Firewall
原理說明與實際檢測

臺灣大學計資中心網路組
游子興
davisyou@ntu.edu.tw
02-33665008

大綱

- Port Scan
  - TCP Port Status
  - UDP Port Status
- Firewall Rules vs. Router ACL
- Firewall Rules Block vs. Reject
- Firewall Logs Review
- 防火牆規則整理
- Firewall Rules Detection
  - For Server: 外對內
  - For Client:內對外
  - For 中途

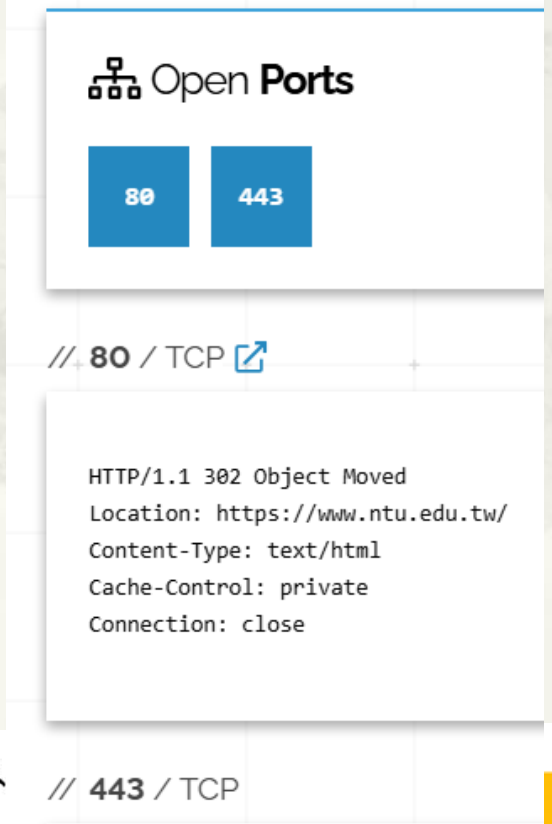
Port Scan
TCP Port Status

Port Scan

台大首頁 www.ntu.edu.tw

* Shodan

https://www.shodan.io/host/140.112.8.116



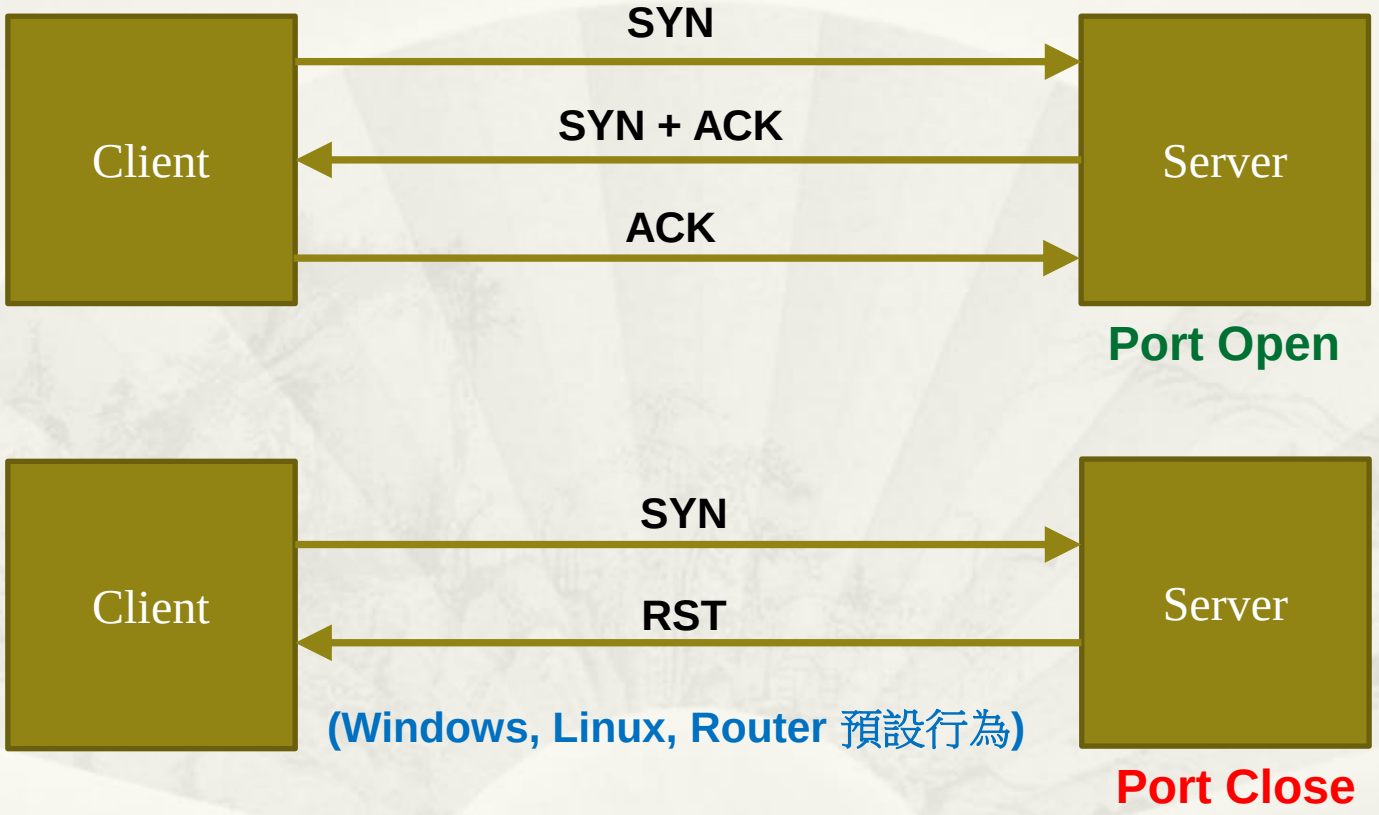

```
S:\>ping www.ntu.edu.tw

Ping www.ntu.edu.tw [140.112.8.116] (使用 32 位元組的資料):
回覆自 140.112.8.116: 位元組=32 時間<1ms TTL=253
回覆自 140.112.8.116: 位元組=32 時間<1ms TTL=253
回覆自 140.112.8.116: 位元組=32 時間<1ms TTL=253
```

* Nmap Port Scan
  * 掃描 Top 1000 Ports(預設)

```
C:\Users\user\Downloads\Nmap7.97>nmap www.ntu.edu.tw
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-25 09:39 +0800
Nmap scan report for www.ntu.edu.tw (140.112.8.116)
Host is up (0.0083s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
3011/tcp closed trusted-web
```

  * Ref. https://nmap.org/

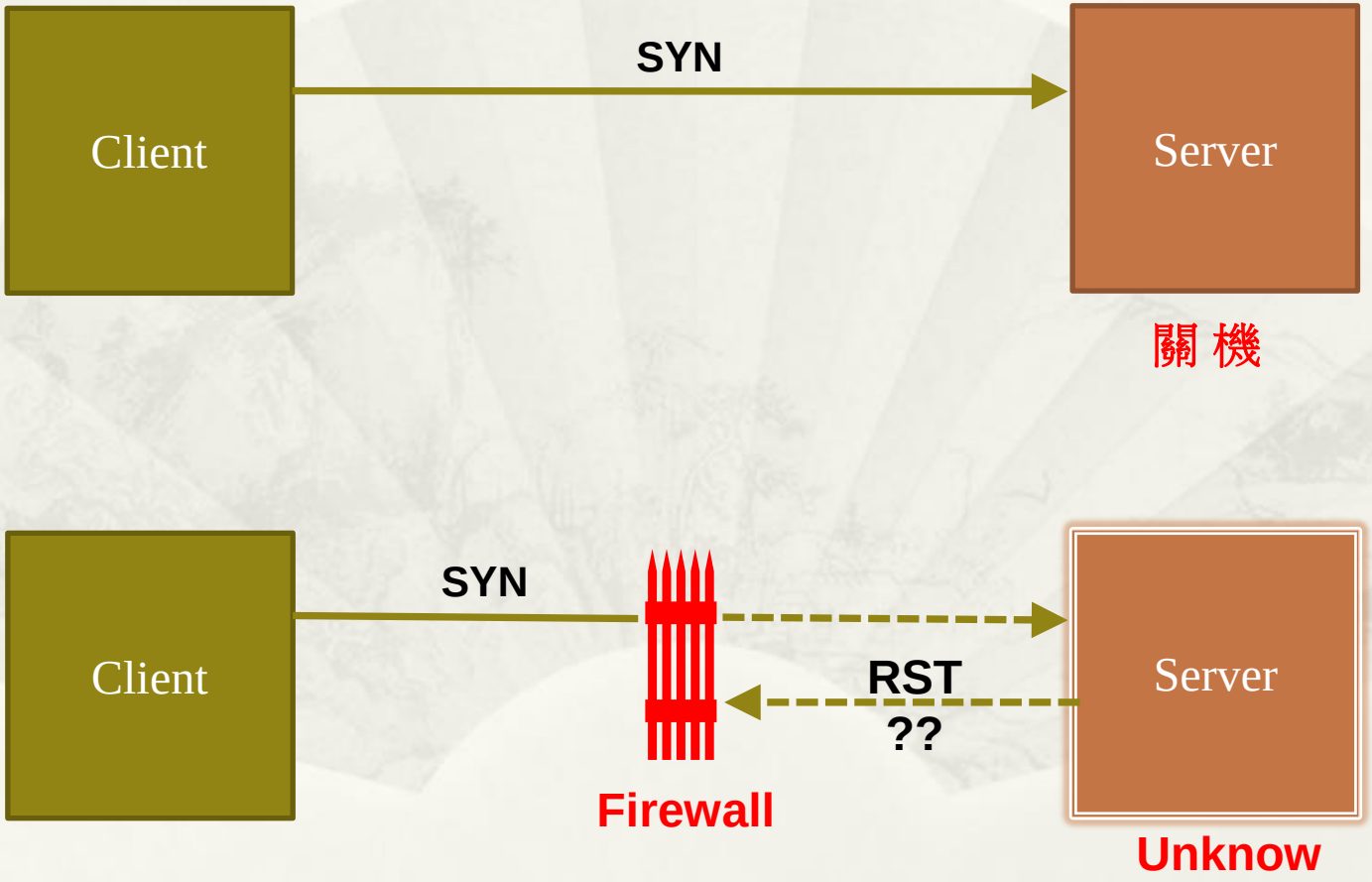
TCP Port Status



If the port is closed but unfiltered(無防火牆), the target will respond with an RST packet.

Ref. https://en.wikipedia.org/wiki/Port_scanner

TCP Port Status
No response (filtered)



TCP Port Status 驗證與觀察

- Nmap TCP Port Status
  - Open
    - 有回應 SYN + ACK 封包.
  - Closed
    - 有回應 RST 封包.
  - Filtered
    - 無回應封包.
    - Cannot determine whether port is open.
    - Drop by Firewall or Server down.

測試及側錄封包

- nmap www.ntu.edu.tw -p 80
  - PORT STATE SERVICE
  - 80/tcp open http
- nmap www.nccu.edu.tw -p 80
  - PORT STATE SERVICE
  - 80/tcp open http
- nmap www.ntu.edu.tw -p 81
  - PORT STATE SERVICE
  - 81/tcp filtered hosts2-ns
- nmap www.nccu.edu.tw -p 81
  - PORT STATE SERVICE
  - 81/tcp closed hosts2-ns

測試及側錄封包

- Nmap 建議加上參數 -Pn
  - Treat all hosts as online (skip Host Discovery)
- Host Discovery 動作包含:
  - ICMP Echo request(Type8)
  - TCP SYN Port 443
  - TCP ACK Port 80
  - ICMP Timestamp request(Type13)
  - ref. https://nmap.org/book/man-host-discovery.html

Wireshark
Capture Filter

! or not
&& or and
|| or or

ether host 08:00:08:15:ca:fe
ether multicast
ether broadcast

host 163.21.158.135
src host 163.21.158.135
dst host 163.21.158.135

net 192.168.0.0/24
src net 192.168.0.0/24
dst net 140.112.0.0/16

port 53
src port 53
dst port 53

Wireshark
Display Filter

== Equal
!= Not Equal
> Greater Than
< Less Than

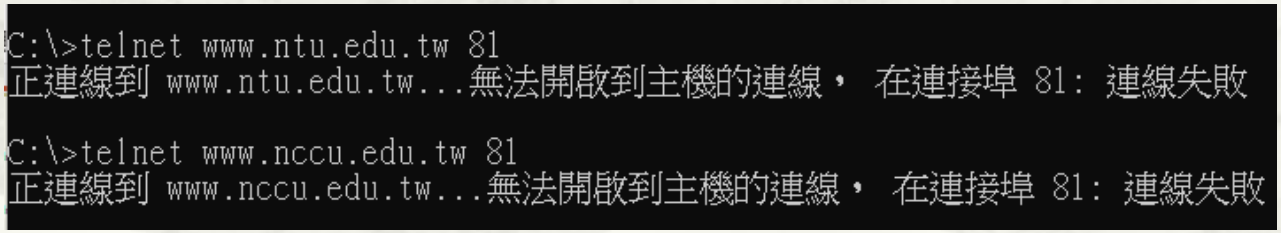
and, && Logical AND
or, || Logical OR
not, ! Logical NOT

ip.addr==172.30.2.100
ip.dst == x.x.x.x
ip.src == x.x.x.x

tcp.port == 80

TCP Port Status 驗證與觀察
Telnet

- telnet 回應
  - Open: 順利連線
  - Closed: 無法開啟到主機的連線(回應時間短)
  - Filtered: 無法開啟到主機的連線(回應時間長)
- telnet 測試
  - telnet www.ntu.edu.tw 80
  - telnet www.nccu.edu.tw 80
  - telnet www.ntu.edu.tw 81
  - telnet www.nccu.edu.tw 81



- 補充: The firewall doesn't block/inspect the localhost/loopback address (127.0.0.1) because it's your computer.

TCP Port Status 驗證與觀察

nping (nmap 套件中程式)

- nping --tcp -p 80 www.ntu.edu.tw
  - Port Open: 回應 SYN +ACT

```
S:\Tools\Nmap7.96>nping --tcp -p 80 www.ntu.edu.tw

Starting Nping 0.7.96 ( https://nmap.org/nping ) at 2025-07-14 11:00 台北標準時間
SENT (0.0950s) TCP 172.16.0.12:22757 > 140.112.8.116:80 S ttl=64 id=8604 iplen=40  seq=3295717420 win=1480
RCVD (0.1110s) TCP 140.112.8.116:80 > 172.16.0.12:22757 SA ttl=253 id=12782 iplen=44  seq=2863752268 win=8190 <mss 536
SENT (1.1010s) TCP 172.16.0.12:22757 > 140.112.8.116:80 S ttl=64 id=8604 iplen=40  seq=3295717420 win=1480
RCVD (1.1170s) TCP 140.112.8.116:80 > 172.16.0.12:22757 SA ttl=253 id=12783 iplen=44  seq=3567190152 win=8190 <mss 536
```

- nping --tcp -p 80 www.nccu.edu.tw
  - Port Open: 回應 SYN +ACT

```
S:\Tools\Nmap7.96>nping --tcp -p 80 www.nccu.edu.tw

Starting Nping 0.7.96 ( https://nmap.org/nping ) at 2025-07-14 11:00 台北標準時間
SENT (0.0990s) TCP 172.16.0.12:9944 > 140.119.168.10:80 S ttl=64 id=3930 iplen=40  seq=2506676069 win=1480
RCVD (0.1150s) TCP 140.119.168.10:80 > 172.16.0.12:9944 SA ttl=246 id=10833 iplen=44  seq=885677501 win=8190 <mss 536>
SENT (1.1100s) TCP 172.16.0.12:9944 > 140.119.168.10:80 S ttl=64 id=3930 iplen=40  seq=2506676069 win=1480
RCVD (1.1260s) TCP 140.119.168.10:80 > 172.16.0.12:9944 SA ttl=246 id=36654 iplen=44  seq=1072748316 win=8190 <mss 536>
```

TCP Port Status 驗證與觀察

nping

* nping --tcp -p 81 www.ntu.edu.tw
  * Port Filtered: 無回應

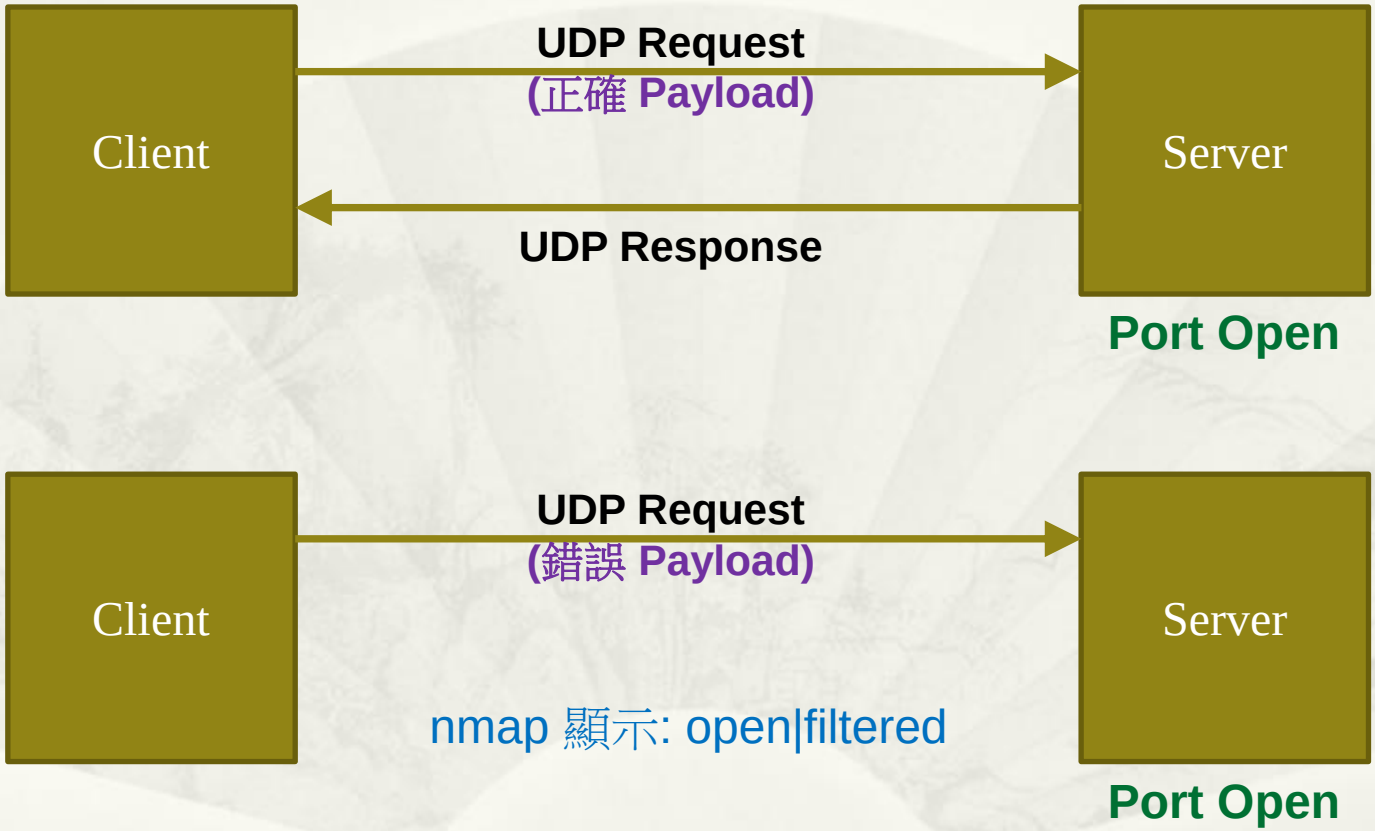
```
S:\Tools\Nmap7.96>nping --tcp -p 81 www.ntu.edu.tw

Starting Nping 0.7.96 ( https://nmap.org/nping ) at 2025-07-14 11:00 台北標準時間
SENT (0.0720s) TCP 172.16.0.12:27962 > 140.112.8.116:81 S ttl=64 id=31463 iplen=40  seq=1928795980 win=1480
SENT (1.0820s) TCP 172.16.0.12:27962 > 140.112.8.116:81 S ttl=64 id=31463 iplen=40  seq=1928795980 win=1480
SENT (2.0890s) TCP 172.16.0.12:27962 > 140.112.8.116:81 S ttl=64 id=31463 iplen=40  seq=1928795980 win=1480
```

* nping --tcp -p 81 www.nccu.edu.tw
  * Port Close: 回應 RST

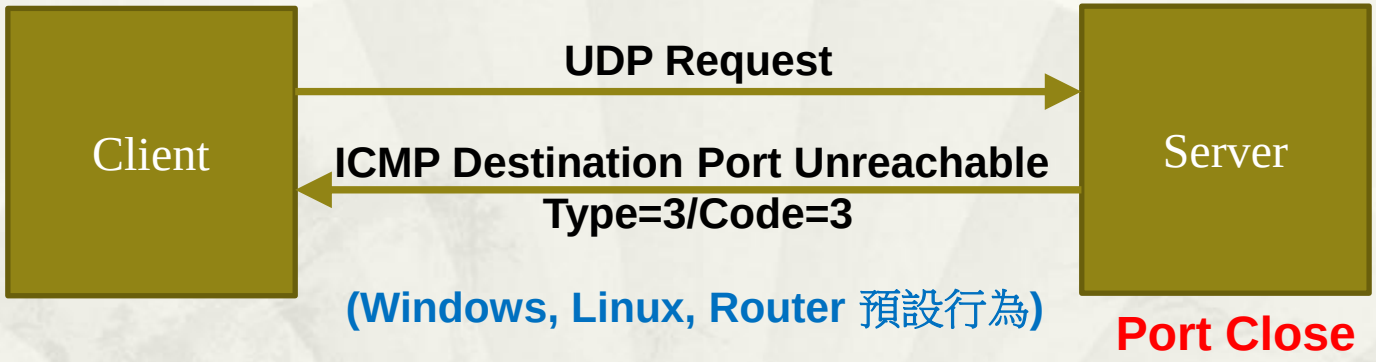
```
S:\Tools\Nmap7.96>nping --tcp -p 81 www.nccu.edu.tw

Starting Nping 0.7.96 ( https://nmap.org/nping ) at 2025-07-14 11:00 台北標準時間
SENT (0.0680s) TCP 172.16.0.12:15775 > 140.119.168.10:81 S ttl=64 id=17871 iplen=40  seq=1591426321 win=1480
RCVD (0.0850s) TCP 140.119.168.10:81 > 172.16.0.12:15775 RA ttl=246 id=10835 iplen=40  seq=0 win=8212
SENT (1.0820s) TCP 172.16.0.12:15775 > 140.119.168.10:81 S ttl=64 id=17871 iplen=40  seq=1591426321 win=1480
RCVD (1.0990s) TCP 140.119.168.10:81 > 172.16.0.12:15775 RA ttl=246 id=10836 iplen=40  seq=0 win=8212
```

Port Scan
UDP Port Status

UDP Port Status

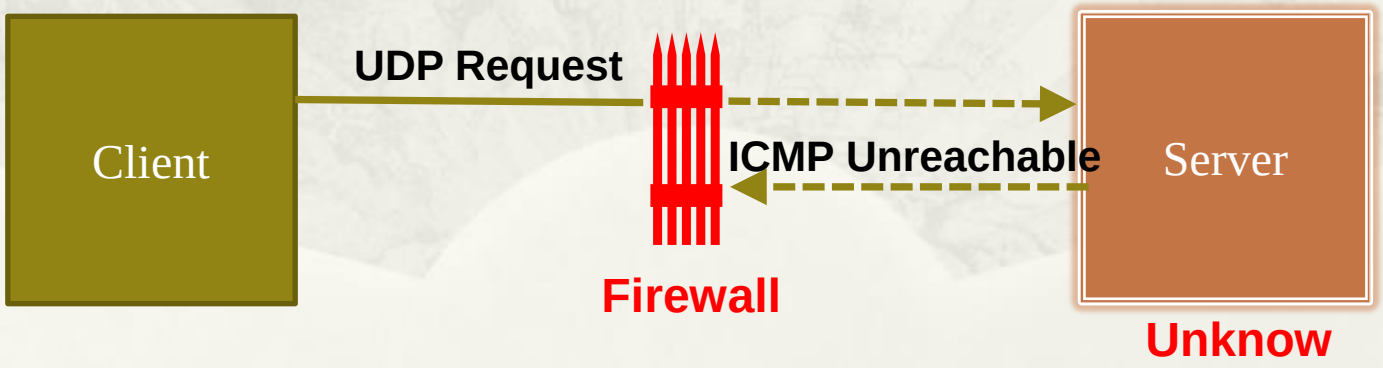


UDP Port Status



UDP Port Status
No response (filtered)

nmap 顯示: open|filtered



UDP Port Status 驗證與觀察 Nmap

- Nmap UDP Port Status
  - Open
    - 回應正確 payload 封包
  - Closed
    - 回應 ICMP Destination Port unreachable (Type=3/Code=3)
  - open|filtered
    - 無回應.
    - Cannot determine whether port is open.
    - Drop by firewall or Server down.

UDP Port Status 驗證與觀察
Nmap Port 123

* nmap -sU -p 123 -Pn time.stdtime.gov.tw
  * PORT STATE SERVICE
  * 123/udp open ntp

No.	udp.	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0	172.16.0.12	49526	118.163.81.61	123	NTP	90	NTP Version 4, client
2	0	172.16.0.12	49526	118.163.81.61	123	NTP	90	NTP Version 3, symmetric active
3	0	118.163.81.61	123	172.16.0.12	49526	NTP	90	NTP Version 4, server

* nmap -sU -p 123 -Pn 140.112.254.4
  * PORT STATE SERVICE
  * 123/udp closed ntp

No.	udp.	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0	172.16.0.12	62091	140.112.254.4	123	NTP	90	NTP Version 4, client
2	0	172.16.0.12	62091	140.112.254.4	123	NTP	90	NTP Version 3, symmetric active
3	0	140.112.254.4		172.16.0.12		ICMP	70	Destination unreachable (Port unreachable)
4	0	140.112.254.4		172.16.0.12		ICMP	70	Destination unreachable (Port unreachable)

UDP Port Status 驗證與觀察
Nmap Port 123

- nmap -sU -p 123 -Pn www.nccu.edu.tw
  - PORT STATE SERVICE
  - 123/udp open|filtered ntp
  - 無收到任何回應

No.	udp.	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0	172.16.0.12	37919	140.119.168.10	123	NTP	90	NTP Version 4, client
2	0	172.16.0.12	37919	140.119.168.10	123	NTP	90	NTP Version 3, symmetric active
3	1	172.16.0.12	37921	140.119.168.10	123	NTP	90	NTP Version 4, client
4	1	172.16.0.12	37921	140.119.168.10	123	NTP	90	NTP Version 3, symmetric active

UDP Port Status 驗證與觀察
Nmap Port 53

* nmap -sU -p 53 -Pn 140.112.254.4
  * PORT STATE SERVICE
  * 53/udp open domain

No.	udp.	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0	172.16.0.12	39219	140.112.254.4	53	DNS	72	Standard query 0x0006 TXT version.bind
2	0	172.16.0.12	39219	140.112.254.4	53	DNS	54	Server status request 0x0000
3	0	172.16.0.12	39219	140.112.254.4	53	DNS	88	Standard query 0x0000 PTR _services._dns-sd._udp.local
4	0	140.112.254.4	53	172.16.0.12	39219	DNS	92	Standard query response 0x0006 TXT version.bind TXT
6	0	140.112.254.4	53	172.16.0.12	39219	DNS	60	Server status request response 0x0000 Not implemented
7	0	140.112.254.4	53	172.16.0.12	39219	DNS	547	Standard query response 0x0000 PTR _services._dns-sd._udp.local NS

* nmap -sU -p 53 -Pn 140.112.0.70
  * PORT STATE SERVICE
  * 53/udp closed domain

No.	udp.	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0	172.16.0.12	63610	140.112.0.70	53	DNS	72	Standard query 0x0006 TXT version.bind
2	0	172.16.0.12	63610	140.112.0.70	53	DNS	54	Server status request 0x0000
3	0	172.16.0.12	63610	140.112.0.70	53	DNS	88	Standard query 0x0000 PTR _services._dns-sd._udp.local
4	0	140.112.0.70		172.16.0.12		ICMP	110	Destination unreachable (Port unreachable)

UDP Port Status 驗證與觀察
Nmap Port 53

- nmap -sU -p 53 -Pn www.nccu.edu.tw
  - PORT STATE SERVICE
  - 53/udp open|filtered domain
  - 無收到任何回應

No.	udp.	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0	172.16.0.12	51455	140.119.168.10	53	DNS	72	Standard query 0x0006 TXT version.bind
2	0	172.16.0.12	51455	140.119.168.10	53	DNS	54	Server status request 0x0000
3	0	172.16.0.12	51455	140.119.168.10	53	DNS	88	Standard query 0x0000 PTR _services._dns-sd._udp.local
4	1	172.16.0.12	51457	140.119.168.10	53	DNS	72	Standard query 0x0006 TXT version.bind
5	1	172.16.0.12	51457	140.119.168.10	53	DNS	54	Server status request 0x0000
6	1	172.16.0.12	51457	140.119.168.10	53	DNS	88	Standard query 0x0000 PTR _services._dns-sd._udp.local

UDP Port Status 驗證與觀察

nping

* nping 程式無法產生正確 UDP Payload
  * 因此 Server 無回應，無法偵測 UDP Port Open

```
D:\Downloads\nmap-7.92>nping --udp -p 53 140.112.254.4

Starting Nping 0.7.92 ( https://nmap.org/nping ) at 2022-04-21 16:33 台北標準時間
SENT (0.1390s) UDP 172.16.0.17:53 > 140.112.254.4:53 ttl=64 id=64224 iplen=28
SENT (1.1400s) UDP 172.16.0.17:53 > 140.112.254.4:53 ttl=64 id=64224 iplen=28
```

```
175 39.161559  172.16.0.17   53 140.112.254.4   53 UDP   42 53 → 53 Len=0
184 40.160991  172.16.0.17   53 140.112.254.4   53 UDP   42 53 → 53 Len=0

> Frame 175: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Dev
> Ethernet II, Src: VMware_af:2c:8f (00:0c:29:af:2c:8f), Dst: VMware_06:53:db (00:0c:29:
> Internet Protocol Version 4, Src: 172.16.0.17, Dst: 140.112.254.4
v User Datagram Protocol, Src Port: 53, Dst Port: 53
    Source Port: 53
    Destination Port: 53
    Length: 8
    Checksum: 0xc8dd [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
```

UDP Port Status 驗證與觀察

nping

* nping 程式無法產生正確 UDP Payload

```
D:\Downloads\nmap-7.92>nping --udp -p 123 ntp.ntu.edu.tw

Starting Nping 0.7.92 ( https://nmap.org/nping ) at 2022-04-21 16:33 台北標準時間
SENT (0.1720s) UDP 172.16.0.17:53 > 140.112.2.189:123 ttl=64 id=52811 iplen=28
SENT (1.1730s) UDP 172.16.0.17:53 > 140.112.2.189:123 ttl=64 id=52811 iplen=28
```

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
78	3.513986	172.16.0.17	53	140.112.2.189	123	UDP	42	53 → 123 Len=0
81	4.513989	172.16.0.17	53	140.112.2.189	123	UDP	42	53 → 123 Len=0

```
> Frame 78: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Devi
> Ethernet II, Src: VMware_af:2c:8f (00:0c:29:af:2c:8f), Dst: VMware_06:53:db (00:0c:29:
> Internet Protocol Version 4, Src: 172.16.0.17, Dst: 140.112.2.189
v User Datagram Protocol, Src Port: 53, Dst Port: 123
    Source Port: 53
    Destination Port: 123
    Length: 8
    Checksum: 0xc3df [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
```

UDP Port Status 驗證與觀察

nping

- 僅能偵測 UDP Port Closed
- nping --udp -p 80 163.28.16.254

```
C:\Users\user\Downloads\Nmap7.97>nping --udp -p 80 163.28.16.254

Starting Nping 0.7.97 ( https://nmap.org/nping ) at 2025-07-25 10:04 台北標準時間
SENT (0.0760s) UDP 10.4.1.2:53 > 163.28.16.254:80 ttl=64 id=35968 iplen=28
RCVD (0.0940s) ICMP [163.28.16.254 > 10.4.1.2 Port 80 unreachable (type=3/code=3) ] IP [ttl=254 id=10562 iplen=96 ]
SENT (1.0820s) UDP 10.4.1.2:53 > 163.28.16.254:80 ttl=64 id=35968 iplen=28
RCVD (1.0860s) ICMP [163.28.16.254 > 10.4.1.2 Port 80 unreachable (type=3/code=3) ] IP [ttl=254 id=10563 iplen=96 ]
```

Port Scan 總結
TCP vs. UDP

* TCP Port Scan: 皆用 SYN 封包
* UDP Port Scan: 不同 Port 需使用不同 Payload 封包
  * Nmap 支援哪些 UDP Payload ?
  * Check file nmap-services 有出現 UDP… (待確認)

```
tcpmux  1/udp   0.001236    # TCP Port Service Multiplexer
compressnet 2/udp   0.001845    # Management Utility
compressnet 3/udp   0.001532    # Compression Process
rje 5/udp   0.000593    # Remote Job Entry
echo    7/udp   0.024679
discard 9/udp   0.015733    # sink null
systat  11/udp  0.000577    # Active Users
daytime 13/udp  0.004827
qotd    17/udp  0.009209    # Quote of the Day
msp 18/udp  0.000610    # Message Send Protocol
chargen 19/udp  0.015865    # ttytst source Character Generator
ftp-data    20/udp  0.001878    # File Transfer [Default Data]
ftp 21/udp  0.004844    # File Transfer [Control]
ssh 22/udp  0.003905    # Secure Shell Login
telnet  23/udp  0.006211
priv-mail   24/udp  0.000329    # any private mail system
smtp    25/udp  0.001285    # Simple Mail Transfer
nsw-fe  27/udp  0.000395    # NSW User System FE
msg-icp 29/udp  0.000560    # MSG ICP
msg-auth    31/udp  0.000939    # MSG Authentication
dsp 33/udp  0.000560    # Display Support Protocol
priv-print  35/udp  0.000708    # any private printer server
time    37/udp  0.006458    # timserver
rap 38/udp  0.002043    # Route Access Protocol
rlp 39/udp  0.000478    # Resource Location Protocol
```

不同 Port 需使用不同 Payload 封包 DNS

* nmap -sU -p 53 140.112.254.4

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
3	0.026489	172.16.0.17	42056	140.112.254.4	53	DNS	54	Server status request 0x0000
4	0.026544	172.16.0.17	42056	140.112.254.4	53	DNS	72	Standard query 0x7777 TXT version.bind
5	0.026945	140.112.254.4	53	172.16.0.17	42056	DNS	60	Server status request response 0x0000 Not implemented
6	0.027051	140.112.254.4	53	172.16.0.17	42056	DNS	72	Standard query response 0x7777 Refused TXT version.bind

```
> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{CCE5347F-35B0-4718-94C6-B136AC036A
> Ethernet II, Src: VMware_af:2c:8f (00:0c:29:af:2c:8f), Dst: VMware_06:53:db (00:0c:29:06:53:db)
> Internet Protocol Version 4, Src: 172.16.0.17, Dst: 140.112.254.4
v User Datagram Protocol, Src Port: 42056, Dst Port: 53
    Source Port: 42056
    Destination Port: 53
    Length: 20
    Checksum: 0x14b2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (12 bytes)
v Domain Name System (query)
    Transaction ID: 0x0000
  > Flags: 0x1000 Server status request
    Questions: 0
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    [Response In: 5]
```

不同 Port 需使用不同 Payload 封包 NTP

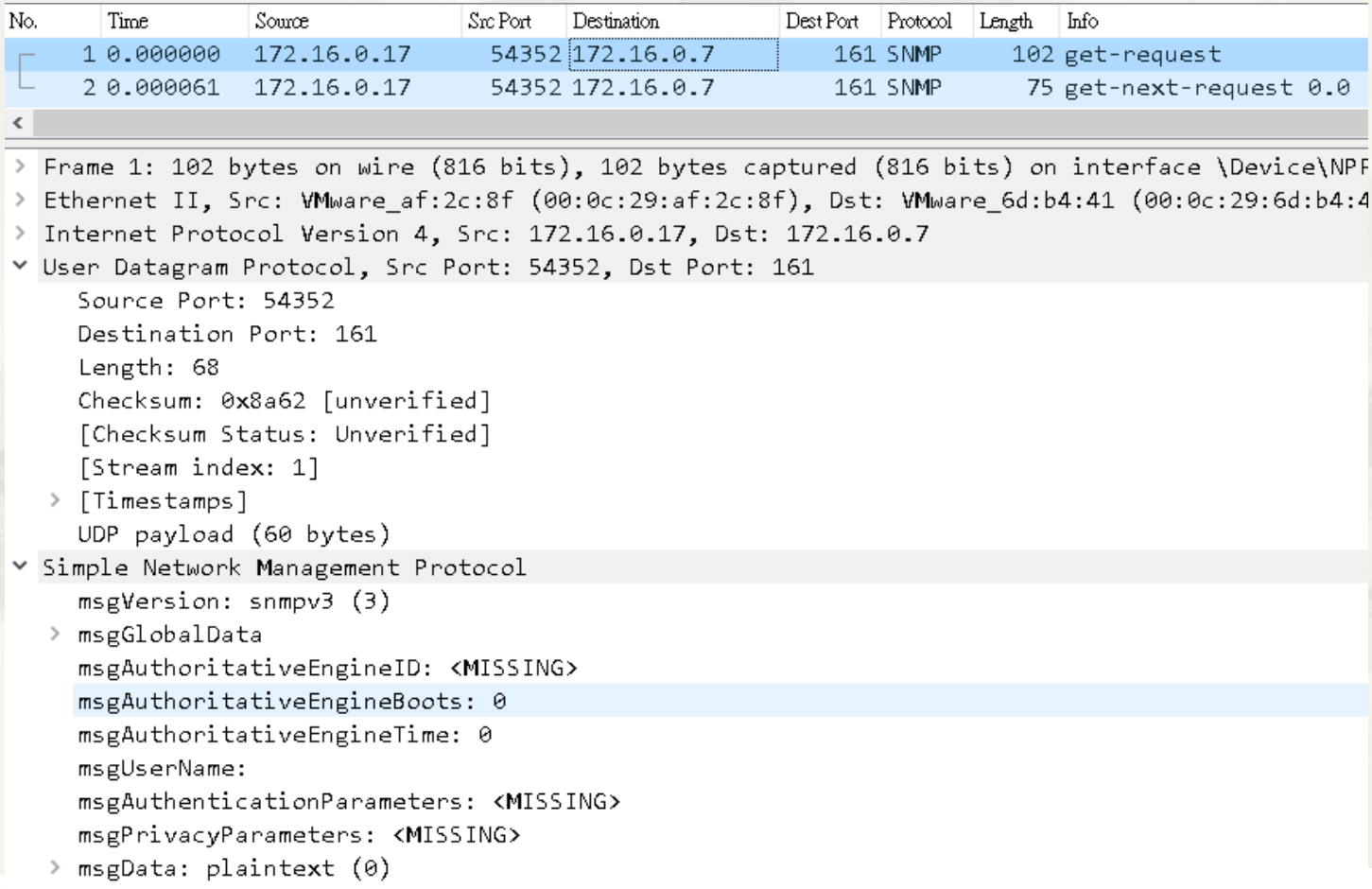
* nmap -sU -p 123 ntp.ntu.edu.tw

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
5	0.143290	172.16.0.17	48461	140.112.2.189	123	NTP	90	NTP Version 4, client
6	0.143333	172.16.0.17	48461	140.112.2.189	123	NTP	90	NTP Version 3, symmetric active
7	0.143725	140.112.2.189	123	172.16.0.17	48461	NTP	90	NTP Version 4, server
8	0.143794	140.112.2.189	123	172.16.0.17	48461	NTP	90	NTP Version 3, symmetric passive

```
> Frame 5: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{CCE5347F-35
> Ethernet II, Src: VMware_af:2c:8f (00:0c:29:af:2c:8f), Dst: VMware_06:53:db (00:0c:29:06:53:db)
> Internet Protocol Version 4, Src: 172.16.0.17, Dst: 140.112.2.189
v User Datagram Protocol, Src Port: 48461, Dst Port: 123
    Source Port: 48461
    Destination Port: 123
    Length: 56
    Checksum: 0x712a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (48 bytes)
v Network Time Protocol (NTP Version 4, client)
  > Flags: 0xe3, Leap Indicator: unknown (clock unsynchronized), Version number: NTP Version 4, Mode: cli
    [Response In: 7]
    Peer Clock Stratum: unspecified or invalid (0)
    Peer Polling Interval: 4 (16 seconds)
    Peer Clock Precision: 0.015625 seconds
    Root Delay: 1.000000 seconds
    Root Dispersion: 1.000000 seconds
    Reference ID: NULL
    Reference Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
    Origin Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
    Receive Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
    Transmit Timestamp: Nov 24, 2004 15:12:11.444111999 UTC
```

不同 Port 需使用不同 Payload 封包 SNMP

* nmap -sU -p 161 172.16.0.7



No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	172.16.0.17	54352	172.16.0.7	161	SNMP	102	get-request
2	0.000061	172.16.0.17	54352	172.16.0.7	161	SNMP	75	get-next-request 0.0

```
> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF
> Ethernet II, Src: VMware_af:2c:8f (00:0c:29:af:2c:8f), Dst: VMware_6d:b4:41 (00:0c:29:6d:b4:4
> Internet Protocol Version 4, Src: 172.16.0.17, Dst: 172.16.0.7
v User Datagram Protocol, Src Port: 54352, Dst Port: 161
    Source Port: 54352
    Destination Port: 161
    Length: 68
    Checksum: 0x8a62 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (60 bytes)
v Simple Network Management Protocol
    msgVersion: snmpv3 (3)
  > msgGlobalData
    msgAuthoritativeEngineID: <MISSING>
    msgAuthoritativeEngineBoots: 0
    msgAuthoritativeEngineTime: 0
    msgUserName:
    msgAuthenticationParameters: <MISSING>
    msgPrivacyParameters: <MISSING>
  > msgData: plaintext (0)
```

不同 Port 需使用不同 Payload 封包 ECHO

* nmap -sU -p 7 140.112.254.4

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
3	0.005257	172.16.0.17	40147	140.112.254.4	7	ECHO	46	Request

```
> Frame 3: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface
> Ethernet II, Src: VMware_af:2c:8f (00:0c:29:af:2c:8f), Dst: VMware_06:53:db (00
> Internet Protocol Version 4, Src: 172.16.0.17, Dst: 140.112.254.4
v User Datagram Protocol, Src Port: 40147, Dst Port: 7
    Source Port: 40147
    Destination Port: 7
    Length: 12
    Checksum: 0x1251 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (4 bytes)
v Echo
    Echo data: 0d0a0d0a
```

Firewall Rules vs. Router ACL

Firewall Rules vs. Router ACL

Firewall Rules	Router ACL
Session-based(Stateful)	Non Session-based(Stateless)
Control “介面 In” only	Control 介面 In/Out
Implicit Deny (預設拒絕)	Implicit Allow (預設允許) 除非設定 ACL

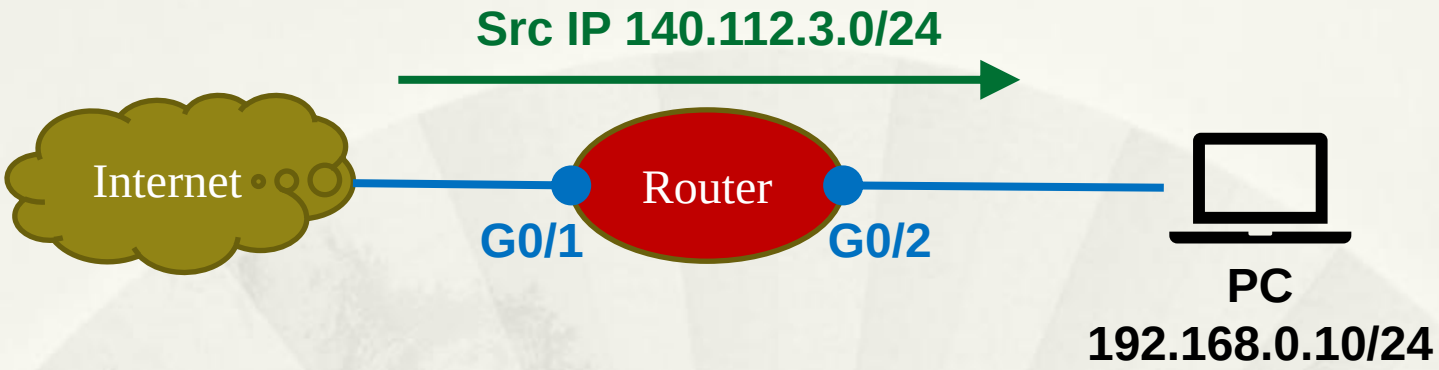
- Session-based(Stateful)
  - 僅需設定在連線發起方向(Initial Session)，封包回覆方向不需設定
  - 缺點: 使用記憶體記錄 Sessions，易受 SYN Flood 攻擊
- Firewall Interface 未設定任何規則前，會顯示如下警告訊息
  - No XXX rules are currently defined. All incoming connections on this interface will be blocked until you add a pass rule.

Firewall Rules vs. Router ACL

- Firewall Rules 測試平台
  - pfsense: https://www.pfsense.org/
  - OPNsense: https://opnsense.org/
- Router ACL 測試平台
  - Cisco Catalyst Series

Case1. 外對內
僅允許 Src IP 140.112.3.0/24

Case1. Router ACL




```
ipv4 access-list acl
  permit ipv4 140.112.3.0 0.0.0.255 any
```

* 方法1: 設定於介面 G0/1 In 方向

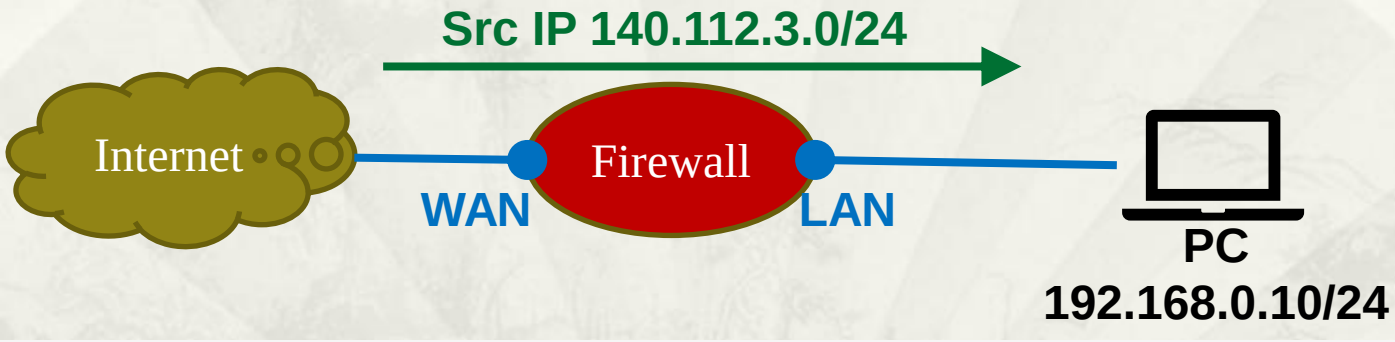
```
int G0/1
  ipv4 access-group acl ingress
```

* 方法2: 設定於介面 G0/2 Out 方向

```
int G0/2
  ipv4 access-group acl egress
```

Case1. Firewall Rules

- 僅能控制 “介面 In” 封包
  - WAN(介面 In): 允許 Src IP 140.112.3.0/24
  - LAN(介面 Out): 不需設定



Floating WAN LAN

允許 **Src IP: 140.112.3.0/24**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Gateway	Queue	Schedule	Description	Actions
✔	0 /0 B	IPv4 *	ACL_1	*	*	none			

Alias details

Value
140.112.3.0/24

Floating WAN LAN

不需設定 **(介面 Out)**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

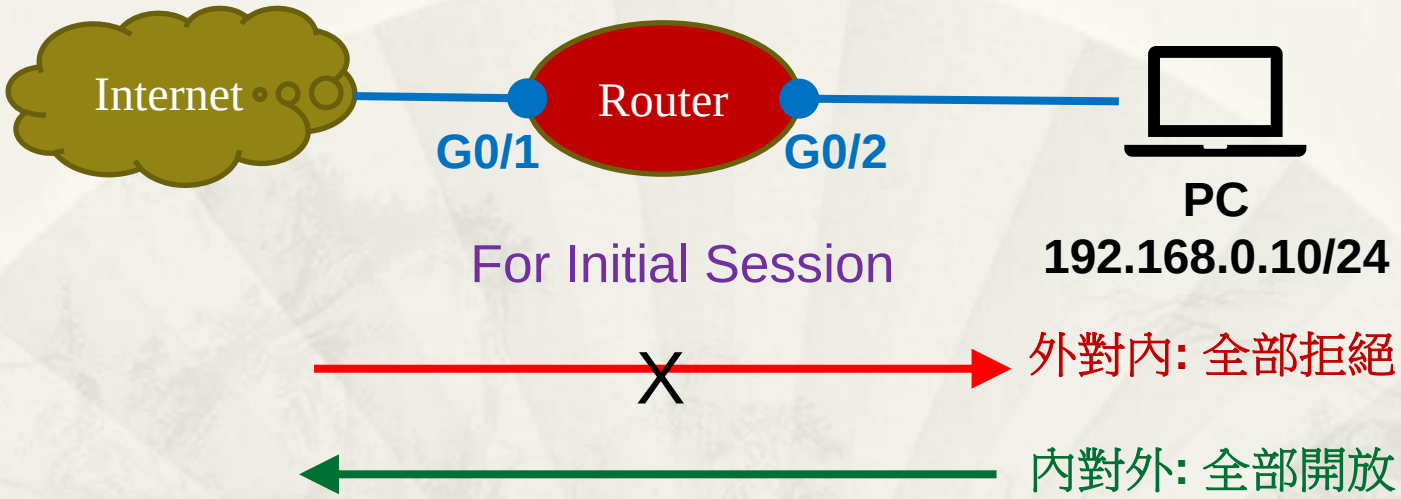
Case1. 差異比較

	Router ACL	Firewall Rules
外對內 (符合要求)	僅允許 Src IP 140.112.3.0/24	僅允許 Src IP 140.112.3.0/24
內對外	僅允許 Dst IP 140.112.3.0/24	未限制

Case2.
外對內: 全部拒絕
內對外: 全部開放

For Initial Session

Case2. Router ACL



* Non Session-based 不支援，無法設定

Case2. Firewall Rules

- 因為 Implicit Deny，僅需設定”內對外: 全部開放”
- 僅能控制 “介面 In” 封包: 僅需設定於 LAN
  - Allow Rules 僅需設定在連線發起方向(Initial session)，封包回覆方向不需設定

Floating WAN LAN

不需設定 (介面 Out)

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

Floating WAN LAN

內對外: 允許 LAN net 192.168.0.0/24

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	14 /4.50 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

Firewall Rules
Block vs. Reject

Firewall Rules
Block vs. Reject

- Block: Implicit Deny(預設拒絕) 之預設動作
  - Drop Packets Silently.

- Reject: 手動增加一筆 Rule 於最後
  - Post Close 需回覆封包
    - For TCP -> RST
    - For UDP -> ICMP port unreachable

Reject: 手動增加一筆 Rule 於最後

Floating | WAN | LAN_0 | LAN_1 | IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0 /35.83 MiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✗	0 /1.98 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
☐ ✋	0 /0 B	IPv4 *	*	*	*	手動加上	*	none			⚓ ✎ ⧉ ⊘ 🗑

Edit Firewall Rule

Action Reject

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface WAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol Any

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any

Destination

Firewall Rules
Block vs. Reject 測試

* nmap 163.28.16.43

Block

```
S:\Tools\Nmap7.97>nmap 163.28.16.43
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-25
Nmap scan report for ilearning2.tanet.edu.tw (163.28.1
Host is up (0.0019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3389/tcp open  ms-wbt-server
```

Reject

```
S:\Tools\Nmap7.97>nmap 163.28.16.43
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-25 10
Nmap scan report for ilearning2.tanet.edu.tw (163.28.16.
Host is up (0.0029s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE
80/tcp   open     http
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
3389/tcp open     ms-wbt-server
3390/tcp filtered dsc
```

* nping --tcp -p 81 163.28.16.43

Block

```
S:\Tools\Nmap7.97>nping --tcp -p 81 163.28.16.43

Starting Nping 0.7.97 ( https://nmap.org/nping ) at 2025-07-25 10:58 台北標準時間
SENT (0.0540s) TCP 172.16.0.12:12467 > 163.28.16.43:81 S ttl=64 id=1036 iplen=40  seq=3254056632 win=1480
SENT (1.0680s) TCP 172.16.0.12:12467 > 163.28.16.43:81 S ttl=64 id=1036 iplen=40  seq=3254056632 win=1480
SENT (2.0760s) TCP 172.16.0.12:12467 > 163.28.16.43:81 S ttl=64 id=1036 iplen=40  seq=3254056632 win=1480
SENT (3.0820s) TCP 172.16.0.12:12467 > 163.28.16.43:81 S ttl=64 id=1036 iplen=40  seq=3254056632 win=1480
^C
```

Reject

```
S:\Tools\Nmap7.97>nping --tcp -p 81 163.28.16.43

Starting Nping 0.7.97 ( https://nmap.org/nping ) at 2025-07-25 10:58 台北標準時間
SENT (0.0650s) TCP 172.16.0.12:27681 > 163.28.16.43:81 S ttl=64 id=20912 iplen=40  seq=1748109342 win=1480
RCVD (0.0810s) TCP 163.28.16.43:81 > 172.16.0.12:27681 RA ttl=59 id=0 iplen=40  seq=0 win=0
SENT (1.0730s) TCP 172.16.0.12:27681 > 163.28.16.43:81 S ttl=64 id=20912 iplen=40  seq=1748109342 win=1480
RCVD (1.0880s) TCP 163.28.16.43:81 > 172.16.0.12:27681 RA ttl=59 id=0 iplen=40  seq=0 win=0
```

Firewall Rules
Block vs. Reject 測試封包

No.	Time	TCP Seq	Source	Src Port	Destination	Dest Port	Src MAC	Dst MAC	Protocol	Length	Info
15	13.747019	0	10.2.1.2	54097	140.112.3.82	10	Vmware_72:bf:01	Vmware_a8:16:3e	TCP	66	54097 → 10 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
19	16.748323	0	10.2.1.2	54097	140.112.3.82	10	Vmware_72:bf:01	Vmware_a8:16:3e	TCP	66	[TCP Retransmission] 54097 → 10 [SYN] Seq=0 Wi
26	22.754324	0	10.2.1.2	54097	140.112.3.82	10	Vmware_72:bf:01	Vmware_a8:16:3e	TCP	62	[TCP Retransmission] 54097 → 10 [SYN] Seq=0 Wi
48	39.142315	0	10.2.1.2	54098	140.112.3.82	10	Vmware_72:bf:01	Vmware_a8:16:3e	TCP	66	54098 → 10 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
49	39.143587	1	140.112.3.82	10	10.2.1.2	54098	Vmware_a8:16:3e	Vmware_72:bf:01	TCP	60	10 → 54098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
50	39.649112	0	10.2.1.2	54098	140.112.3.82	10	Vmware_72:bf:01	Vmware_a8:16:3e	TCP	66	[TCP Retransmission] 54098 → 10 [SYN] Seq=0 Wi
51	39.650391	1	140.112.3.82	10	10.2.1.2	54098	Vmware_a8:16:3e	Vmware_72:bf:01	TCP	60	10 → 54098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53	40.148297	0	10.2.1.2	54098	140.112.3.82	10	Vmware_72:bf:01	Vmware_a8:16:3e	TCP	62	[TCP Retransmission] 54098 → 10 [SYN] Seq=0 Wi
54	40.150093	1	140.112.3.82	10	10.2.1.2	54098	Vmware_a8:16:3e	Vmware_72:bf:01	TCP	60	10 → 54098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

* 前三個封包
  * Block: Implicit Deny

* 後六個封包
  * Reject: 手動增加一筆 Rule 於最後

Firewall Logs Review

Firewall Logs 應開啟記錄於？

Deny Rules

Or

Allow Rules

Firewall Logs Review

* Deny Rules Logs
  * 預設開啟記錄
  * 用途: 情資分享(IP Scan、Port Scan 黑名單)
  * 入侵分析: 幫助有限, 因為已經被 Deny 無入侵風險.
* Allow Rules Logs
  * 預設未開啟記錄.
  * 建議應開啟, 才能分析是否有異常資安事件.
  * 歷程記錄、入侵分析

防火牆規則整理

Firewall Rules
IP 網段

	IP 網段	內對外	外對內	內對內
辦公室 工作區	Private IP	Permit all Dest IP: 黑名單 (惡意 IP)	Reject all 僅允許: 校內網段	Permit Private IP
網路設備/ IoT 設備	Private IP	Reject all	Reject all	Permit Private IP
Server Farm	Private IP + Public IP	For 軟體更新: Dest IP: 白名單 (Zero Trust)	80/443: Permit all For 管理 Port: 22: Src IP 白名單 3389:Src IP 白名單 或 Out of Band 內部網段	跳板機/VPN

Firewall Logs Review
連線分析

- 個人電腦
  - 外對內連線: 不應有.
  - 內對外連線
    - Review 所有Dest Port != 80, 443, 53 連線
    - 搭配 Snort/Layer7 分析
      - Dest Port 80 但非 http protocol
      - Dest Port 443 但非 https protocol
      - Dest Port 53 但非 DNS protocol
    - 使用 GEOIP 進行 Country & ASN 分析, 針對冷門之 Country & ASN 應特別留意是否可能是後門程式在運作.
- Server Farm
  - 外對內連線
    - Web Server: 連線記錄之頻率與次數分析
    - 可用 Size & 頻率 看出是否進行 SQL Injection & try 密碼攻擊
  - 內對外
    - ☆☆☆應僅有 Window Update, Linux OS Update 等系統更新連線記錄, 不應有主動內對外連線行為.

網路管理控制措施檢測
Scan from Internet

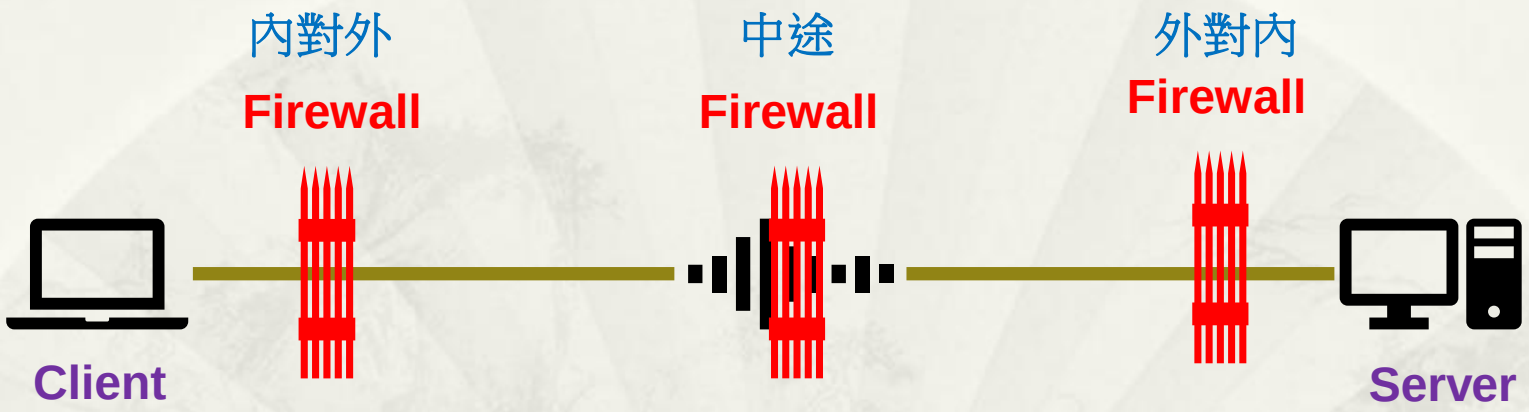
- 工作區電腦、網路設備、IoT 設備
  - 不應有任何外對內可連線服務
    - ftp, ntp, http, https … (21, 123, 80, 443, …)
  - 不應有遠端管理連線服務
    - ssh, telnet,snmp, vnc, rdp (22,23,161,5900,3389)
- Server Farm
  - http, https 不應有後台管理系統
  - 不應有遠端管理連線服務

Firewall Rules Detection

大綱

- For Server: 外對內
- For Client: 內對外
- For 中途

Firewalls



Firewall Rules Detection For Server

外對內

Firewalls

Firewall Rules Detection For Server

* 以下兩個 IP，何者有外對內 Firewall？
  * 140.112.8.116(www.ntu.edu.tw)

```
C:\Users\user>ping 140.112.8.116

Ping 140.112.8.116 (使用 32 位元組的資料):
要求等候逾時。
要求等候逾時。
要求等候逾時。
```

  * 140.112.3.126

```
C:\Users\user>ping 140.112.3.126

Ping 140.112.3.126 (使用 32 位元組的資料):
回覆自 140.112.3.126: 位元組=32 時間=2ms TTL=250
回覆自 140.112.3.126: 位元組=32 時間=1ms TTL=250
回覆自 140.112.3.126: 位元組=32 時間=1ms TTL=250
```

  * Hint: ping

Firewall Rules Detection For Server

* 以下兩個 IP，何者有外對內 Firewall？
  * 180.222.102.202(tw.yahoo.com)

```
C:\Users\user>ping 180.222.102.202

Ping 180.222.102.202 (使用 32 位元組的資料):
回覆自 180.222.102.202: 位元組=32 時間=1ms TTL=48
回覆自 180.222.102.202: 位元組=32 時間=1ms TTL=48
回覆自 180.222.102.202: 位元組=32 時間=1ms TTL=48
```

  * 140.112.3.126

```
C:\Users\user>ping 140.112.3.126

Ping 140.112.3.126 (使用 32 位元組的資料):
回覆自 140.112.3.126: 位元組=32 時間=2ms TTL=250
回覆自 140.112.3.126: 位元組=32 時間=1ms TTL=250
回覆自 140.112.3.126: 位元組=32 時間=1ms TTL=250
```

  * Hint1: ping (皆有回應)
  * Hint2: telnet port 81 …

Firewall Rules Detection For Server

* 測試前提:
  * @Client 本身無 Firewall
  * 內對外、中途無Firewall

Firewall Rules Detection For Server

* 外對內防火牆規則?
  * 開放/封鎖哪些 Protocols/Ports ?
  * 測試 TCP Port 1~1024
    * nmap 180.222.102.202 -p 1-1024

```
Not shown: 1022 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

      * 僅開放 TCP: 80/443
    * nmap 140.112.3.126 -p 1-1024

```
All 1024 scanned ports on ntuccgw.cc.ntu.edu.tw (140.112.3.126) are in ignored states.
Not shown: 1024 closed tcp ports (reset)
```

      * TCP: 1 ~ 1024 無防火牆封鎖

Firewall Rules Detection For Server

- 找出在 Internet 上 10 個 IP “有”外對內Firewall?
  - Hint: Top 100 Website
- 找出在 Internet 上 10 個 IP “無”外對內Firewall?
  - Hint: TraceRoute 途中 Router
    - 同 AS 內部 Router
    - 不同 ISP: HiNet, FET….

From 光世代 To 168.95.1.1

```
C:\>tracert -d 168.95.1.1

在上限 30 個躍點上追蹤 168.95.1.1 的路由

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     3 ms     2 ms     2 ms  168.95.98.254
  3     2 ms     2 ms     2 ms  168.95.74.50
  4     2 ms     2 ms     2 ms  220.128.3.10
  5     2 ms     2 ms     2 ms  220.128.3.189
  6     2 ms     2 ms     2 ms  210.59.204.217
  7     5 ms     2 ms     3 ms  220.128.32.69
  8     3 ms     2 ms     2 ms  168.95.1.1
```

From 台大 To 成大

```
C:\Users\user>tracert www.ncku.edu.tw

在上限 30 個躍點上
追蹤 www.ncku.edu.tw [140.116.241.51] 的路由:

  1    <1 ms    <1 ms    <1 ms  pfSense.localdomain [172.16.0.1]
  2    <1 ms    <1 ms    <1 ms  ntuccgw.cc.ntu.edu.tw [140.112.3.126]
  3    <1 ms    <1 ms    <1 ms  140.112.0.170
  4     1 ms     1 ms     1 ms  140.112.0.206
  5     1 ms     1 ms     1 ms  140.112.0.70
  6     2 ms     1 ms     2 ms  192.192.61.82
  7     5 ms     5 ms     5 ms  192.192.61.22
  8     6 ms     5 ms     6 ms  192.192.61.145
  9     6 ms     5 ms     5 ms  140.116.243.178
 10     6 ms     5 ms     5 ms  140.116.243.186
 11     5 ms     5 ms     6 ms  www.ncku.edu.tw [140.116.241.51]
```

TraceRoute 途中 Router

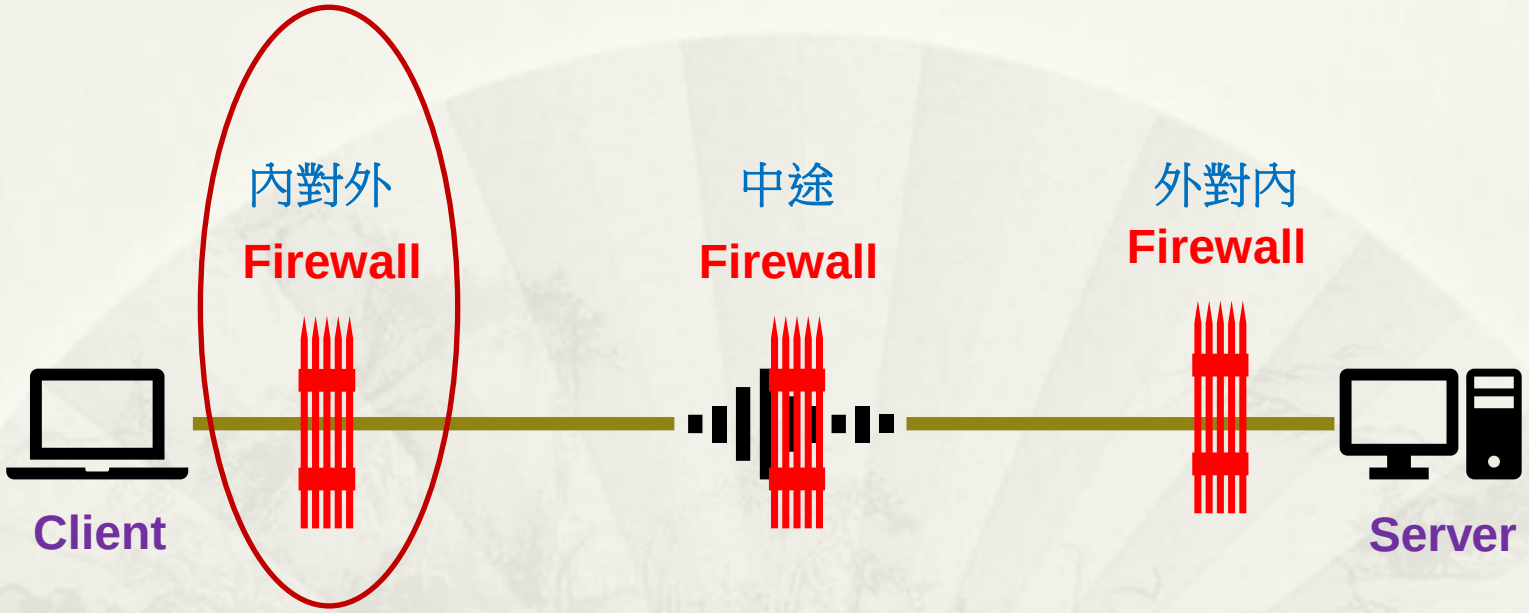
```
S:\Tools\Nmap7.97>nmap 140.112.0.70
Starting Nmap 7.97 ( https://nmap.org )
Nmap scan report for wan_tanet_0070.cc.n
Host is up (0.0015s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  filtered ssh
111/tcp filtered rpcbind
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
```

```
S:\Tools\Nmap7.97>nmap 192.192.61.82
Starting Nmap 7.97 ( https://nmap.org )
Nmap scan report for 192.192.61.82
Host is up (0.0022s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  filtered ssh
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
```

Firewall Rules Detection For Client

內對外

Firewalls



Firewall Rules Detection For Client

- @Where ?
  - 台中某旅宿 SSID:TCXXX_HOTEL
  - 台科大 eduroam
  - 教育部科技大樓 eduroam
- 連線狀況
  - 無法使用 telnet 連線 ptt.cc
  - 無法使用 ssh 連線 遠端 Server
  - 無法使用 ftp 下載檔案
  - 無法使用 Outlook 收發信
  - 無法使用 Windows 遠端桌面連回個人電腦
  - 無法使用手機 Android App 程式 Speed Test 進行測速

Firewall Rules Detection For Client

- 內部出口防火牆”內對外”規則?
  - 開放/封鎖哪些 Protocols/Ports ?
- 測試方法:
  - 連線 Internet 網頁 -> 正常
    - 已開放 TCP: 80, 443
  - ping 8.8.8.8 -> 有回應
    - 已開放 ICMP
  - nslookup www.ibm.com 8.8.8.8 -> 解析成功
    - 已開放 UDP: 53
  - 無法使用 ssh 連線 遠端 Server
    - 被封鎖 TCP: 22
  - 無法使用 Outlook 收發信
    - 被封鎖 TCP: POP3/IMP4 + SMTP
  - 無法使用遠端桌面
  - telnet 163.28.17.100 3389 -> 無回應
    - 被封鎖 TCP: 3389

Firewall Rules Detection For Client

* 測試前提:
  * @Server 本身無 Firewall
  * 中途、外對內無 Firewall

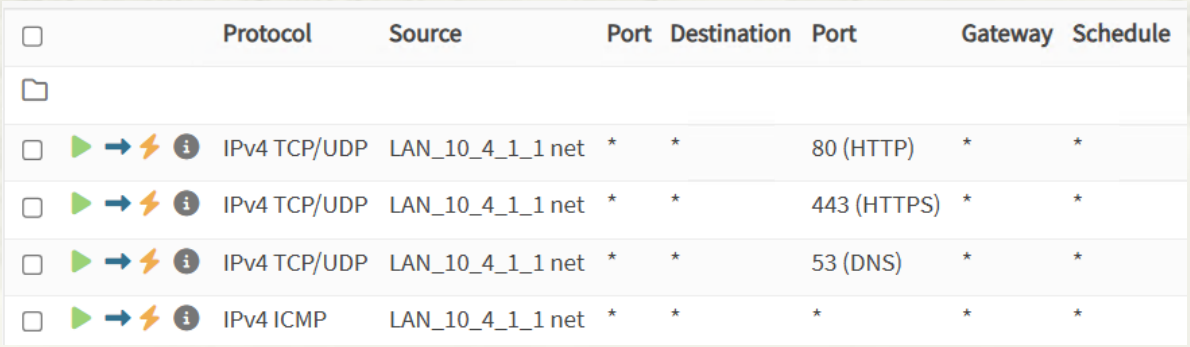
方法1. 自行架設
方法2: Any Router

Firewall Rules Detection For Client

* nmap -p1-1024 192.192.61.82

```
Nmap scan report for 192.192.61.82
Host is up (0.0020s latency).
Not shown: 1021 filtered tcp ports (no-response)
PORT    STATE  SERVICE
53/tcp  closed domain
80/tcp  closed http
443/tcp closed https
```

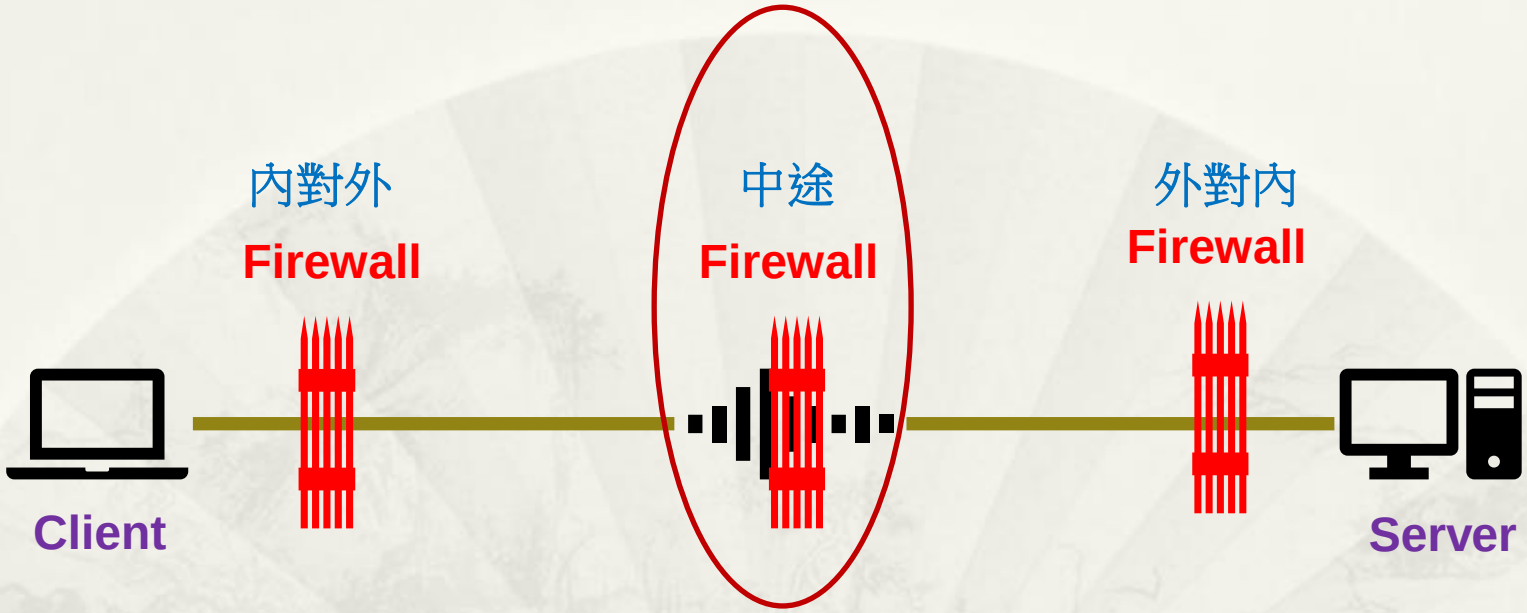
* 結論:
  * 僅有TCP Port: 53/80/443 有開放內對外連線，其餘全被封鎖(filtered).
* 解決方法
  * SSLVPN



	Protocol	Source	Port	Destination	Port	Gateway	Schedule
	IPv4 TCP/UDP	LAN_10_4_1_1 net	*	*	80 (HTTP)	*	*
	IPv4 TCP/UDP	LAN_10_4_1_1 net	*	*	443 (HTTPS)	*	*
	IPv4 TCP/UDP	LAN_10_4_1_1 net	*	*	53 (DNS)	*	*
	IPv4 ICMP	LAN_10_4_1_1 net	*	*	*	*	*

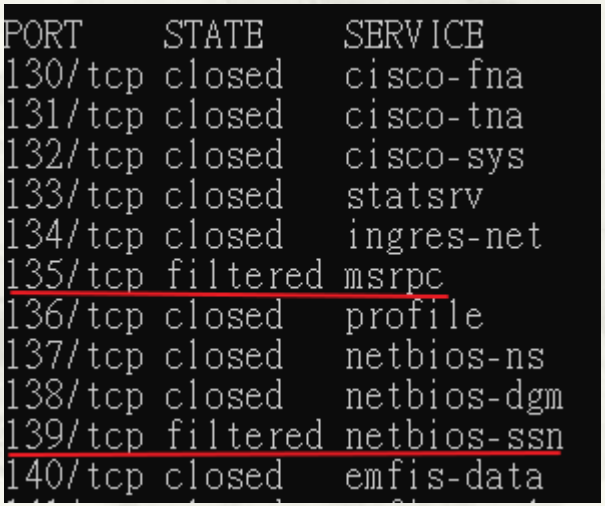
Firewall Rules Detection For 中途

Firewall Rules Detection For 中途



Firewall Rules Detection For 中途

- From:台大校內 To: TANet 三峽主節點
- 測試 TCP port 130 ~ 140 是否開放？
  - nmap -p 130-140 192.192.61.82



← 135 被封鎖

← 139 被封鎖

Firewall Rules Detection For 中途

- From :台大校內 To: TANet 三峽主節點
- 測試 TCP port 440 ~ 450 是否開放？
  - nmap -p 440-450 192.192.61.82

```
PORT    STATE    SERVICE
440/tcp closed   sgcp
441/tcp closed   decvms-sysmgt
442/tcp closed   cvc_hostd
443/tcp closed   https
444/tcp closed   snpp
445/tcp filtered microsoft-ds
446/tcp closed   ddm-rdb
447/tcp closed   ddm-dfm
448/tcp closed   ddm-ssl
449/tcp closed   as-servermap
450/tcp closed   tserver
```

← 445 被封鎖

- Port 445 在路徑中哪個節點被封鎖?
  - 使用 TraceRoute By TCP 測試
    - tracetcp、 nping、nmap NSE: firewalk
    - (建議先介紹 TraceRoute 原理)

For 中途
方法1: tracetcp.exe

- 找一個 IP & Port 可順利 TraceRoute完成
  - tracetcp 192.192.61.82:440 -n

```
Tracing route to 192.192.61.82 on port 440
Over a maximum of 30 hops.
1       16 ms    0 ms    1 ms    172.16.0.1
2       4 ms    48 ms    1 ms    140.112.3.126
3       1 ms     0 ms    5 ms    140.112.0.170
4       2 ms    35 ms    3 ms    140.112.0.206
5       4 ms     4 ms    2 ms    140.112.0.70
6       Destination Reached in 4 ms. Port closed on 192.192.61.82
Trace Complete.
```

- 測試被阻擋 port
  - tracetcp 192.192.61.82:445 -n

```
Tracing route to 192.192.61.82 on port 445
Over a maximum of 30 hops.
1        2 ms     4 ms     1 ms     172.16.0.1
2        *        *        *        Request timed out.
3        *        *        *        Request timed out.
4        *        *        *        Request timed out.
5        *        *        *        Request timed out.
6        *        *        *        Request timed out.
7        *        *        *        Request timed out.
8        *        *        *        Request timed out.
9        *        *        *        Request timed out.
```

For 中途
方法2: nping

- nping --tr --tcp -p 440 192.192.61.82

```
Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2025-07-15 11:24 台北標準時間
SENT (0.0580s) TCP 172.16.0.12:19274 > 192.192.61.82:440 S ttl=1 id=26279 iplen=40  seq=1998538657 win=1480
RCVD (0.0600s) ICMP [172.16.0.1 > 172.16.0.12 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=56001 iplen=68 ]
SENT (1.0600s) TCP 172.16.0.12:19274 > 192.192.61.82:440 S ttl=2 id=26279 iplen=40  seq=1998538657 win=1480
RCVD (1.0600s) ICMP [140.112.3.126 > 172.16.0.12 TTL=0 during transit (type=11/code=0) ] IP [ttl=253 id=26496 iplen=56 ]
SENT (2.0600s) TCP 172.16.0.12:19274 > 192.192.61.82:440 S ttl=3 id=26279 iplen=40  seq=1998538657 win=1480
RCVD (2.0600s) ICMP [140.112.0.170 > 172.16.0.12 TTL=0 during transit (type=11/code=0) ] IP [ttl=253 id=53391 iplen=56 ]
SENT (3.1320s) TCP 172.16.0.12:19274 > 192.192.61.82:440 S ttl=4 id=26279 iplen=40  seq=1998538657 win=1480
RCVD (3.1350s) ICMP [140.112.0.206 > 172.16.0.12 TTL=0 during transit (type=11/code=0) ] IP [ttl=252 id=46562 iplen=96 ]
SENT (4.1330s) TCP 172.16.0.12:19274 > 192.192.61.82:440 S ttl=5 id=26279 iplen=40  seq=1998538657 win=1480
RCVD (4.1360s) ICMP [140.112.0.70 > 172.16.0.12 TTL=0 during transit (type=11/code=0) ] IP [ttl=251 id=24850 iplen=96 ]
SENT (5.1330s) TCP 172.16.0.12:19274 > 192.192.61.82:440 S ttl=6 id=26279 iplen=40  seq=1998538657 win=1480
RCVD (5.1340s) TCP 192.192.61.82:440 > 172.16.0.12:19274 RA ttl=250 id=14432 iplen=40  seq=0 win=0
```

- nping --tr --tcp -p 445 192.192.61.82

```
Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2025-07-15 11:25 台北標準時間
SENT (0.0570s) TCP 172.16.0.12:27966 > 192.192.61.82:445 S ttl=1 id=32305 iplen=40  seq=3881933797 win=1480
RCVD (0.0580s) ICMP [172.16.0.1 > 172.16.0.12 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=32030 iplen=68 ]
SENT (1.0580s) TCP 172.16.0.12:27966 > 192.192.61.82:445 S ttl=2 id=32305 iplen=40  seq=3881933797 win=1480
SENT (2.0580s) TCP 172.16.0.12:27966 > 192.192.61.82:445 S ttl=3 id=32305 iplen=40  seq=3881933797 win=1480
SENT (3.0580s) TCP 172.16.0.12:27966 > 192.192.61.82:445 S ttl=4 id=32305 iplen=40  seq=3881933797 win=1480
SENT (4.0580s) TCP 172.16.0.12:27966 > 192.192.61.82:445 S ttl=5 id=32305 iplen=40  seq=3881933797 win=1480
SENT (5.0580s) TCP 172.16.0.12:27966 > 192.192.61.82:445 S ttl=6 id=32305 iplen=40  seq=3881933797 win=1480
```

For 中途
方法3: nmap NSE: firewalk

- nmap NSE(NMAP Scripting Engine): firewalk
  - Script types: hostrule
  - Categories: safe, discovery
  - Tries to discover firewall rules using an IP TTL expiration technique known as firewalking.
- 語法: nmap --script firewalk --traceroute <target>
  - 需以系統管理員身分執行
  - 優點: 可同時偵測被阻擋 Ports 與 節點

For 中途
nmap NSE: firewalk

* nmap --script firewalk --traceroute -p 440-450 192.192.61.82

```
PORT    STATE    SERVICE
440/tcp closed   sgcp
441/tcp closed   decvms-sysmgt
442/tcp closed   cvc_hostd
443/tcp closed   https
444/tcp closed   snpp
445/tcp filtered microsoft-ds
446/tcp closed   ddm-rdb
447/tcp closed   ddm-dfm
448/tcp closed   ddm-ssl
449/tcp closed   as-servermap
450/tcp closed   tserver

Host script results:
| firewalk:
| HOP  HOST        PROTOCOL  BLOCKED PORTS
|_1    172.16.0.1  tcp       445

TRACEROUTE (using port 441/tcp)
HOP RTT     ADDRESS
1   0.00 ms 172.16.0.1
2   0.00 ms ntuccgw.cc.ntu.edu.tw (140.112.3.126)
3   0.00 ms core_serv_0170.cc.ntu.edu.tw (140.112.0.170)
4   1.00 ms wan0206.cc.ntu.edu.tw (140.112.0.206)
5   2.00 ms wan_tanet_0070.cc.ntu.edu.tw (140.112.0.70)
6   2.00 ms 192.192.61.82
```

For 中途
nmap NSE: firewalk

* nmap --script firewalk --traceroute -p 6345-6349 www.google.com

```
Nmap scan report for www.google.com (172.217.163.36)
Host is up (0.0020s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4012:4::2004
rDNS record for 172.217.163.36: tsa01s13-in-f4.1e100.net

PORT     STATE    SERVICE
6345/tcp filtered unknown
6346/tcp filtered gnutella
6347/tcp filtered gnutella2
6348/tcp filtered unknown
6349/tcp filtered unknown

Host script results:
| firewalk:
| HOP  HOST           PROTOCOL  BLOCKED PORTS
| 4    140.112.0.206  tcp       6346-6349
|_6    72.14.204.212  tcp       6345

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   1.00 ms 172.16.0.1
2   1.00 ms ntuccgw.cc.ntu.edu.tw (140.112.3.126)
3   1.00 ms core_serv_0210.cc.ntu.edu.tw (140.112.0.210)
4   2.00 ms wan0206.cc.ntu.edu.tw (140.112.0.206)
5   2.00 ms wan_sinica_0034.cc.ntu.edu.tw (140.112.0.34)
6   3.00 ms 72.14.204.212
7   3.00 ms 142.250.228.181
8   3.00 ms 142.251.226.169
9   2.00 ms tsa01s13-in-f4.1e100.net (172.217.163.36)
```

被 ALLOT 阻擋
(目前已解決)

nmap NSE: firewalk
Check Top 1000 common ports

* nmap --script firewalk --traceroute 192.192.61.89

```
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  filtered ssh
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Host script results:
| firewalk:
| HOP  HOST          PROTOCOL  BLOCKED PORTS
| 1    172.16.0.1    tcp       135,139,445
|_7    192.192.61.1  tcp       22

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   0.00 ms 172.16.0.1
2   1.00 ms ntuccgw.cc.ntu.edu.tw (140.112.3.126)
3   1.00 ms core_serv_0170.cc.ntu.edu.tw (140.112.0.170)
4   2.00 ms wan0206.cc.ntu.edu.tw (140.112.0.206)
5   2.00 ms wan_tanet_0070.cc.ntu.edu.tw (140.112.0.70)
6   3.00 ms 192.192.61.82
7   2.00 ms 192.192.61.1
8   3.00 ms 192.192.61.89
```

簡報完畢
謝謝