

L4 Revers Proxy

臺大計資中心網路組
游子興

davisyou@ntu.edu.tw

02-33665008

大綱

- * L4 Revers Proxy 原理與實做
 - * With HTTP Server
 - * With HTTPs Server
 - * IPv6 to IPv4
 - * With SSH Server
 - * Bypass Web Server IP ACL Control
- * Transparent Proxy Mode

NGINX Module

- * Ubuntu 24.04/26.04 預設不支援 ngx_stream_core_module, ngx_stream_proxy_module
- * 需安裝
 - ~# apt install libnginx-mod-stream

L4 Revers Proxy with HTTP Server

L4 Reverse Proxy (HTTP Server)

TCP Port 8080 to 80



使用者連線:

demo1:

`http://140.112.237.5:8080/icons/ubuntu-logo.png`

demo2:

`http://proxy01.buda.idv.tw:8080/icons/ubuntu-logo.png`

```
* /etc/nginx/nginx.conf
stream {
    server {
        listen 8080; #不可再使用 Port 80
        proxy_pass 172.16.0.7:80;
    }
}
```

L4 Reverse Proxy

封包檔

* 2 TCP Sessions : L7 Payload 1對1 對映、但 TTL、Length 都不相同

* L4_HTTP_ReverseProxy_1_WAN.pcap

	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	124	120.96.0.222	23587	140.112.237.5	8080	TCP	66	23587 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
2	0.000026	64	140.112.237.5	8080	120.96.0.222	23587	TCP	66	8080 → 23587 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
3	0.000757	124	120.96.0.222	23587	140.112.237.5	8080	TCP	60	23587 → 8080 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	0.002454	124	120.96.0.222	23587	140.112.237.5	8080	HTTP	508	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.002464	64	140.112.237.5	8080	120.96.0.222	23587	TCP	54	8080 → 23587 [ACK] Seq=1 Ack=455 Win=64128 Len=0
6	0.002860	64	140.112.237.5	8080	120.96.0.222	23587	HTTP	3678	HTTP/1.1 200 OK (PNG)
7	0.003952	124	120.96.0.222	23587	140.112.237.5	8080	TCP	60	23587 → 8080 [ACK] Seq=455 Ack=2921 Win=262656 Len=0

* L4_HTTP_ReverseProxy_2_LAN.pcap

	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	64	172.16.0.226	36912	172.16.0.7	80	TCP	74	36912 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
2	0.000093	64	172.16.0.7	80	172.16.0.226	36912	TCP	74	80 → 36912 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
3	0.000116	64	172.16.0.226	36912	172.16.0.7	80	TCP	66	36912 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
4	0.001639	64	172.16.0.226	36912	172.16.0.7	80	HTTP	520	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.001710	64	172.16.0.7	80	172.16.0.226	36912	TCP	66	80 → 36912 [ACK] Seq=1 Ack=455 Win=64768 Len=0 TSv
6	0.001946	64	172.16.0.7	80	172.16.0.226	36912	HTTP	3690	HTTP/1.1 200 OK (PNG)
7	0.001967	64	172.16.0.226	36912	172.16.0.7	80	TCP	66	36912 → 80 [ACK] Seq=455 Ack=3625 Win=62464 Len=0

L4 Reverse Proxy

Payload(L7) 完全相同

連線: <http://140.112.237.5:8080/icons/ubuntu-logo.png>

L4_HTTP_ReverseProxy_1_WAN.pcap

L4_HTTP_ReverseProxy_2_LAN.pcap

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L4_HTTP_ReverseProxy_1_WAN.pcap

HTTP Request Header

GET /icons/ubuntu-logo.png HTTP/1.1
Host: 140.112.237.5:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9

HTTP Response Header

HTTP/1.1 200 OK
Date: Mon, 23 Oct 2023 09:02:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 08 Mar 2023 17:32:54 GMT
ETag: "d0a-5f666eb0abd80"
Accept-Ranges: bytes
Content-Length: 3338
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

HTTP Body

.PNG
...
IHDR...w...c.....~.....IDATx...].t.H..1.Z.....<.....03...t.0.#.VG...,{.;`..]n.
..+..r...VV7.r.....l..b.]6.m.69.N.....cj.E.+;.R?.....+...../.e.\$Yb..S.....'....Y.8.

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L4_HTTP_ReverseProxy_2_LAN.pcap

HTTP Request Header

GET /icons/ubuntu-logo.png HTTP/1.1
Host: 140.112.237.5:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9

HTTP Response Header

HTTP/1.1 200 OK
Date: Mon, 23 Oct 2023 09:02:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 08 Mar 2023 17:32:54 GMT
ETag: "d0a-5f666eb0abd80"
Accept-Ranges: bytes
Content-Length: 3338
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

HTTP Body

.PNG
...
IHDR...w...c.....~.....IDATx...].t.H..1.Z.....<.....03...t.0.#.VG...,{.;`..]n.
..+..r...VV7.r.....l..b.]6.m.69.N.....cj.E.+;.R?.....+...../.e.\$Yb..S.....'....Y.8.

L4 Reverse Proxy

Payload(L7) 完全相同

連線: <http://proxy01.buda.idv.tw:8080/icons/ubuntu-logo.png>

L4_HTTP_ReverseProxy_1_WAN_Host.pcap

L4_HTTP_ReverseProxy_2_LAN_Host.pcap

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L4_HTTP_ReverseProxy_1_WAN_HostName.pcap

HTTP Request Header

GET /icons/ubuntu-logo.png HTTP/1.1
Host: demo1.buda.idv.tw:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9

HTTP Response Header

HTTP/1.1 200 OK
Date: Mon, 23 Oct 2023 09:02:19 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 08 Mar 2023 17:32:54 GMT
ETag: "d0a-5f666eb0abd80"
Accept-Ranges: bytes
Content-Length: 3338
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

HTTP Body

.PNG
...
IHDR...w...c.....~.....IDATx...].t.H..1.Z.....<.....03...t.0.#.VG...{.;`..]n.
...+..r...VV7.r.....l..b.]6.m.69.N.....cj.E.+;.R?.....+...../..e.\$Yb..S.....'.....Y.8.

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L4_HTTP_ReverseProxy_1_LAN_HostName.pcap

HTTP Request Header

GET /icons/ubuntu-logo.png HTTP/1.1
Host: demo1.buda.idv.tw:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9

HTTP Response Header

HTTP/1.1 200 OK
Date: Mon, 23 Oct 2023 09:02:19 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 08 Mar 2023 17:32:54 GMT
ETag: "d0a-5f666eb0abd80"
Accept-Ranges: bytes
Content-Length: 3338
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

HTTP Body

.PNG
...
IHDR...w...c.....~.....IDATx...].t.H..1.Z.....<.....03...t.0.#.VG...{.;`..]n.
...+..r...VV7.r.....l..b.]6.m.69.N.....cj.E.+;.R?.....+...../..e.\$Yb..S.....'.....Y.8.

L4 Reverse Proxy

Identify technologies on websites

- * Can Not Hide Original Web Server/OS



L4 Reverse Proxy with HTTPs Server

L4 Reverse Proxy (HTTPs Server) TCP Port 8443 to 443



使用者連線:

<http://140.112.237.5:8443/>
<https://140.112.237.5:8443/>
<https://proxy01.buda.idv.tw:8443/>

```
* /etc/nginx/nginx.conf
stream {
    server {
        listen 8443;
        proxy_pass www.tp1rc.edu.tw:443;
    }
}
```

L4 Reverse Proxy (HTTPs Server) Demo1

- * `http://140.112.237.5:8443/`

- * 錯誤:

400 Bad Request

The plain HTTP request was sent to HTTPS port

nginx/1.20.2

- * 失敗原因

- * 等同 `http://www.tp1rc.edu.tw:443/`

- * 使用 http 連線 https Service

L4 Reverse Proxy (HTTPs Server)

Demo1

* L4_443_ReverseProxy_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	66	57196 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
2	0.000038	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	66	8443 → 57196 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
3	0.000938	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	60	57196 → 8443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	0.003003	0	125	120.96.0.222	57196	140.112.237.5	8443	HTTP	788	GET / HTTP/1.1
5	0.003016	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	54	8443 → 57196 [ACK] Seq=1 Ack=735 Win=64128 Len=0
6	0.003876	0	64	140.112.237.5	8443	120.96.0.222	57196	HTTP	863	HTTP/1.1 400 Bad Request (text/html)
7	0.003984	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	54	8443 → 57196 [FIN, ACK] Seq=810 Ack=735 Win=64128 Len=0
8	0.004734	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	60	57196 → 8443 [ACK] Seq=735 Ack=811 Win=261888 Len=0
9	0.005545	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	60	57196 → 8443 [FIN, ACK] Seq=735 Ack=811 Win=261888 Len=0
10	0.005552	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	54	8443 → 57196 [ACK] Seq=811 Ack=736 Win=64128 Len=0

* L4_443_ReverseProxy_2_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	74	51924 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000709	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	74	443 → 51924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
3	0.000726	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	66	51924 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
4	0.002077	0	64	140.112.237.5	51924	140.112.2.208	443	HTTP	800	GET / HTTP/1.1
5	0.002419	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	66	443 → 51924 [ACK] Seq=1 Ack=735 Win=64512 Len=0 T
6	0.002847	0	62	140.112.2.208	443	140.112.237.5	51924	HTTP	875	HTTP/1.1 400 Bad Request (text/html)
7	0.002853	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	66	51924 → 443 [ACK] Seq=735 Ack=810 Win=64128 Len=0
8	0.002962	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	66	443 → 51924 [FIN, ACK] Seq=810 Ack=735 Win=64512
9	0.002987	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	66	51924 → 443 [FIN, ACK] Seq=735 Ack=811 Win=64128
10	0.003198	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	66	443 → 51924 [ACK] Seq=811 Ack=736 Win=64512 Len=0

L4 Reverse Proxy (HTTPs Server)

Demo2

* <https://140.112.237.5:8443/>

你的連線不是私人連線

攻擊者可能會試圖從 **140.112.237.5** 竊取你的資訊 (例如密碼、郵件或信用卡資料)。 [瞭解詳情](#)

NET::ERR_CERT_COMMON_NAME_INVALID

💡 要獲得 Chrome 最高等級的安全防護，請[啟用強化防護功能](#)

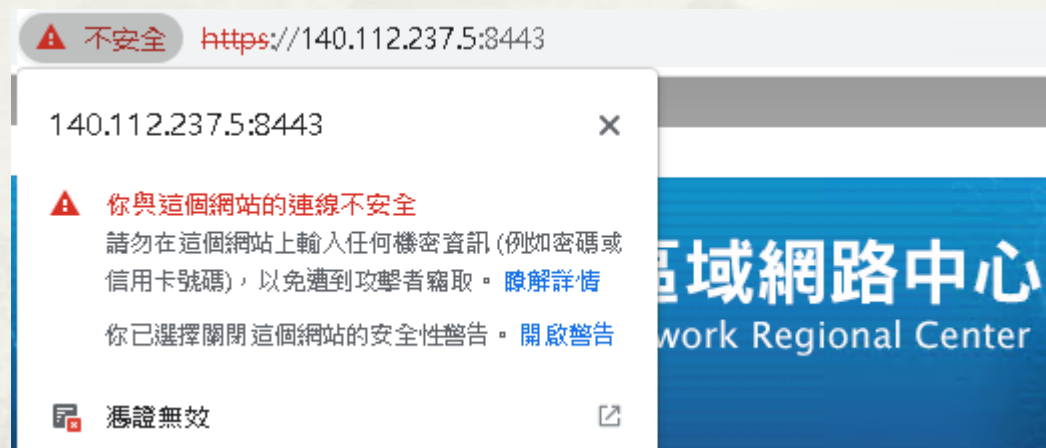
隱藏詳細資料

返回安全性瀏覽

伺服器無法證明其屬於 **140.112.237.5** 網域；其安全性憑證來自 www.tp1rc.edu.tw 網域。這可能是因為設定錯誤，或有攻擊者攔截你的連線所致。

[繼續前往 140.112.237.5 網站 \(不安全\)](#)

* 成功連線，但顯示憑證無效。



L4 Revers Proxy IPv6 to IPv4

L4 Revers Proxy

IPv6 to IPv4

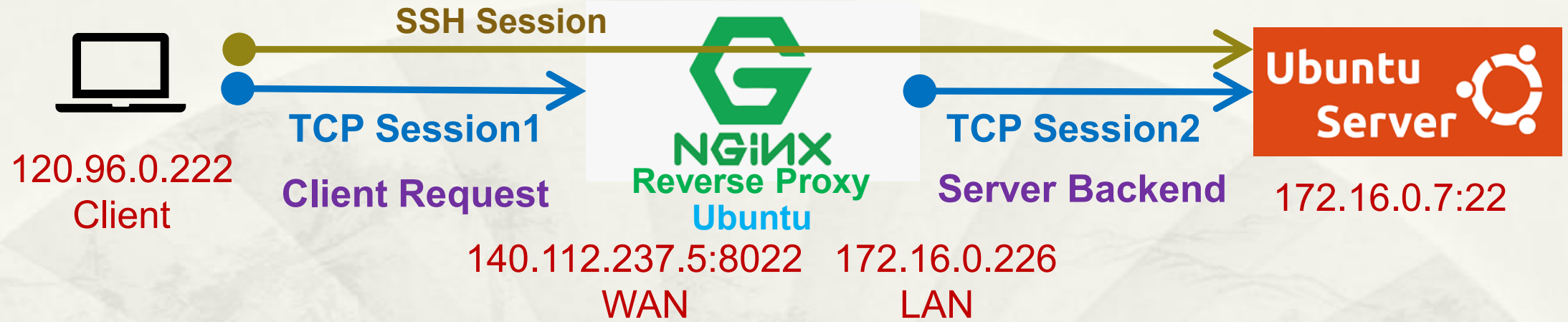


L4 Reverse Proxy with SSH Server

Payload 1 對 1 對映
(不包含 TCP Flag only 封包)

L4 Reverse Proxy (SSH Server)

TCP Port 8022 to 22



使用者連線:

SSH to 140.112.237.5:8022

```
* /etc/nginx/nginx.conf
stream {
    server {
        listen 8022;
        proxy_pass 172.16.0.7:22;
    }
}
```

L4 Reverse Proxy (SSH Server)

TCP Port 8022 to 22

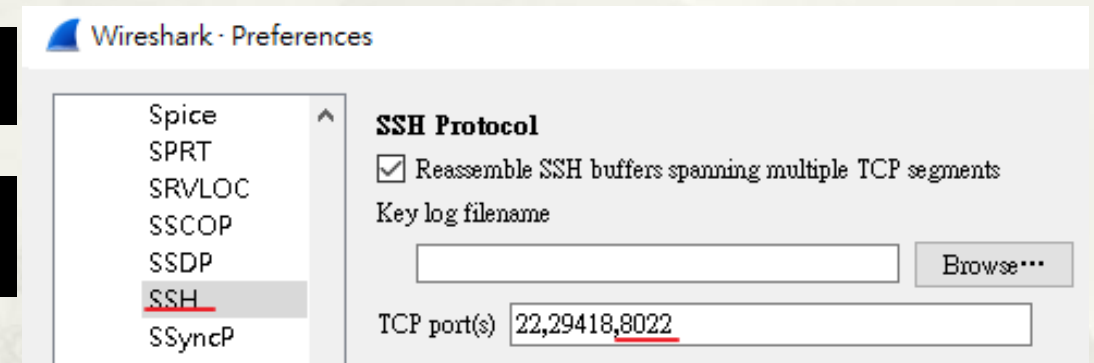
- * SSH to 140.112.237.5:8022
 - * SSH Login

- * Wireshark

- * 預設無法辨識 Port: 8022

```
user@140.112.237.5's password:  
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-125-generic x86_64)
```

```
user@ubuntu20:~$ ifconfig  
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 172.16.0.7 netmask 255.255.255.0 broadcast 172.16.0.255
```



No.	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	125	120.96.0.222	55098	140.112.237.5	8022	TCP	66	55098 → 8022 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	64	140.112.237.5	8022	120.96.0.222	55098	TCP	66	8022 → 55098 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	125	120.96.0.222	55098	140.112.237.5	8022	TCP	60	55098 → 8022 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1 Ack=29 Win=64256 Len=0
6	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
7	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	1110	Server: Key Exchange Init
8	125	120.96.0.222	55098	140.112.237.5	8022	TCP	60	55098 → 8022 [ACK] Seq=29 Ack=1098 Win=261632 Len=0
9	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	1310	Client: Key Exchange Init
10	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1098 Ack=1285 Win=64128 Len=0
11	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
12	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1098 Ack=1333 Win=64128 Len=0
13	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	518	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=256)
14	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	134	Client: New Keys, Encrypted packet (len=64)
15	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1562 Ack=1413 Win=64128 Len=0
16	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	118	Server: Encrypted packet (len=64)
17	125	120.96.0.222	55098	140.112.237.5	8022	TCP	60	55098 → 8022 [ACK] Seq=1413 Ack=1626 Win=262656 Len=0
1	64	172.16.0.226	35084	172.16.0.7	22	TCP	74	35084 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2823702048 TSecr=0 WS=128
2	64	172.16.0.7	22	172.16.0.226	35084	TCP	74	22 → 35084 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1475222517 TSecr=
3	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2823702048 TSecr=1475222517
4	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	94	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1 Ack=29 Win=65152 Len=0 TSval=1475222517 TSecr=2823702049
6	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	107	Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
7	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=29 Ack=42 Win=64256 Len=0 TSval=2823702057 TSecr=1475222525
8	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	1122	Server: Key Exchange Init
9	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=29 Ack=1098 Win=64128 Len=0 TSval=2823702057 TSecr=1475222526
10	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	1322	Client: Key Exchange Init
11	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1098 Ack=1285 Win=64128 Len=0 TSval=1475222527 TSecr=2823702059
12	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
13	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1098 Ack=1333 Win=64128 Len=0 TSval=1475222529 TSecr=2823702061
14	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	530	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=256)
15	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=1333 Ack=1562 Win=64128 Len=0 TSval=2823702064 TSecr=1475222533
16	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	146	Client: New Keys, Encrypted packet (len=64)
17	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1562 Ack=1413 Win=64128 Len=0 TSval=1475222545 TSecr=2823702077
18	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	130	Server: Encrypted packet (len=64)
19	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=1413 Ack=1626 Win=64128 Len=0 TSval=2823702077 TSecr=1475222545

L4_SSH_ReverseProxy_1_WAN.pcap

非每個 Payload 皆回應 ACK Windows

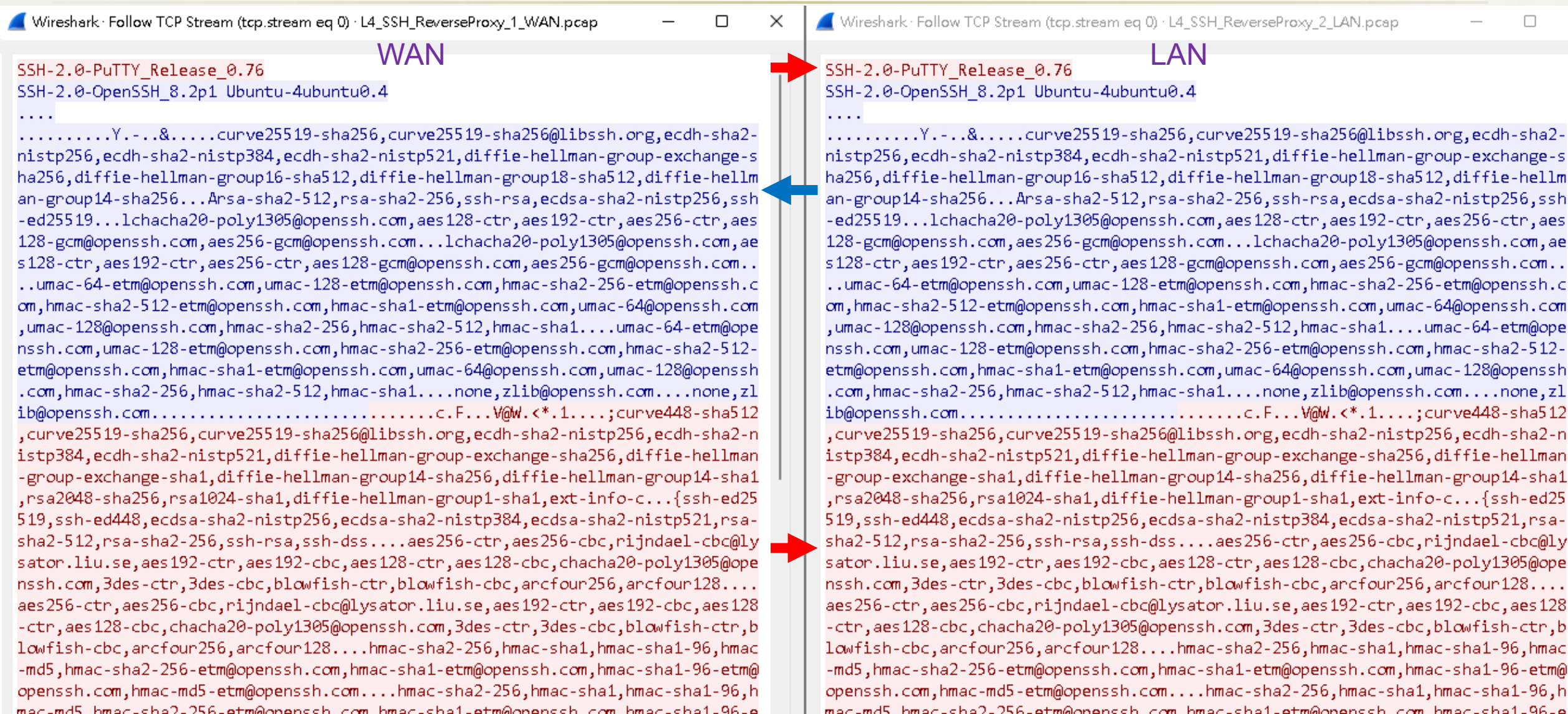
L4_SSH_ReverseProxy_2_LAN.pcap

每個 Payload 皆回應 ACK Ubuntu

封包數不同

L4 Reverse Proxy (SSH Server)

Payload(L7) 完全相同





簡報完畢
謝謝