Project4: SOCKS4

NP TA 余玄

1/6 23:55

Project 4 Deadline.

Demo: 1/7 Tue.

Project4 Requirements

I. [20%] SOCKS4 Server **Connect Mode**

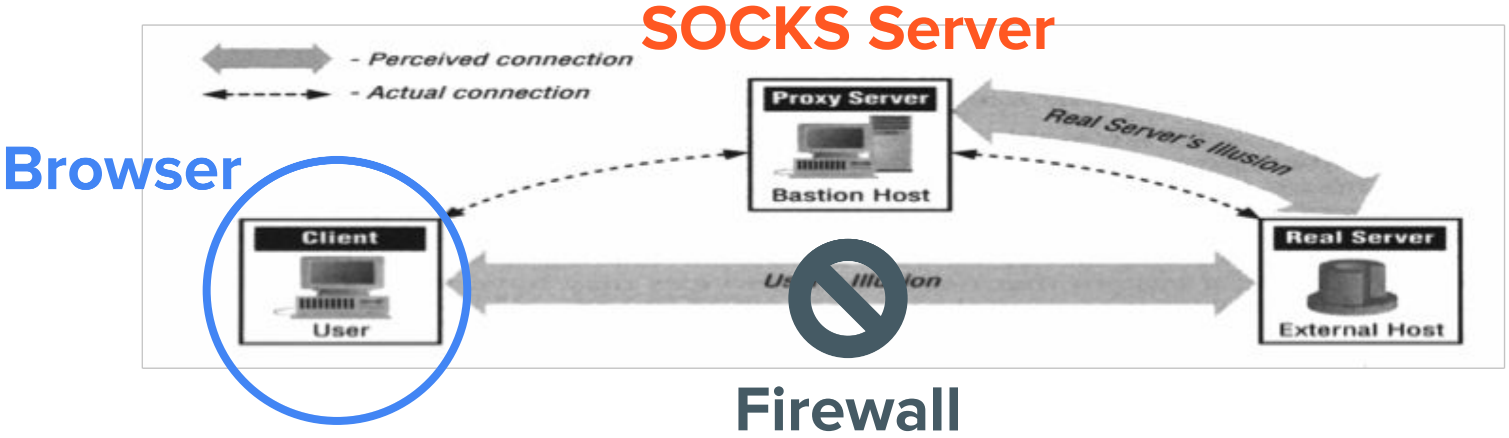
II. [20%] SOCKS4 Server **Bind Mode**

III. [20%] CGI Proxy

IV. [10%] Firewall

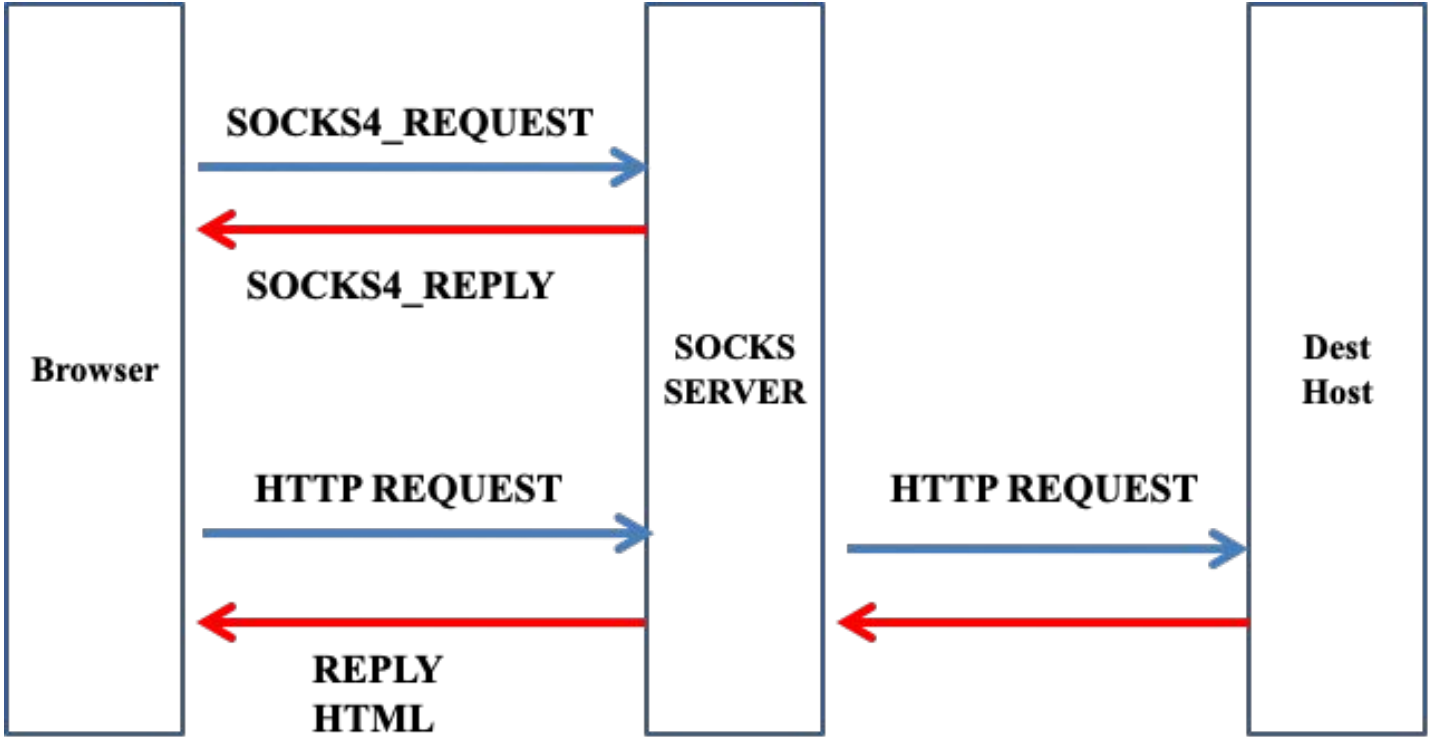
I. Connect Mode

Network Programming Proxying



交通大學資訊工程系吳毅成 第2頁

Connect Mode (HTTP Example)



SOCKS4_REQUEST

```
             +----+----+----+----+----+----+----+----+----+----+....+----+
             | VN | CD | DSTPORT |      DSTIP        | USERID       |NULL|
             +----+----+----+----+----+----+----+----+----+----+....+----+
 # of bytes:    1    1      2              4           variable       1

Example      +----+----+----+----+----+----+----+----+----+----+....+----+
(CONNECT)    |  4 |  1 |  8    0 | 140  113   43   7 |              |  0 |
             +----+----+----+----+----+----+----+----+----+----+....+----+
```

- VN is the SOCKS protocol version number and should be **4**.
- CD is the command code and should be **1** for **CONNECT** request.
- NULL is a byte of all zero bits.

SOCKS4_REQUEST (SOCK 4A)

```
             +----+----+----+----+----+----+----+----+----+----+....+----+----+----+....+----+
             | VN | CD | DSTPORT |      DSTIP        | USERID       |NULL| DOMAIN NAME  |NULL|
             +----+----+----+----+----+----+----+----+----+----+....+----+----+----+....+----+
# of bytes:     1    1      2              4           variable       1      variable       1

Example      +----+----+----+----+----+----+----+----+----+----+....+----+----+----+....+----+
(CONNECT)    |  4 |  1 |  8    0 |  0    0    0    1 |              |  0 | 'w'  'w' ....|  0 |
             +----+----+----+----+----+----+----+----+----+----+....+----+----+----+....+----+
```

- DSTIP should be **0.0.0.x** with nonzero x.

SOCKS4_REPLY

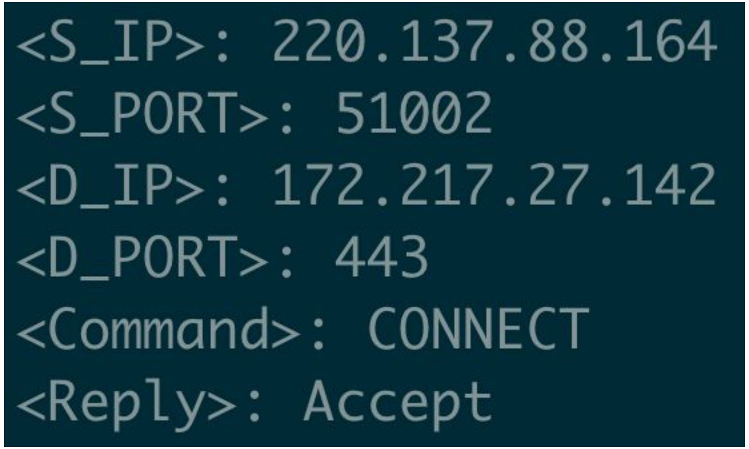
```
             +----+----+----+----+----+----+----+----+
             | VN | CD | DSTPORT |      DSTIP        |
             +----+----+----+----+----+----+----+----+
 # of bytes:    1    1      2              4

Example      +----+----+----+----+----+----+----+----+
(CONNECT)    |  0 | 90 |  0    0 |  0    0    0    0 |
             +----+----+----+----+----+----+----+----+
```

- VN is the version of the reply code and should be **0**.
- CD is the result code with one of the following values:
  - **90**: request granted
  - **91**: request rejected or failed
- DSTPORT and DSTIP are ignored in CONNECT mode.

SOCKS Server Messages

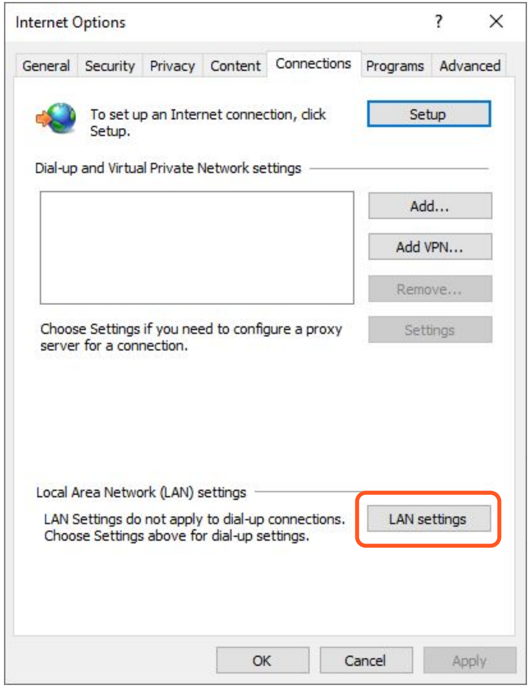
Your server should show messages in the following format:

- <S_IP>: source ip
- <S_PORT>: source port
- <D_IP>: destination ip
- <D_PORT>: destination port
- <Command>: CONNECT or BIND
- <Reply>: Accept or Reject



```
<S_IP>: 220.137.88.164
<S_PORT>: 51002
<D_IP>: 172.217.27.142
<D_PORT>: 443
<Command>: CONNECT
<Reply>: Accept
```

Setup Browser (IE)


Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

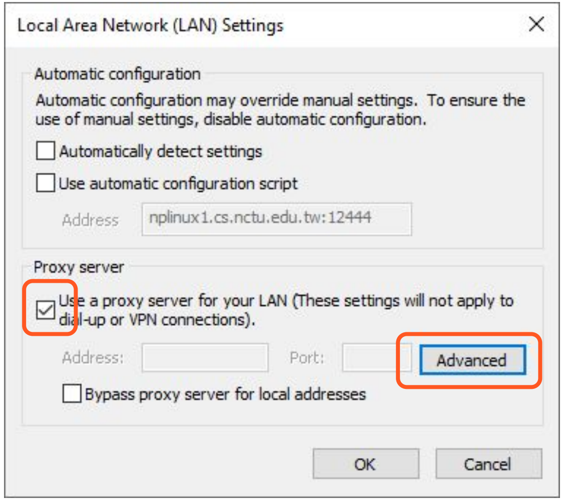
To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.


Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

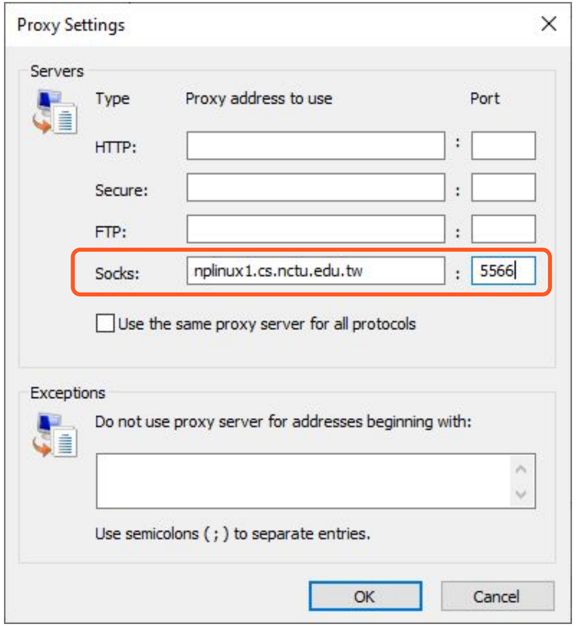
Address: nplinux1.cs.nctu.edu.tw:12444

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☐ Bypass proxy server for local addresses


Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:		
Secure:		
FTP:		
Socks:	nplinux1.cs.nctu.edu.tw	5566

☐ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

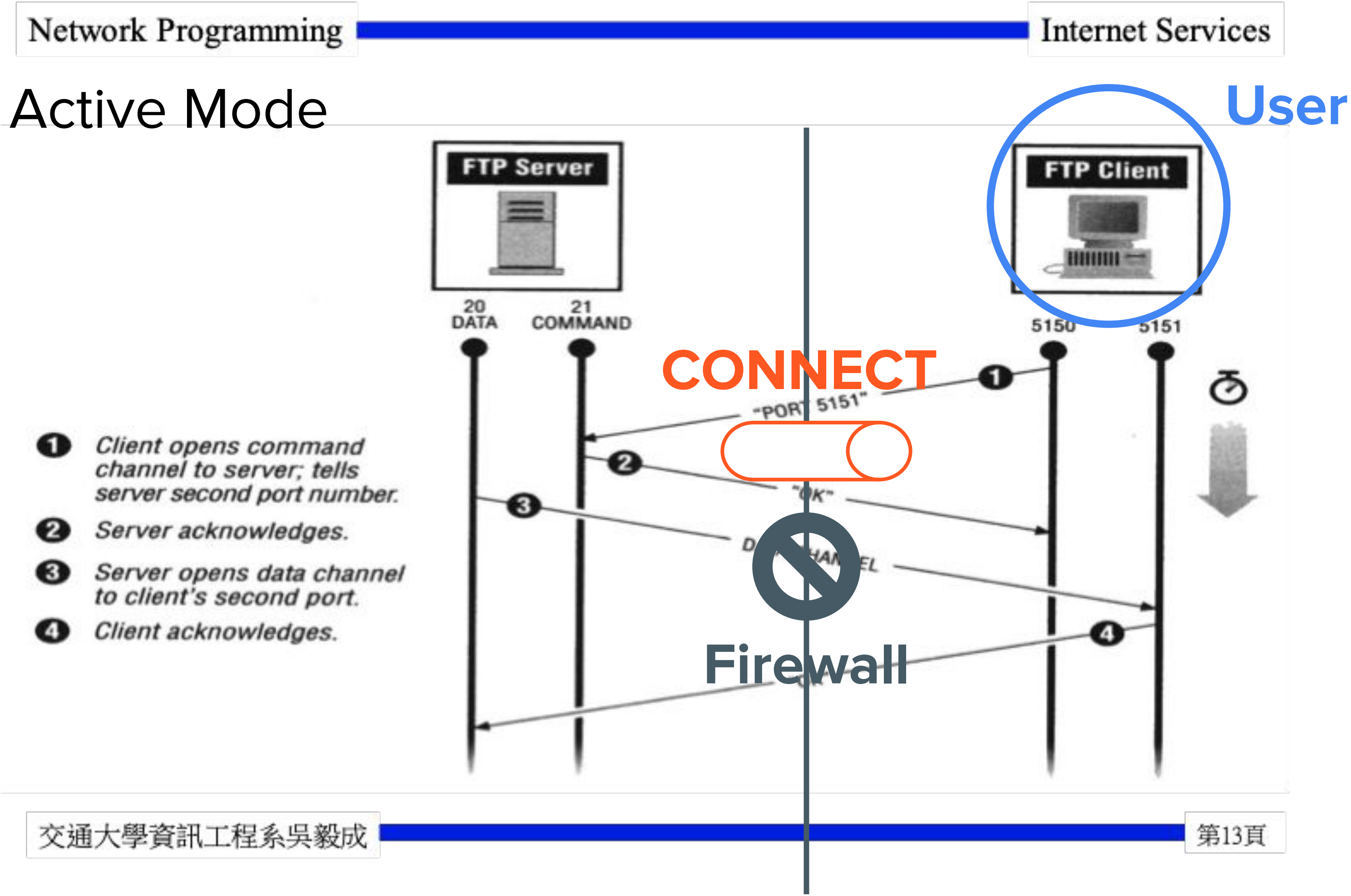
Use semicolons (;) to separate entries.

Scoring Criteria

- Setup browser and connect to your SOCKS server.
- Be able to connect any webpages via Google search. (5%)
- Turn off your socks server, connection should failed. (5%)
- Turn on your socks server, the connection should be built again. (5%)
- Show correct server messages. (5%)

II. Bind Mode

FTP Active Mode



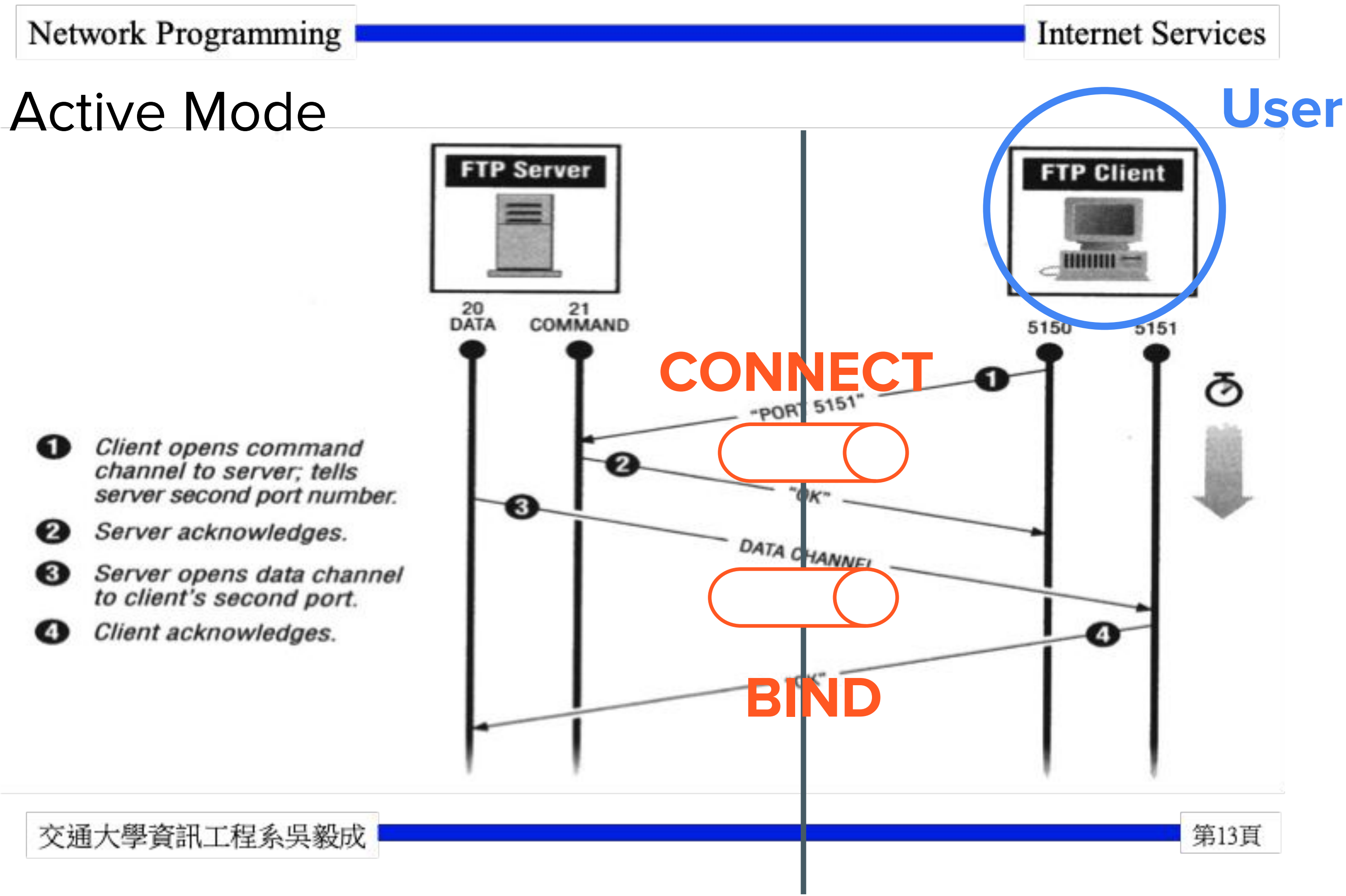
1 Client opens command channel to server; tells server second port number.

2 Server acknowledges.

3 Server opens data channel to client's second port.

4 Client acknowledges.

FTP Active Mode

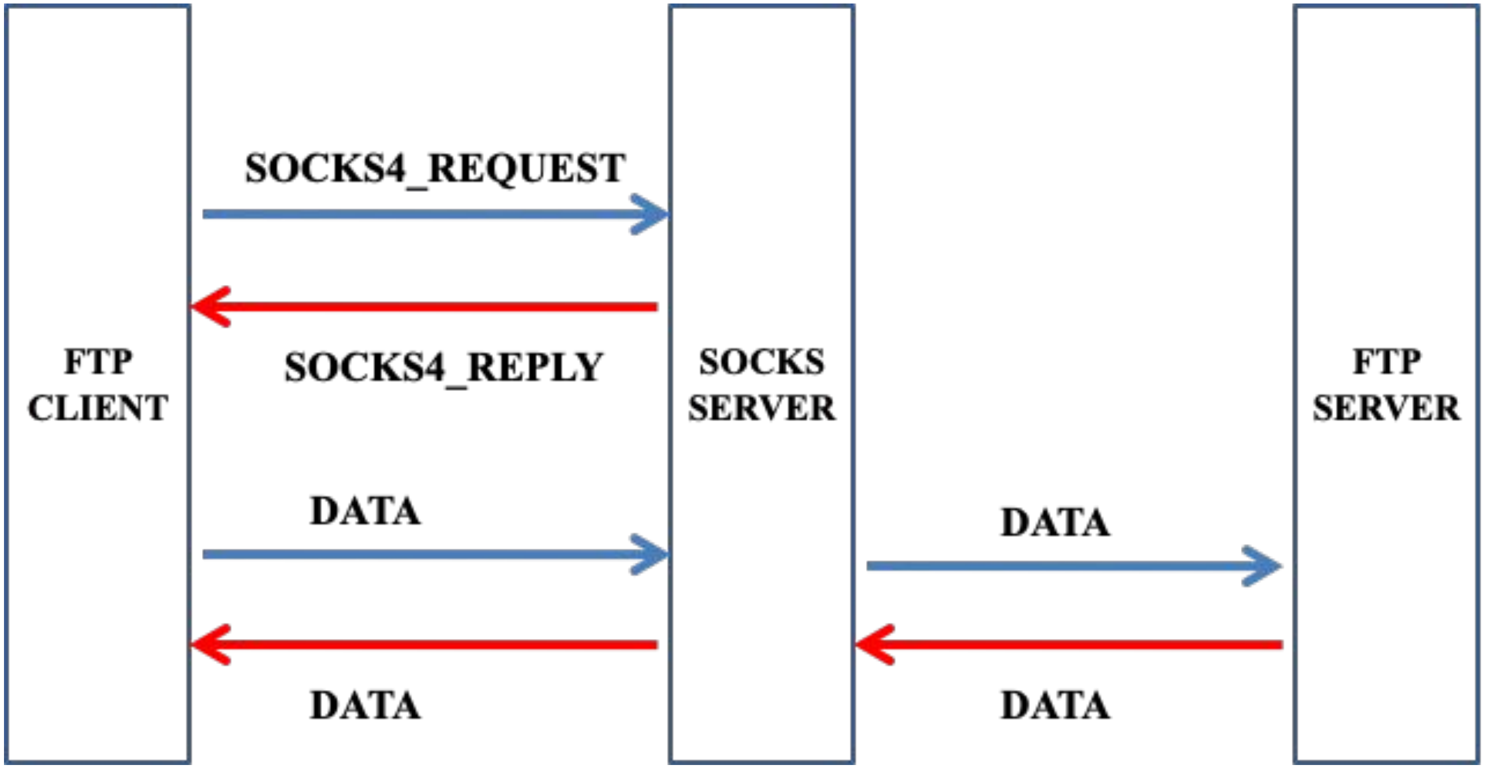


Network Programming — Internet Services

1. Client opens command channel to server; tells server second port number.
2. Server acknowledges.
3. Server opens data channel to client's second port.
4. Client acknowledges.

交通大學資訊工程系吳毅成 — 第13頁

Bind Mode (FTP Example)



SOCKS4_REQUEST

```
             +----+----+----+----+----+----+----+----+----+----+....+----+
             | VN | CD | DSTPORT |      DSTIP        | USERID       |NULL|
             +----+----+----+----+----+----+----+----+----+----+....+----+
 # of bytes:    1    1      2              4           variable       1

Example      +----+----+----+----+----+----+----+----+----+----+....+----+
(BIND)       |  4 |  2 |  2    1 | 140  113  158  61 |              |  0 |
             +----+----+----+----+----+----+----+----+----+----+....+----+
```

- VN is the SOCKS protocol version number and should be **4**.
- CD is the command code and should be **2** for **BIND** request.
- NULL is a byte of all zero bits.

SOCKS4_REPLY

Need to send REPLY again to SOCKS client after connection accepted from destination.

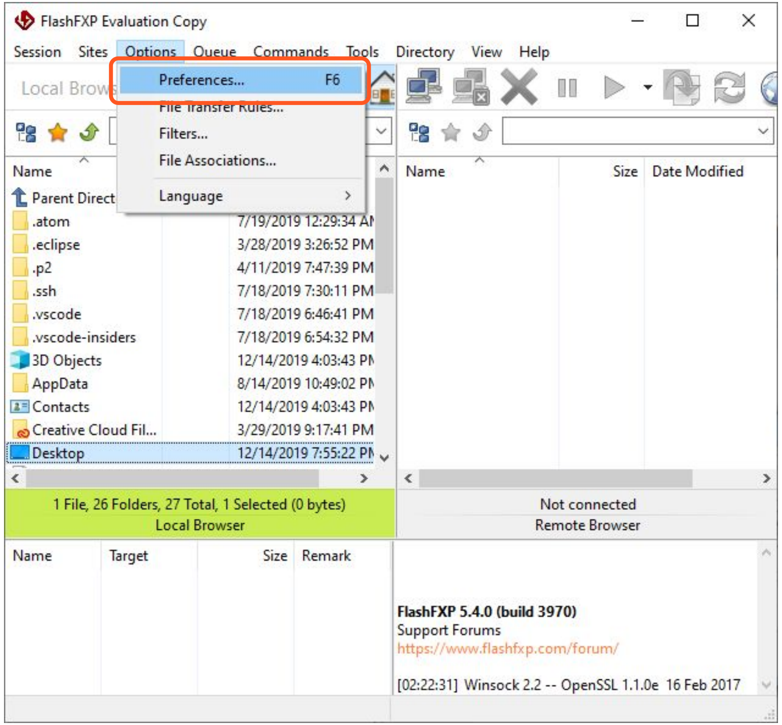
```
            +----+----+----+----+----+----+----+----+
            | VN | CD | DSTPORT |      DSTIP        |
            +----+----+----+----+----+----+----+----+
# of bytes:    1    1      2              4

Example     +----+----+----+----+----+----+----+----+
(BIND)      |  0 | 90 | 55   11 |  0    0    0    0 |
            +----+----+----+----+----+----+----+----+
```

- VN is the version of the reply code and should be **0**.
- CD is the result code with one of the following values:
  - **90**: request granted
  - **91**: request rejected or failed
- DSTPORT and DSTIP are meaningful in BIND mode.

FTP Server / Client

- FTP Server
  - You need to setup your own FTP server for testing.
  - Example: FileZilla Server
- We will use **FlashFXP** (http://www.flashfxp.com/) for FTP client.

FlashFXP - Setup SOCKS Server



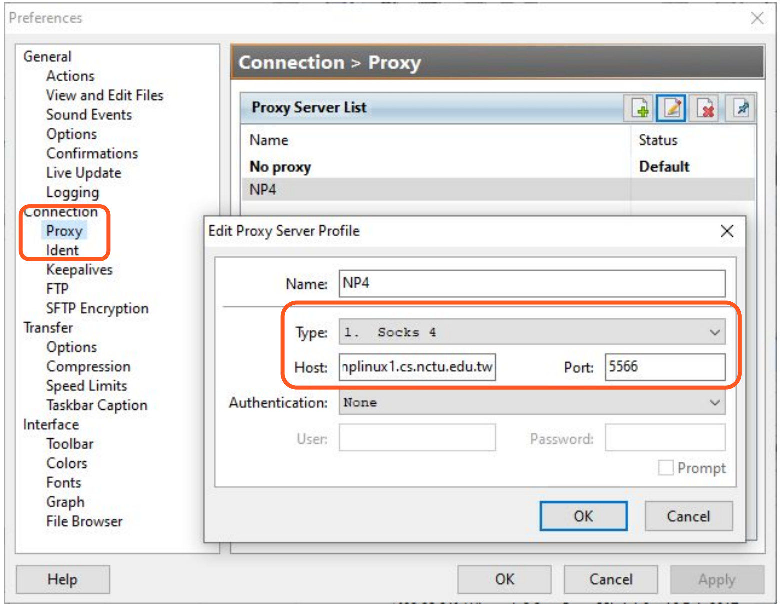
Name	Size	Date Modified
Parent Direct		
.atom		7/19/2019 12:29:34 AI
.eclipse		3/28/2019 3:26:52 PM
.p2		4/11/2019 7:47:39 PM
.ssh		7/18/2019 7:30:11 PM
.vscode		7/18/2019 6:46:41 PM
.vscode-insiders		7/18/2019 6:54:32 PM
3D Objects		12/14/2019 4:03:43 PI
AppData		8/14/2019 10:49:02 PI
Contacts		12/14/2019 4:03:43 PI
Creative Cloud Fil...		3/29/2019 9:17:41 PM
Desktop		12/14/2019 7:55:22 PI

1 File, 26 Folders, 27 Total, 1 Selected (0 bytes)
Local Browser

Not connected
Remote Browser

Name	Target	Size	Remark

```
FlashFXP 5.4.0 (build 3970)
Support Forums
https://www.flashfxp.com/forum/

[02:22:31] Winsock 2.2 -- OpenSSL 1.1.0e 16 Feb 2017
```



Name	Status
No proxy	Default
NP4	

Name: NP4

Type: 1. Socks 4

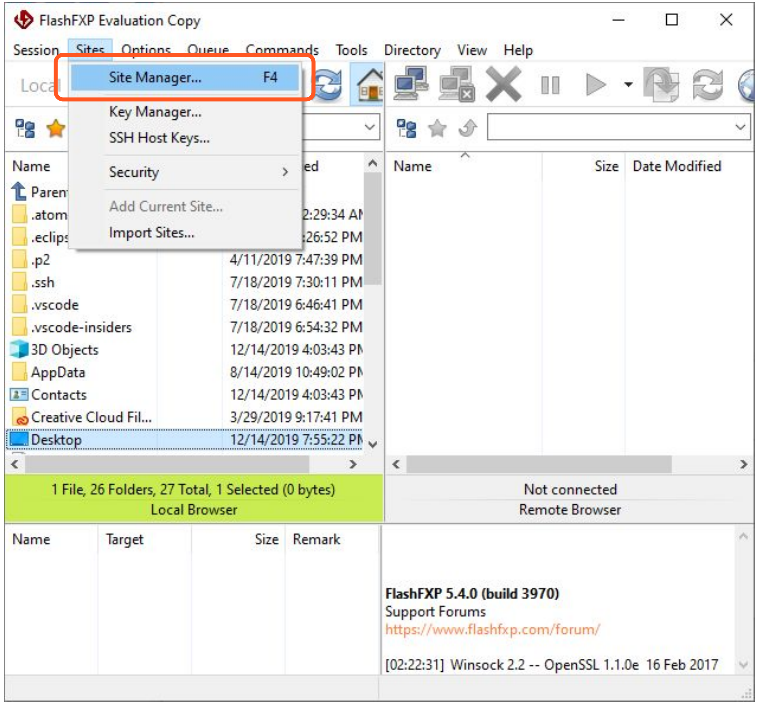
Host: nplinux1.cs.nctu.edu.tw Port: 5566

Authentication: None

User: Password:

□ Prompt

FlashFXP - Setup SOCKS Server



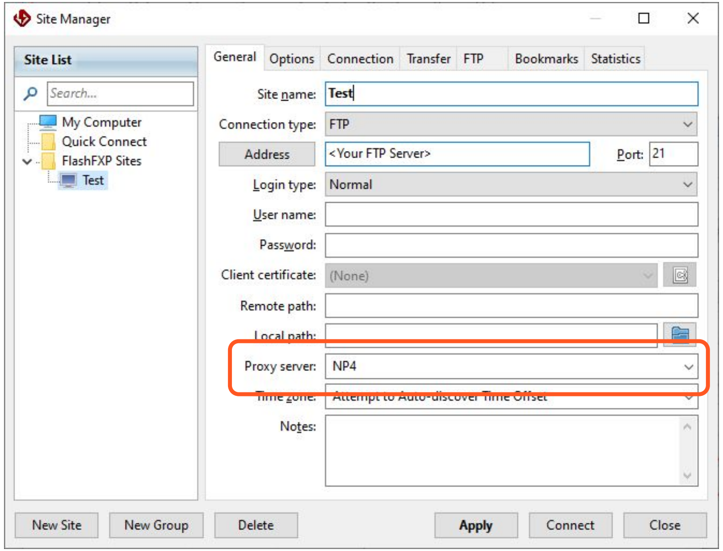
Name	Modified
Parent	
.atom	2:29:34 AM
.eclips	:26:52 PM
.p2	4/11/2019 7:47:39 PM
.ssh	7/18/2019 7:30:11 PM
.vscode	7/18/2019 6:46:41 PM
.vscode-insiders	7/18/2019 6:54:32 PM
3D Objects	12/14/2019 4:03:43 PM
AppData	8/14/2019 10:49:02 PM
Contacts	12/14/2019 4:03:43 PM
Creative Cloud Fil...	3/29/2019 9:17:41 PM
Desktop	12/14/2019 7:55:22 PM

1 File, 26 Folders, 27 Total, 1 Selected (0 bytes)
Local Browser

Not connected
Remote Browser

FlashFXP 5.4.0 (build 3970)
Support Forums
https://www.flashfxp.com/forum/

[02:22:31] Winsock 2.2 -- OpenSSL 1.1.0e 16 Feb 2017



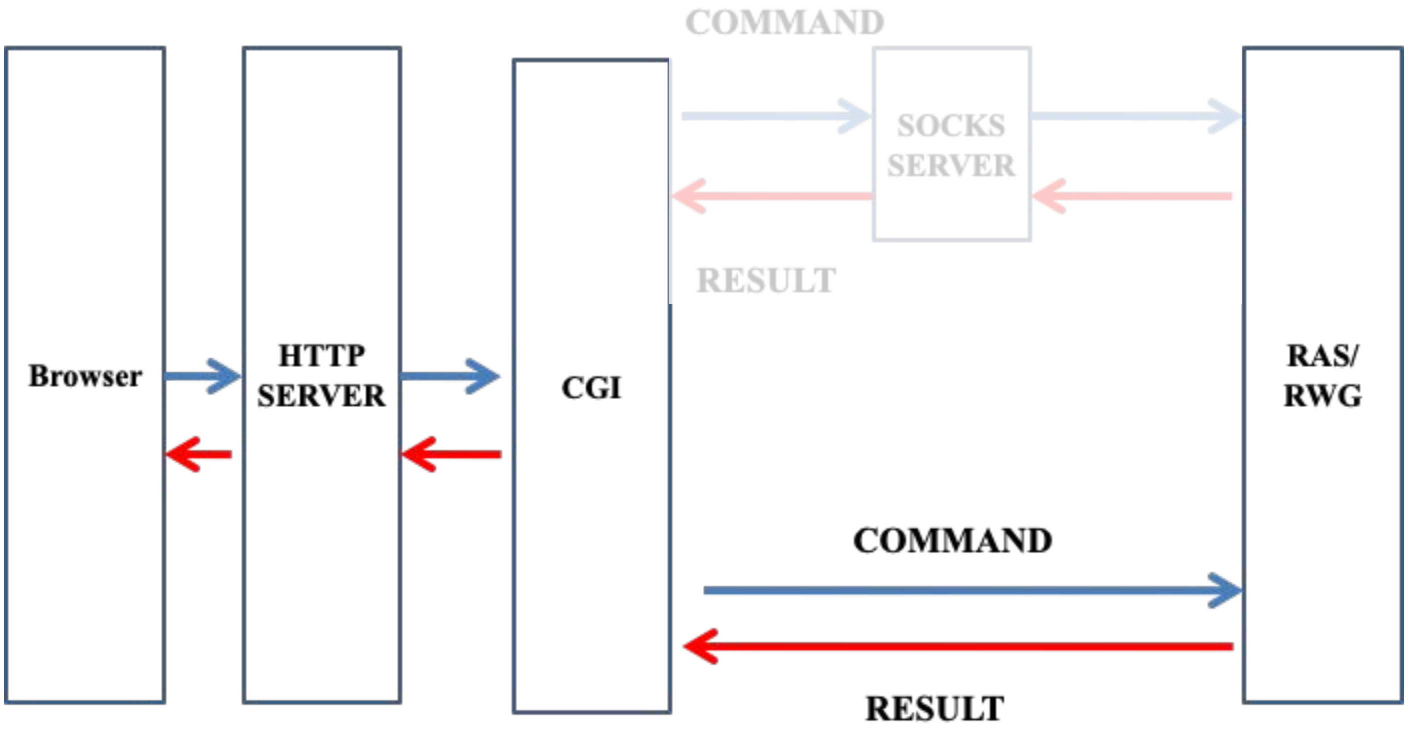
Site name: Test
Connection type: FTP
Address: <Your FTP Server> Port: 21
Login type: Normal
User name:
Password:
Client certificate: (None)
Remote path:
Local path:
Proxy server: NP4
Time zone: Attempt to Auto-discover Time Offset
Notes:

Scoring Criteria

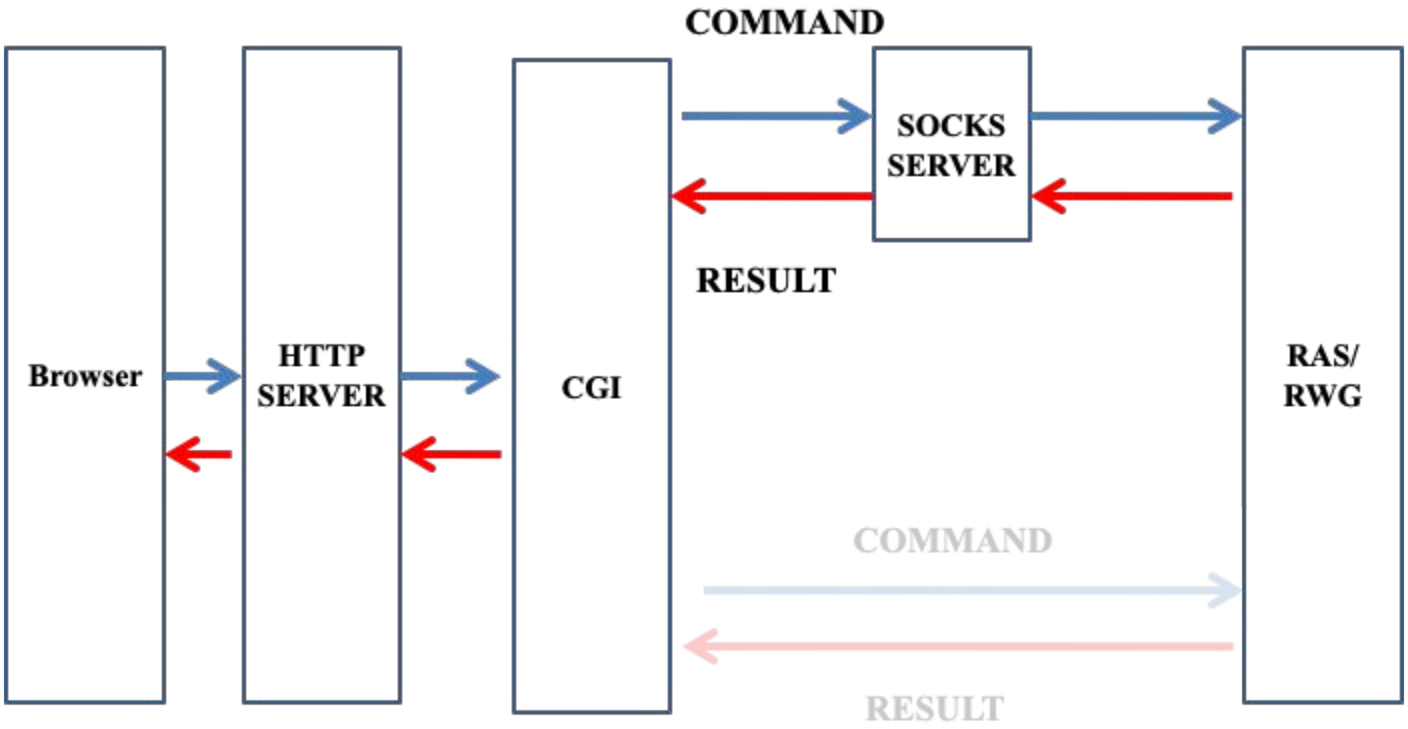
- Open FlashFXP and setup your socks server.
- Upload executable file > 1GB. (5%)
- Download the file. (5%)
- Check size and if the file still executable. (5%)
- Check whether SOCKS server’s output has used BIND mode. (5%)

III. CGI Proxy

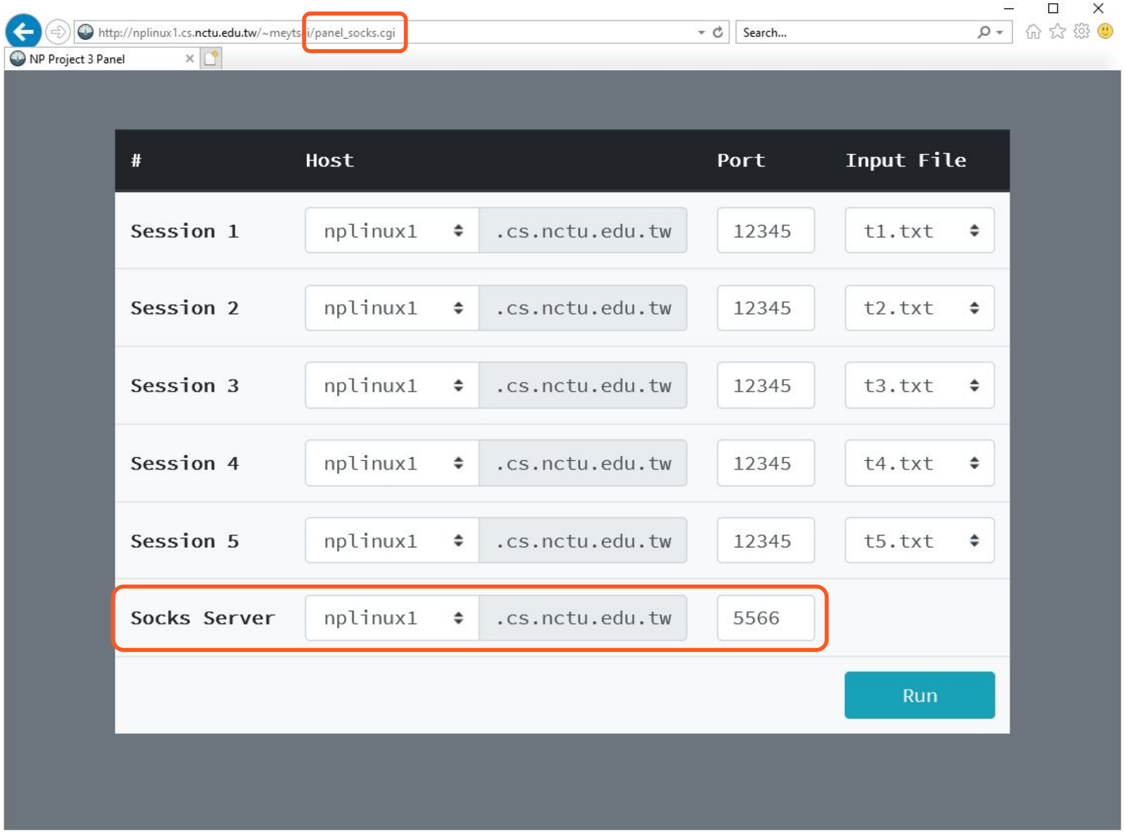
CGI Connection



CGI Connection



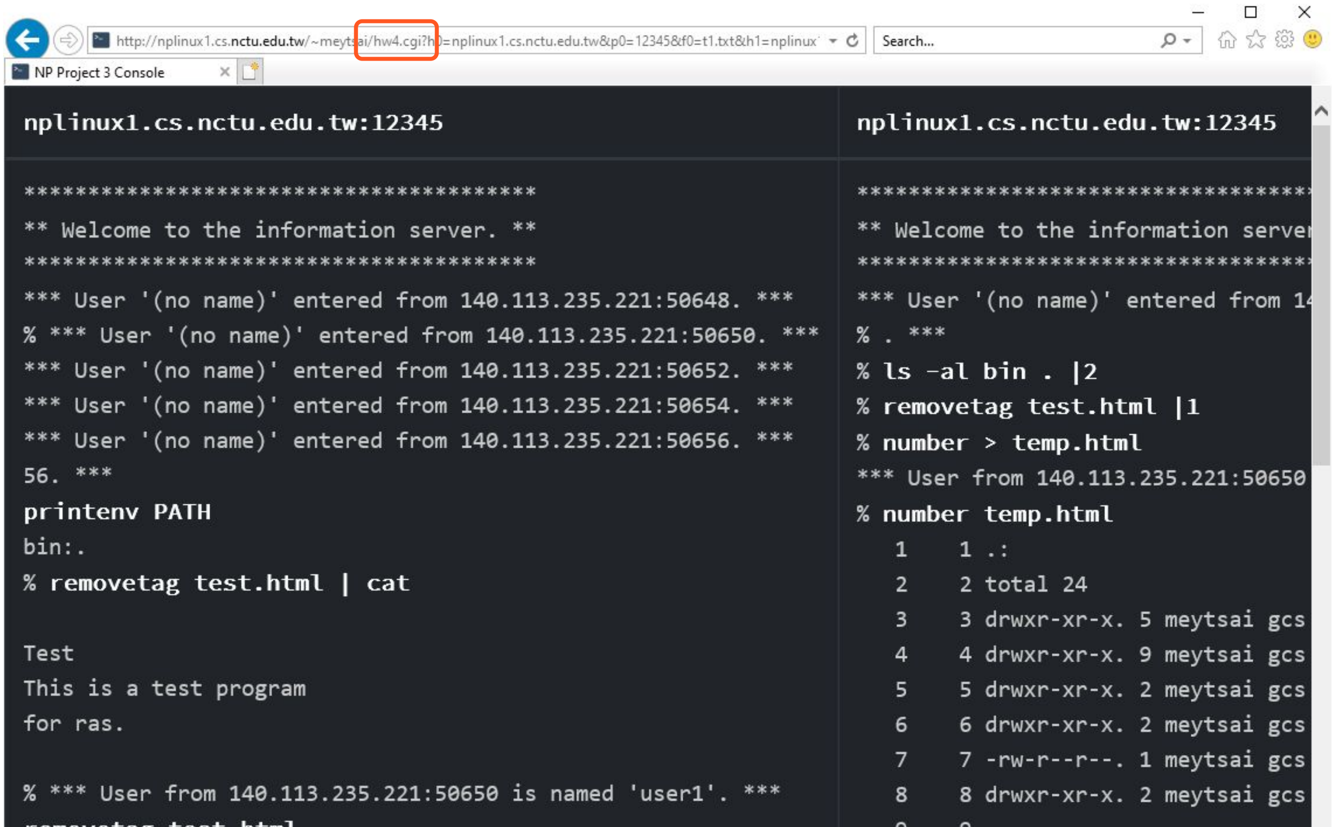
panel_socks.cgi



#	Host		Port	Input File
Session 1	nplinux1	.cs.nctu.edu.tw	12345	t1.txt
Session 2	nplinux1	.cs.nctu.edu.tw	12345	t2.txt
Session 3	nplinux1	.cs.nctu.edu.tw	12345	t3.txt
Session 4	nplinux1	.cs.nctu.edu.tw	12345	t4.txt
Session 5	nplinux1	.cs.nctu.edu.tw	12345	t5.txt
Socks Server	nplinux1	.cs.nctu.edu.tw	5566	

Demo Example

sh=nplinux1.cs.nctu.edu.tw&sp=5566


http://nplinux1.cs.nctu.edu.tw/~meytsai/hw4.cgi?h0=nplinux1.cs.nctu.edu.tw&p0=12345&f0=t1.txt&h1=nplinux
Search...
NP Project 3 Console

```
nplinux1.cs.nctu.edu.tw:12345

****************************************
** Welcome to the information server. **
****************************************
*** User '(no name)' entered from 140.113.235.221:50648. ***
% *** User '(no name)' entered from 140.113.235.221:50650. ***
*** User '(no name)' entered from 140.113.235.221:50652. ***
*** User '(no name)' entered from 140.113.235.221:50654. ***
*** User '(no name)' entered from 140.113.235.221:50656. ***
56. ***
printenv PATH
bin:.
% removetag test.html | cat

Test
This is a test program
for ras.

% *** User from 140.113.235.221:50650 is named 'user1'. ***
removetag test.html
```

```
nplinux1.cs.nctu.edu.tw:12345

**********************************
** Welcome to the information serve
**********************************
*** User '(no name)' entered from 14
% . ***
% ls -al bin . |2
% removetag test.html |1
% number > temp.html
*** User from 140.113.235.221:50650
% number temp.html
   1    1 .:
   2    2 total 24
   3    3 drwxr-xr-x. 5 meytsai gcs
   4    4 drwxr-xr-x. 9 meytsai gcs
   5    5 drwxr-xr-x. 2 meytsai gcs
   6    6 drwxr-xr-x. 2 meytsai gcs
   7    7 -rw-r--r--. 1 meytsai gcs
   8    8 drwxr-xr-x. 2 meytsai gcs
```

Details

- Modify project3 console.cpp to implement **SOCK4 client** (**hw4.cgi**).
  - In `QUERYSTRING`, `sh=<SocksHost>&sp=<SocksPort>`
- We will provide `panel_socks.cgi`
- Testing steps
  - Close proxy setting of your browser.
  - Put test_case, **panel_socks.cgi** and **hw4.cgi** in ~/public_html
  - Run your **socks server** and **np_single_golden** on nplinux
  - Connect and run panel_socks.cgi
    - e.g. nplinux1.cs.nctu.edu.tw/~<yourname>/panel_socks.cgi

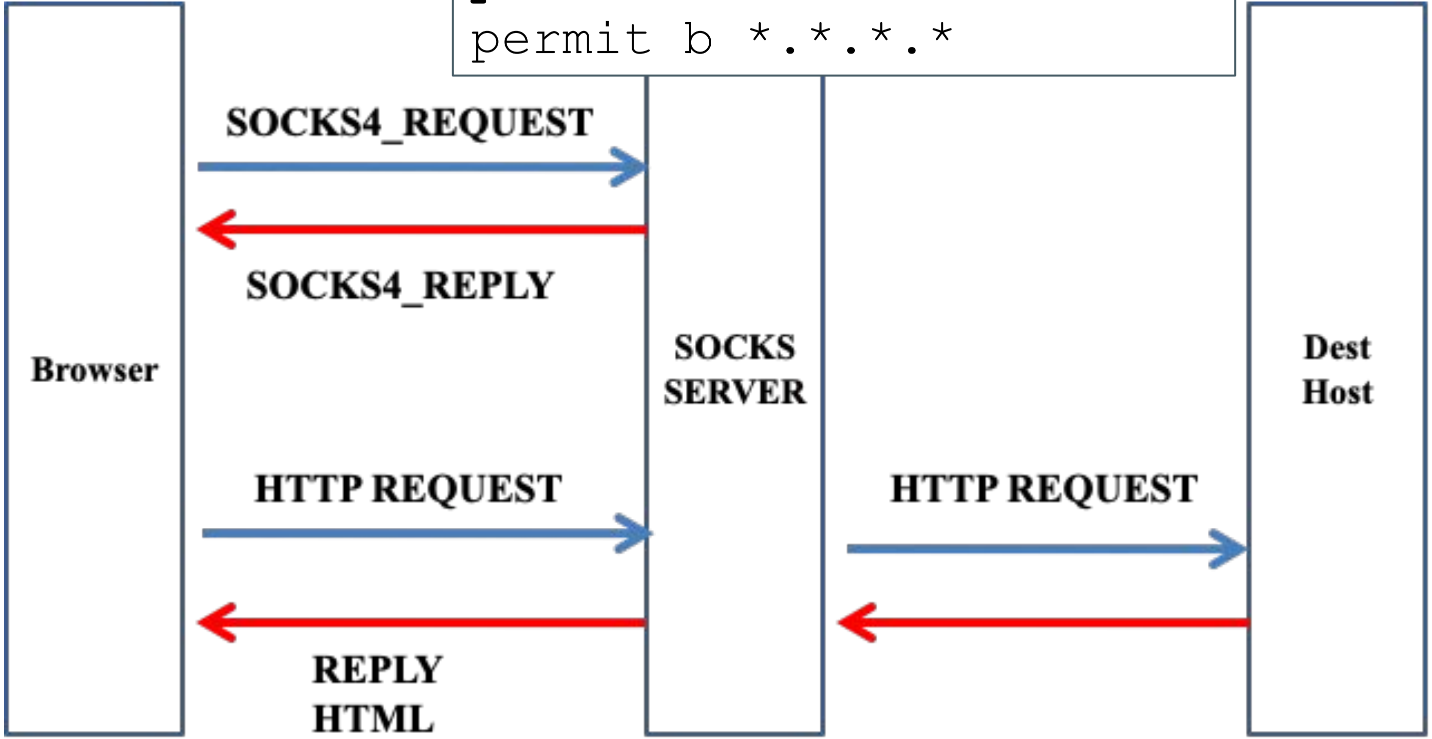
IV. Firewall

Connect Mode

(deny all traffic by default)

socks.conf

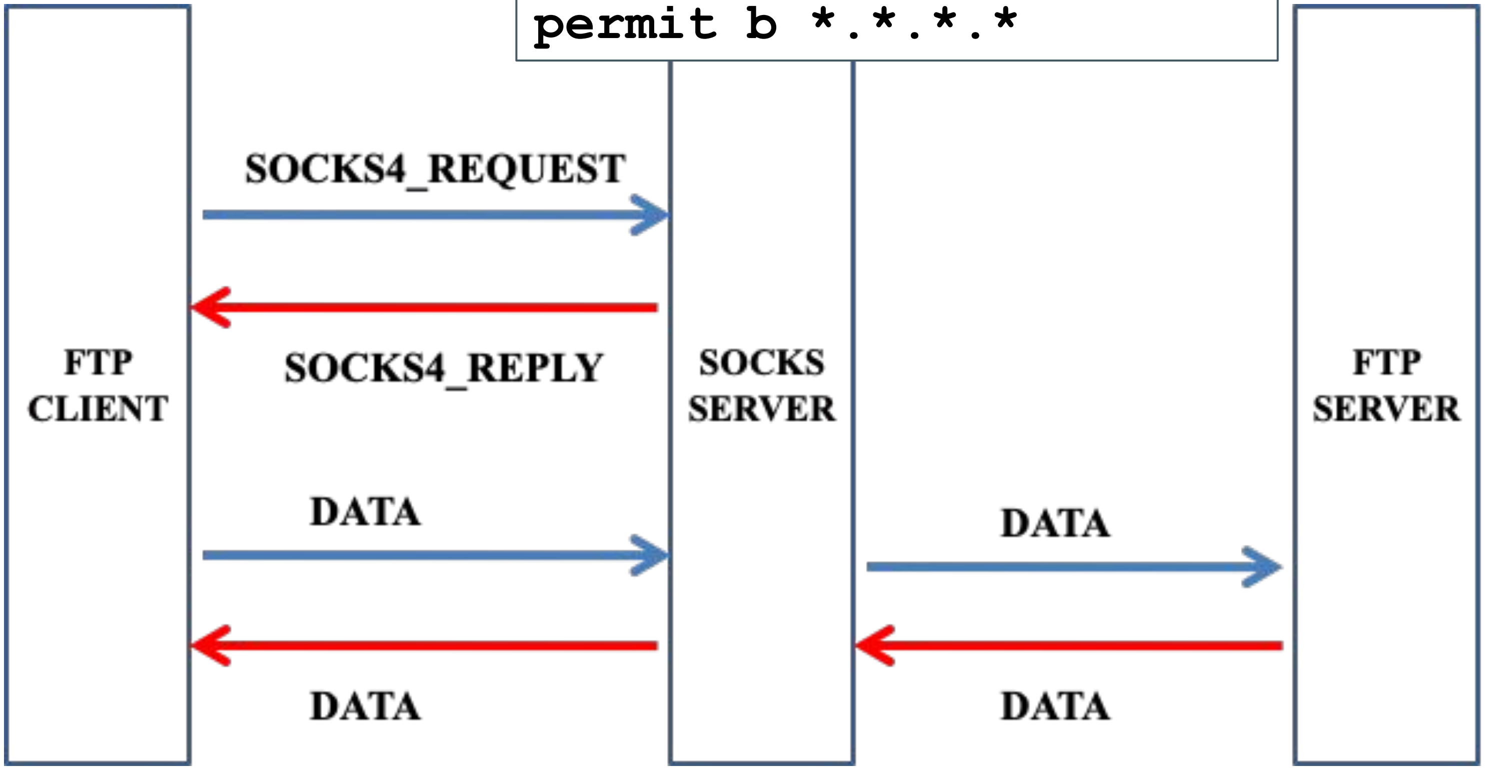
```
permit c 140.113.*.*
permit b *.*.*.*
```



Bind Mode

(deny all traffic by default) socks.conf

```
permit c 140.113.*.*
permit b *.*.*.*
```



Scoring Criteria for Part III and IV

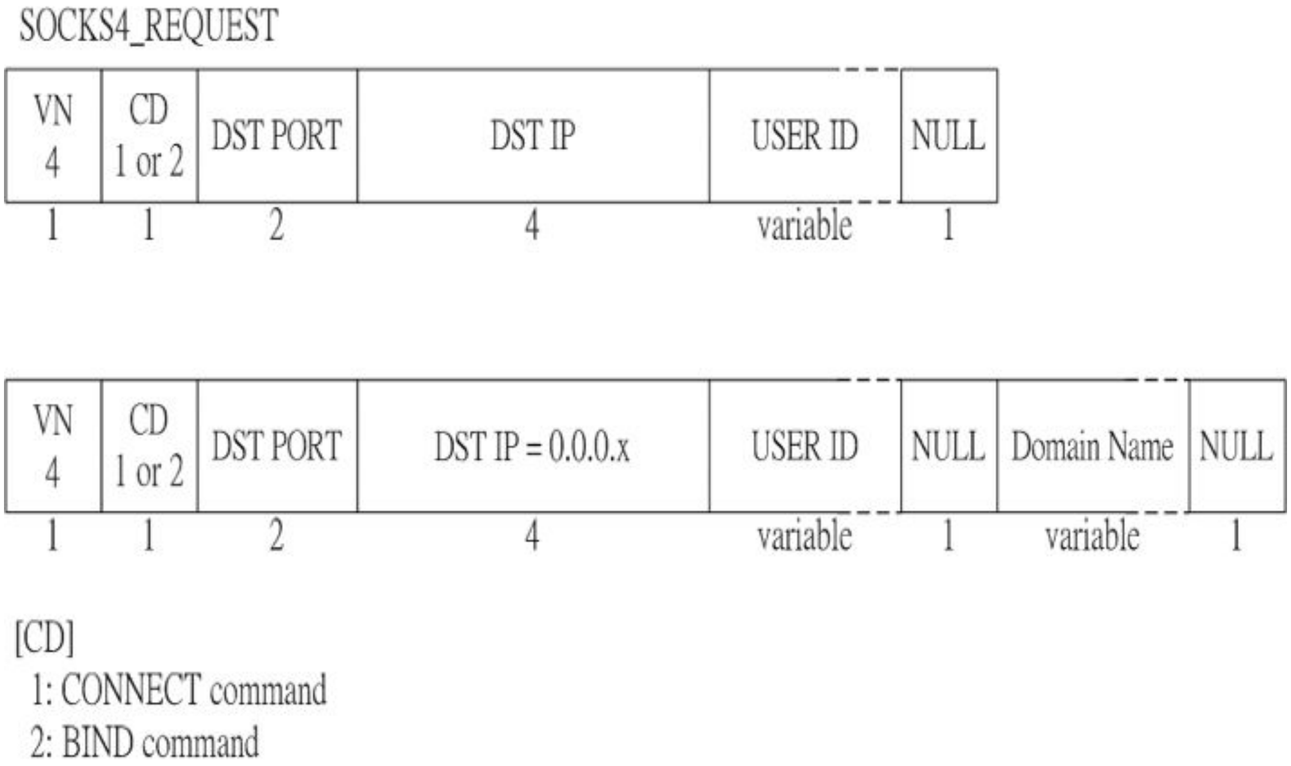
- CGI Proxy
    - Success run all testcases (20%)
        - No hidden testcases
- Firewall Example:
    - Only allow connections to NCTU (5%)
        - “permit c 140.113.*.*”
    - Only allow connections to NTHU (5%)
        - “permit c 140.114.*.*”

Reference

- SOCKS4 Protocol
- SOCKS4a Protocol

Appendix

SOCKS4_REQUEST



SOCKS4_REQUEST

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

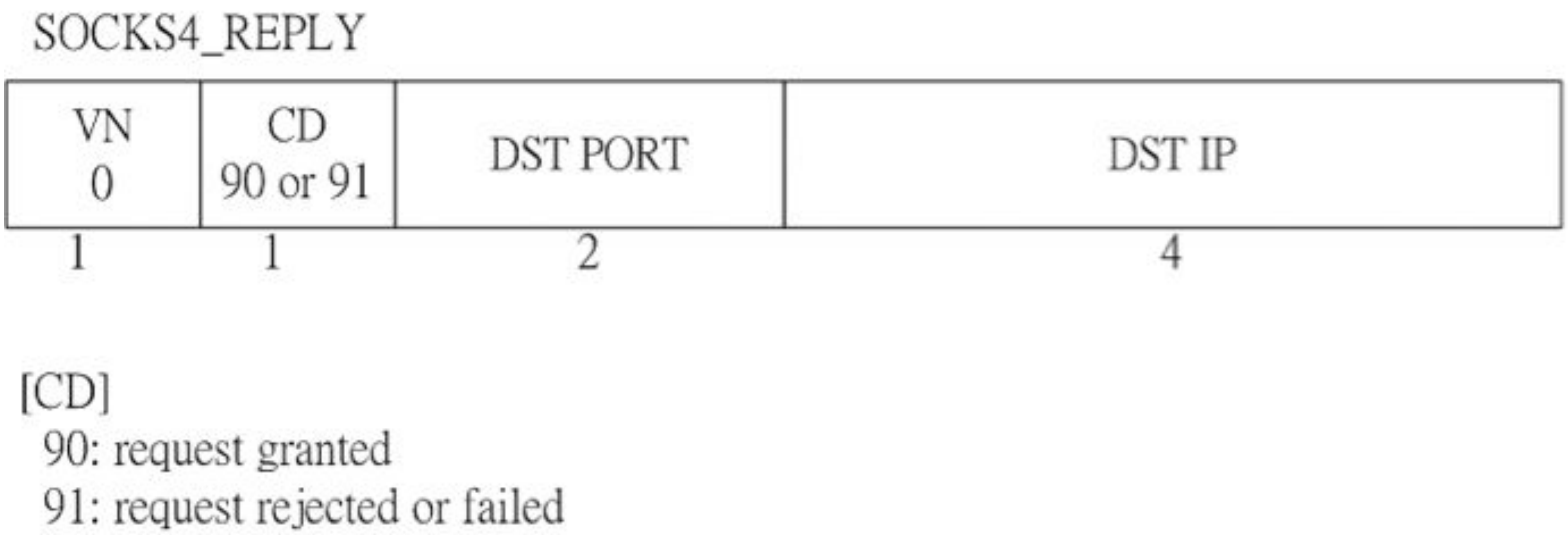
VN 4	CD 1 or 2	DST PORT	DST IP = 0.0.0.x	USER ID	NULL	Domain Name	NULL
1	1	2	4	variable	1	variable	1

[CD]

1: CONNECT command

2: BIND command

SOCKS4_REPLY



SOCKS4_REPLY

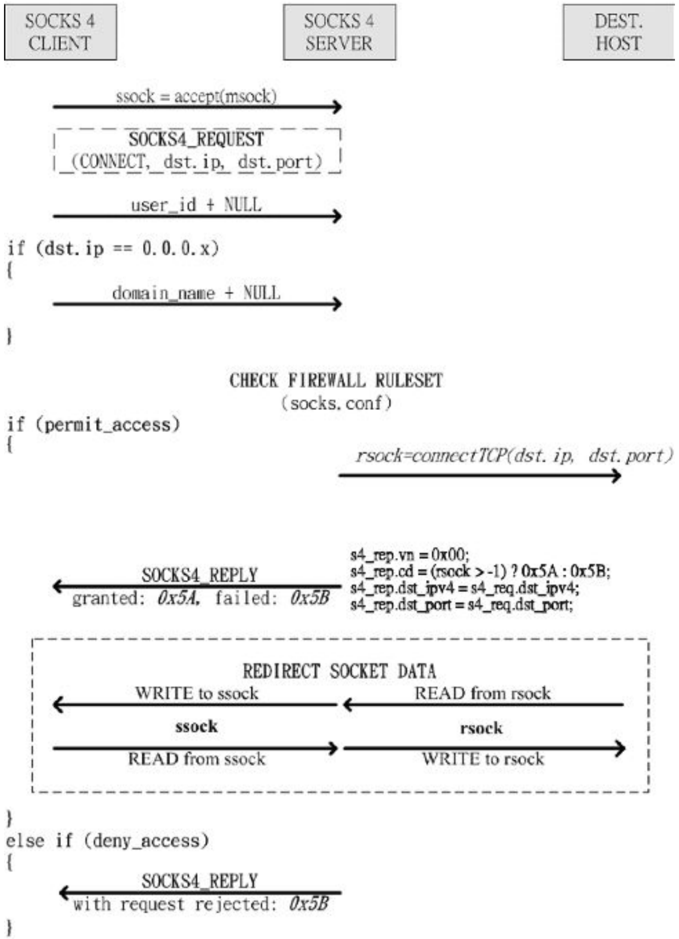
VN 0	CD 90 or 91	DST PORT	DST IP
1	1	2	4

[CD]

90: request granted

91: request rejected or failed

SOCKS Version 4 Protocol
(CONNECT Operation)



SOCKS 4 CLIENT

SOCKS 4 SERVER

DEST. HOST

ssock = accept(msock)

SOCKS4_REQUEST
(CONNECT, dst. ip, dst. port)

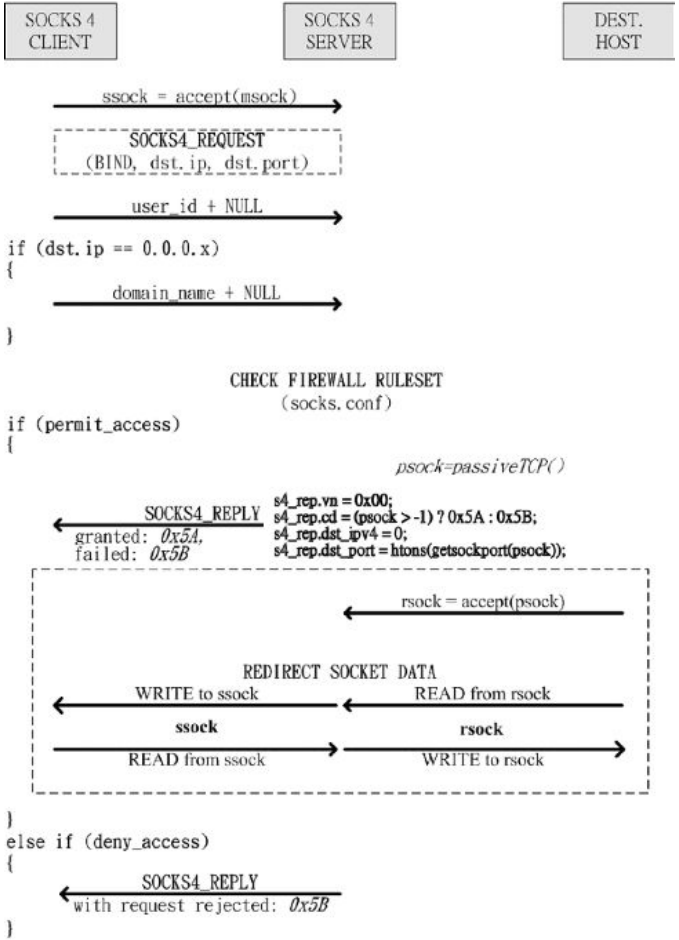
user_id + NULL

```
if (dst. ip == 0. 0. 0. x)
{
    domain_name + NULL
}
```

CHECK FIREWALL RULESET
(socks. conf)

```
if (permit_access)
{
    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
    WRITE to ssock    READ from rsock
    ssock             rsock
    READ from ssock   WRITE to rsock
}
else if (deny_access)
{
    SOCKS4_REPLY
    with request rejected: 0x5B
}
```

SOCKS Version 4 Protocol
(BIND Operation)



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
}
```

CHECK FIREWALL RULESET
(socks. conf)

```
if (permit_access)
{
    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));

    rsock = accept(psock)

    REDIRECT SOCKET DATA
    WRITE to ssock    READ from rsock
    ssock             rsock
    READ from ssock   WRITE to rsock
}
else if (deny_access)
{
    SOCKS4_REPLY
    with request rejected: 0x5B
}
```