

Reverse Proxy 運作原理與實做 以 NGINX 為例

臺大計資中心網路組
游子興

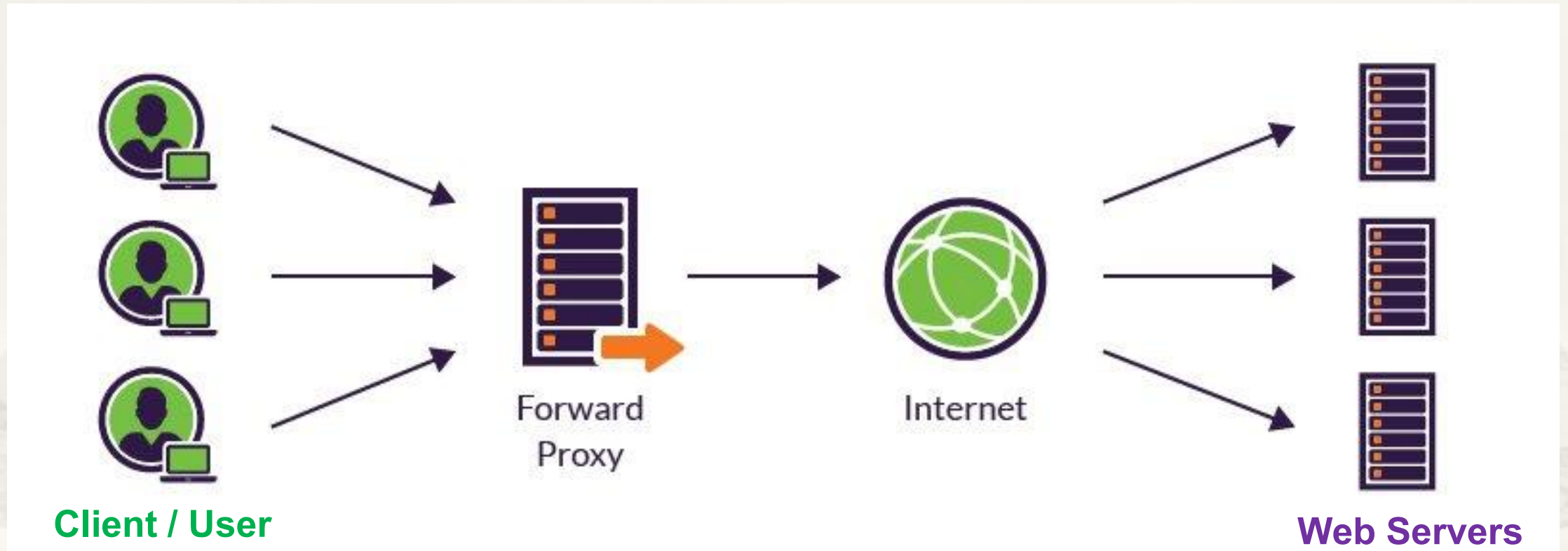
davisyou@ntu.edu.tw
02-33665008

大綱

- * Reverse Proxy 運作原理
 - * Forward Proxy vs. Reverse Proxy
- * L7/L4 Revers Proxy、Dst/Src NAT 運作原理與差異比較

Forward Proxy

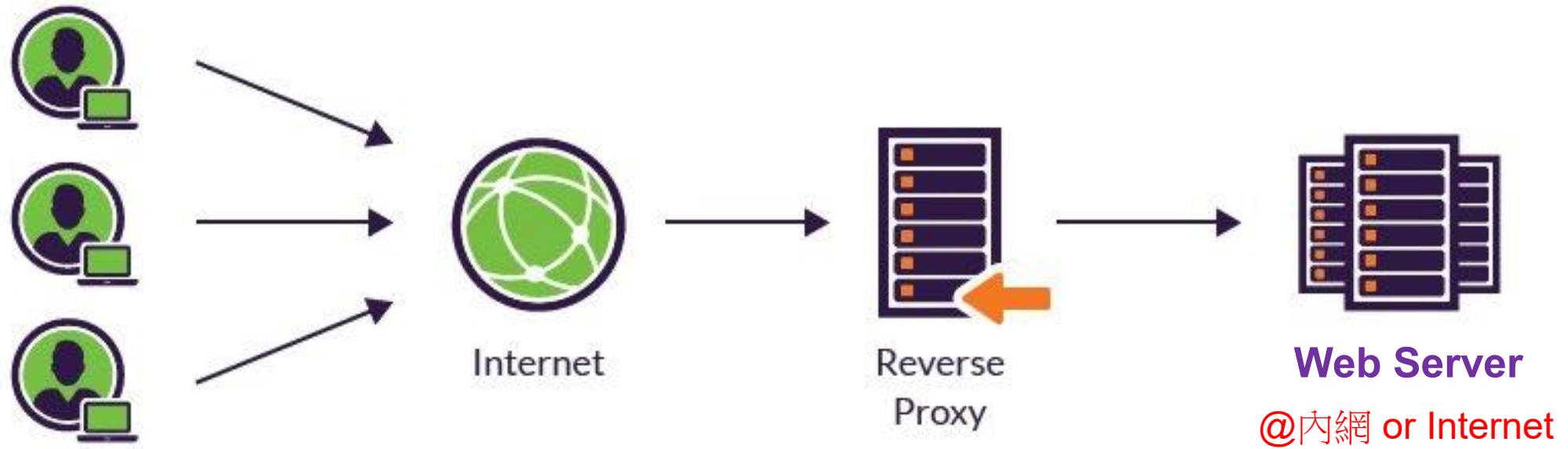
正向代理



<https://www.imperva.com/learn/performance/reverse-proxy>

Reverse Proxy

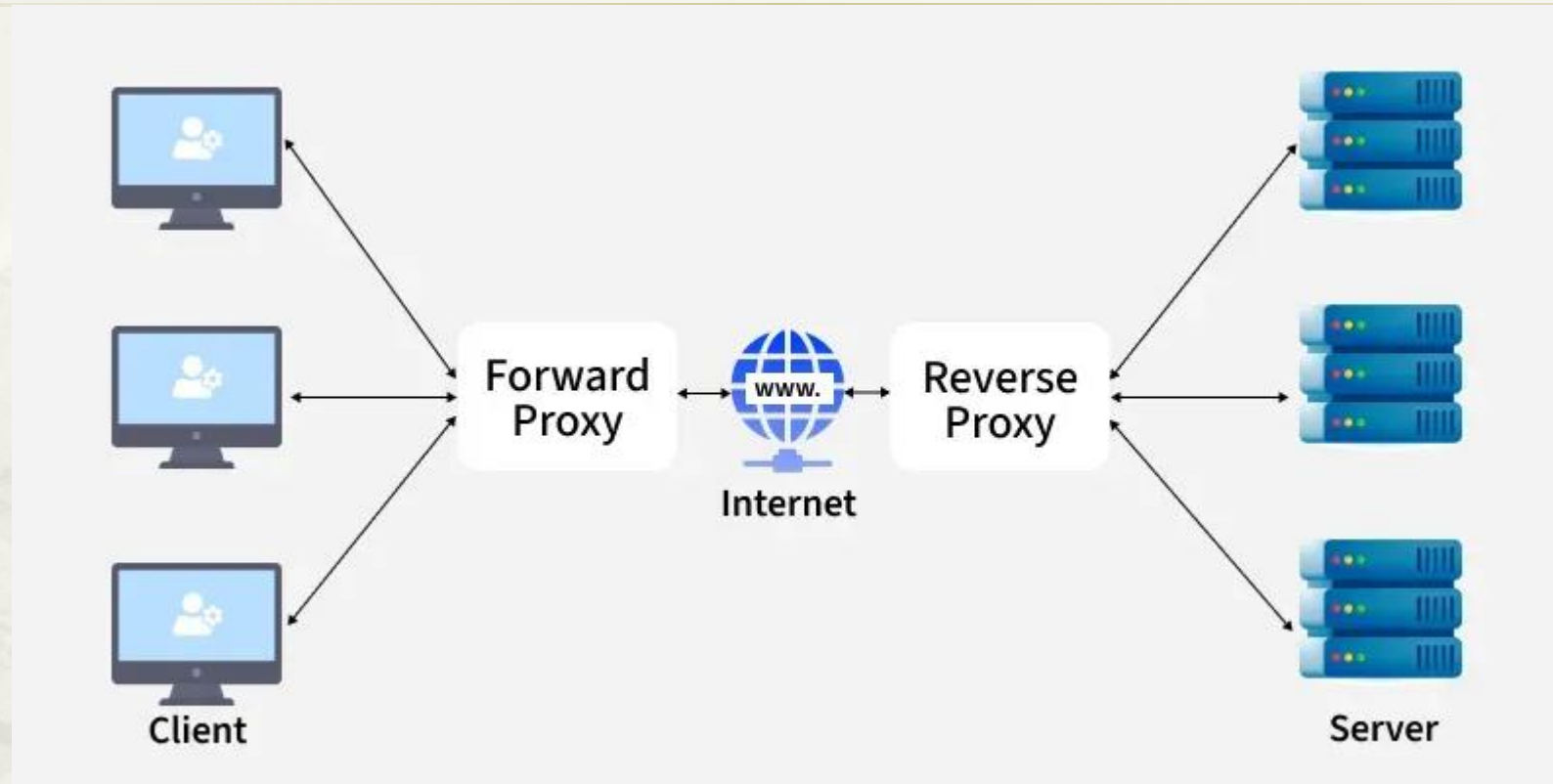
反向代理



Client / User

<https://www.imperva.com/learn/performance/reverse-proxy>

Forward Proxy vs. Reverse Proxy



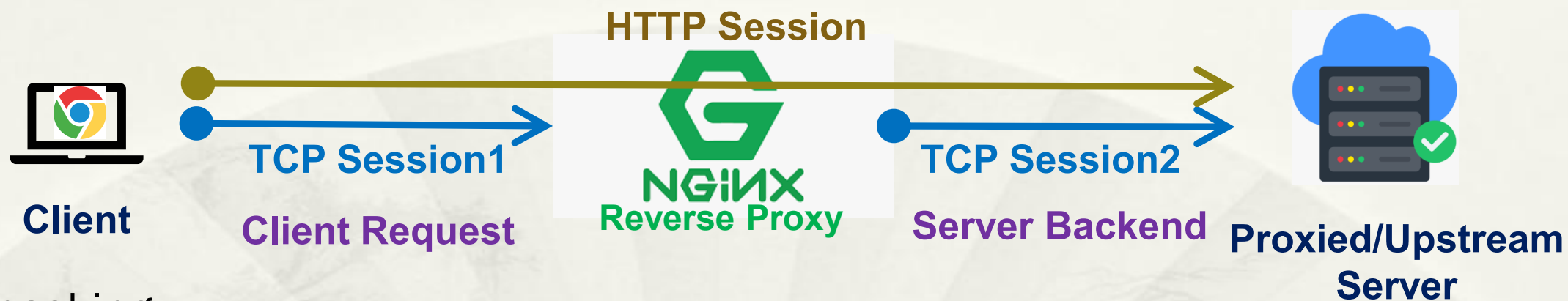
- * <https://www.geeksforgeeks.org/system-design/difference-between-forward-proxy-and-reverse-proxy/>

L7 Reverse Proxy



- * Server/OS 軟體與版本隱藏
 - * 隱藏 Server/OS 弱點與漏洞
 - * Intercept "Client Request" & "Server Backend Reply"
- * SSL Termination: Terminate HTTPS traffic from clients
 - * Relieving Web Server Load of SSL/TLS encryption
 - * 快速導入 HTTPS 加密協定: Support Let's Encrypt 免費憑證 (Certbot)
- * 快取服務 (Content Caching)
 - * Cache both static and dynamic content from web and application servers
- * WAF(Web Application Firewall) 部署

L4 Reverse Proxy



- * IP masking
 - * IPv6 to IPv4
 - * Server IP 隱藏
 - * Zero Trust 架構: 阻擋木馬 C2
 - * Bypass Origin Server IP ACL Control
- * 流量清洗 (Traffic Scrubbing)
 - * DDoS mitigation
- * 負載平衡 (Load Balancing)

Destination NAT/Port Mapping



Destination NAT/Port Mapping 封包檔

* 1 TCP Session: 僅變更 Dst IP/Port

* DNAT_HTTP_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	126	140.112.2.215	4679	140.112.3.82	8080	TCP	66	4679 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
2	0.000160	0	63	140.112.3.82	8080	140.112.2.215	4679	TCP	66	8080 → 4679 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000765	0	126	140.112.2.215	4679	140.112.3.82	8080	TCP	60	4679 → 8080 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4	0.012915	0	126	140.112.2.215	4679	140.112.3.82	8080	HTTP	618	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.013011	0	63	140.112.3.82	8080	140.112.2.215	4679	TCP	54	8080 → 4679 [ACK] Seq=1 Ack=565 Win=64128 Len=0
6	0.013257	0	63	140.112.3.82	8080	140.112.2.215	4679	HTTP	235	HTTP/1.1 304 Not Modified
7	0.217562	0	126	140.112.2.215	4679	140.112.3.82	8080	TCP	60	4679 → 8080 [ACK] Seq=565 Ack=182 Win=66048 Len=0

相同

不同

* DNAT_HTTP_2_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	125	140.112.2.215	4679	172.16.0.7	80	TCP	66	4679 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=960 WS=
2	0.000118	0	64	172.16.0.7	80	140.112.2.215	4679	TCP	66	80 → 4679 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000742	0	125	140.112.2.215	4679	172.16.0.7	80	TCP	54	4679 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4	0.012892	0	125	140.112.2.215	4679	172.16.0.7	80	HTTP	618	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.012973	0	64	172.16.0.7	80	140.112.2.215	4679	TCP	60	80 → 4679 [ACK] Seq=1 Ack=565 Win=64128 Len=0
6	0.013218	0	64	172.16.0.7	80	140.112.2.215	4679	HTTP	235	HTTP/1.1 304 Not Modified
7	0.217538	0	125	140.112.2.215	4679	172.16.0.7	80	TCP	54	4679 → 80 [ACK] Seq=565 Ack=182 Win=66048 Len=0

Source NAT/Outbound NAT



Source NAT/Outbound NAT

* 1 TCP Session: 僅變更 Src IP/Port

* SNAT_RDP_1_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	128	172.16.0.17	59493	120.96.0.222	3389	TCP	66	59493 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
2	0.000816	0	124	120.96.0.222	3389	172.16.0.17	59493	TCP	66	3389 → 59493 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0
3	0.002090	0	128	172.16.0.17	59493	120.96.0.222	3389	TCP	60	59493 → 3389 [ACK] Seq=1 Ack=1 Win=262912 Len=0
4	1.931637	0	128	172.16.0.17	59493	120.96.0.222	3389	TCP	60	59493 → 3389 [FIN, ACK] Seq=1 Ack=1 Win=262912 Len=0
5	1.932199	0	124	120.96.0.222	3389	172.16.0.17	59493	TCP	54	3389 → 59493 [ACK] Seq=1 Ack=2 Win=64000 Len=0

不同

相同

* SNAT_RDP_2_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	127	140.112.3.82	59671	120.96.0.222	3389	TCP	66	59671 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=960 WS=
2	0.000783	0	125	120.96.0.222	3389	140.112.3.82	59671	TCP	66	3389 → 59671 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0
3	0.002072	0	127	140.112.3.82	59671	120.96.0.222	3389	TCP	54	59671 → 3389 [ACK] Seq=1 Ack=1 Win=262912 Len=0
4	1.931621	0	127	140.112.3.82	59671	120.96.0.222	3389	TCP	54	59671 → 3389 [FIN, ACK] Seq=1 Ack=1 Win=262912 Len=0
5	1.932166	0	125	120.96.0.222	3389	140.112.3.82	59671	TCP	60	3389 → 59671 [ACK] Seq=1 Ack=2 Win=64000 Len=0

L7/L4 Revers Proxy 、Dst/Src NAT

運作原理比較

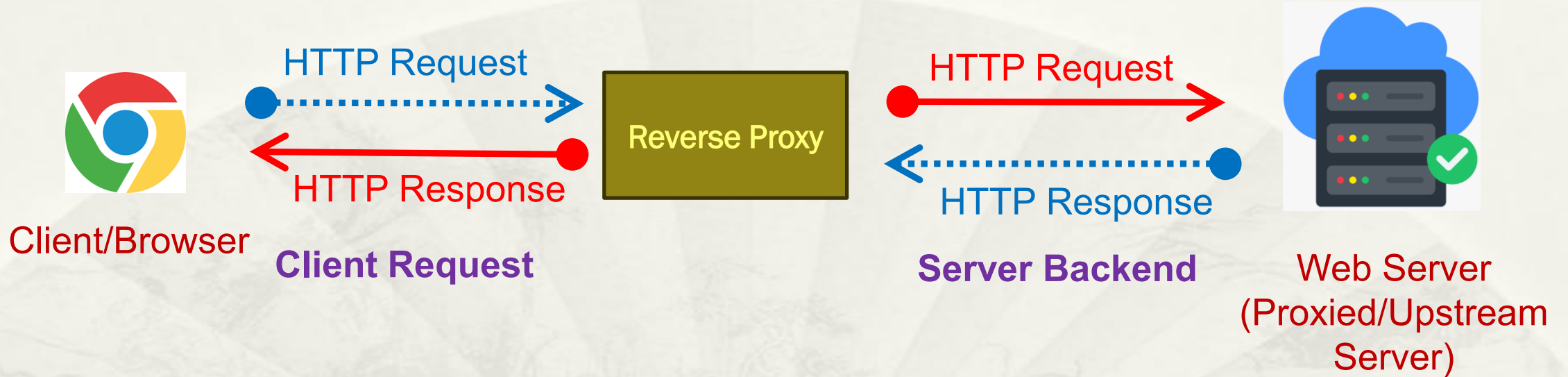
	Payload (L7 Protocol)	TCP Sessions (L4 Protocol)	Web Server 連線對象	Virtual Host/URL 、 Content Cache 、 WAF 、 Web Server/OS Hiding	Protocol Support
L7 Revers Proxy	不同 (Support Modify HTTP Header 、 Body)	2 (Support IPv6 to IPv4)	NGINX (Zero Trust)	Support	HTTP HTTPs
L4 Revers Proxy	相同	2 (Support IPv6 to IPv4)	NGINX (Zero Trust)	N/A	TCP UDP
Dest NAT/ Port Mapping	N/A	1	Client	N/A	All
Src NAT	N/A	1	N/A	N/A	All

L7/L4 Revers Proxy 、Dst/Src NAT 運作原理比較

	Initial Pkt Changed (L3)	Reply Pkt Changed (L3)
L7 Revers Proxy (Load Balance)	Src IP: Client -> Proxy Dst IP: Proxy -> Server	Src IP: Server -> Proxy Dst IP: Proxy -> Client
L4 Revers Proxy (Load Balance)	Src IP: Client -> Proxy Dst IP: Proxy -> Server	Src IP: Server -> Proxy Dst IP: Proxy -> Client
Dest NAT (Port Mapping)	Dst IP: Firewall -> Server	Src IP: Server -> Firewall
Src NAT	Src IP: Client -> Firewall	Dst IP: Firewall -> Client

L7 Reverse Proxy

可修改 HTTP Request/Response





L7 Revers Proxy 運作原理

大綱

- * L7 Revers Proxy HTTP to HTTP
- * HTTP Request Header 變數傳遞
- * L7 Revers Proxy 運作過程

L7 Revers Proxy HTTP to HTTP

L7 Reverse Proxy

HTTP to HTTP



使用者連線:

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

```
* /etc/nginx/sites-enabled/L7_proxy01.conf
server {
    listen 80;
    server_name proxy01.buda.idv.tw; #Virtual Host
    location / {
        proxy_pass http://172.16.0.7;
    }
}
```

L7 Reverse Proxy

封包檔

* 2 TCP Sessions: 兩個獨立 Session, 無關連.

* L7_HTTP_ReverseProxy1_1_WAN.pcap: 尚未 FIN 結束

No.	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	124	120.96.0.222	37460	140.112.237.5	80	TCP	66	37460 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
2	0.000020	64	140.112.237.5	80	120.96.0.222	37460	TCP	66	80 → 37460 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS
3	0.000865	124	120.96.0.222	37460	140.112.237.5	80	TCP	60	37460 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
4	0.001365	124	120.96.0.222	37460	140.112.237.5	80	HTTP	507	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.001377	64	140.112.237.5	80	120.96.0.222	37460	TCP	54	80 → 37460 [ACK] Seq=1 Ack=454 Win=64128 Len=0
6	0.004795	64	140.112.237.5	80	120.96.0.222	37460	HTTP	3636	HTTP/1.1 200 OK (PNG)
7	0.005768	124	120.96.0.222	37460	140.112.237.5	80	TCP	60	37460 → 80 [ACK] Seq=454 Ack=2921 Win=2102272 Len=0
8	0.054937	124	120.96.0.222	37460	140.112.237.5	80	TCP	60	37460 → 80 [ACK] Seq=454 Ack=3583 Win=2101504 Len=0

* L7_HTTP_ReverseProxy1_2_LAN.pcap: FIN 結束

No.	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	64	172.16.0.226	35112	172.16.0.7	80	TCP	74	35112 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
2	0.000072	64	172.16.0.7	80	172.16.0.226	35112	TCP	74	80 → 35112 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
3	0.000079	64	172.16.0.226	35112	172.16.0.7	80	TCP	66	35112 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
4	0.000117	64	172.16.0.226	35112	172.16.0.7	80	HTTP	507	GET /icons/ubuntu-logo.png HTTP/1.0
5	0.000154	64	172.16.0.7	80	172.16.0.226	35112	TCP	66	80 → 35112 [ACK] Seq=1 Ack=442 Win=64768 Len=0 TSv
6	0.003173	64	172.16.0.7	80	172.16.0.226	35112	HTTP	3653	HTTP/1.1 200 OK (PNG)
7	0.003180	64	172.16.0.226	35112	172.16.0.7	80	TCP	66	35112 → 80 [ACK] Seq=442 Ack=3588 Win=62336 Len=0
8	0.003227	64	172.16.0.7	80	172.16.0.226	35112	TCP	66	80 → 35112 [FIN, ACK] Seq=3588 Ack=442 Win=64768
9	0.003304	64	172.16.0.226	35112	172.16.0.7	80	TCP	66	35112 → 80 [FIN, ACK] Seq=442 Ack=3589 Win=64128
10	0.003324	64	172.16.0.7	80	172.16.0.226	35112	TCP	66	80 → 35112 [ACK] Seq=3589 Ack=443 Win=64768 Len=0

L7 Reverse Proxy Payload(L7) 不同

L7_HTTP_ReverseProxy1_1_WAN.pcap

L7_HTTP_ReverseProxy1_2_LAN.pcap

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L7_HTTP_ReverseProxy1_1_WAN.pcap

HTTP Request Header
Different Host
Different Connection

```
GET /icons/ubuntu-logo.png HTTP/1.1
Host: demo1.buda.idv.tw
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/116.0.0.0 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
Different Server
Different Connection

```
HTTP/1.1 200 OK
Server: nginx/1.24.0
Date: Sat, 26 Aug 2023 07:14:12 GMT
Content-Type: image/png
Content-Length: 3338
Connection: keep-alive
Last-Modified: Wed, 08 Mar 2023 17:32:54 GMT
ETag: "d0a-5f666eb0abd80"
Accept-Ranges: bytes
```

HTTP Body

```
.PNG
.
...
IHDR...w...c.....~.....IDATx..].t.H..1.Z.....<....03...t.O.#.VG.
{ : ln + n VV7 n 1 b 16 m 69 N ci E +: R? +
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L7_HTTP_ReverseProxy1_2_LAN.pcap

```
GET /icons/ubuntu-logo.png HTTP/1.0
Host: 172.16.0.7
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 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/1.1 200 OK
Date: Sat, 26 Aug 2023 07:14:12 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
Connection: close
Content-Type: image/png
```

```
.PNG
.
...
IHDR...w...c.....~.....IDATx..].t.H..1.Z.....<....03...t.O.#.VG.
{ : ln + n VV7 n 1 b 16 m 69 N ci E +: R? +
```

L7 Reverse Proxy

Identify technologies on websites

- * Hiding Original Web Server/OS
 - * 可隱藏原 Web Server or OS 弱點與漏洞

Wappalyzer 原始網站

技術 更多資訊

安全性 [HSTS](#)

程式語言 [PHP](#)

網頁伺服器 [Apache HTTP Server](#) 2.2.15

作業系統 [CentOS](#)

The screenshot shows the Wappalyzer interface for a website. The technology stack is displayed in a grid. The '網頁伺服器' (Web Server) and '作業系統' (Operating System) sections are highlighted with a red box, indicating the original server and OS information that can be hidden.

Wappalyzer L7 Reverse Proxy

技術 更多資訊

安全性 [HSTS](#)

程式語言 [PHP](#)

網頁伺服器 [Nginx](#) 1.22.1

反向代理伺服器 [Nginx](#) 1.22.1

The screenshot shows the Wappalyzer interface for a website configured with an L7 Reverse Proxy. The technology stack is displayed in a grid. The '網頁伺服器' (Web Server) and '反向代理伺服器' (Reverse Proxy Server) sections are highlighted with a red box, indicating the proxy server information that is used to hide the original server and OS.

HTTP Redirect vs. L7 ReversProxy

- * HTTP Redirect: Restart a New TCP Session
- * L7 ReversProxy: 維持原 TCP Session

L7 Reverse Proxy

HTTP to HTTP

HTTP Request Header 變數傳遞

L7 Reverse Proxy

HTTP to HTTP



使用者連線:

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

```
* /etc/nginx/sites-enabled/L7_proxy01.conf
server {
    listen 80;
    server_name proxy01.buda.idv.tw;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    location / {
        proxy_pass http://172.16.0.7;
    }
}
```

L7_HTTP_ReverseProxy2_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	59741	140.112.237.5	80	TCP	66	59741 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
2	0.000058	0	64	140.112.237.5	80	120.96.0.222	59741	TCP	66	80 → 59741 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.001031	0	125	120.96.0.222	59741	140.112.237.5	80	TCP	60	59741 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	0.002895	0	125	120.96.0.222	59741	140.112.237.5	80	HTTP	619	<u>GET /icons/ubuntu-logo.png HTTP/1.1</u>
5	0.002910	0	64	140.112.237.5	80	120.96.0.222	59741	TCP	54	80 → 59741 [ACK] Seq=1 Ack=566 Win=64128 Len=0
6	0.003704	0	64	140.112.237.5	80	120.96.0.222	59741	HTTP	193	HTTP/1.1 304 Not Modified
7	0.059254	0	125	120.96.0.222	59741	140.112.237.5	80	TCP	60	59741 → 80 [ACK] Seq=566 Ack=140 Win=262656 Len=0

> Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)

> Ethernet II, Src: Cisco_f8:21:08 (8c:94:1f:f8:21:08), Dst: VMWare_f9:ad:9b (00:0c:29:f9:ad:9b)

> Internet Protocol Version 4, Src: 120.96.0.222, Dst: 140.112.237.5

> Transmission Control Protocol, Src Port: 59741, Dst Port: 80, Seq: 1, Ack: 1, Len: 565

✓ Hypertext Transfer Protocol

> GET /icons/ubuntu-logo.png HTTP/1.1\r\n

Host: demo1.buda.idv.tw\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n

L7_HTTP_ReverseProxy2_2_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	74	58050 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
2	0.000097	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	74	80 → 58050 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460
3	0.000114	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1000000
4	0.000142	0	64	172.16.0.226	58050	172.16.0.7	80	HTTP	675	GET /icons/ubuntu-logo.png HTTP/1.0
5	0.000190	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	66	80 → 58050 [ACK] Seq=1 Ack=610 Win=64640 Len=0 TSval=1000000
6	0.000646	0	64	172.16.0.7	80	172.16.0.226	58050	HTTP	210	HTTP/1.1 304 Not Modified
7	0.000648	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [ACK] Seq=610 Ack=145 Win=64128 Len=0 TSval=1000000
8	0.000699	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [FIN, ACK] Seq=610 Ack=145 Win=64128 Len=0 TSval=1000000
9	0.000708	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	66	80 → 58050 [FIN, ACK] Seq=145 Ack=610 Win=64640 Len=0 TSval=1000000
10	0.000716	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [ACK] Seq=611 Ack=146 Win=64128 Len=0 TSval=1000000
11	0.000738	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	66	80 → 58050 [ACK] Seq=146 Ack=611 Win=64640 Len=0 TSval=1000000

<

- > Frame 4: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits)
- > Ethernet II, Src: VMware_f9:ad:91 (00:0c:29:f9:ad:91), Dst: VMware_6d:b4:41 (00:0c:29:6d:b4:41)
- > Internet Protocol Version 4, Src: 172.16.0.226, Dst: 172.16.0.7
- > Transmission Control Protocol, Src Port: 58050, Dst Port: 80, Seq: 1, Ack: 1, Len: 609

▼ Hypertext Transfer Protocol

> GET /icons/ubuntu-logo.png HTTP/1.0\r\n

X-Real-IP: 120.96.0.222\r\n

X-Forwarded-For: 120.96.0.222\r\n

多了兩個 HTTP Header

Host: 172.16.0.7\r\n

Connection: close\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n

L7 Reverse Proxy

HTTP to HTTP

L7_HTTP_ReverseProxy2_1_WAN.pcap

L7_HTTP_ReverseProxy2_2_LAN.pcap

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L7_HTTP_ReverseProxy2_1_WAN.pcap

HTTP Request Header

```
GET /icons/ubuntu-logo.png HTTP/1.1
Host: demo1.buda.idv.tw
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9
If-None-Match: "d0a-5e1686a0341c0"
If-Modified-Since: Tue, 14 Jun 2022 13:30:55 GMT
```

HTTP Response Header

```
HTTP/1.1 304 Not Modified
Server: nginx/1.22.0
Date: Fri, 30 Sep 2022 07:27:19 GMT
Connection: keep-alive
ETag: "d0a-5e1686a0341c0"
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · L7_HTTP_ReverseProxy2_2_LAN.pcap

```
GET /icons/ubuntu-logo.png HTTP/1.0
X-Real-IP: 120.96.0.222
X-Forwarded-For: 120.96.0.222
Host: 172.16.0.7
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9
If-None-Match: "d0a-5e1686a0341c0"
If-Modified-Since: Tue, 14 Jun 2022 13:30:55 GMT
```

```
HTTP/1.1 304 Not Modified
Date: Fri, 30 Sep 2022 07:27:19 GMT
Server: Apache/2.4.41 (Ubuntu)
Connection: close
ETag: "d0a-5e1686a0341c0"
```



L7 Revers Proxy 運作過程

Reverse Proxy 運作過程

- * Step1. 人工下載

- * Browser URL Input or Click HyperLink
- * Browser request html file to Reverse Proxy
 - * `http://proxy01.buda.idv.tw/index.html`

- * Step2. Browser 自動下載

- * 2.1. Browser 解析 html 檔案內之超連結
 - * 相對或絕對路徑: 加上 FQDN of Reverse Proxy (`proxy01.buda.idv.tw`)
 - * Absolute URL: 維持不變更
- * 2.2. Browser request 上述超連結
 - * URL 必須是 `proxy01.buda.idv.tw` 才會經過 Reverse Proxy

Mixed Contents

- * URL: http://
 - * 超連結: 允許 http:// 及 "有合法憑證之 https://"
- * URL: https://
 - * 超連結: 僅允許 "有合法憑證之 https://"

NGINX Config File

```
/etc/nginx/sites-enabled/L7_proxy01.conf
```

```
server {  
    listen 80;  
    server_name proxy01.buda.idv.tw;  
    location / {  
        proxy_pass http://apache.buda.idv.tw;  
    }  
}
```

Reverse Proxy 運作過程

mixed01.html

Local Disk

<P>

http://127.0.0.1/

<P>

http://asoc52.cc.ntu.edu.tw

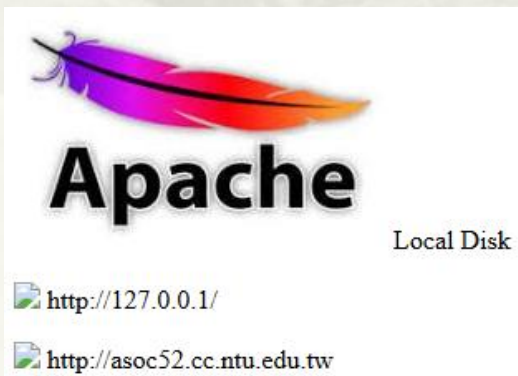
Testing 1

* <http://proxy01.buda.idv.tw/mixed/mixed01.html>



Name	Met...	Status	Sche...	Domain	Remote address
mixed01.html	GET	200	http	proxy01.buda.idv.tw	140.112.237.6:80
local.png	GET	200	http	proxy01.buda.idv.tw	140.112.237.6:80
http_127.0.0.1.png	GET	(failed) net::ERR_CONNECTION_REFUSED	http	127.0.0.1	
mrtg_title.jpg	GET	200	http	asoc52.cc.ntu.edu.tw	163.28.16.52:80

* <https://proxy01.buda.idv.tw/mixed/mixed01.html>



Name	Met...	Status	Sche...	Domain	Remote address
mixed01.html	GET	200	https	proxy01.buda.idv.tw	140.112.237.6:443
local.png	GET	200	https	proxy01.buda.idv.tw	140.112.237.6:443
http_127.0.0.1.png	GET	(failed) net::ERR_CONNECTION_REFUSED	http	127.0.0.1	
mrtg_title.jpg	GET	(failed) net::ERR_CONNECTION_REFUSED	https	asoc52.cc.ntu.edu.tw	

Reverse Proxy 運作過程

mixed02.html

http://apache.buda.idv.tw/

<P>

https://apache.buda.idv.tw/

<P>

http://163.28.16.43/

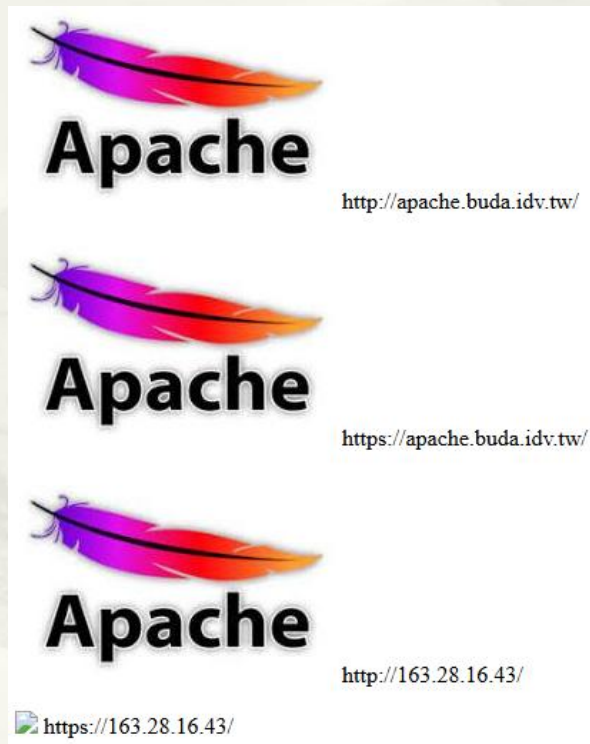
<P>

https://163.28.16.43/

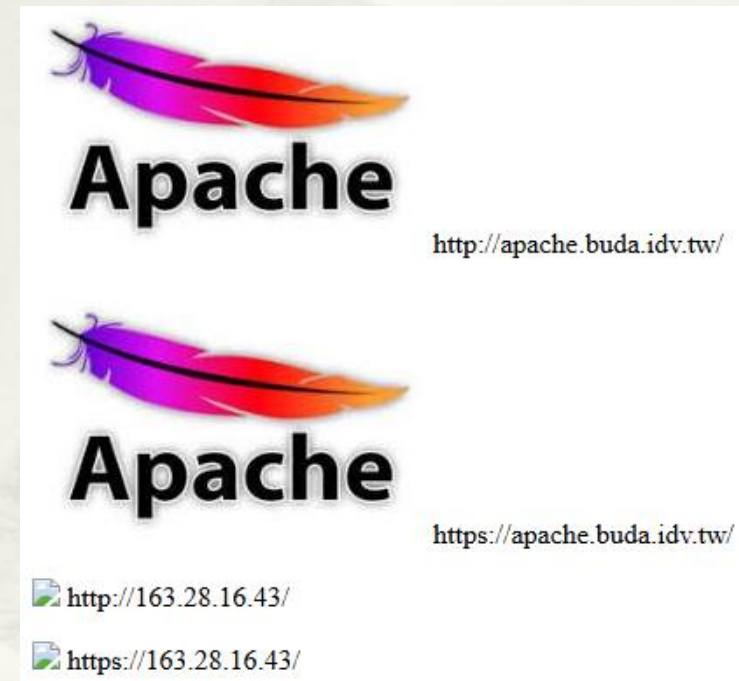
<P>

Testing 2

http://proxy01.buda.idv.tw/mixed/mixed02.html



https://proxy01.buda.idv.tw/mixed/mixed02.html



Name	Method	Status	Scheme	Domain	Remote address
mixed02.html	GET	200	http	proxy01.buda.idv.tw	140.112.237.6:80
http_apache.png	GET	200	http	apache.buda.idv.tw	163.28.16.43:80
https_apache.png	GET	200	https	apache.buda.idv.tw	163.28.16.43:443
http_163.28.16.43.png	GET	200	http	163.28.16.43	163.28.16.43:80
https_163.28.16.43.png	GET	(failed) net::ERR_CERT_COMMON_NAME_INVALID	https	163.28.16.43	

Name	Method	Status	Scheme	Domain	Remote address
mixed02.html	GET	200	https	proxy01.buda.idv.tw	140.112.237.6:443
http_apache.png	GET	200	https	apache.buda.idv.tw	163.28.16.43:443
https_apache.png	GET	200	https	apache.buda.idv.tw	163.28.16.43:443
https_163.28.16.43.png	GET	(failed) net::ERR_CERT_COMMON_NAME_INVALID	https	163.28.16.43	
http_163.28.16.43.png	GET	(blocked:mixed-content)	http	163.28.16.43	

Reverse Proxy 運作過程

mixed03.html

http://proxy01.buda.idv.tw/

<P>

https://proxy01.buda.idv.tw/

<P>

http://140.112.237.6/

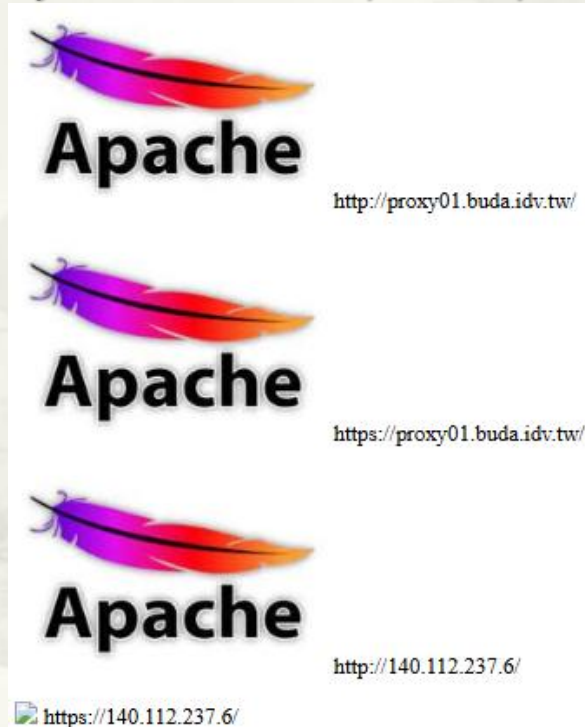
<P>

https://140.112.237.6/

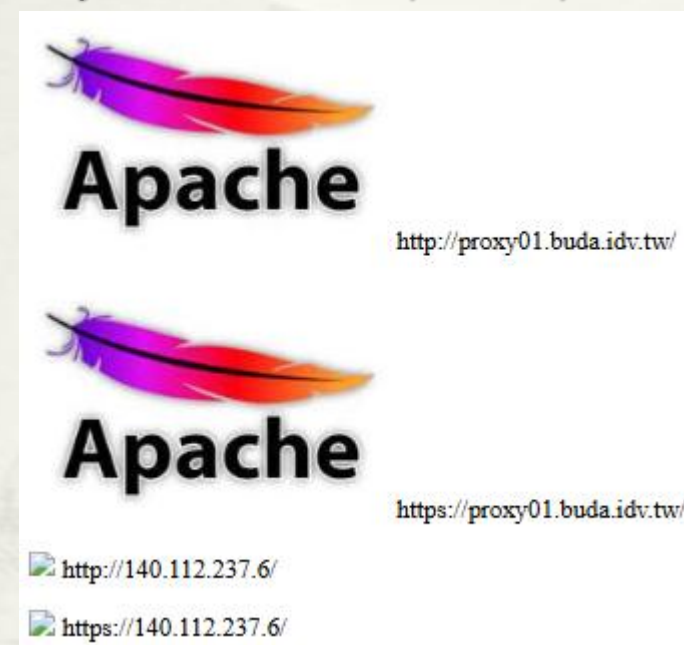
<P>

Testing 3

http://proxy01.buda.idv.tw/mixed/mixed03.html



https://proxy01.buda.idv.tw/mixed/mixed03.html



Name	Method	Status	Scheme	Domain	Remote address
mixed03.html	GET	200	http	proxy01.buda.idv.tw	140.112.237.6:80
http_proxy01.png	GET	200	http	proxy01.buda.idv.tw	140.112.237.6:80
https_proxy01.png	GET	200	https	proxy01.buda.idv.tw	140.112.237.6:443
http_140.112.237.6.png	GET	200	http	140.112.237.6	140.112.237.6:80
https_140.112.237.6.png	GET	(failed) net::ERR_CERT_COMMON_NAME_INVALID	https	140.112.237.6	

Name	Method	Status	Scheme	Domain	Remote address
mixed03.html	GET	200	https	proxy01.buda.idv.tw	140.112.237.6:443
http_proxy01.png	GET	200	https	proxy01.buda.idv.tw	140.112.237.6:443
https_proxy01.png	GET	200	https	proxy01.buda.idv.tw	140.112.237.6:443
https_140.112.237.6.png	GET	(failed) net::ERR_CERT_COMMON_NAME_INVALID	https	140.112.237.6	
http_140.112.237.6.png	GET	(blocked:mixed-content)	http	140.112.237.6	

Reverse Proxy 運作方式

經過 Reverse Proxy

- * 相對或絕對路徑連結
 - * `` 無路徑
 - * `` 相對路徑
 - * `<script src="/script/valid.js"></script>` 絕對路徑
- * Absolute URL with FQDN of Reverse Proxy
 - * ``
 - * `<script src="http://apache.buda.idv.tw/valid.js"></script>`
- * Absolute URL with IP of Reverse Proxy
 - * ``
 - * `<script src="http://140.112.237.6/valid.js"></script>`

不經過 Reverse Proxy

- * Absolute URL with FQDN of 本機
 - * ``
 - * `<script src="http://apache.buda.idv.tw/valid.js"></script>`
- * Absolute URL with IP of 本機
 - * ``
 - * `<script src="http://163.28.16.43/valid.js"></script>`
- * Absolute URL with FQDN of Others
 - * ``
 - * `<script src="http://www.other.com/valid.js"></script>`
- * 不提供代理 Cookie 功能
 - * Cookie will Forward to Browser(End User).

解決方法

將 **Absolute URL with FDQN** of 本機

- * 更換成 絕對路徑
 - * `sub_filter 'http://apache.buda.idv.tw/' '/';`
 - * `sub_filter_once off;`
- * 更換成 "FQDN of Rever Proxy"
 - * `sub_filter 'http://apache.buda.idv.tw/' 'http://proxy01.buda.idv.tw/';`
 - * `sub_filter_once off;`



簡報完畢
謝謝