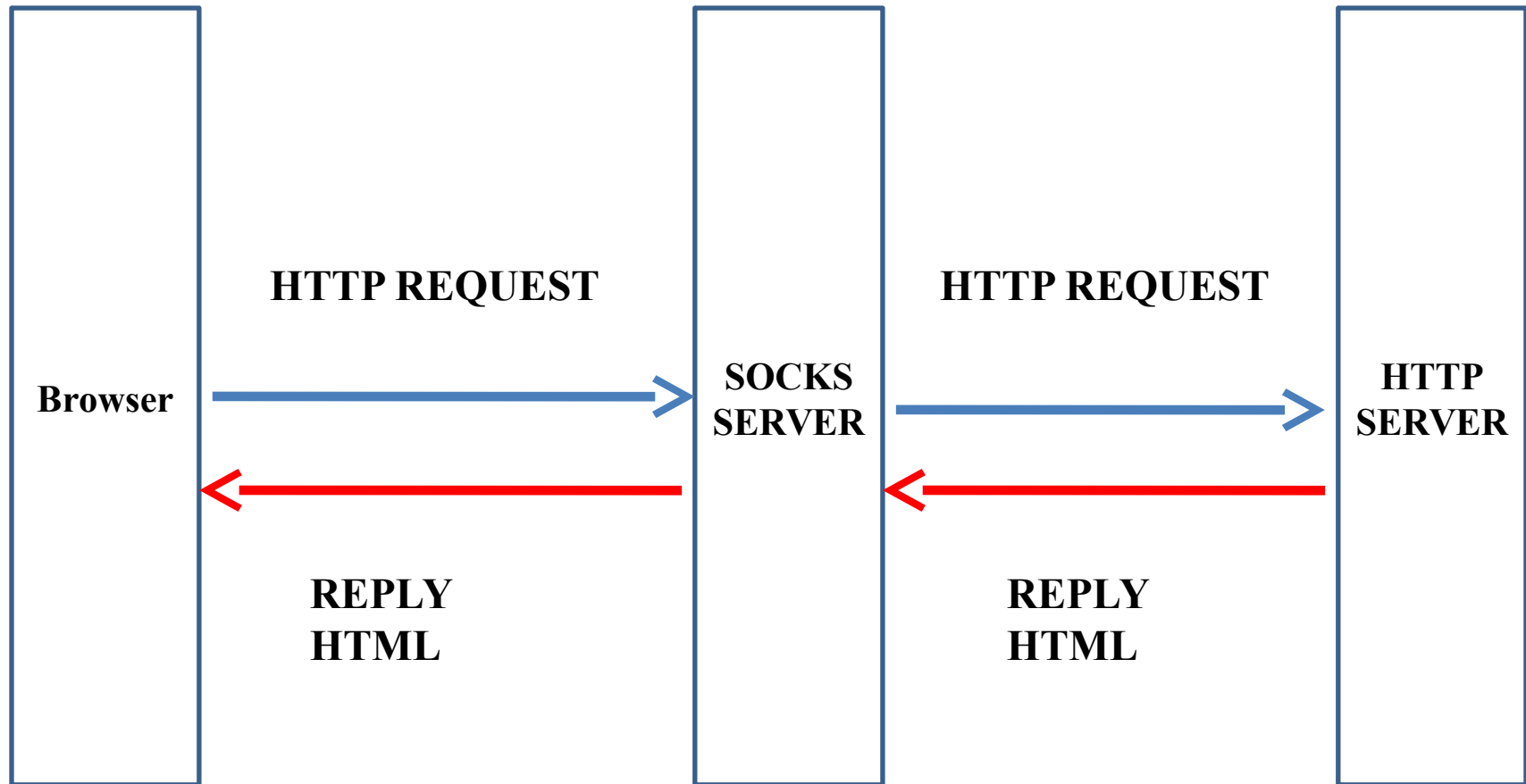


# **Project IV: SOCKS4 Server**

**指導教授：吳毅成**

# Architecture (1/3)



# Architecture (1/3): Browser Setting

設定 使用網路服務時應瞭解的隱私權政策

☐ 自動傳送使用統計資料及當機報告給 Google

☐ 將「不追蹤」要求與瀏覽流量一併送出

密碼和表單

☒ 啟用「自動填入」功能，輕鬆一按即可填妥網路表單。 [管理自動填入設定](#)

☒ 詢問是否儲存我在網站上輸入的密碼。 [管理系统儲存的密碼](#)

網頁內容

字型大小： [自訂字型...](#)

頁面縮放：

網路

Google Chrome 目前透過您電腦系統的 Proxy 設定來連線到網路。

[變更 Proxy 設定...](#)

語言

變更 Chrome 處理和顯示各種語言的方式

[語言和輸入設定...](#)

☒ 翻譯我正在閱讀的網頁。 [管理語言](#)

下載

檔案下載儲存位置： [變更...](#)

☐ 下載每個檔案前先詢問儲存位置

HTTPS/SSL

[管理憑證...](#)

☐ 檢查伺服器憑證的撤銷情況

Google 雲端列印

設定或管理 Google 雲端列印的印表機。 [瞭解詳情](#)

[管理](#)

☐ 在網路上偵測到新印表機時顯示通知

系統

☒ Google Chrome 關閉時繼續執行背景應用程式

網路網路 - 內容

一般 安全性 隱私權 內容 連線 程式 進階

要設定網路連線，請按 [安裝]。

安裝(U)

撥號及虛擬私人網路設定值

新增(D)...

新增 VPN(F)...

移除(R)...

設定(S)

如果您設定連線時必須設定 proxy 伺服器，請選擇 [設定值]。

☒ 永遠不撥號連線(C)

☐ 網路連線不存在時撥號(W)

☐ 永遠使用預設的連線撥號(O)

目前的預設值：無

讀取預設值(B)

區域網路 (LAN) 設定

區域網路設定不可套用到撥號連線。請選擇上述設定來進行撥號設定。

[區域網路設定\(L\)](#)

確定 取消 套用(A)

區域網路 (LAN) 設定

自動設定

自動設定會取代手動設定。要確保使用自動設定，請停用自動設定。

☒ 自動偵測設定(A)

☐ 使用自動組態指令碼(S)

位址(R)

Proxy 伺服器

☒ 在您的區域網路使用 Proxy 伺服器 (這些設定將不會套用到撥號或 VPN 連線)(X)

位址(B):  連接埠(T):  [進階\(C\)](#)

☐ 近端網址不使用 Proxy 伺服器(B)

確定 取消

Proxy 設定

伺服器

類型	要使用的 Proxy 位址	連接埠
HTTP(H):	<input type="text"/>	<input type="text"/>
Secure(S):	<input type="text"/>	<input type="text"/>
FTP(F):	<input type="text"/>	<input type="text"/>
Socks(C):	<input type="text" value="hpbsd1.cs.nctu.edu.tw"/>	<input type="text" value="5566"/>

☐ 所有通訊協定都使用相同的 Proxy 伺服器(U)

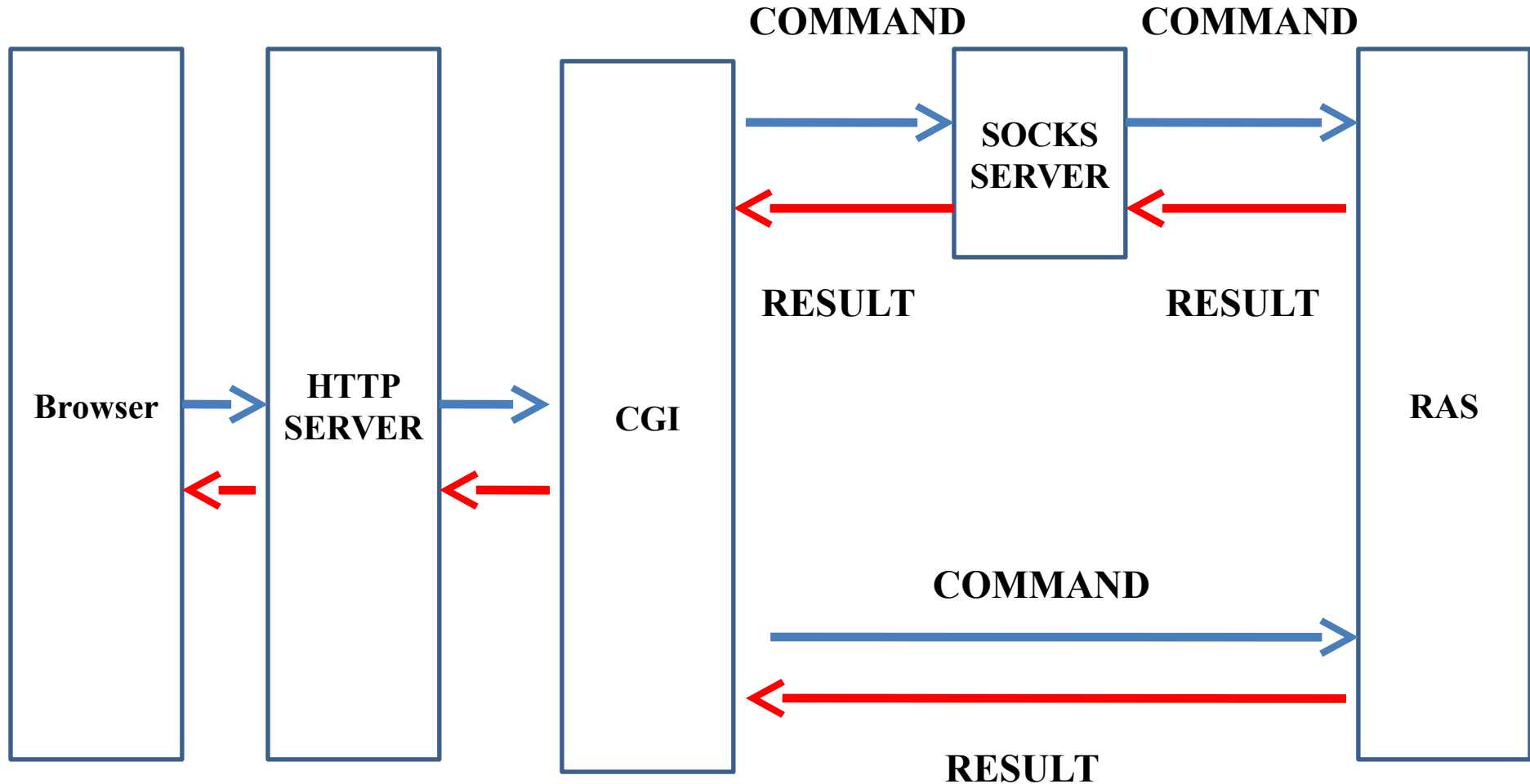
例外

請勿使用下列位址開頭的 Proxy 伺服器(N):

請用分號 (;) 來分隔項目

確定 取消

# Architecture (2/3)



# Architecture (2/3): Demo

Network Programming + x

← → ↻ 🏠 [nplinux3.cs.nctu.edu.tw:2048/form\\_get2.htm](http://nplinux3.cs.nctu.edu.tw:2048/form_get2.htm)

	IP	PORT	Patch File Name
Host1	nplinux3.cs.nctu.edu.tw	10001	t1.txt
Host2	nplinux3.cs.nctu.edu.tw	10001	t2.txt
Host3	nplinux3.cs.nctu.edu.tw	10001	t3.txt
Host4	nplinux3.cs.nctu.edu.tw	10001	t4.txt
Host5	nplinux3.cs.nctu.edu.tw	10001	t5.txt

	IP	PORT
Socks Server1	nplinux3.cs.nctu.edu.tw	10000
Socks Server2	nplinux3.cs.nctu.edu.tw	10000
Socks Server3	nplinux3.cs.nctu.edu.tw	10000
Socks Server4	nplinux3.cs.nctu.edu.tw	10000
Socks Server5	nplinux3.cs.nctu.edu.tw	10000

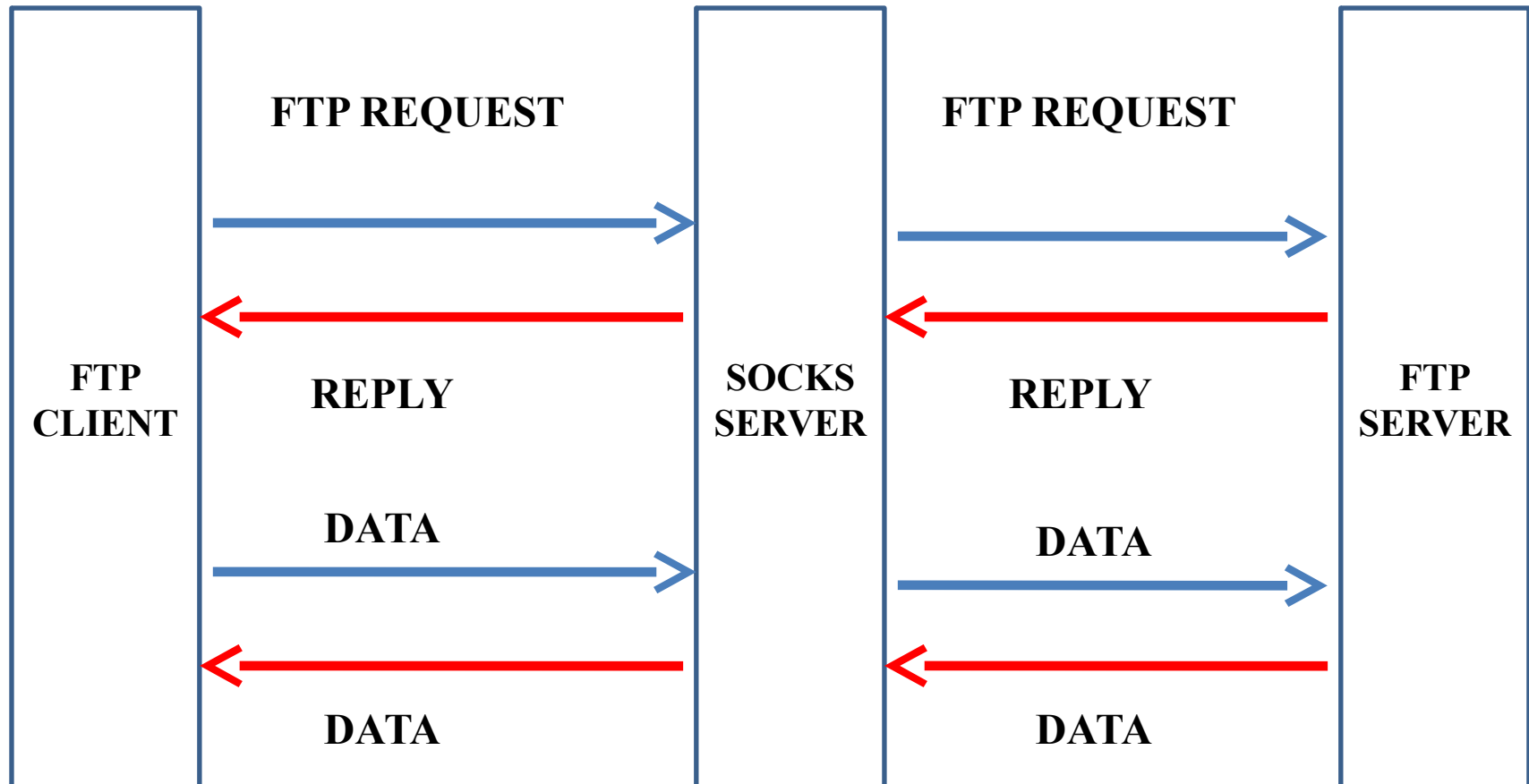
# Architecture (2/3): Demo

```
nplinux3.cs.nctu.edu.tw
*****
** Welcome to the information server. **
*****
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
% printenv PATH
PATH=bin:.
% removetag test.html | cat
*** User from CGILAB/511 is named
user1. ***

nplinux3.cs.nctu.edu.tw
*****
** Welcome to the information server. **
*****
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
% ls -al bin . |2
% removetag test.html |1
*** User from CGILAB/511 is named
'user1'. ***
% number > temp.html
% number temp.html

nplinux3.cs.nctu.edu.tw
*****
** Welcome to the information server. **
*****
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
*** User '(no name)' entered from
CGILAB/511. ***
% removetag0 test.html | number
Error: illegal tag "!test.html"
1
2 Test
3 This is a test program
4 for ras.
5
% removetag0 test.html |1
Error: illegal tag "!test.html"
```

# Architecture (3/3)



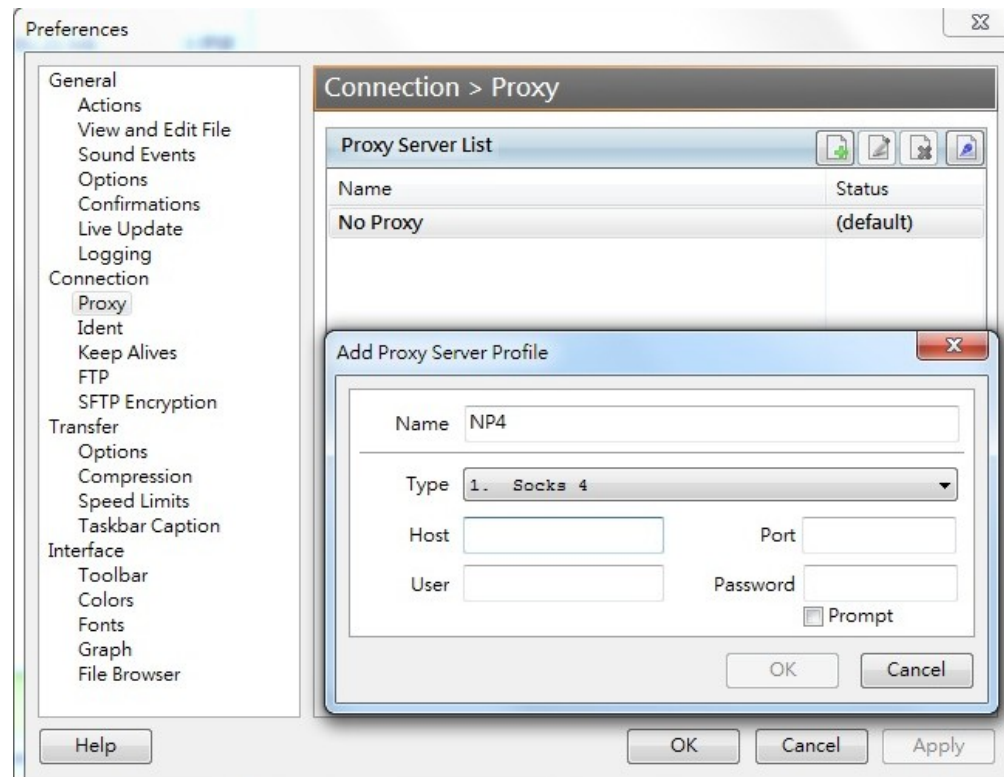
# Architecture (3/3): FlashFXP

- 測試請不要用 FileZilla
- 建議使用 FlashFXP



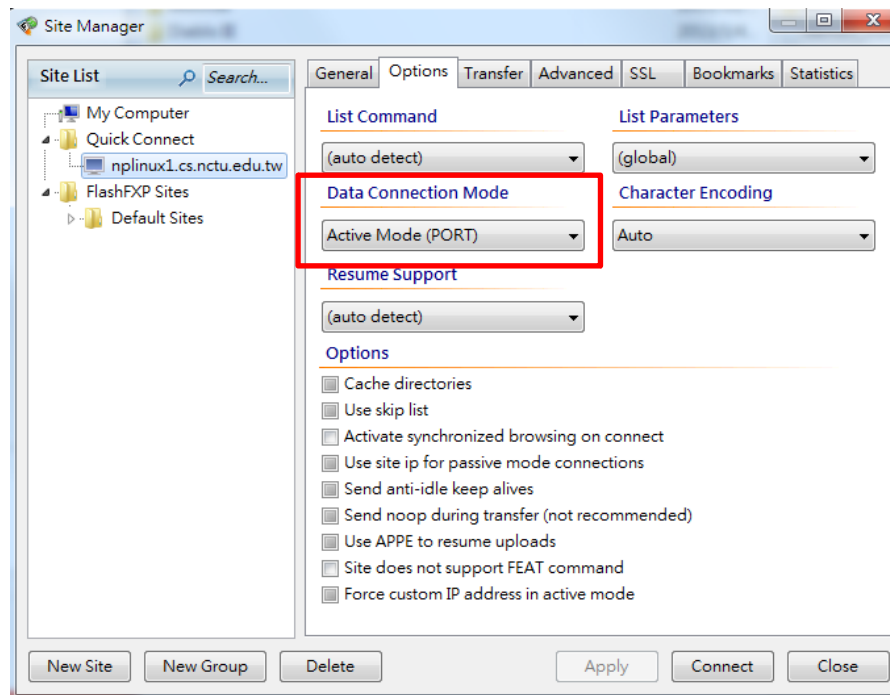
# Architecture (3/3): FlashFXP

- Options □ Preferences □ Connection □ Proxy
  - Add entry
    - Socks4, Host/Port



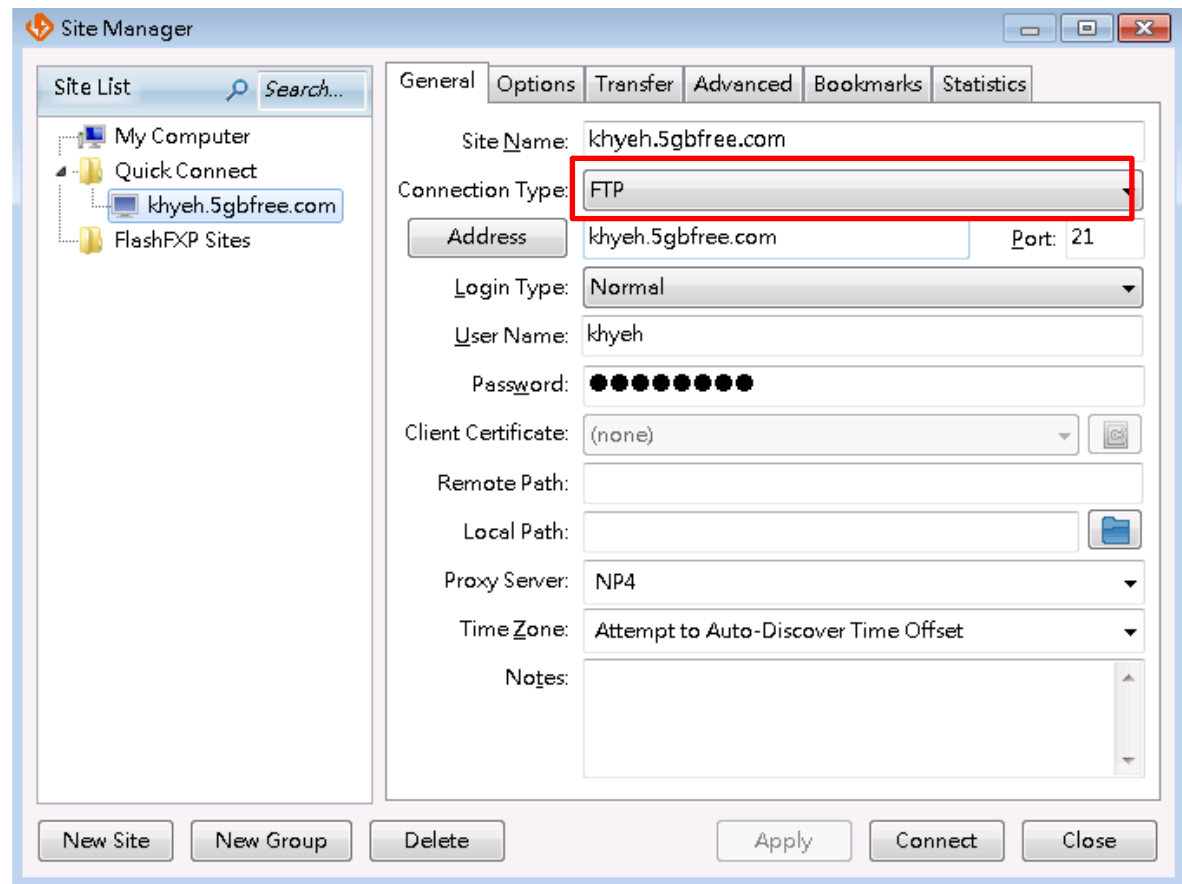
# Architecture (3/3): FlashFXP

- Sites □ Site Manager □ Option □ Data Connection Mode
  - Change to Active Mode(PORT)



# Architecture (3/3): FlashFXP

- Sites □ Site Manager □ General □ Apply
  - Connect



# Architecture (3/3): FlashFXP

- 需要一個 FTP Server 來測試 Bind mode
  - 網路上申請可當 FTP server 上傳 / 下載的空間
    - 可以在 <http://5gbfree.com/> 申請一個 5GB 的空間
      - 假設你申請的帳戶名為 : UserName
        - » Server: <ftp.UserName.5gbfree.com:21>
        - » Account: UserName
  - 或是自行在自己電腦架設 FTP server
    - 可參考 : <http://goo.gl/UjrFwy>
- 整體流程 :
  - 下載 & 設定好 FlashFXP
    - 透過 Socks server 使用 active mode 連線
  - 連線至 FTP server
  - 開始上傳和下載資料

# Implementation

SOCKS4\_REQUEST

VN 4	CD 1 or 2	DST PORT	DST IP	USER ID	NULL
1	1	2	4	variable	1

VN 4	CD 1 or 2	DST PORT	DST IP = 0.0.0.x	USER ID	NULL	Domain Name	NULL
1	1	2	4	variable	1	variable	1

[CD]

1: CONNECT command

2: BIND command

# Implementation

## Request

```
read(sock, buffer, size);  
unsigned char VN = buffer[0] ;  
unsigned char CD = buffer[1] ;  
unsigned int DST_PORT = buffer[2] << 8 |  
                        buffer[3] ;  
unsigned int DST_IP = buffer[4] << 24 |  
                    buffer[5] << 16 |  
                    buffer[6] << 8 |  
                    buffer[7] ;  
char* USER_ID = buffer + 8 ;
```

# Implementation

SOCKS4\_REPLY

VN	CD	DST PORT	DST IP
0	90 or 91		
1	1	2	4

[CD]

90: request granted

91: request rejected or failed

# Implementation

## Reply

```
package[0] = 0;
package[1] = (unsigned char) CD ; // 90 or 91
package[2] = port / 256;
package[3] = port % 256;
package[4] = ip >> 24;
    // ip = ip in SOCKS4_REQUEST for connect mode
    // ip = 0 for bind mode
package[5] = (ip >> 16) & 0xFF;
package[6] = (ip >> 8) & 0xFF;
package[7] = ip & 0xFF;
write(sock, package, 8);
```



# Protocol

- Connect mode
- Bind mode

# Connect mode

SOCKS 4  
CLIENT

SOCKS 4  
SERVER

DEST.  
HOST

`ssock = accept(msock)`

`[ SOCKS4_REQUEST  
(CONNECT, dst.ip, dst.port) ]`

`user_id + NULL`

`if (dst.ip == 0.0.0.x)`

`{`

`domain_name + NULL`

`}`

# Connect mode

CHECK FIREWALL RULESET  
(socks.conf)

```
if (deny_access)
{
    ← SOCKS4_REPLY
    with request rejected: 0x5B
}
```

# Connect mode

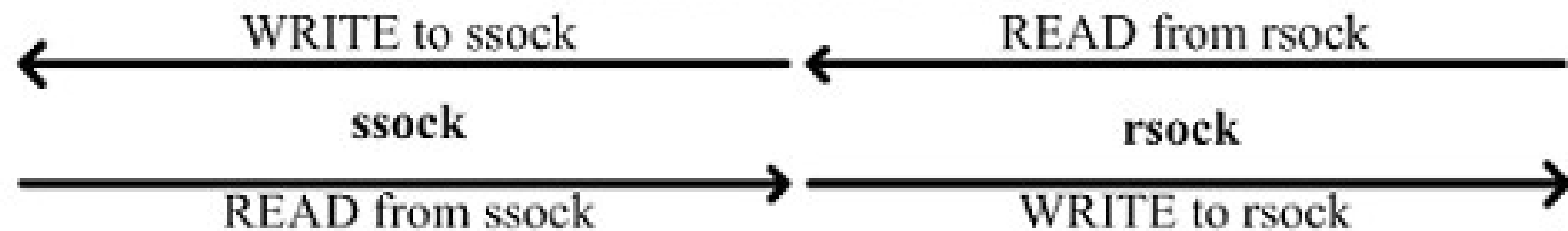
```
else  
{
```

```
    rsock=connectTCP(dst.ip, dst.port)
```

← SOCKS4\_REPLY  
granted: 0x5A, failed: 0x5B

```
    s4_rep.vn = 0x00;  
    s4_rep.cd = (rsock > -1) ? 0x5A : 0x5B;  
    s4_rep.dst_ipv4 = s4_req.dst_ipv4;  
    s4_rep.dst_port = s4_req.dst_port;
```

## REDIRECT SOCKET DATA



# Bind mode

SOCKS 4  
CLIENT

SOCKS 4  
SERVER

DEST.  
HOST

`ssock = accept(msock)`

`SOCKS4_REQUEST`  
`(BIND, dst.ip, dst.port)`

`user_id + NULL`

```
if (dst.ip == 0.0.0.x)
{
```

`domain_name + NULL`

```
}
```

# Bind mode

CHECK FIREWALL RULESET  
(socks.conf)

```
if (deny_access)
{

```

← SOCKS4\_REPLY  
with request rejected: *0x5B*

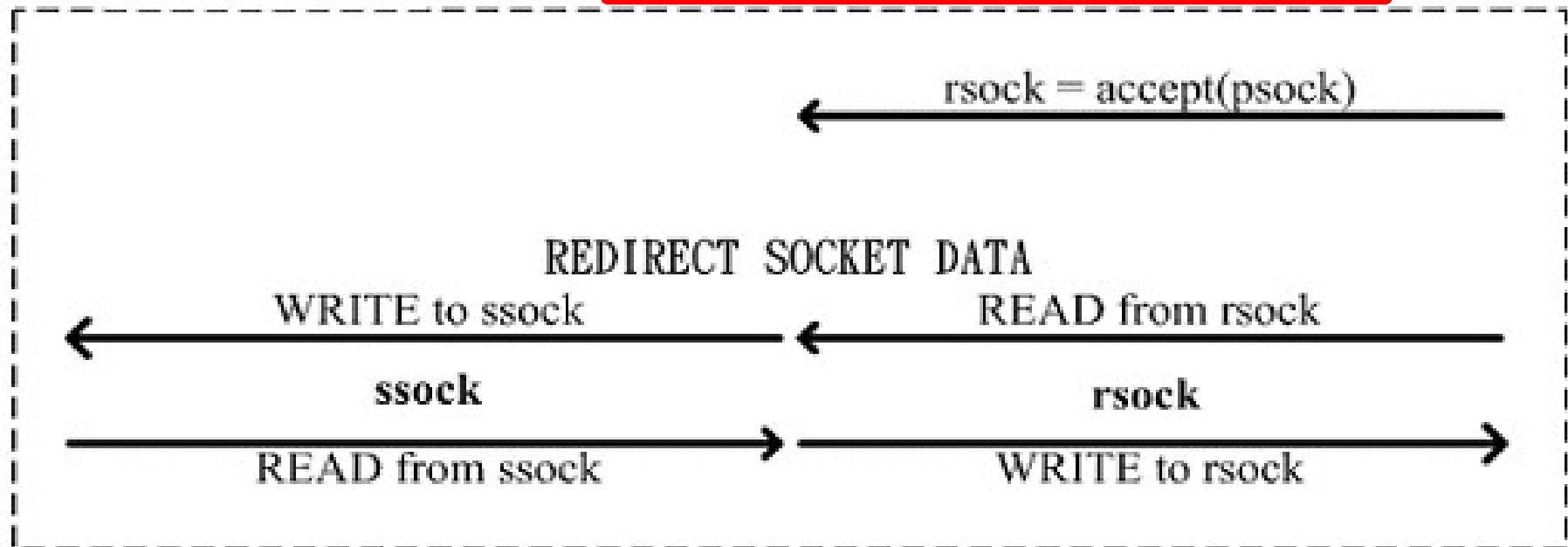
```
}
```

# Bind mode

```
else  
{
```

```
psock=passiveTCP()
```

```
SOCKS4_REPLY  
← granted: 0x5A,  
failed: 0x5B  
s4_rep.vn = 0x00;  
s4_rep.cd = (psock > -1) ? 0x5A : 0x5B;  
s4_rep.dst_ipv4 = 0;  
s4_rep.dst_port = htons(getsockport(psock));
```



```
}
```

**END**