

Project 4: SOCKS 4



NP TA 睿德

12/22 23:55

Project 4 Deadline
Demo: 12/24 Sat.

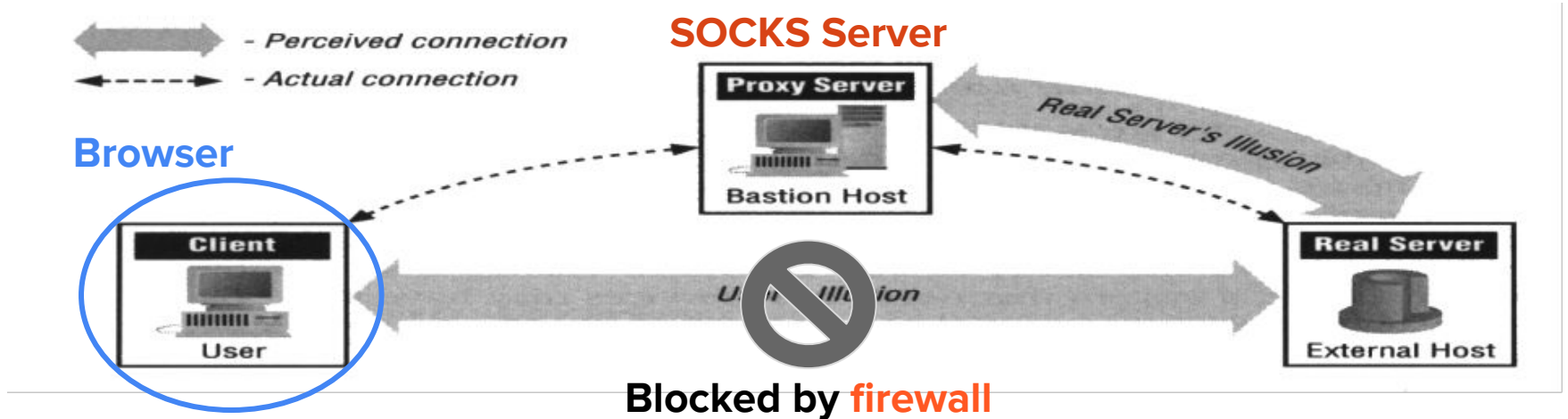
Project Requirements

- I. SOCKS 4 Server **Connect** Operation
- II. SOCKS 4 Server **Bind** Operation
- III. CGI Proxy
- IV. Firewall

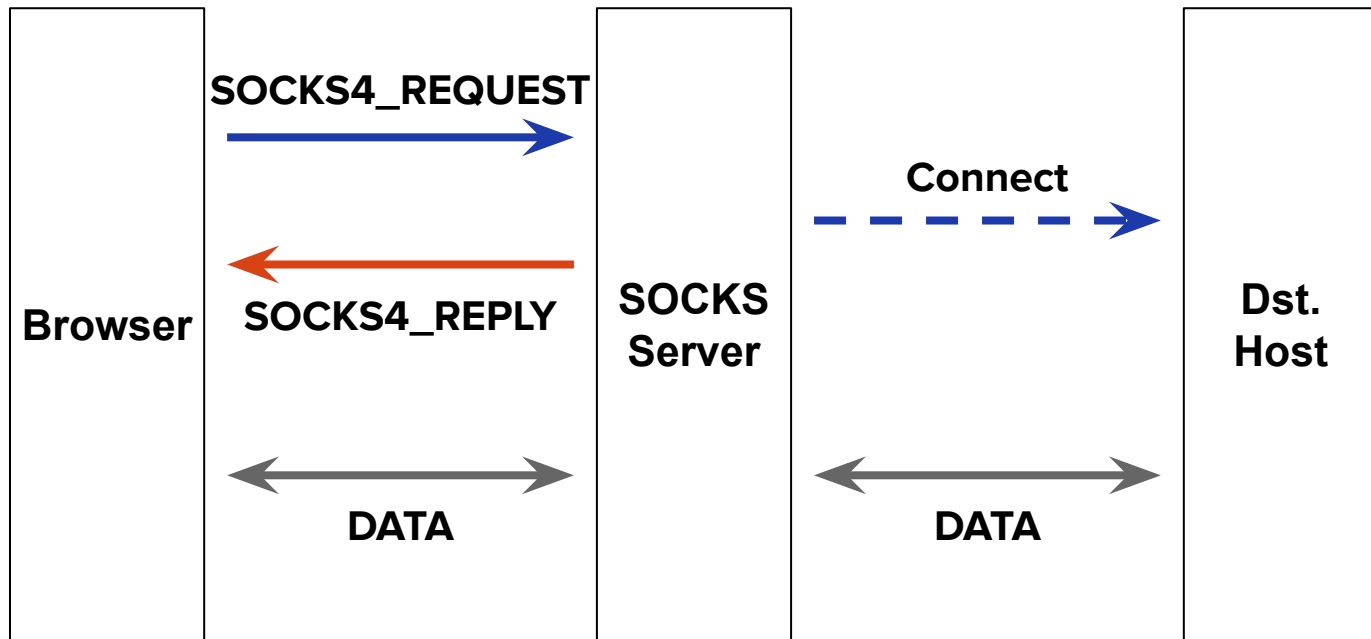
I. Connect Operation

Connect Request

- A client wants to establish a connection to an application server



Connect Operation (HTTP Example)



SOCKS4_REQUEST

	VN	CD	DSTPORT	DSTIP	USERID	NULL
# of bytes	1	1	2	4	variable	1

Example:(Connect)

4	1	80	140	113	43	7	0
---	---	----	-----	-----	----	---	-------	---

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

SOCKS4_REQUEST (SOCKS 4A)

- If the client cannot resolve the destination host's domain name itself

	VN	CD	DSTPORT	DSTIP	USERID	NULL	DOMAIN NAME	NULL
# of bytes	1	1	2	4	variable	1	variable	1

Example:(Connect)

4	1	80	0	0	0	1		0	'w'	'w'	...	0
---	---	----	---	---	---	---	--	---	-----	-----	-----	---

- DSTIP should be 0.0.0.x with nonzero x
- The SOCKS server resolves the domain name
- You may test with ``curl --socks4a <host[:port]> <URL>``

SOCKS4_REPLY

	VN	CD	DSTPORT	DSTIP
# of bytes	1	1	2	4

Example:(Connect)

0	90	0	0	0	0	0	0
---	----	---	---	---	---	---	---

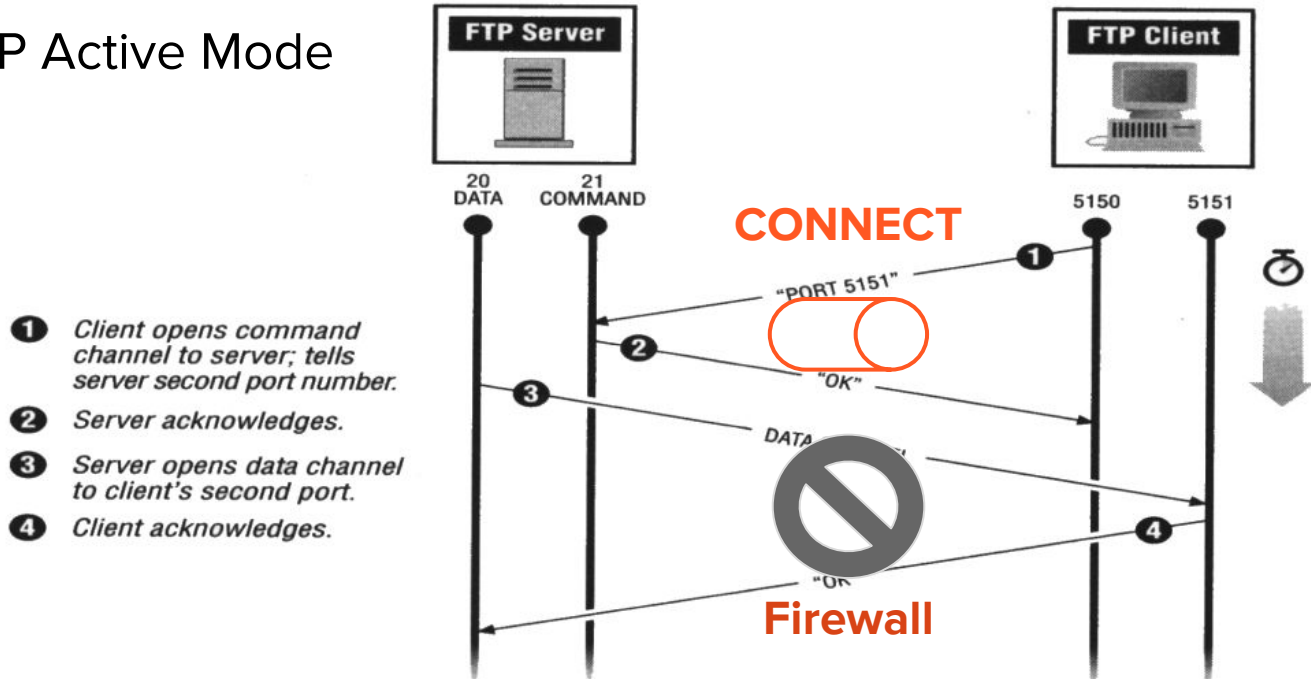
- VN is the version of the reply code and should be **0**
- CD is the result code:
 - **90**: request granted
 - **91**: request rejected or failed
- DSTPORT and DSTIP fields are ignored in CONNECT reply

II. Bind Operation

Bind Request

- A client wants to prepare for an **inbound** connection from an application server

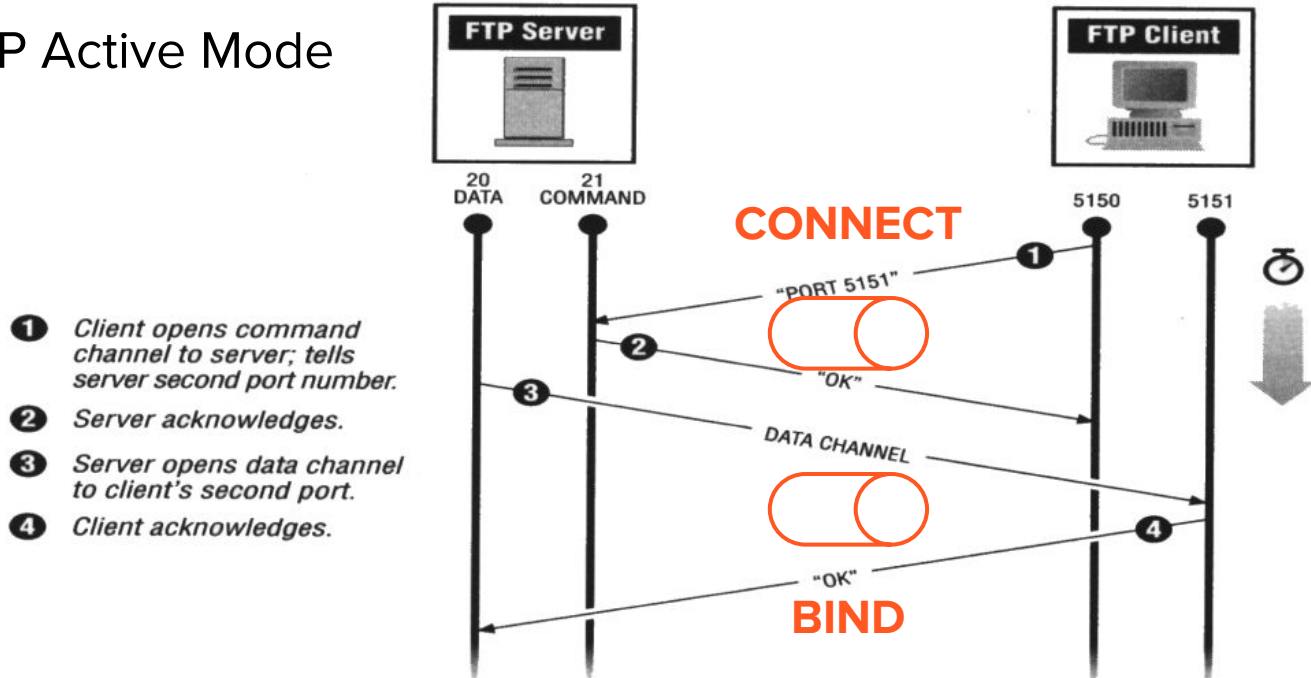
FTP Active Mode



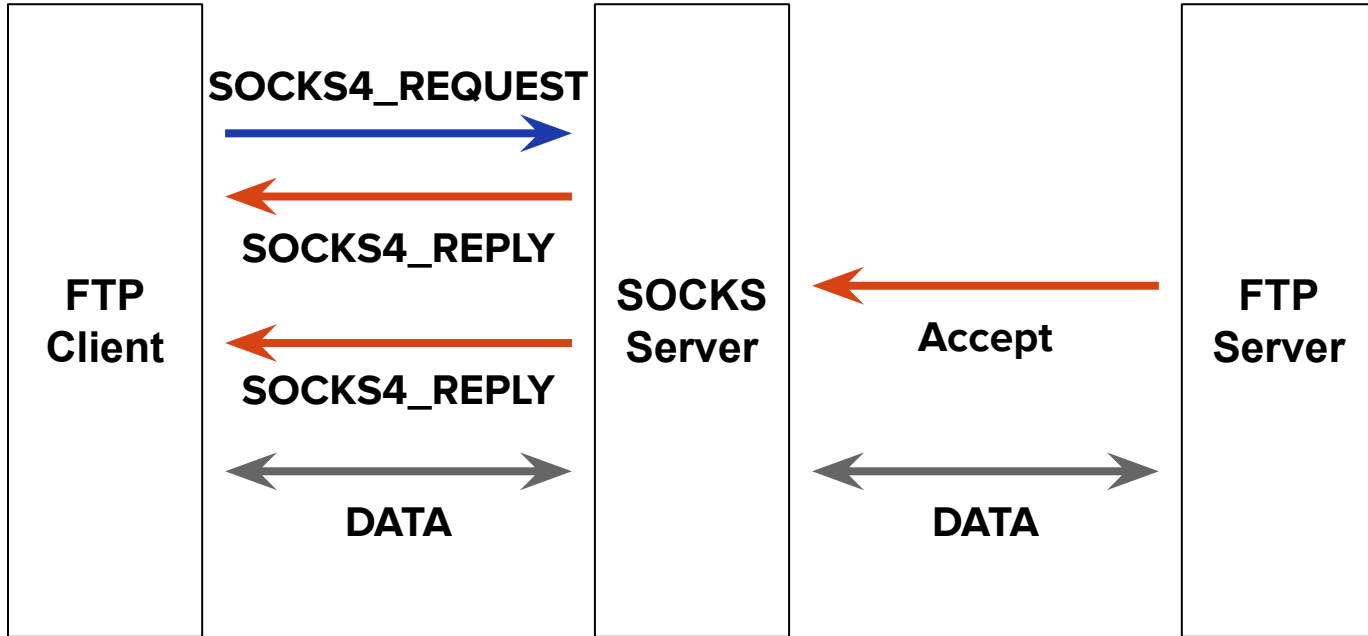
Bind Request

- A client wants to prepare for an **inbound** connection from an application server

FTP Active Mode



Bind Operation (FTP Example)



SOCKS4_REQUEST

	VN	CD	DSTPORT	DSTIP	USERID	NULL
# of bytes	1	1	2	4	variable	1

Example:(Bind)

4	2	20	140	113	9	151	0
---	---	----	-----	-----	---	-----	-------	---

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

SOCKS4_REPLY

	VN	CD	DSTPORT	DSTIP
# of bytes	1	1	2	4

Example:(Connect)

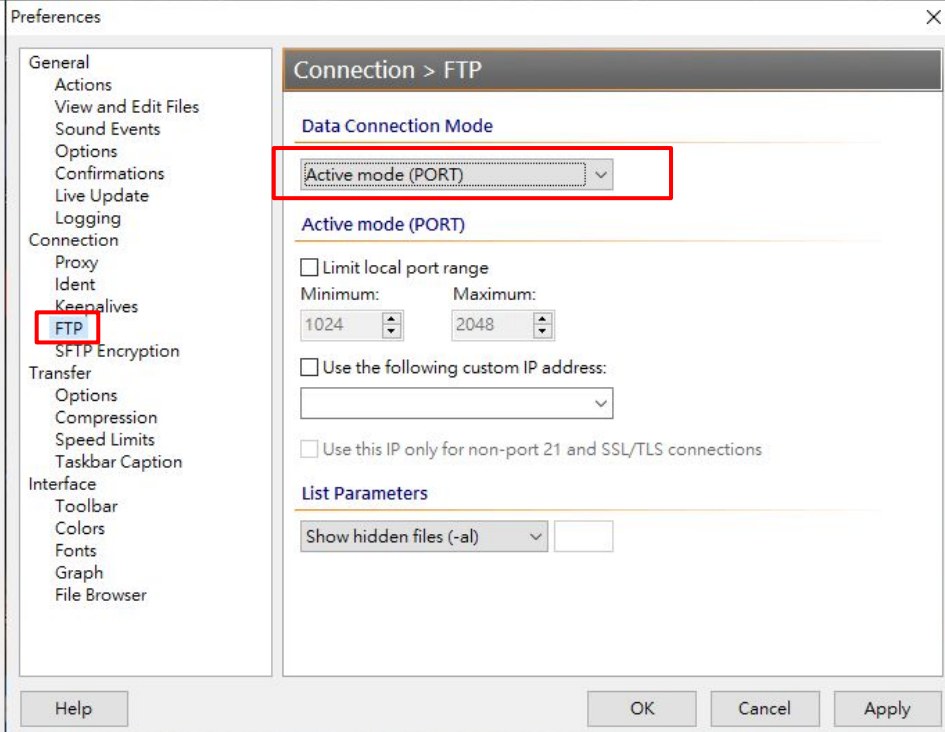
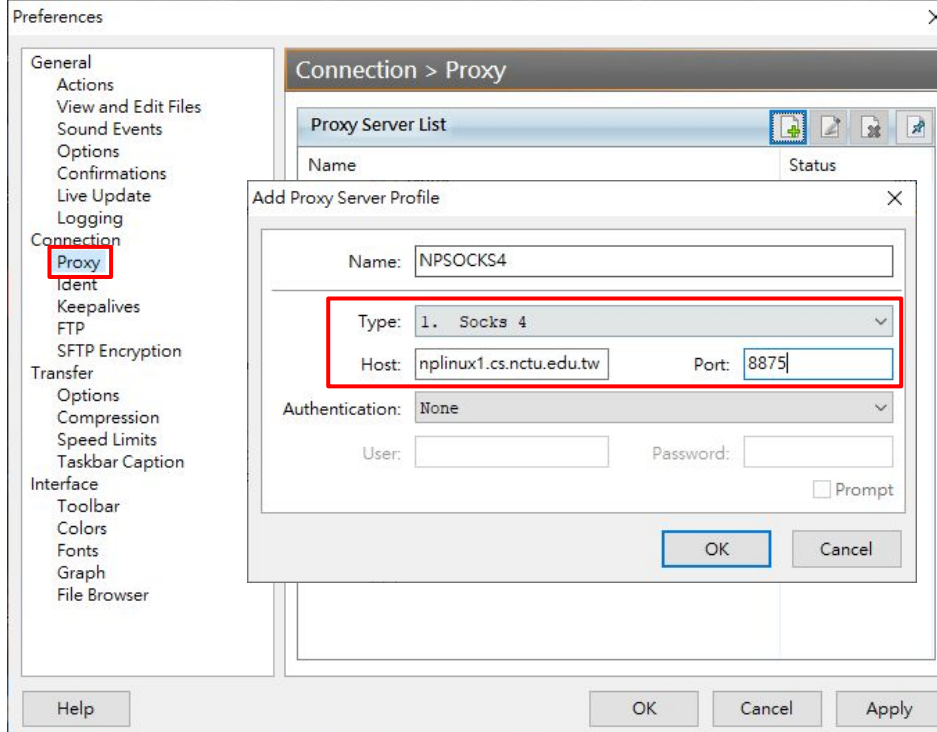
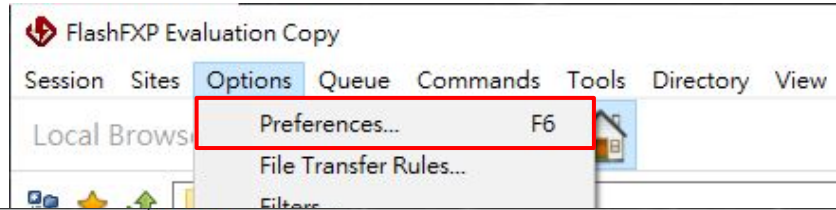
0	90	55	11	0	0	0	0
---	----	----	----	---	---	---	---

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

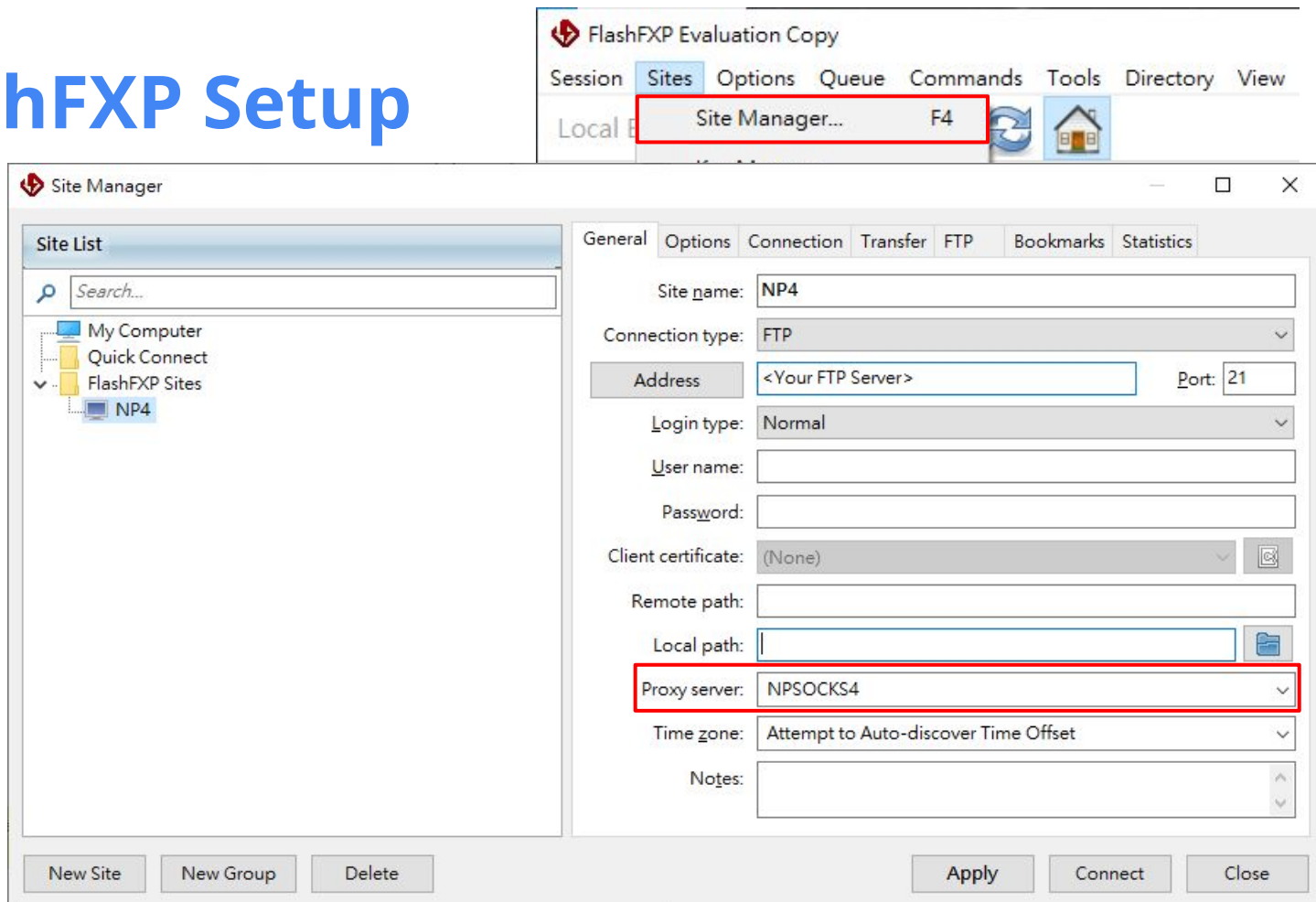
FTP Server / Client

- FTP Server
 - You should setup your own FTP server for testing
 - E.g., FileZilla Server
- FTP Client
 - We will use **FlashFXP** ([link](#)) as FTP client
 - The client has to support FTP Active Mode with Proxy on

FlashFXP Setup



FlashFXP Setup



SOCKS Server Messages

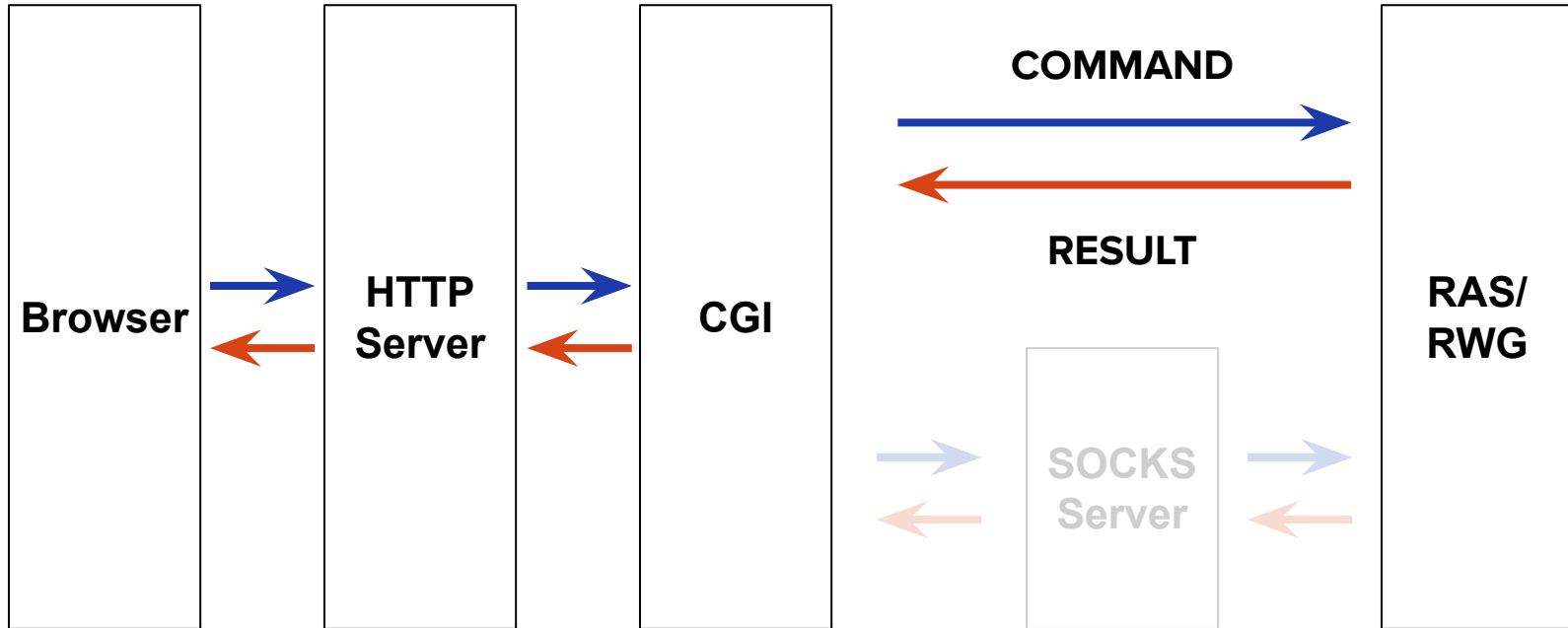
Your server should print messages in the following format:

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

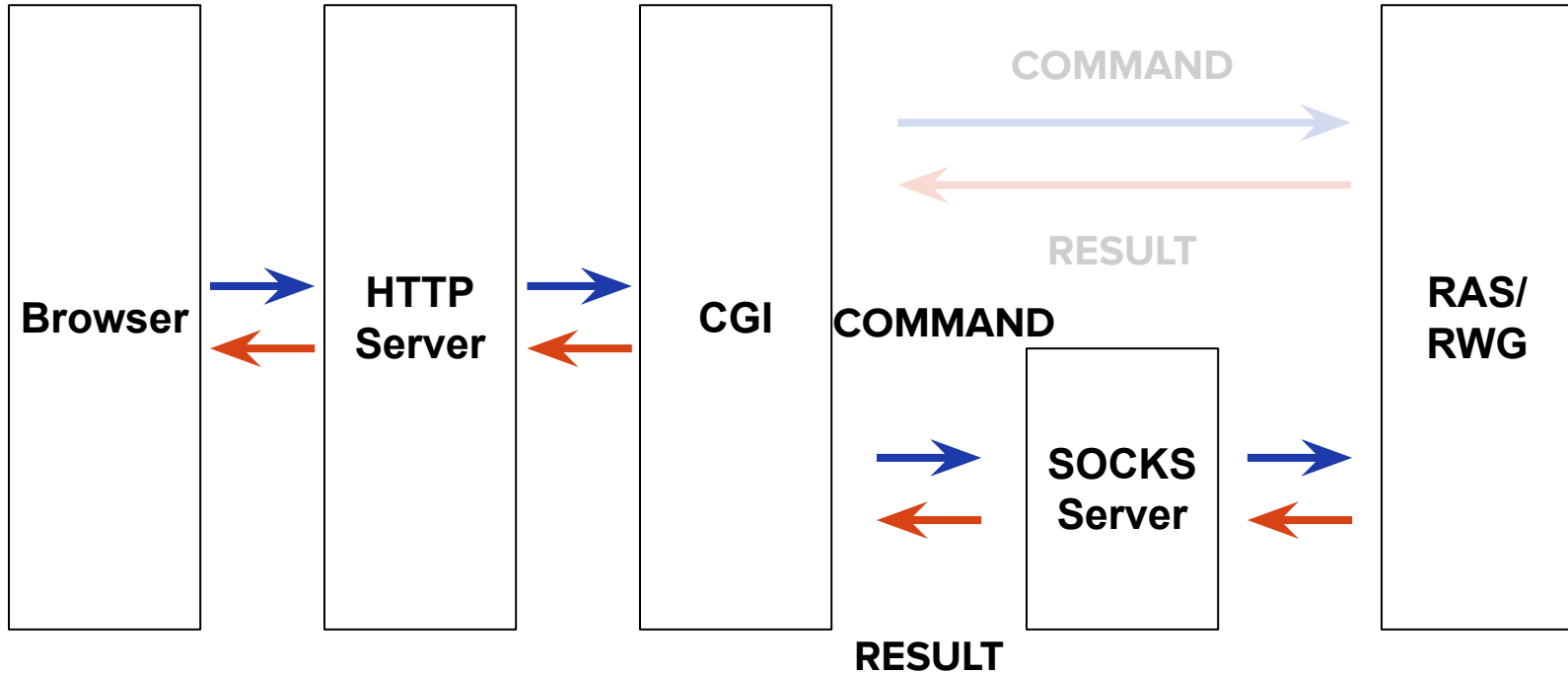
```
<S_IP>: 114.34.225.168  
<S_PORT>: 10089  
<D_IP>: 140.113.199.168  
<D_PORT>: 443  
<Command>: CONNECT  
<Reply>: Accept
```

III. CGI Proxy

CGI Connection (Project 3)



CGI Connection with SOCKS



panel_socks.cgi

NP Project 3 Panel

nplinux11.cs.nctu.edu.tw/~kuokt0404/panel_socks.cgi

#	Host	Port	Input File
Session 1	nplinux2 ▾ .cs.nctu.edu.tw	16677	t1.txt ▾
Session 2	nplinux2 ▾ .cs.nctu.edu.tw	16677	t2.txt ▾
Session 3	nplinux2 ▾ .cs.nctu.edu.tw	16677	t3.txt ▾
Session 4	nplinux2 ▾ .cs.nctu.edu.tw	16677	t4.txt ▾
Session 5	nplinux2 ▾ .cs.nctu.edu.tw	16677	t5.txt ▾
Socks Server	nplinux3 ▾ .cs.nctu.edu.tw	12345	

Run

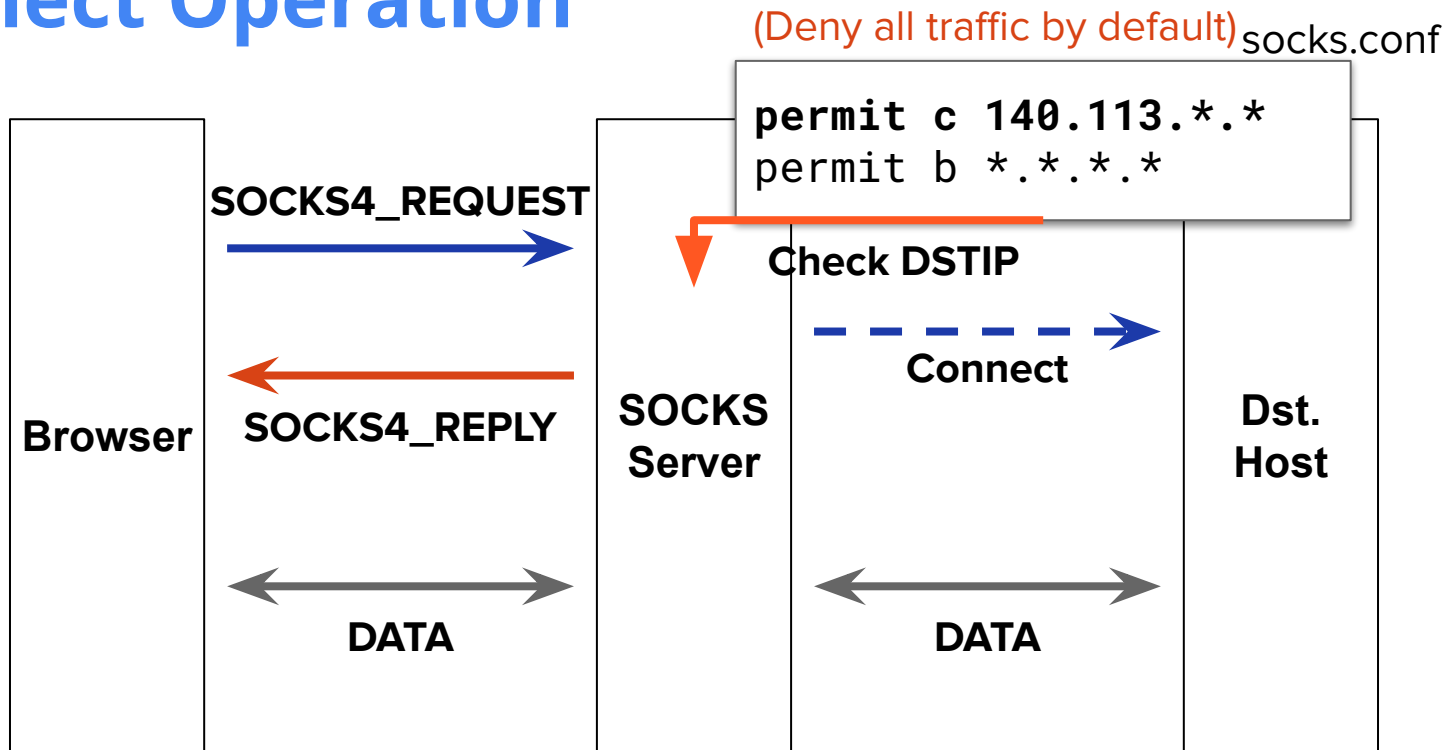
...&sh=nplinux3.cs.nctu.edu.tw&sp=12345

Details

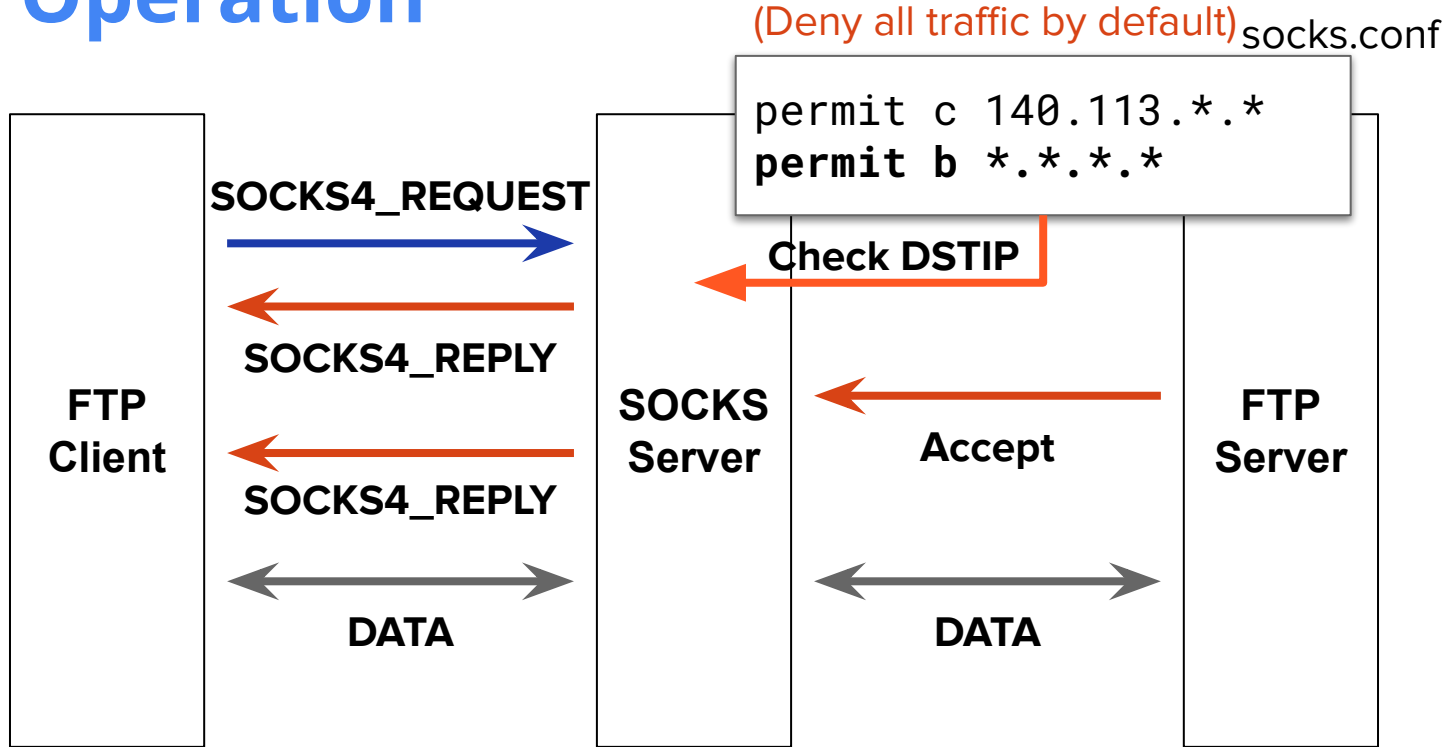
- Modify Project3 *console.cpp* to implement **SOCKS 4 client** (*hw4.cgi*)
 - In QUERYSTRING, there will be **sh=<SocksHost>&sp=<SocksPort>**
- *panel_socks.cgi* will be provided
- Testing steps
 - Close proxy setting of your browser
 - Put *test_case*, *panel_socks.cgi* and *hw4.cgi* in *~/public_html*
 - Run your **socks server** and ***np_single_golden*** on nplinux
 - Connect and run *panel_socks.cgi*
 - E.g., `nplinux2.cs.nctu.edu.tw/~<yourname>/panel_socks.cgi`
 - We had open a socks server on `nplinux[6-10].cs.nctu.edu.tw:8787`
 - You can test your *console.cgi* with this socks server

IV. Firewall

Connect Operation



Bind Operation



Reference

- [SOCKS 4](#)
- [SOCKS 4A](#)
- [Regular expressions library - cppreference.com](#)

Note

- You are **HIGHLY** encouraged to ask your questions on E3
- For personal problems, you can mail to all the TAs:
 - franklp97531@gmail.com
 - sciencethebird@gmail.com
 - pikachin.cs10@nycu.edu.tw
 - yoway.cs10@nycu.edu.tw