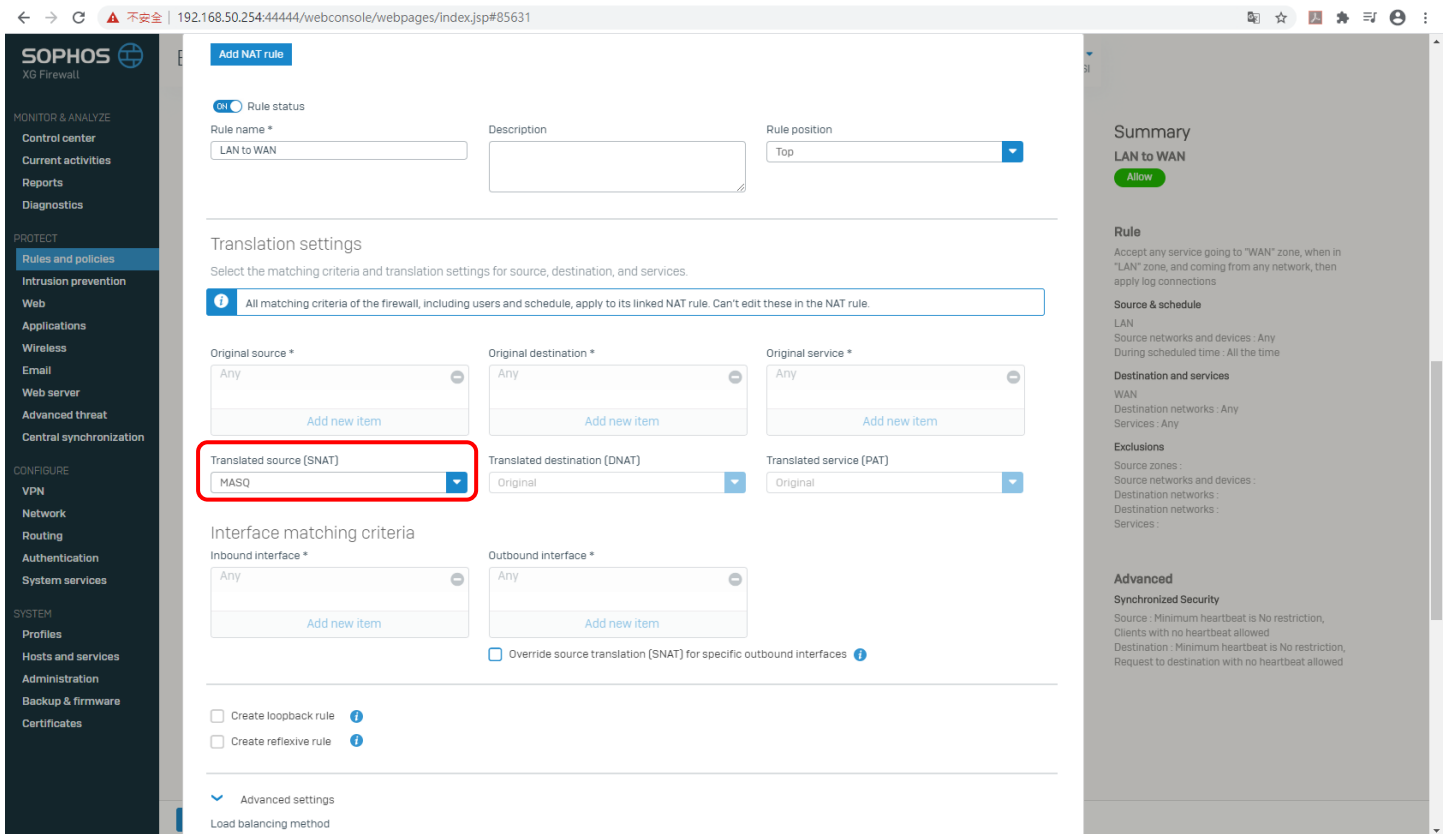
試著新增一般 LAN to WAN 方向，上半部設定沒有太大的問題

The screenshot shows the 'Add firewall rule' configuration page in the Sophos XG Firewall web console. The rule is named 'LAN to WAN' and is set to 'Accept' action. The source zone is 'LAN' and the destination zone is 'WAN'. The rule is positioned at the top. The summary on the right indicates the rule is 'Allow' and applies to traffic from the LAN zone to the WAN zone.

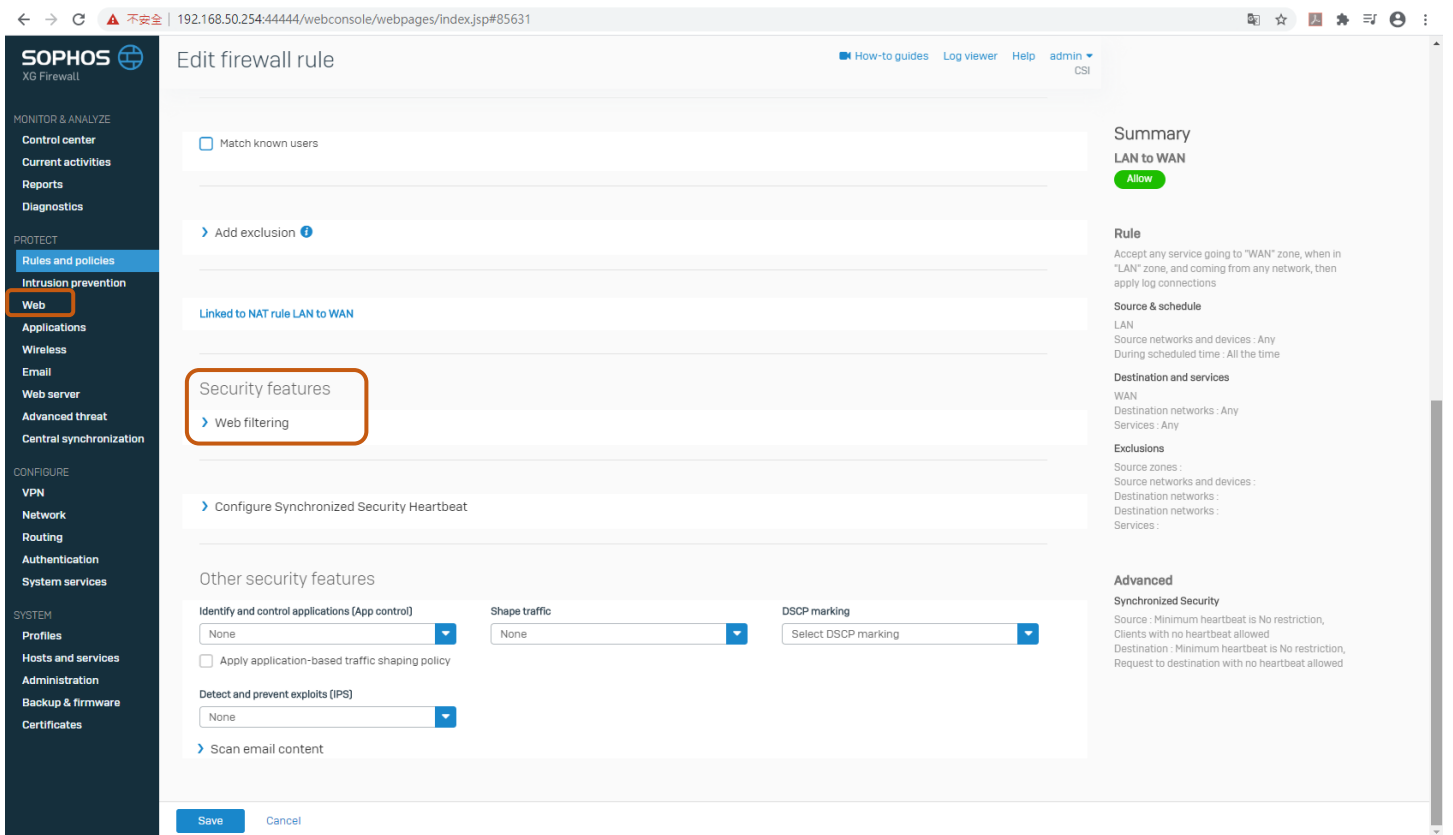
但是下半部有個需要注意的地方，Create Linked NAT rule 裡面還需要設定，點擊它，

The screenshot shows the 'Create linked NAT rule' configuration page. The 'Create linked NAT rule' link is highlighted with a red box. The page shows various security features like Web filtering, Synchronized Security Heartbeat, and App control. The summary on the right indicates the rule is 'Allow' and applies to traffic from the LAN zone to the WAN zone.

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

NAT type	Name	Original	Translated	Interface	ID	Usage
IPV4	LAN to WAN Firewall rule ID: 4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2020-07-15 10:15... used:	#6	38
	fw#8-migrated-NAT-Ru...	Source: Any host Service: FTP Destination: #Port2:36.236.1...	Source: Original Service: migrated_service_fw...	Inbound: Port2 Outbound: Any interface Last used: Unused	#4	0
	fw#10-migrated-NAT-Ru...	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2020-07-15 10:04... used:	#1	26
	fw#1-migrated-NAT-Ru...	Source: Any host Service: SMTP, SMTP(S), SMT...	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#2	0
	fw#5-migrated-NAT-Ru...	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#3	0
	Default SNAT IPv4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Port2 Last used: Unused	#5	0

剛好就是對應 LAN to WAN ,

Rule type	Name	Source zone	Destination zone	Status	Rule ID	Action	Feature and service
	VPN to LAN in 0 B, out 0 B	VPN, Any host	LAN, Any host	Any service	#3	Accept	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]
	LAN to VPN in 0 B, out 0 B	LAN, Any host	VPN, Any host	Any service	#2	Accept	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]
	FTP Server in 0 B, out 0 B	WAN, Any host	LAN, #Port2	FTP	#8	Accept	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]
	Block-Mail-Video in 41.54 KB, out 36.95 KB	LAN, Any host	WAN, Any host	Any service	#10	Accept	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]
	Auto-added firewall in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S), SMTPS, H65, POP3...	#1	Accept	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]
	#Default_Network_P... in 0 B, out 0 B	LAN, Any host	WAN, Any host	Any service	#5	Accept	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]
	LAN to WAN in 2.82 MB, out 455.47 KB	LAN, Any host	WAN, Any host	Any service	#4	Accept	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]
	Drop all in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	[PS] AV [WEB] [APP] [G] [H] [L] [U] [N] [P] [X] [E] [G]

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

Match known users

Add exclusion

Nat rule ID: 6

Summary
LAN to WAN
Allow

Rule
Accept any service going to "WAN" zone, when in "LAN" zone, and coming from any network, then apply log connections

Source & schedule
LAN
Source networks and devices: Any

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。

The screenshot shows the 'Edit firewall rule' interface in the Sophos XG Firewall web console. The rule is named 'WAN to LAN' and is set to 'Accept' action. The source is 'WAN' and the destination is 'LAN'. The service is 'Client Port 3396'. The rule is highlighted with a red box.

Rule name: WAN to LAN
Description: Enter Description
Rule group: None
Action: Accept
Log firewall traffic: Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source:
Select the source zones, networks, and devices. The rule applies to traffic from these sources during the scheduled time period.
Source zones: WAN
Source networks and devices: Any
During scheduled time: All the time

Destination and services:
Select the destination zones, networks, devices, and services. The rule applies to traffic to these destinations.
Destination zones: LAN
Destination networks: #Port2
Services: Client Port 3396

Summary:
WAN to LAN
Allow
Rule: Accept "Client Port 3396" service going to "LAN" zone, when in "WAN" zone, and coming from any network, then apply log connections
Source & schedule: WAN
Source networks and devices: Any
During scheduled time: All the time
Destination and services: LAN
Destination networks: #Port2
Services: Client Port 3396
Exclusions: Source zones: Source networks and devices: Destination networks: Services:

Advanced:
Synchronized Security:
Source: Minimum heartbeat is No restriction, Clients with no heartbeat allowed
Destination: Minimum heartbeat is No restriction, Request to destination with no heartbeat allowed

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。

The screenshot shows the 'Edit NAT rule' interface in the Sophos XG Firewall web console. The rule is named 'WAN to LAN DNAT'. The original source is 'Any', original destination is '#Port2', and original service is 'Client Port 3396'. The translated destination is 'FTP PC' and translated service is 'RDP-3389'. The interface matching criteria are 'Port2' for inbound and 'Any' for outbound. The rule is highlighted with a red box.

Rule name: WAN to LAN DNAT
Description: Enter Description

Translation settings:
Select the matching criteria and translation settings for source, destination, and services.
Original source: Any
Original destination: #Port2
Original service: Client Port 3396
Translated source (SNAT): Original
Translated destination (DNAT): FTP PC
Translated service (PAT): RDP-3389

Interface matching criteria:
Inbound interface: Port2
Outbound interface: Any
 Override source translation (SNAT) for specific outbound interfaces

Advanced settings:
Load balancing method: Select

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

The screenshot shows the 'Rules and policies' page in the Sophos XG Firewall web console. The 'Firewall rules' tab is selected. The interface includes a left sidebar with navigation options like 'Control center', 'Reports', and 'Rules and policies'. The main area displays a table of firewall rules with columns for Rule type, Name, Source, Destination, What, ID, Action, and Feature and service. The table shows 9 rules, including 'WAN to LAN', 'VPN to LAN', 'LAN to VPN', 'FTP Server', 'Block-Mails-Videos', 'Auto-added-Firewall...', '#Default- Network-P...', 'LAN to WAN', and 'Drop all'. A 'Watch: How to use NAT' button is visible above the table.

Rule type	Name	Source	Destination	What	ID	Action	Feature and service
IPV4	WAN to LAN in 169.57 KB, out 33.93 KB	WAN, Any host	LAN, #Port2	Client Port 3396	#6	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	VPN to LAN in 0 B, out 0 B	VPN, Any host	LAN, Any host	Any service	#3	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	LAN to VPN in 0 B, out 0 B	LAN, Any host	VPN, Any host	Any service	#2	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	FTP Server in 0 B, out 0 B	WAN, Any host	LAN, #Port2	FTP	#8	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	Block-Mails-Videos in 41.54 KB, out 36.95 KB	LAN, Any host	WAN, Any host	Any service	#10	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	Auto-added-Firewall- in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S), SMTPS, H65, POP3...	#1	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	#Default- Network-P- in 0 B, out 0 B	LAN, Any host	WAN, Any host	Any service	#5	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	LAN to WAN in 26.72 MB, out 2.35 MB	LAN, Any host	WAN, Any host	Any service	#4	Accept	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]
IPV4	Drop all in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	[PS] [AV] [WEB] [APP] [OS] [HE] [Link] [NAT] [PRX] [LOG]

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

The screenshot shows the 'Rules and policies' page in the Sophos XG Firewall web console, with the 'NAT rules' tab selected. A warning message is displayed: 'Many masqueraded linked NAT (SNAT) rules were created during migration. We didn't prune them automatically to ensure there's no behavior change after migration. You can delete the MASQ rules with destination set only to WAN and turn on the default MASQ rule at the bottom of the NAT rule table. For details, go to the online help.' Below the message is a button: 'Delete linked NAT rules (only MASQ; Destination: WAN) Understood. Don't delete rules'. The main area displays a table of NAT rules with columns for NAT type, Name, Original, Translated, Interface, ID, and Usage. The table shows 7 rules, including 'WAN to LAN DNAT', 'LAN to WAN', and several 'fw#X-migrated-NAT-Rule' entries.

NAT type	Name	Original	Translated	Interface	ID	Usage
IPV4	WAN to LAN DNAT	Source: Any host Service: Client Port 3396 Destination: #Port2:36.236.1...	Source: Original Service: RDP-3389 Destination: FTP PC:192.168...	Inbound: Port2 Outbound: Any interface Last used: Unused	#7	0
IPV4	LAN to WAN Firewall rule ID: 4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2020-07-15 11:32... used:	#6	167
IPV4	fw#8-migrated-NAT-Rule- Firewall rule ID: 8	Source: Any host Service: FTP Destination: #Port2:36.236.1...	Source: Original Service: migrated_service_fw... Destination: FTP PC:192.168...	Inbound: Port2 Outbound: Any interface Last used: Unused	#4	0
IPV4	fw#10-migrated-NAT-Rule- Firewall rule ID: 10	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2020-07-15 10:04... used:	#1	26
IPV4	fw#1-migrated-NAT-Rule- Firewall rule ID: 1	Source: Any host Service: SMTP, SMTP(S), SMT...	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#2	0
IPV4	fw#5-migrated-NAT-Rule- Firewall rule ID: 5	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#3	0

Network 介面沒多大改動，

Network

Interfaces ZONES WAN link manager DNS DHCP IPv6 router advertisement Cellular WAN IP tunnels Neighbors (ARP-NDR) Dynamic DNS

All VLAN RED Add interface

Interface	Status/Interface speed	IP address	Misc
GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	Hardware: GuestAP
Port1 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.50.254/255.255.255.0 Static	Hardware: Port1
Port2 WAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	36.236.124.12/255.255.255.255 PPPoE	Hardware: Port2
Port3 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: Port3
Port4 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: Port4

IPsec VPN 也沒改變，

VPN

IPsec connections SSL VPN (remote access) SSL VPN (site-to-site) Sophos Connect client L2TP (remote access) Clientless access Bookmarks Bookmark groups PPTP (remote access) IPsec policies

General settings

Name: SiteA_to_SiteB IP version: IPv4 IPv6 Dual Activate on save Create firewall rule

Description: [Text Area] Connection type: Site-to-site Gateway type: Respond only

Encryption

Policy: DefaultHeadOffice Authentication type: Preshared key Change preshared key

Gateway settings

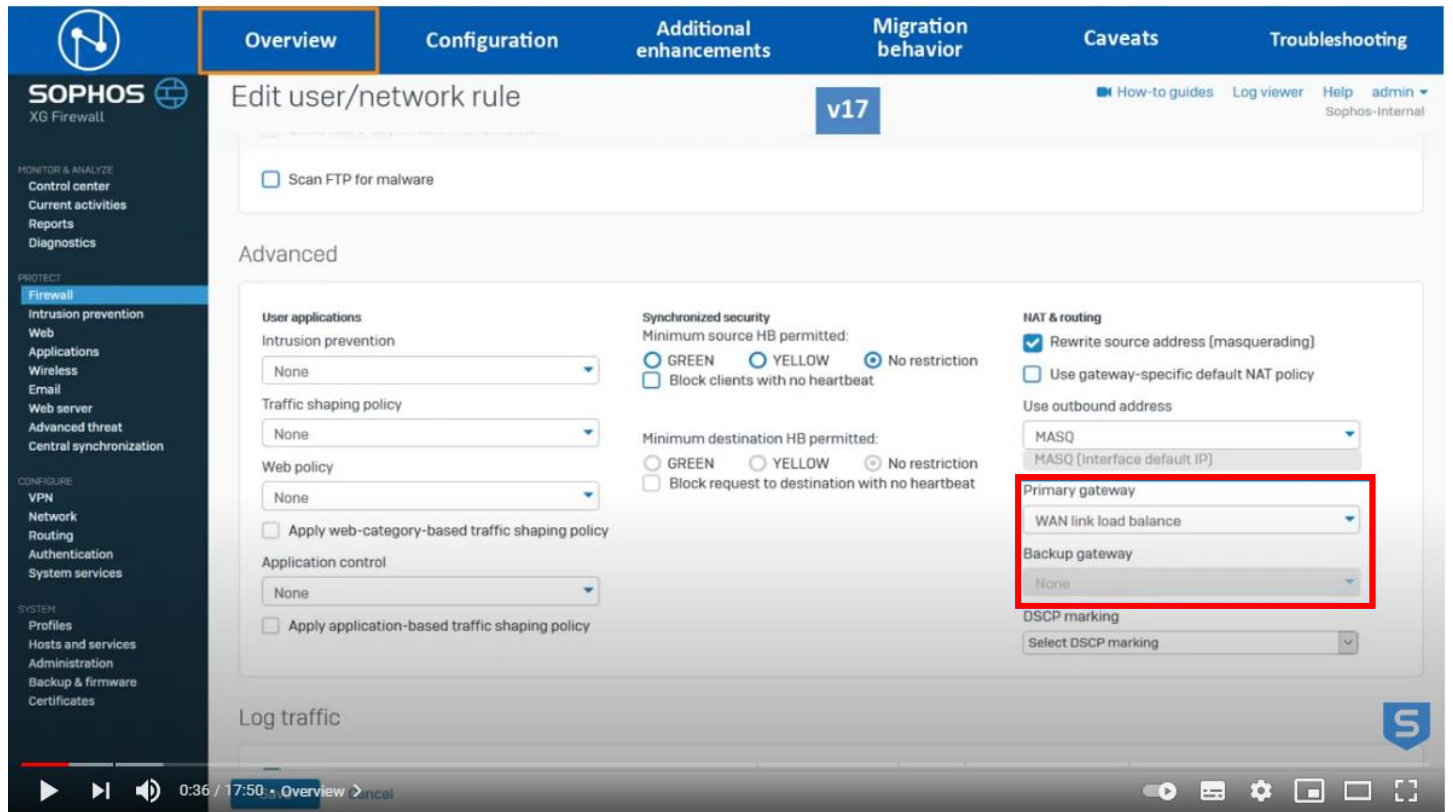
Local gateway: Listening interface: Port2 - 36.236.124.12 Local ID type: Select local ID Local ID: [Text Field]

Remote gateway: Gateway address: 0.0.0.0 Remote ID type: Select remote ID Remote ID: [Text Field]

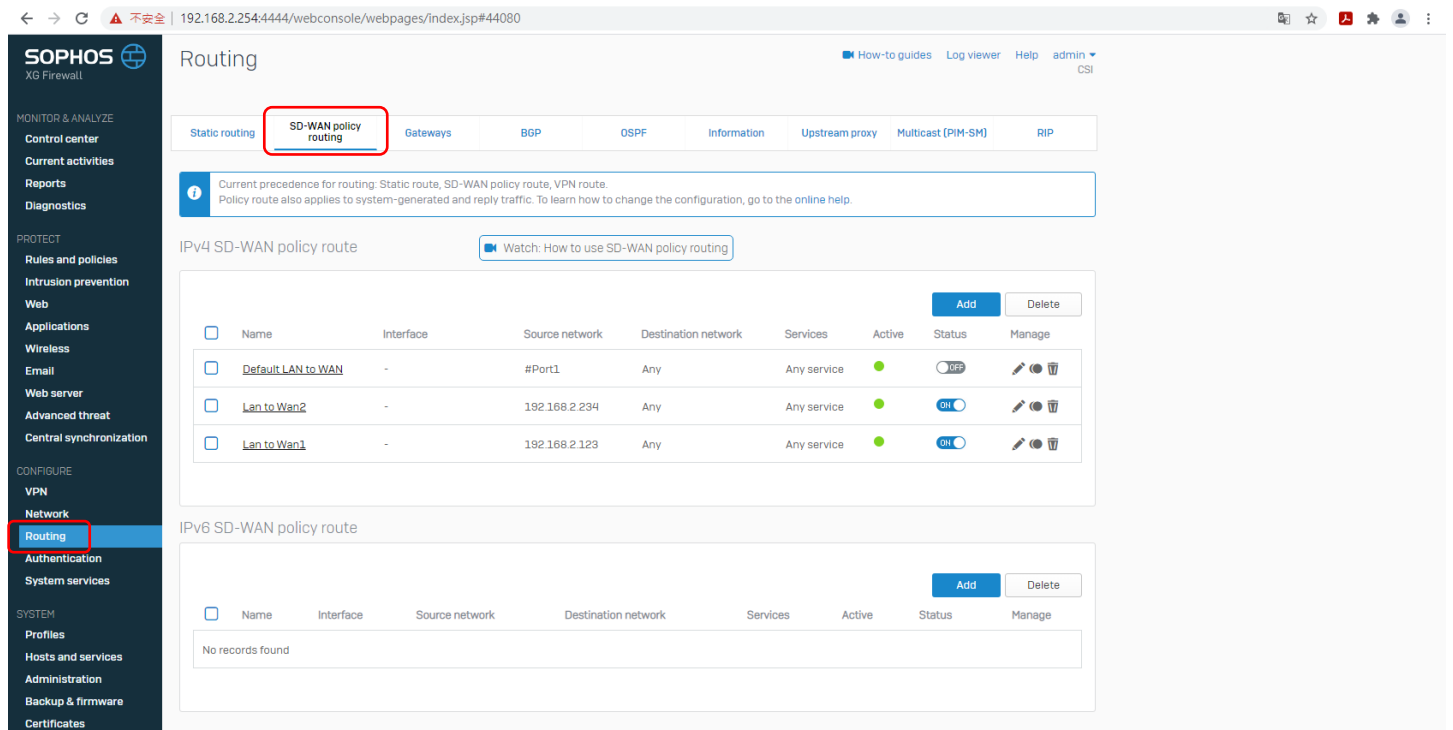
Save Cancel

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

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，

Interface	Status/Interface speed	IP address	Misc
Port1 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.2.254/255.255.255.0 Static	Hardware: Port1
Port2 WAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	1.172.198.180/255.255.255.255 PPPoE	Hardware: Port2
Port3 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: Port3
Port4 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: Port4
Port5 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: Port5
Port6 WAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	36.238.208.125/255.255.255.255 PPPoE	Hardware: Port6

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

#	Name	Source	Destination	What	ID	Action	Feature and service
1	LAN to DMZ	LAN, Any host	DMZ, Any host	Any service	#6	Accept	IPS AV WEB APP G5 HB Link NAT PRX LOG
2	Mail_Server	WAN, Any host	DMZ, #Port2	IMAP, POP3, SMTP(S), Port 4443...	#4	Accept	IPS AV WEB APP G5 HB Link NAT PRX LOG
3	Synology rule	WAN, Any host	LAN, #Port2	Synology Port 5000 - 5001	#3	Accept	IPS AV WEB APP G5 HB Link NAT PRX LOG
4	Home to Csi	WAN, Any host	LAN, #Port2	Port 3395	#1	Accept	IPS AV WEB APP G5 HB Link NAT PRX LOG
5	DMZ to WAN	DMZ, Any host	WAN, Any host	Any service	#2	Accept	IPS AV WEB APP G5 HB Link NAT PRX LOG
6	#Default_Network_P...	LAN, Any host	WAN, Any host	Any service	#5	Accept	IPS AV WEB APP G5 HB Link NAT PRX LOG
7	Drop all	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	IPS AV WEB APP G5 HB Link NAT PRX LOG

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，

The screenshot shows the 'Rules and policies' page in the Sophos XG Firewall web console. The 'NAT rules' tab is selected. A table lists five NAT rules. Rules #4 and #5 are highlighted with a red box. Rule #4 is '#NAT_Default_Network_Policy' and rule #5 is 'Default SNAT IPv4'.

#	Name	Original	Translated	Interface	ID	Usage
1	Mail_Server	Source: Any host Service: IMAP POP3 SMTP[S]... Destination: #Port2.1172.19...	Source: Original Service: Original Destination: 192.168.100.25...	Inbound: Port2 Outbound: Any interface Last used: 2021-06-16 09:51... used:	#5	19
2	Synology.v.rule	Source: Any host Service: Synology Port 5000... Destination: #Port2.1172.19...	Source: Original Service: Original Destination: 192.168.2.144.1...	Inbound: Port2 Outbound: Any interface Last used: 2021-06-16 10:07... used:	#4	6
3	Home to Cai	Source: Any host Service: Port 3395 Destination: #Port2.1172.19...	Source: Original Service: Port 3389 Destination: 192.168.2.44.19...	Inbound: Port2 Outbound: Any interface Last used: 2021-06-16 11:28... used:	#1	6
4	#NAT_Default_Network_Policy	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#3	0
5	Default SNAT IPv4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Port2, Port6 Last used: 2021-06-16 11:44... used:	#2	44

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)，

The screenshot shows the 'Edit NAT rule' page for the 'Default SNAT IPv4' rule. The 'Outbound interface' field is highlighted with a red box, showing 'Port2' and 'Port6'.

Rule name: Default SNAT IPv4

Description: Auto created IPv4 SNAT MASQ rule for traffic from "ANY" inbound interface to WAN outbound interface. Updated automatically with WAN

Translation settings:

- Original source: Any
- Original destination: Any
- Original service: Any
- Translated source (SNAT): MASQ
- Translated destination (DNAT): Original
- Translated service (PAT): Original

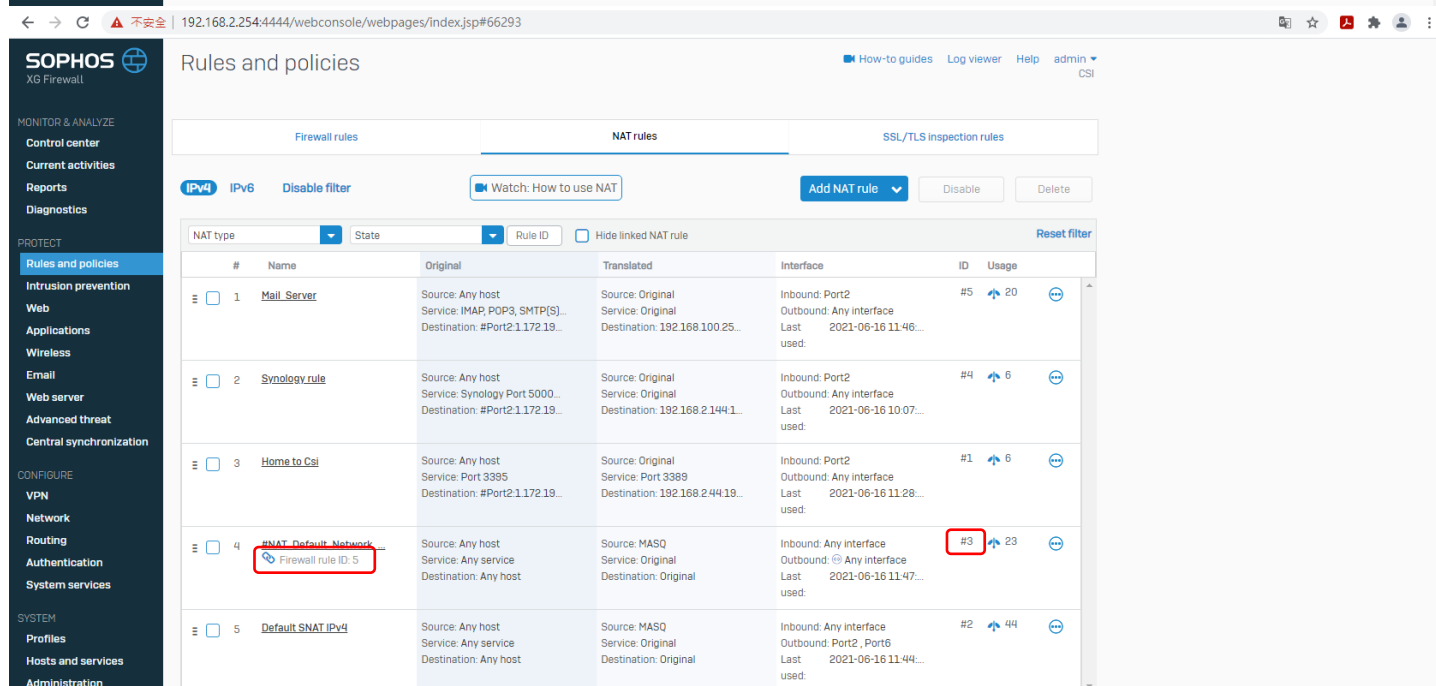
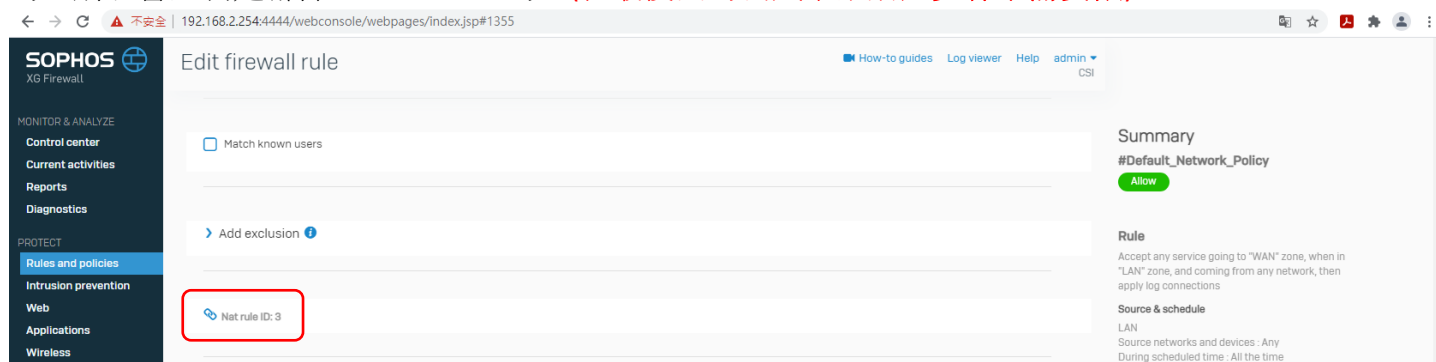
Interface matching criteria:

- Inbound interface: Any
- Outbound interface: Port2, Port6
- Override source translation (SNAT) for specific outbound interfaces

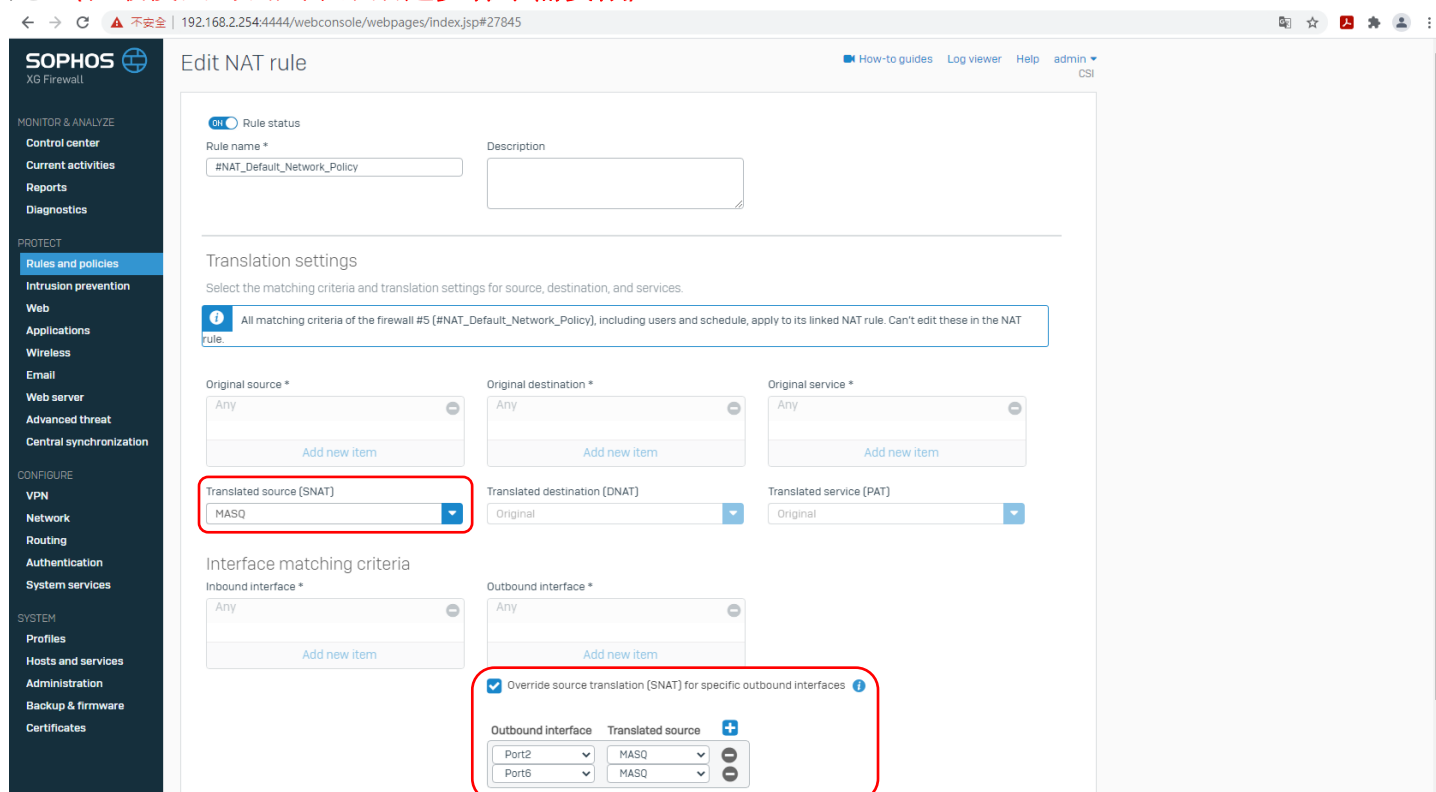
Advanced settings:

- Load balancing method: Select

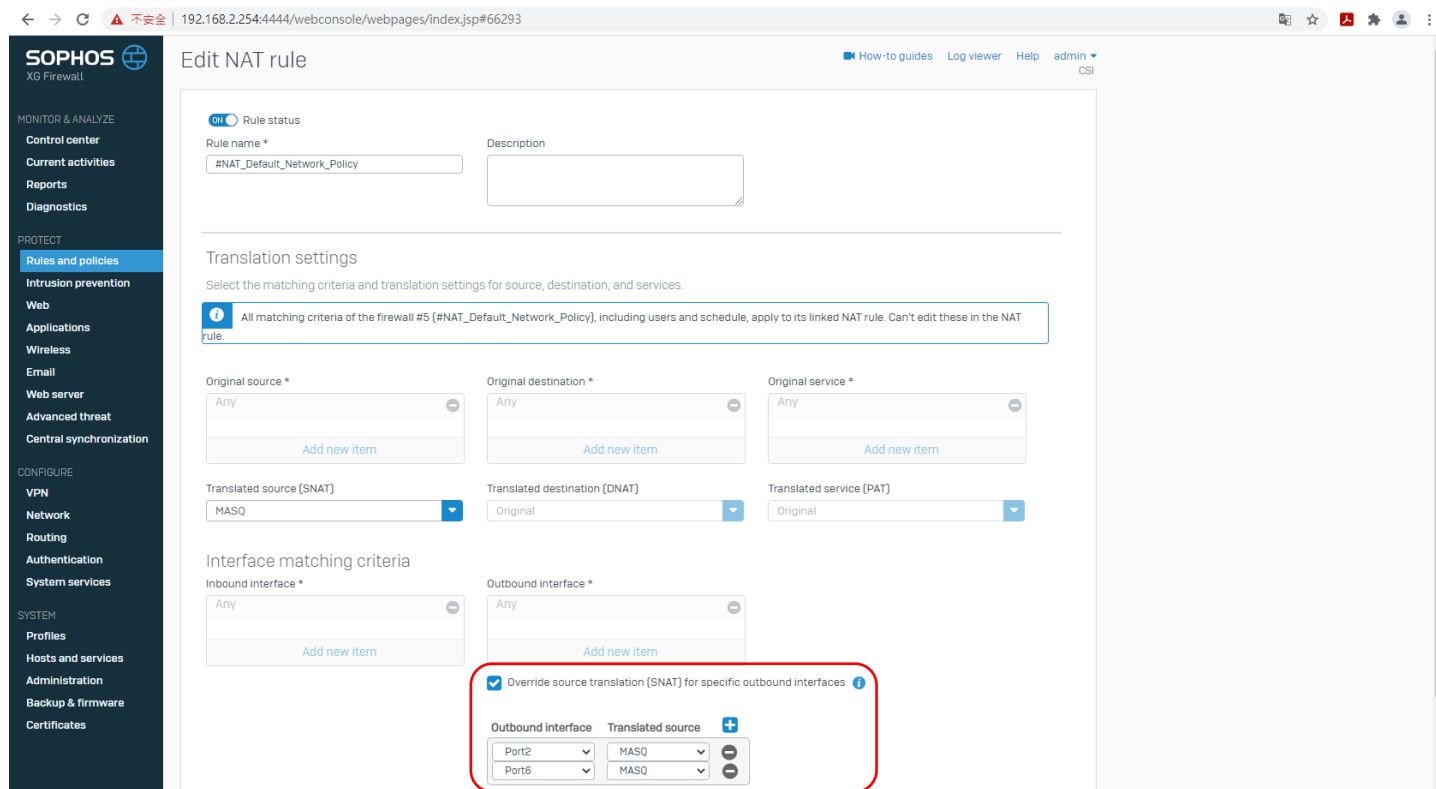
接著是#NAT_Default_Network_Policy，這條 NAT rule 是在 Firewall rule 的#Default_Network_Policy 裡新增的，所以會註明是哪條 Firewall rule 的，(在最後面的測試中結論這步驟不需要做)



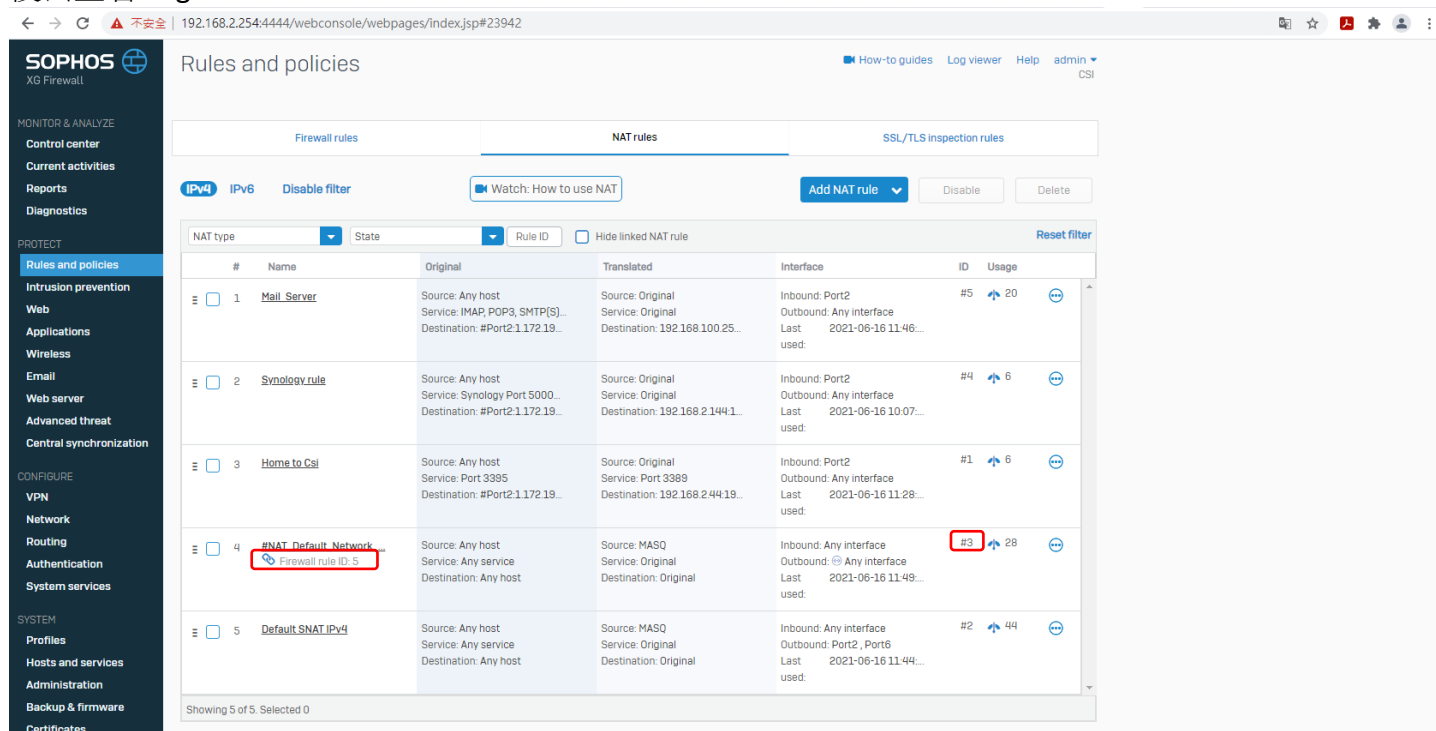
而如果 NAT rule 是在 Firewall rule 裡新增的，基本上能修改的地方不多，只有紅框所匡列的地方可以設定，(在最後面的測試中結論這步驟不需要做)



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，

Log viewer

Policy test

Src IP is 192.168.2.44

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。

Log viewer

Policy test

Src IP is 192.168.2.44

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	106.10.218.198	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 connection.

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

The screenshot shows the 'Rules and policies' page in the Sophos XG Firewall web console. The 'NAT rules' tab is active. A table lists five NAT rules. Rule #4, named '#NAT-Default-Network', is highlighted with a red rectangular box. The table columns are: #, Name, Original, Translated, Interface, ID, and Usage.

#	Name	Original	Translated	Interface	ID	Usage
1	Mail_Server	Source: Any host Service: IMAP, POP3, SMTP(S).. Destination: #Port2.1.172.19...	Source: Original Service: Original Destination: 192.168.100.25...	Inbound: Port2 Outbound: Any interface Last used: 2021-06-16 11:46...	#5	20
2	Synology_rule	Source: Any host Service: Synology Port 5000.. Destination: #Port2.1.172.19...	Source: Original Service: Original Destination: 192.168.2.144.1...	Inbound: Port2 Outbound: Any interface Last used: 2021-06-16 10:07...	#4	6
3	Home_to_Cai	Source: Any host Service: Port 3389 Destination: #Port2.1.172.19...	Source: Original Service: Port 3389 Destination: 192.168.2.44.19...	Inbound: Port2 Outbound: Any interface Last used: 2021-06-16 11:28...	#1	6
4	#NAT-Default-Network Firewall rule ID: 5	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2021-06-16 11:48...	#3	28
5	Default-SNAT-IPv4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Port2_Port6 Last used: 2021-06-16 11:44...	#2	44

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

The screenshot shows the 'Routing' page in the Sophos XG Firewall web console, specifically the 'SD-WAN policy routing' tab. The configuration form is as follows:

- Name:** Default LAN to WAN
- Description:** Enter Description
- Traffic selector:**
 - Incoming interface:** Select interface
 - DSCP marking:** Select DSCP marking
 - Source networks:** #Port1
 - Destination networks:** Any
 - Services:** Any
 - Application object:** Any
 - User or groups:** Any
- Routing:**
 - Primary gateway:** Port6_WAN
 - Backup gateway:** Port2_WAN
 - Override gateway monitoring decision

Buttons for 'Save' and 'Cancel' are visible at the bottom.

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)

Edit NAT rule

Rule name: #NAT_Default_Network_Policy

Translation settings:

- Translated source (SNAT): MASQ
- Translated destination (DNAT): Original
- Translated service (PAT): Original

Interface matching criteria:

- Inbound interface: Any
- Outbound interface: Any

Override source translation (SNAT) for specific outbound interfaces:

Outbound interface	Translated source
Port6	MASQ
Port2	MASQ

SD-WAN policy route 也是先 Port6 再 Port2 ,

The screenshot shows the Sophos XG Firewall configuration interface for SD-WAN policy routing. The configuration is as follows:

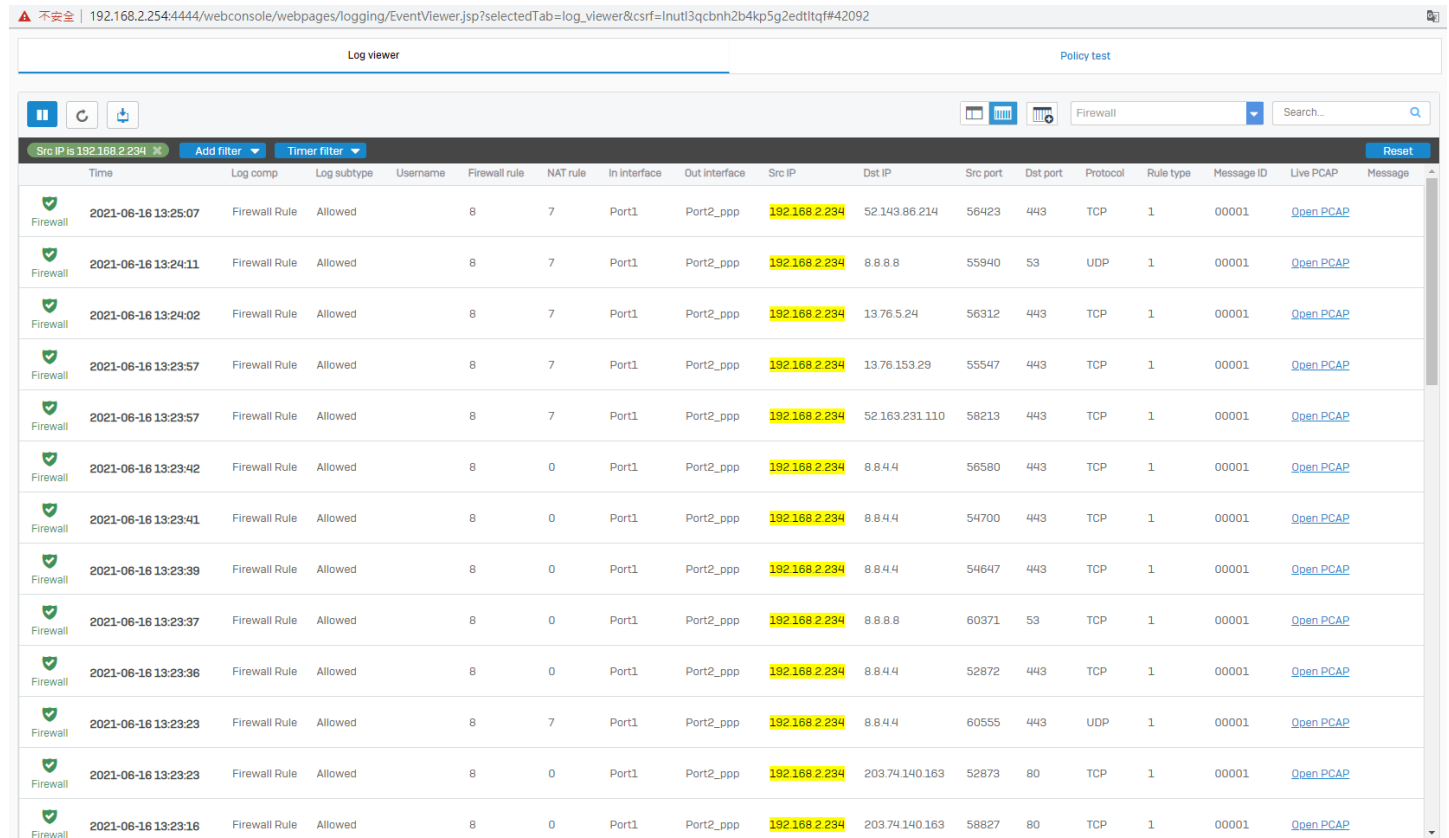
- Name:** Default LAN to WAN
- Description:** Enter Description
- Traffic selector:**
 - Incoming interface: Select interface
 - DSCP marking: Select DSCP marking
 - Source networks: #Port1
 - Destination networks: Any
 - Services: Any
 - Application object: Any
 - User or groups: Any
- Routing:**
 - Primary gateway: Port6_WAN
 - Backup gateway: Port2_WAN
 - Override gateway monitoring decision

這樣設定沒有效果，

The screenshot shows the Log viewer interface with a list of firewall logs. The logs are filtered by source IP 192.168.2.44. The table below represents the data shown in the logs:

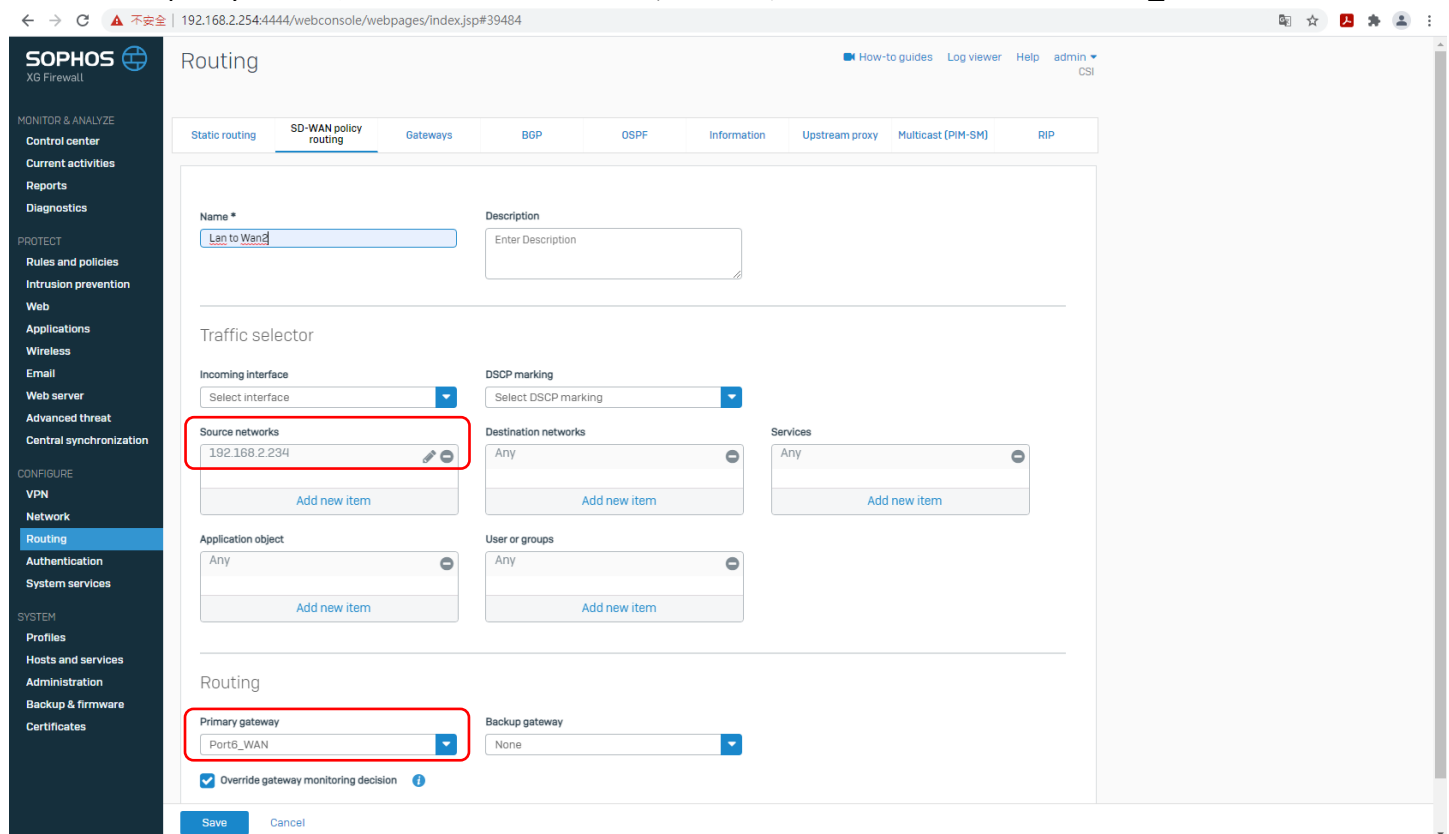
Time	Log comp	Log subtype	Username	Firewall rule	NAT rule	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Message ID	Live PCAP	Message
2021-06-16 12:13:15	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	162.243.161.5	58330	8443	TCP	1	00001	Open PCAP	
2021-06-16 12:13:15	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	162.243.161.5	51658	8443	TCP	1	00001	Open PCAP	
2021-06-16 12:13:14	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	162.243.161.5	58330	8443	TCP	1	00001	Open PCAP	
2021-06-16 12:13:14	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	162.243.161.5	51658	8443	TCP	1	00001	Open PCAP	
2021-06-16 12:13:14	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	162.243.161.5	58330	8443	TCP	1	00001	Open PCAP	
2021-06-16 12:13:09	Invalid Traffic	Denied		N/A	0			192.168.2.44	8.8.8.8	63794	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 12:13:08	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	8.8.8.8	52519	53	UDP	1	00001	Open PCAP	
2021-06-16 12:12:53	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	35.190.90.30	56692	443	TCP	1	00001	Open PCAP	
2021-06-16 12:12:48	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	35.190.12.84	58872	443	TCP	1	00001	Open PCAP	
2021-06-16 12:12:48	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	52.114.133.60	59391	443	TCP	1	00001	Open PCAP	
2021-06-16 12:12:47	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	203.226.255.40	61566	443	TCP	1	00001	Open PCAP	
2021-06-16 12:12:44	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	103.243.202.190	62931	443	TCP	1	00001	Open PCAP	
2021-06-16 12:12:43	Firewall Rule	Allowed		5	3	Port1	Port2_ppp	192.168.2.44	35.72.220.165	52978	443	TCP	1	00001	Open PCAP	

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，



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
2021-06-16 13:25:07	Firewall Rule	Allowed		8	7	Port1	Port2_ppp	192.168.2.234	52.143.86.214	56423	443	TCP	1	00001	Open PCAP
2021-06-16 13:24:11	Firewall Rule	Allowed		8	7	Port1	Port2_ppp	192.168.2.234	8.8.8.8	55940	53	UDP	1	00001	Open PCAP
2021-06-16 13:24:02	Firewall Rule	Allowed		8	7	Port1	Port2_ppp	192.168.2.234	13.76.5.24	56312	443	TCP	1	00001	Open PCAP
2021-06-16 13:23:57	Firewall Rule	Allowed		8	7	Port1	Port2_ppp	192.168.2.234	13.76.153.28	55547	443	TCP	1	00001	Open PCAP
2021-06-16 13:23:57	Firewall Rule	Allowed		8	7	Port1	Port2_ppp	192.168.2.234	52.163.231.110	58213	443	TCP	1	00001	Open PCAP
2021-06-16 13:23:42	Firewall Rule	Allowed		8	0	Port1	Port2_ppp	192.168.2.234	8.8.4.4	56580	443	TCP	1	00001	Open PCAP
2021-06-16 13:23:41	Firewall Rule	Allowed		8	0	Port1	Port2_ppp	192.168.2.234	8.8.4.4	54700	443	TCP	1	00001	Open PCAP
2021-06-16 13:23:39	Firewall Rule	Allowed		8	0	Port1	Port2_ppp	192.168.2.234	8.8.4.4	54647	443	TCP	1	00001	Open PCAP
2021-06-16 13:23:37	Firewall Rule	Allowed		8	0	Port1	Port2_ppp	192.168.2.234	8.8.8.8	60371	53	TCP	1	00001	Open PCAP
2021-06-16 13:23:36	Firewall Rule	Allowed		8	0	Port1	Port2_ppp	192.168.2.234	8.8.4.4	52872	443	TCP	1	00001	Open PCAP
2021-06-16 13:23:23	Firewall Rule	Allowed		8	7	Port1	Port2_ppp	192.168.2.234	8.8.4.4	60555	443	UDP	1	00001	Open PCAP
2021-06-16 13:23:23	Firewall Rule	Allowed		8	0	Port1	Port2_ppp	192.168.2.234	203.74.140.163	52873	80	TCP	1	00001	Open PCAP
2021-06-16 13:23:16	Firewall Rule	Allowed		8	0	Port1	Port2_ppp	192.168.2.234	203.74.140.163	58827	80	TCP	1	00001	Open PCAP

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



The screenshot shows the 'Routing' configuration page in the Sophos XG Firewall web console. The 'SD-WAN policy routing' tab is selected. The configuration includes:

- Name:** Lan to Wan2
- Traffic selector:**
 - Incoming interface:** Select interface
 - DSCP marking:** Select DSCP marking
 - Source networks:** 192.168.2.234 (highlighted with a red box)
 - Destination networks:** Any
 - Services:** Any
- Application object:** Any
- User or groups:** Any
- Routing:**
 - Primary gateway:** Port6_WAN (highlighted with a red box)
 - Backup gateway:** None
- Override gateway monitoring decision

新增完成，

Routing

Static routing | SD-WAN policy routing | Gateways | BGP | OSPF | Information | Upstream proxy | Multicast (PIM-SM) | RIP

Current precedence for routing: Static route, SD-WAN policy route, VPN route.
Policy route also applies to system-generated and reply traffic. To learn how to change the configuration, go to the online help.

IPv4 SD-WAN policy route [Watch: How to use SD-WAN policy routing](#)

Name	Interface	Source network	Destination network	Services	Active	Status	Manage
Default LAN to WAN	-	#Port1	Any	Any service	●	OFF	
Lan to Wan2	-	192.168.2.234	Any	Any service	●	ON	

有作用，192.168.2.234 從 Port6_WAN 出去，

Log viewer

Src IP is 192.168.2.234

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 13:29:52	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	52.74.13.196	53232	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:49	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	103.43.90.54	52739	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:47	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	52.77.152.198	59095	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:47	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	18.178.22.21	50914	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:46	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	52.74.13.196	50883	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:46	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	52.77.152.198	57812	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:46	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	210.61.248.40	57225	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:46	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	8.8.8.8	49296	53	UDP	1	00001	Open PCAP	
2021-06-16 13:29:45	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	152.199.39.51	55028	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:45	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	52.77.152.198	63212	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:43	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	103.43.90.54	57298	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:39	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	50.116.239.135	54426	443	TCP	1	00001	Open PCAP	
2021-06-16 13:29:37	Firewall Rule	Allowed		8	7	Port1	Port6_ppp	192.168.2.234	103.43.90.54	55323	443	TCP	1	00001	Open PCAP	

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

The screenshot shows the 'Rules and policies' page in the Sophos XG Firewall web console. The 'NAT rules' tab is selected. A table lists several NAT rules. Two rules are highlighted with red boxes: Rule 1 and Rule 7.

#	Name	Original	Translated	Interface	ID	Usage
1	LAN to WAN Firewall rule ID: 8	Source: 192.168.2.234:192.1... Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2021-06-16 13:31... used	#7	293
2	LAN to WAN Firewall rule ID: 7	Source: 192.168.2.123:192.1... Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#6	0
3	Mail Server	Source: Any host Service: IMAP, POP3, SMTP[S]... Destination: #Port2:36.238.2...	Source: Original Service: Original Destination: 192.168.100.25...	Inbound: Port2 Outbound: Any interface Last used: 2021-06-16 12:48... used	#5	1
4	Synology rule	Source: Any host Service: Synology Port 5000... Destination: #Port2:36.238.2...	Source: Original Service: Original Destination: 192.168.2.144:1...	Inbound: Port2 Outbound: Any interface Last used: Unused	#4	0
5	Home to Cai	Source: Any host Service: Port 3395 Destination: #Port2:36.238.2...	Source: Original Service: Port 3389 Destination: 192.168.2.44:19...	Inbound: Port2 Outbound: Any interface Last used: Unused	#1	0
6	#NAT-Default-Network-... Firewall rule ID: 5	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2021-06-16 13:30... used	#3	522
7	Default SNAT IPv4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Port2, Port6 Last used: Unused	#2	0

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，

The screenshot shows the 'Log viewer' page in the Sophos XG Firewall web console. The logs show traffic passing through Firewall Rule 2 (Default SNAT IPv4) and being sent out through Port6_ppp. The 'NAT rule' and 'Out interface' columns are highlighted with red boxes.

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 13:34:45	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	172.217.167.99	53092	443	UDP	1	00001	Open PCAP	
2021-06-16 13:34:44	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	172.217.160.99	64748	443	UDP	1	00001	Open PCAP	
2021-06-16 13:34:43	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	172.217.27.130	62581	443	UDP	1	00001	Open PCAP	
2021-06-16 13:34:42	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	52.220.166.192	61723	443	TCP	1	00001	Open PCAP	
2021-06-16 13:34:39	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	139.162.117.182	61819	443	TCP	1	00001	Open PCAP	
2021-06-16 13:34:39	Invalid Traffic	Denied		N/A	0			192.168.2.234	139.162.117.182	61819	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 13:34:39	Invalid Traffic	Denied		N/A	0			192.168.2.234	139.162.117.182	61819	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 13:34:39	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	23.108.100.139	63765	443	TCP	1	00001	Open PCAP	
2021-06-16 13:34:39	Invalid Traffic	Denied		N/A	0			192.168.2.234	23.108.100.139	63765	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 13:34:39	Invalid Traffic	Denied		N/A	0			192.168.2.234	23.108.100.139	63765	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 13:34:39	Invalid Traffic	Denied		N/A	0			192.168.2.234	98.137.11.153	62763	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 13:34:39	Invalid Traffic	Denied		N/A	0			192.168.2.234	98.137.11.153	62763	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.
2021-06-16 13:34:39	Invalid Traffic	Denied		N/A	0			192.168.2.234	172.104.90.4	58420	443	TCP	0	01001	Open PCAP	Could not associate packet to any connection.

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，

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 13:47:58	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	220.130.119.27	54055	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:55	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	172.217.24.10	54799	443	UDP	1	00001	Open PCAP	
2021-06-16 13:47:54	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	74.125.203.154	64395	443	UDP	1	00001	Open PCAP	
2021-06-16 13:47:50	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	210.242.216.95	52705	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:50	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	210.242.216.102	55108	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:38	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	52.143.86.214	53513	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:37	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	220.130.119.27	61571	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:31	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	130.211.17.193	58997	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:30	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	130.211.17.193	64394	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:24	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	210.242.216.95	65323	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:24	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	8.8.4.4	51503	443	UDP	1	00001	Open PCAP	
2021-06-16 13:47:21	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	210.71.145.102	54172	443	TCP	1	00001	Open PCAP	
2021-06-16 13:47:20	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	172.217.24.10	57334	443	UDP	1	00001	Open PCAP	

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	13.1074.52	51588	80	TCP	1	00001	Open PCAP	
2021-06-16 13:54:57	Invalid Traffic	Denied		N/A	0			192.168.2.234	219.871.142	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	87248.107.201	58201	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	58529	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	59.125.248.49	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	59.125.248.49	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	59.125.248.49	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	59.125.248.49	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	59.125.248.49	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	59.125.248.49	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	59.125.248.49	48496	4444	TCP	1	00001	Open PCAP	
2021-06-16 14:20:54	Firewall Rule	Allowed		8	2	Port1	Port6_ppp	192.168.2.234	59.125.248.49	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	59.125.248.49	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	59.125.248.49	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。

The screenshot displays the Sophos XG Firewall web console interface for configuring SD-WAN policy routing. The page title is "Routing" and the sub-tab is "SD-WAN policy routing". The configuration form includes the following fields:

- Name:** Lan to Wan2
- Description:** Enter Description
- Traffic selector:**
 - Incoming interface:** Select interface
 - DSCP marking:** Select DSCP marking
 - Source networks:** 192.168.2.234 (highlighted with a red box)
 - Destination networks:** Any
 - Services:** Any
- Application object:** Any
- User or groups:** Any
- Routing:**
 - Primary gateway:** Port6_WAN
 - Backup gateway:** Port2_WAN
- Override gateway monitoring decision**

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，

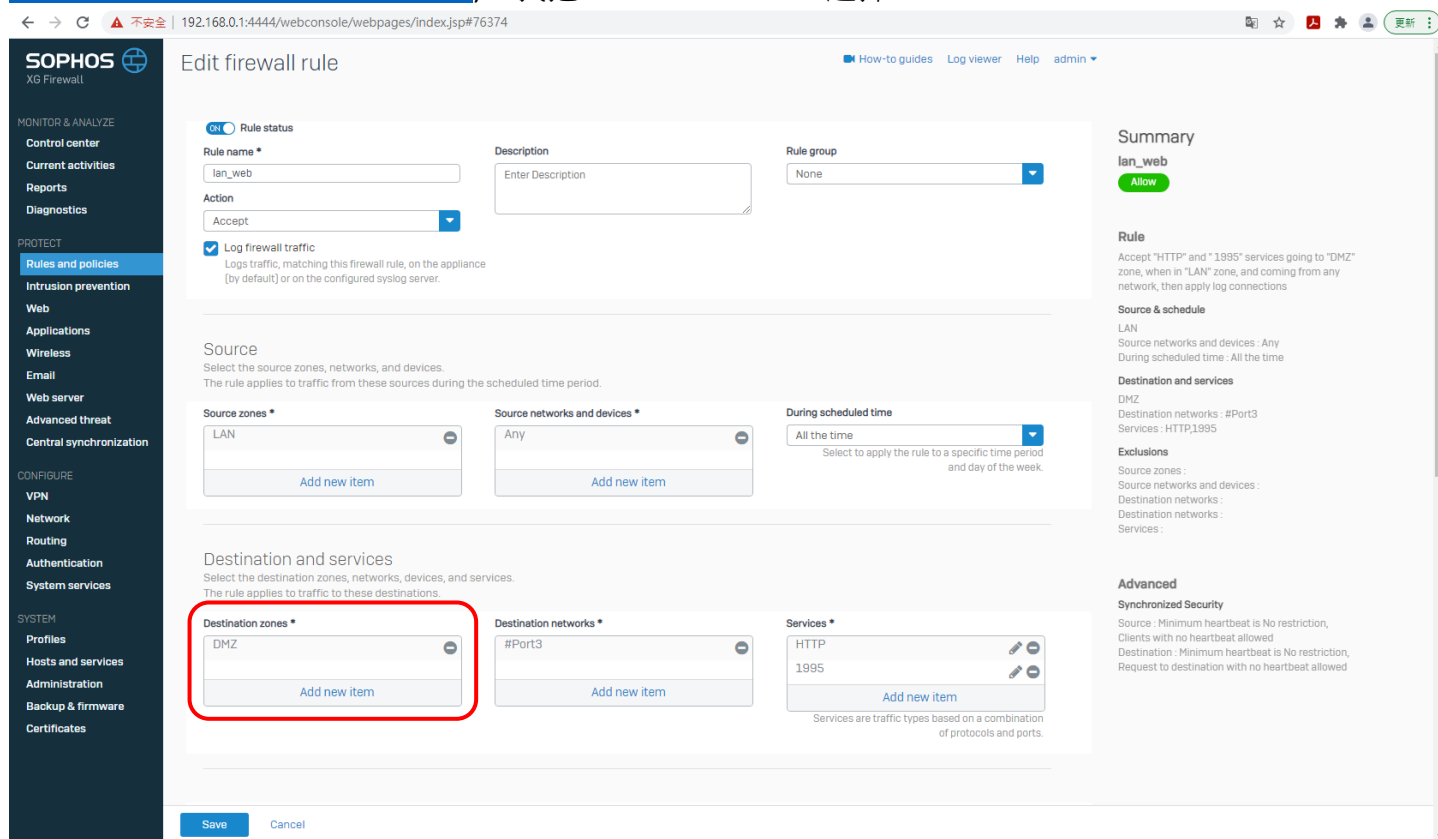
The screenshot shows the 'Edit business application rule' configuration page in the Sophos XG Firewall web console. The rule is named 'lan_web' and is currently in the 'None' group. The configuration is as follows:

- Source:** Source zones: LAN; Allowed client networks: Any; Blocked client networks: (empty).
- Destination & service:** Destination host/network: #Port3-211.20.223.163; Services: HTTP (1995).
- Forward to:** Protected server(s): 192.168.100.61; Mapped port: (empty) To (empty); Protected zone: DMZ.
- Identity:** Match known users: .
- Advanced:**
 - Policies for business applications:** Intrusion prevention: None; Traffic shaping: None.
 - Synchronized security:** Minimum source HB permitted: GREEN (selected), YELLOW, No Restriction; Block clients with no heartbeat: ; Minimum destination HB permitted: GREEN, YELLOW (selected), No Restriction; Block request to destination with no heartbeat: .
 - Routing:** Rewrite source address (masquerading): ; Use outbound address: MASQ (selected); Create reflexive rule: .
- Log traffic:** Log firewall traffic: .

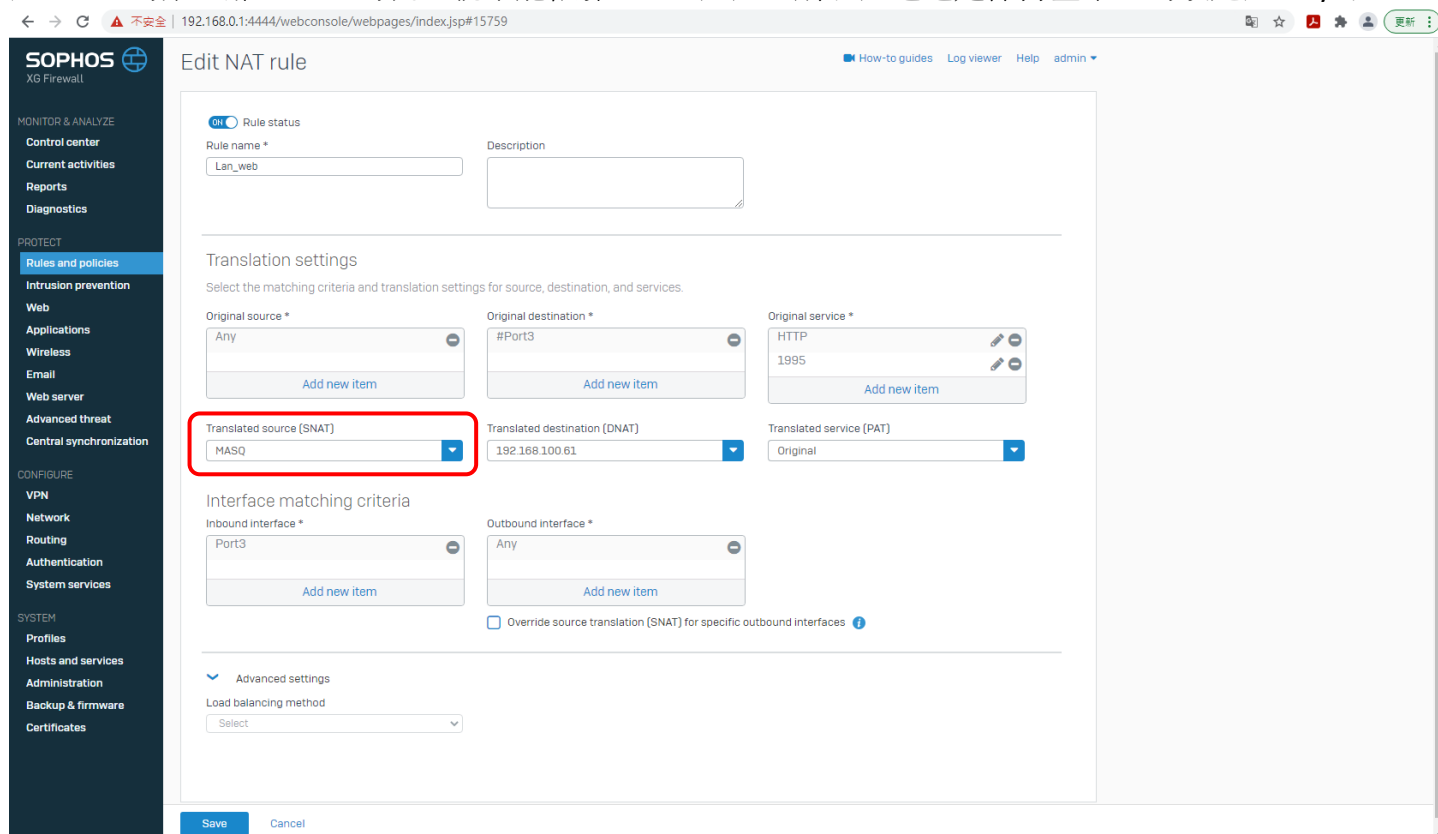
The right-hand side of the page contains a 'Summary' section for the 'lan_web' rule, detailing its source zones, destination, and advanced security settings. At the bottom, there are 'Save' and 'Cancel' buttons.

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，

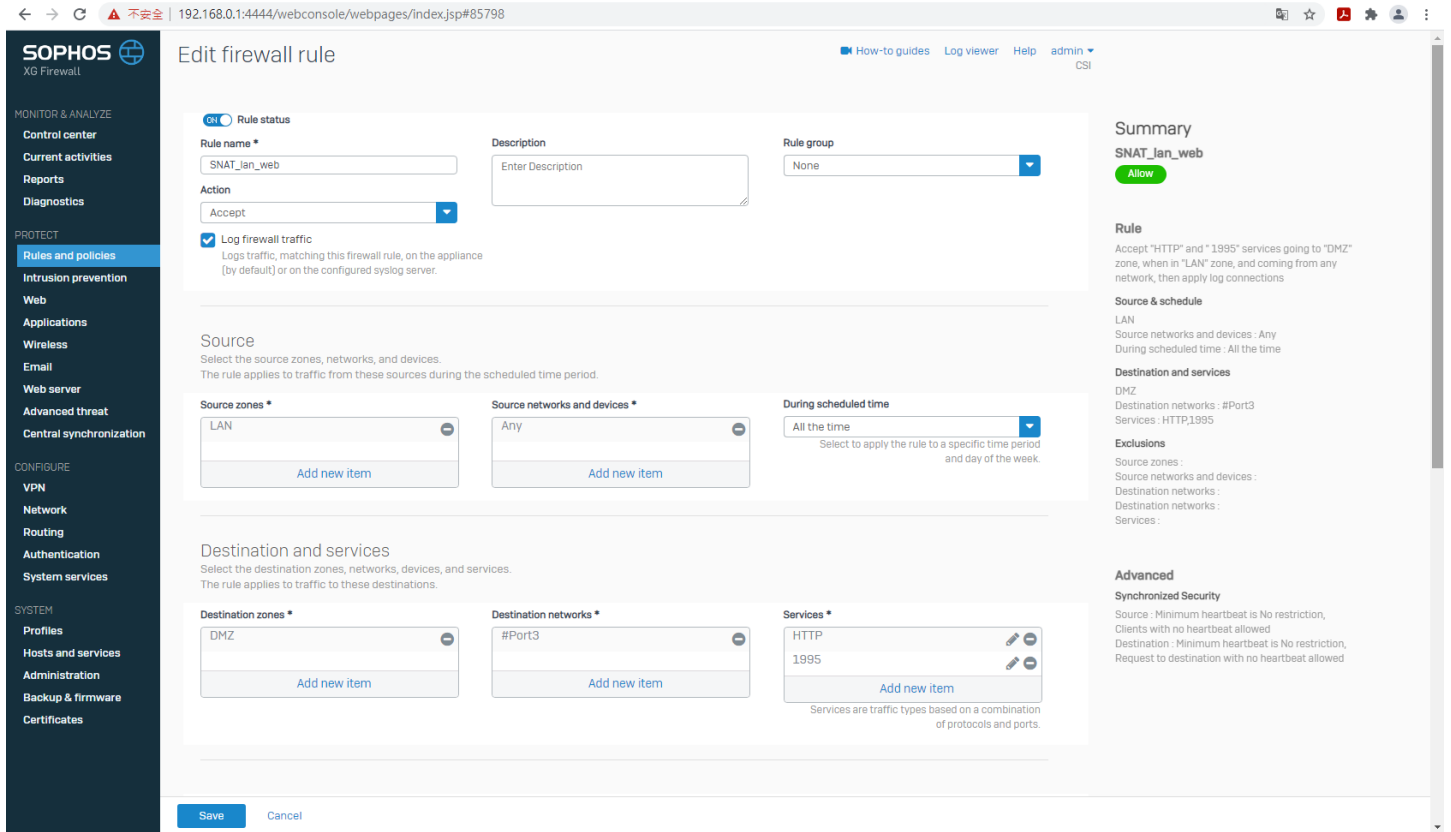


接下來是 NAT rule 這邊，基本上 Original destination 選哪個 Inbound interface 就會選一樣的，所以這邊都是 Port3，另外比較特別的是 Translated source 選了 MASQ(一般都選 Original)，Outbound interface 有考慮要不要選 Port4(DMZ zone)，可是官方討論區那人分享一句話“Outbound interface” is configured to Port1, the DNAT rule won't match inbound HTTPS traffic arriving Port2.”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。



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。

SOPHOS
XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Rules and policies
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Edit NAT rule

How-to guides | Log viewer | Help | admin | CSI

Rule status

Rule name *
Lan_web

Description

Translation settings

Select the matching criteria and translation settings for source, destination, and services.

Original source *
Any

Original destination *
#Port3

Original service *
HTTP
1995

Translated source (SNAT)
MASQ

Translated destination (DNAT)
192.168.100.61

Translated service (PAT)
Original

Interface matching criteria

Inbound interface *
Port1

Outbound interface *
Any

Override source translation (SNAT) for specific outbound interfaces ⓘ

Advanced settings
Load balancing method
Select

Save Cancel