

# NGINX Reverse Proxy Web Server @ 外網

---

臺大計資中心網路組  
游子興

davisyou@ntu.edu.tw  
02-33665008

# 大綱

- \* L7 Reverse Proxy HTTPs to HTTP
  - \* 無法導入 Reverse Proxy, 強制 Redirect to https 原網站
  - \* 導入 HTTPs 後網頁無法正常顯示
- \* L7 Reverse Proxy HTTPs to HTTPs
  - \* Backend Server Server Name Indication(SNI) Support
  - \* Change URI

# L7 Reverse Proxy HTTPS to HTTP

無法導入 Reverse Proxy  
強制 Redirect to 原網站

---

# 無法導入 Reverse Proxy 強制 Redirect to 原網站

\* 連線 <https://proxy01.buda.idv.tw> 卻發生 Redirect to https 原網站

\* /etc/nginx/sites-enabled/L7\_proxy01.conf

```
server {  
    listen 443 ssl;  
    location / {  
        proxy_pass http://www.ntu.edu.tw;  
    }
```

# Redirect to 原網站

- \* 發生原因: <http://www.ntu.edu.tw> redirect to <https://www.ntu.edu.tw>

| Name                  | × | Headers           | Preview                      | Response                        | Initiator | Timing |
|-----------------------|---|-------------------|------------------------------|---------------------------------|-----------|--------|
| proxy01.buda.idv.tw   | ▼ | General           |                              |                                 |           |        |
| www.ntu.edu.tw        |   | Request URL       |                              | https://proxy01.buda.idv.tw/    |           |        |
| AvPK_JA-9SU?mute=1... |   | Request Method    |                              | GET                             |           |        |
| IdKpz0WYScA?mute=...  |   | Status Code       |                              | ● 302 Object Moved              |           |        |
|                       |   | Remote Address    |                              | 140.112.237.5:443               |           |        |
|                       |   | Referrer Policy   |                              | strict-origin-when-cross-origin |           |        |
|                       | ▼ | Response headers  | <input type="checkbox"/> Raw |                                 |           |        |
|                       |   | Cache-Control     |                              | private                         |           |        |
|                       |   | Connection        |                              | keep-alive                      |           |        |
|                       |   | Content-Type      |                              | text/html                       |           |        |
|                       |   | Date              |                              | Tue, 04 Aug 2026 07:21:25 GMT   |           |        |
|                       |   | Location          |                              | https://www.ntu.edu.tw/         |           |        |
|                       |   | Server            |                              | nginx/1.28.3 (Ubuntu)           |           |        |
|                       |   | Transfer-Encoding |                              | chunked                         |           |        |

# L7 Reverse Proxy HTTPS to HTTP 導入 HTTPS 後網頁無法正常顯示

台大分子生醫影像研究中心

<http://mic.ntu.edu.tw/>

# 台大分子生醫影像研究中心

<http://mic.ntu.edu.tw/>

\* 不支援 https:// 加密連線



# L7 Reverse Proxy HTTPs to HTTP



使用者連線:

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

```
* /etc/nginx/sites-enabled/L7_proxy01.conf
server {
    listen 443 ssl;
    server_name proxy01.buda.idv.tw; #Virtual Host
    ssl_certificate /etc/letsencrypt/live/proxy01.buda.idv.tw/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/proxy01.buda.idv.tw/privkey.pem;
    location / {
        proxy_pass http://mic.ntu.edu.tw;
    }
}
```

# 導入 HTTPS 後網頁無法正常顯示

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

### Chrome: 格式異常



### F12: 錯誤訊息 blocked:mixed-content

| Name                         | Method | Status                  | Scheme | Domain             |
|------------------------------|--------|-------------------------|--------|--------------------|
| bootstrap.min.css            | GET    | (blocked:mixed-content) | http   | www.mic.ntu.edu.tw |
| bootstrap-responsive.min.css | GET    | (blocked:mixed-content) | http   | www.mic.ntu.edu.tw |
| font-awesome.css             | GET    | (blocked:mixed-content) | http   | www.mic.ntu.edu.tw |
| mobile-menu.css              | GET    | (blocked:mixed-content) | http   | www.mic.ntu.edu.tw |
| template.css                 | GET    | (blocked:mixed-content) | http   | www.mic.ntu.edu.tw |
| preset1.css                  | GET    | (blocked:mixed-content) | http   | www.mic.ntu.edu.tw |

# 分析

## 網頁 Source Code

\* HTML 檔案含本站或其他網站 HTTP 連結，觸發 **mixed-content 阻擋規則**：

- \* 使用 `https://` 連線網站時，網站頁面有部分圖片或連結，使用未加密 `http://` 連結

```
<head>
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <base href="http://mic.ntu.edu.tw/tw/" />
  <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  <meta name="keywords" content="分子生醫影像、醫學影像、光學影像、分子工程、正子分子影像、磁振影像、紅外線影像、超音波影
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <meta name="description" content="國立臺灣大學分子生醫影像研究中心致力於整合分子生醫影像相關研究、教學工作，推動跨領域
  <meta name="generator" content="Joomla! - Open Source Content Management" />
  <title>國立臺灣大學分子生醫影像研究中心</title>
  <link href="/tw/?format=feed&type=rss" rel="alternate" type="application/rss+xml" title="RSS 2.0" />
  <link href="/tw/?format=feed&type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0" />
  <link href="http://mic.ntu.edu.tw/tw/" rel="alternate" hreflang="zh-TW" />
  <link href="http://mic.ntu.edu.tw/en/" rel="alternate" hreflang="en-GB" />
  <link href="http://mic.ntu.edu.tw/tw/component/search/?Itemid=122&format=opensearch" rel="search" title="搜
  <link href="/images/mic-favicon.png" rel="shortcut icon" type="image/vnd.microsoft.icon" />
```

# L7 Reverse Proxy (HTTPs 無法正常顯示)

## 解決方法 1

- \* Add Response Header to Client Browser.

```
server {  
    add_header Content-Security-Policy "upgrade-insecure-requests";  
}
```

- \* 恢復正常

The screenshot shows a web browser with the URL `proxy01.buda.idv.tw/tw/`. The page displays the logo and name of the National Taiwan University Molecular Imaging Research Center (MIC). The browser's developer tools are open, showing the 'Headers' tab. The 'Response headers' section is expanded, and the 'Content-Security-Policy' header is highlighted with a red box, showing the value 'upgrade-insecure-requests'. The website content includes the MIC logo and navigation links: 中心簡介, 最新消息, 核心實驗室, and 人員介紹.

| Name                    | Value                                |
|-------------------------|--------------------------------------|
| tw/                     |                                      |
| ezset.js                |                                      |
| ezset-custom.js         |                                      |
| jquery.min.js           |                                      |
| jquery-noconflict.js    |                                      |
| jquery-migrate.min.js   |                                      |
| jquery-noconflict.js    |                                      |
| bootstrap.min.js        |                                      |
| modernizr-2.6.2.min.js  |                                      |
| Cache-Control           | no-store, no-cache, must-revalidate, |
| Connection              | keep-alive                           |
| Content-Encoding        | gzip                                 |
| Content-Length          | 10042                                |
| Content-Security-Policy | upgrade-insecure-requests            |
| Content-Type            | text/html; charset=utf-8             |

# L7 Reverse Proxy (HTTPs 無法正常顯示)

## 解決方法 2

- \* Modify Response Header/Body by replacing string.

```
proxy_set_header Accept-Encoding ""; # Force server to return plain text
sub_filter_once off; # Replace repeatedly.
sub_filter "http://mic.ntu.edu.tw/" "/";
}
```

- \* 恢復正常

```
<head>
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <base href="/tw/" />
  <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  <meta name="keywords" content="分子生醫影像、醫學影像、光學影像、分子工程、正子分子影像、磁振影像、
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <meta name="description" content="國立臺灣大學分子生醫影像研究中心致力於整合分子生醫影像相關研究、
  <meta name="generator" content="Joomla! - Open Source Content Management" />
  <title>國立臺灣大學分子生醫影像研究中心</title>
  <link href="/tw/?format=feed&type=rss" rel="alternate" type="application/rss+xml" title="
  <link href="/tw/?format=feed&type=atom" rel="alternate" type="application/atom+xml" title="
  <link href="/tw/" rel="alternate" hreflang="zh-TW" />
  <link href="/en/" rel="alternate" hreflang="en-GB" />
  <link href="/tw/component/search/?Itemid=122&format=opensearch" rel="search" title="搜尋
  <link href="/images/mic-favicon.png" rel="shortcut icon" type="image/vnd.microsoft.icon" />
```

# **L7 Reverse Proxy HTTPS to HTTPs**

---

Backend Server

Server Name Indication(SNI) Support

# Backend Server

## Server Name Indication(SNI) Support

---

\* /etc/nginx/sites-enabled/L7\_proxy01.conf

```
server {  
    listen 443 ssl;  
    server_name proxy01.buda.idv.tw;  
    location / {  
        proxy_pass https://www.ntu.edu.tw;  
    }  
}
```

# Backend Server

## Server Name Indication(SNI) Support

\* 連線失敗?

**502 Bad Gateway**

nginx/1.24.0

\* L7\_HTTP\_ReverseProxy\_ww  
.tw\_Error.pcap

| Time       | TTL | Source        | Src Port | Destination   | Dest Port | Protocol | Length | Info                                                    |
|------------|-----|---------------|----------|---------------|-----------|----------|--------|---------------------------------------------------------|
| 1 0.000000 | 64  | 140.112.237.5 | 34556    | 140.112.8.116 | 443       | TCP      | 74     | 34556 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P |
| 2 0.000086 | 254 | 140.112.8.116 | 443      | 140.112.237.5 | 34556     | TCP      | 66     | 443 → 34556 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1 |
| 3 0.000093 | 64  | 140.112.237.5 | 34556    | 140.112.8.116 | 443       | TCP      | 54     | 34556 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0           |
| 4 0.000442 | 64  | 140.112.237.5 | 34556    | 140.112.8.116 | 443       | TLSv1.2  | 347    | Client Hello                                            |
| 5 0.000575 | 254 | 140.112.8.116 | 443      | 140.112.237.5 | 34556     | TLSv1.2  | 61     | Alert (Level: Fatal, Description: Handshake Failure)    |
| 6 0.000585 | 64  | 140.112.237.5 | 34556    | 140.112.8.116 | 443       | TCP      | 54     | 34556 → 443 [ACK] Seq=294 Ack=8 Win=64256 Len=0         |
| 7 0.000593 | 254 | 140.112.8.116 | 443      | 140.112.237.5 | 34556     | TCP      | 60     | 443 → 34556 [RST, ACK] Seq=8 Ack=294 Win=2511616 Len=0  |

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 288

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 284

Version: TLS 1.2 (0x0303)

> Random: f0952374e849cd31ae88e142c18343130c3e3d6e6ed3e51bbfe81d2d3bb97491

Session ID Length: 32

Session ID: 8b8881320953c44bad3df8410634b43e0f7aff32762963d4cf6301bb5d3fa9e8

Cipher Suites Length: 62

> Cipher Suites (31 suites)

Compression Methods Length: 1

> Compression Methods (1 method)

Extensions Length: 149

> Extension: ec\_point\_formats (len=4)

> Extension: supported\_groups (len=22)

> Extension: session\_ticket (len=0)

> Extension: encrypt\_then\_mac (len=0)

> Extension: extended\_master\_secret (len=0)

> Extension: signature\_algorithms (len=42)

> Extension: supported\_versions (len=5)

> Extension: psk\_key\_exchange\_modes (len=2)

> Extension: key\_share (len=38)

[JA3 Fullstring: 771,4866-4867-4865-49196-49200-159-52393-52392-52394-49195-49199-158-49188-49192-107-49187-49191-103-49162-

[JA3: c216e752cae6f8755fd27f561d031636]

原因:

Client Hello 少了 Server Name Indication(SNI)

# TLS Server Name Indication(SNI)

- \* https 連線方式，在 TCP 連線建立後就立即進入 SSL 交涉階段，然後才由 Browser 送出 HTTP Request 封包
- \* 若網站有使用虛擬主機 Virtual Host 功能(多個網站共用同一個 IP)，HTTP Request 標頭之 "HOST 欄位"，卻是在已經建立 SSL連線之後才能知道，導致無法知道該使用哪一張 "SSL 憑證"進行加密。
- \* 因此 SNI 要解決的問題，就是 Server 不知道要給哪一張 certificate 的問題。

# Backend Server

## Server Name Indication(SNI) Support

設定 /etc/nginx/sites-enabled/ L7\_proxy01.conf

```
server {  
    proxy_ssl_server_name on;  
}
```

| No.  | Time     | TTL | Source        | Src Port | Destination   | Dest Port | Protocol | Length | Info         |
|------|----------|-----|---------------|----------|---------------|-----------|----------|--------|--------------|
| 2... | 7.076391 | 64  | 140.112.237.5 | 56178    | 140.112.8.116 | 443       | TLSv1.3  | 370    | Client Hello |

> Frame 254: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits)  
> Ethernet II, Src: VMware\_a6:67:c1 (00:0c:29:a6:67:c1), Dst: Cisco\_f8:21:08 (8c:94:1f:f8:21:08)  
> Internet Protocol Version 4, Src: 140.112.237.5, Dst: 140.112.8.116  
> Transmission Control Protocol, Src Port: 56178, Dst Port: 443, Seq: 1, Ack: 1, Len: 316  
✓ Transport Layer Security

✓ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 311

✓ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 307

Version: TLS 1.2 (0x0303)

Random: 66bf0906be8b13588f79ac0e6be44c9a232a9c3dda94096d2eb85871dd28767f

Session ID Length: 32

Session ID: 676949d8e20e479c729652e87c528be9b6deed2c2059ee1123ef4064cdf49947

Cipher Suites Length: 62

> Cipher Suites (31 suites)

Compression Methods Length: 1

> Compression Methods (1 method)

Extensions Length: 172

> Extension: server\_name (len=19)

> Extension: ec\_point\_formats (len=4)

> Extension: supported\_groups (len=22)

> Extension: session\_ticket (len=0)

> Extension: encrypt\_then\_mac (len=0)

> Extension: extended\_master\_secret (len=0)

> Extension: signature\_algorithms (len=42)

> Extension: supported\_versions (len=5)

> Extension: psk\_key\_exchange\_modes (len=2)

> Extension: key\_share (len=38)

[JA3 Fullstring [truncated]: 771,4866-4867-4865-49196-49200-159-52393-52392-52394-49195-

[JA3: a3afc2c46ba4a7d7fbe1cfb7a3031c2f]

### Server Name Indication(SNI)

✓ Extension: server\_name (len=19)

Type: server\_name (0)

Length: 19

✓ Server Name Indication extension

Server Name list length: 17

Server Name Type: host\_name (0)

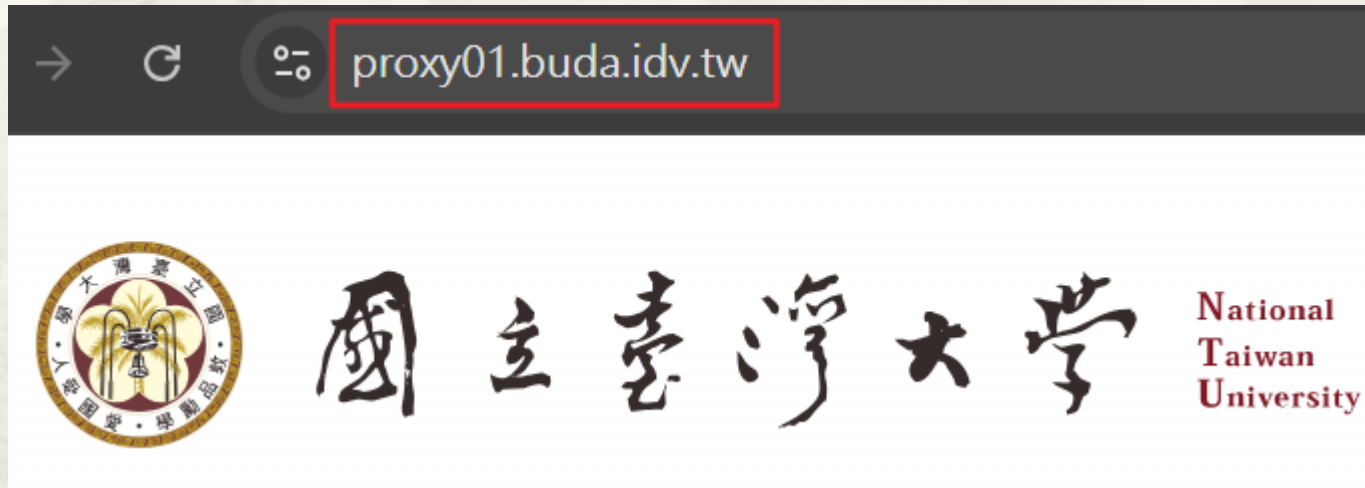
Server Name length: 14

Server Name: www.ntu.edu.tw

# Fake Website

## 台大首頁

- \* 原始: <https://www.ntu.edu.tw>
- \* Fake: <https://proxy01.buda.idv.tw>



# Fake Website

## 台大首頁

- \* Web Server/OS 軟體與版本隱藏
- \* Wappalyzer 偵測



# How to detect Reverse Proxy ?

---

# How to detect Reverse Proxy?

## \* Wappalyzer 服務偵測



Wappalyzer analysis results for [ntu.edu.tw](https://ntu.edu.tw). The interface shows various technologies detected on the page. A red box highlights the '網頁伺服器' (Web Server) section, which lists 'Apache 2.2.9'.

| Category       | Technology       | Version |
|----------------|------------------|---------|
| 分析             | Google Analytics |         |
|                | Open Graph       |         |
| 其他             | Open Graph       |         |
| 網頁伺服器          | Apache           | 2.2.9   |
|                | FreeBSD          |         |
|                | OpenSSL          | 0.9.8e  |
| 網頁伺服器擴充功能      | mod_ssl          | 2.2.9   |
|                | mod_dav          | 2       |
| JavaScript 函式庫 | jQuery           | 1.10.2  |



Wappalyzer analysis results for [demo5.buda.idv.tw](https://demo5.buda.idv.tw). The interface shows various technologies detected on the page. Two red boxes highlight the '反向代理伺服器' (Reverse Proxy) and '網頁伺服器' (Web Server) sections, both listing 'Nginx 1.22.0'.

| Category | Technology       | Version |
|----------|------------------|---------|
| 分析       | Google Analytics |         |
| Security | HSTS             |         |
| 其他       | Open Graph       |         |
| 反向代理伺服器  | Nginx            | 1.22.0  |
|          | jQuery           | 1.10.2  |
| 網頁伺服器    | Nginx            | 1.22.0  |

# How to detect Reverse Proxy ?

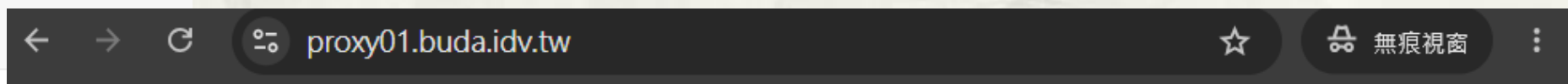
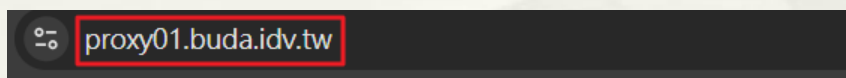
## \* Wappalyzer 服務偵測



# Intercept Client Request GET/POST Info

## OPNsense

- \* 原始: https://172.16.0.1
- \* Fake: https://proxy01.buda.idv.tw



The HTTP\_REFERER "https://proxy01.buda.idv.tw/" does not match the predefined settings. You can disable this check if needed under System: Settings: Administration.



Username:

Password:

Login

# Referer 可用來偵測 Reverse Proxy 環境

## OPNsense

```
GET /mixed/http_127.0.0.1.png HTTP/1.1
Host: proxy01.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/150.0.0.0 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
Referer: http://proxy01.buda.idv.tw/mixed/
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
```

```
HTTP/1.1 200 OK
Server: nginx/1.28.3 (Ubuntu)
Date: Tue, 04 Aug 2026 12:57:46 GMT
Content-Type: image/png
Content-Length: 31478
Connection: keep-alive
Last-Modified: Sat, 01 Aug 2026 10:01:31 GMT
ETag: "7af6-657f963b1c05a"
Accept-Ranges: bytes
```

.PNG

與原來相同

```
GET /mixed/http_127.0.0.1.png HTTP/1.0
X-Real-IP: 140.112.3.82
X-Forwarded-For: 140.112.3.82
Host: apache.buda.idv.tw
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/150.0.0.0 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
Referer: http://proxy01.buda.idv.tw/mixed/
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
```

```
HTTP/1.1 200 OK
Date: Tue, 04 Aug 2026 12:57:46 GMT
Server: Apache/2.4.66 (Ubuntu)
Last-Modified: Sat, 01 Aug 2026 10:01:31 GMT
ETag: "7af6-657f963b1c05a"
Accept-Ranges: bytes
Content-Length: 31478
Connection: close
Content-Type: image/png
```

# How to detect Reverse Proxy ?

---

- \* 學術研究題目:

- \* <https://www.acunetix.com/vulnerabilities/web/reverse-proxy-detected/>
- \* <https://portswigger.net/bappstore/a112997070354d249b64b4cf68eabc04>
- \* <https://www.tenable.com/plugins/nessus/12225>

# **L7 Reverse Proxy**

## **HTTP to HTTPS**

---

Change URI

# 案例 1

- \* FQDN

- \* `https://proxy01.buda.idv.tw`

- \* Backend Server

- \* `https://homepage.ntu.edu.tw/~ntucards/`

- \* NGINX config

```
server {  
    location / {  
        proxy_pass https://homepage.ntu.edu.tw/~ntucards/;  
    }  
}
```

# 案例 2

- \* URL

- \* <https://proxy01.buda.idv.tw/chinese/epaper/home/>

- \* Backend Server

- \* <https://homepage.ntu.edu.tw/~ntuccepaper/home/>

- \* NGINX config

```
server {  
    location /chinese/epaper/home/ {  
        proxy_pass https://homepage.ntu.edu.tw/~ntuccepaper/home/;  
    }  
}
```

# NGINX Config

## location & proxy\_pass

### \* NGINX Config

```
server {  
    location / {  
        proxy_pass https://www.ntu.edu.tw;  
    }  
}
```

### \* proxy\_pass

- \* has no URI: pass original URI (Append Mode)
- \* has URI: replace part of URI (Replacement Mode)

### \* URI 定義

- \* http://172.16.0.7
  - \* URI: 無
- \* http://172.16.0.7/
  - \* URI: /
- \* http://172.16.0.7/cacti
  - \* URI: /cacti

---



簡報完畢  
謝謝