

SOCKU / 4A

SOCKS4A - Proxy Implementation - using - Boost.Aio

- 介紹 SOCKS4: A protocol for TCP proxy across Firewalls.

SOCKS是一種在防火牆主機上轉送(relay)TCP連線的協定，使應用程式使用者能透明地穿越防火牆。由於該協定與應用層無關，它可以作用於許多不同的服務，例如 telnet, ftp, finger, whois, gopher, WWW 等。對每個 TCP 連線的起始階段可以套用存取控制；之後，server 只是在 Client & application server 之間轉送資料，造成的處理負擔極低。因為 SOCKS 不需要知道任何應用層協定的 detail，它也可以容易支援使用加密來保護流量、避免被窺探的應用程式！

Why 該協定與應用層無關，它可以用於許多不同的服務？

⇒ SOCKS在TCP byte stream層面做relay，只關新目的IP/Port & 基本的存取控制，不解析上層協定內容；因此只要是走TCP的應用協定，都能把資料當作「透明的」byte stream，原封不动轉過去，自然就能支援很多服務！

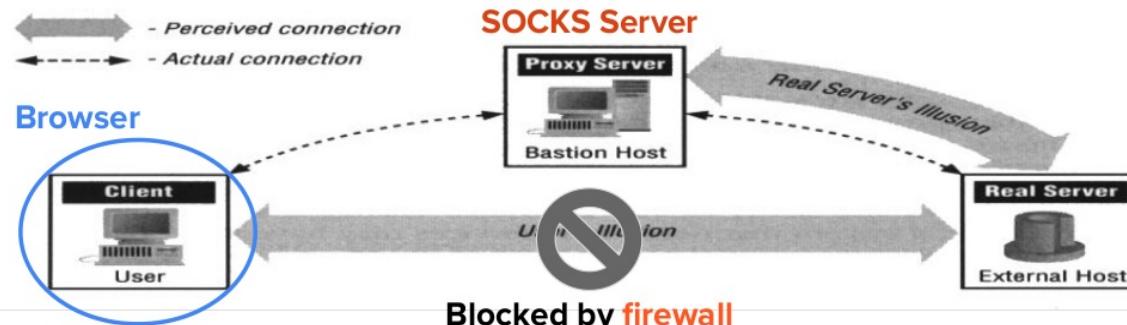
SOCKS定義了兩種操作：CONNECT & BIND

1. CONNECT

→ 當Client端想要與某個Application Server建立連線時，會先連上SOCKS Server並送出Request。

Connect Request

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

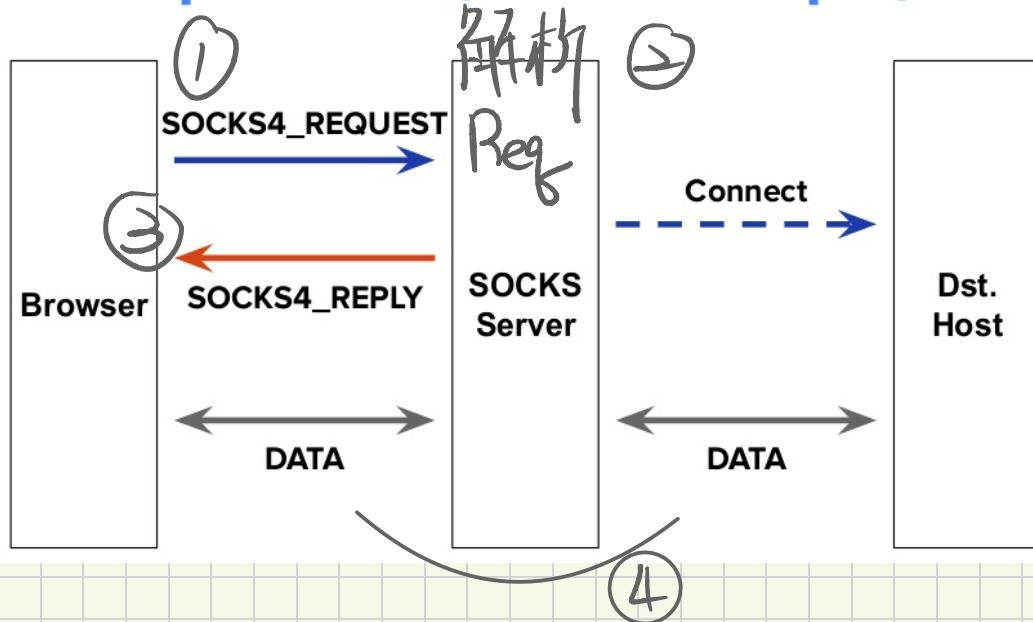


ref. proxy.ppt, p.2

1. CONNECT (cont.) Operation

⇒ Client 在請求封包中會包含目標主机的 IP address & port,
以及使用者 ID (userid)

Connect Operation (HTTP Example)



I. CONNECT (cont.) Request

· 封包格式

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

- VN: SOCKS protocol version num, 為 4 → SOCKS "4".
 - CD: SOCKS command code. CONNECT 請求時為 1.
 - NULL is a byte of all zero bits.

⇒ SOCKS Server 會依據 DSTPORT、DSTIP、USERID & 透過查詢 IDENT 可取得的資訊，來判斷是否核準該請求。

I CONNECT REPLY

→ 當連線建立完成，或是請求被拒絕 / 操作失敗時，Server 會回覆一個封包給 Client 端。

# of bytes:	1	1	2	4
	VN CD DSTPORT DSTIP			

• 封包格式

- VN is the version of the reply code & should be 0.
- CD is the result code
 - > 90: 請求允許.
 - > 91: 請求被拒絕 or 失敗.
 - 92, 93:

其他欄位在此回覆中可以被忽略！

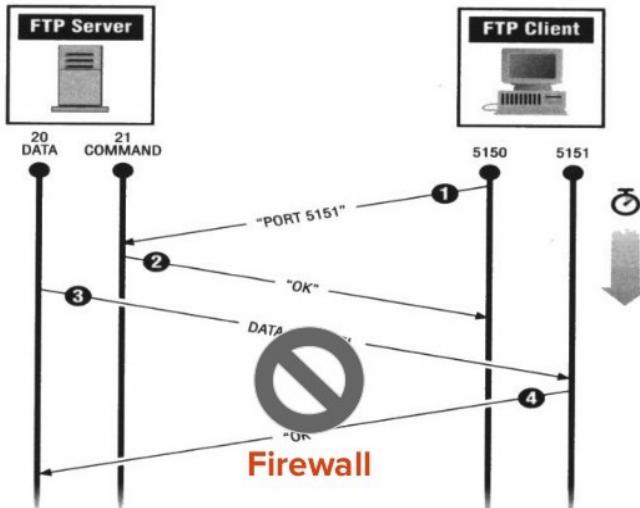
2. Bind Operation

Active Mode

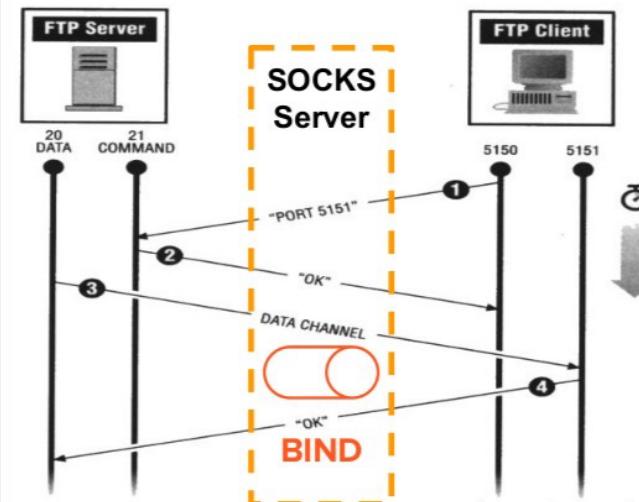
→當 Client 端想要為 Application Server 主動連入做準備時，會連到 SOCKS server 並送出 BIND 請求。這通常只會在已經透過 CONNECT 與 Application server 建立 primary connection 之後發生。

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.



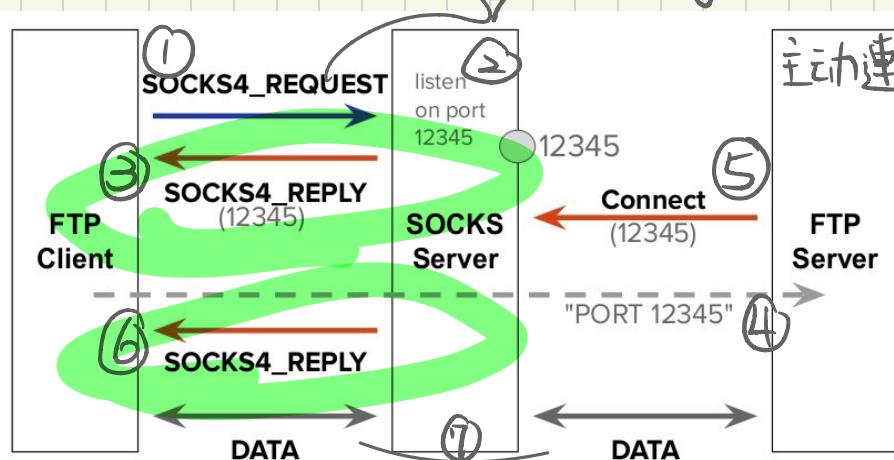
ref. services.ppt, p.13



ref. services.ppt, p.1

2.BIND Operation (cont.)

BIND Request



注！

BIND会有兩個回覆。
 First: 我已開始監聽，請通知
 對端來連。
 Second: 對端真的連上了，開始
 relay。

1. Client → SOCKS : 送出 BIND 請求, SOCKS 依規則決定是否允許.
2. SOCKS 建立一個「等待來連」的 socket (Ex. listen on the port 12345)
3. SOCKS → Client : 回覆第一次 SOCKS4_REPLY, 告訴 Client 建立的 port number.
4. Client → FTP Server : Client 透過 FTP 控制通道 送出 PORT <SOCKS_IP, 12345>, 通知 FTP Server 後去連 SOCKS 的 port 12345.
5. FTP Server → SOCKS : 主動來連 (Connect 12345). SOCKS 接收到來自 FTP Server 的連線後, 會比對來源 IP 是否與 Client 在 BIND 請求中指定的 DSTIP 相同!
6. SOCKS → Client : 回覆第二次 SOCKS4_REPLY !

BIND Request

• 封包格式

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

- VN: 4 → SOCKS4
- CD: 1 復寫 2, 代表 BIND Request.
- NULL is a byte of all zero bits.

⇒ SOCKS Server 會使用 Client 端提供的資訊決定是否允許該請求。

• SOCKS4 Reply (BLIND) 與 Connect 的 Reply 相同！

# of bytes:	1	1	2	4
	VN CD DSTPORT DSTIP			

• 封包格式

- VN is the version of the reply code & should be 0.
- CD is the result code
 - > 90: 請求允許
 - > 91: 請求被拒絕 or 失敗
 - 92, 93, ...

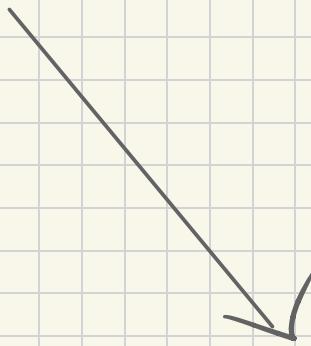
其他欄位在此回覆中可以被忽略！

(Cont.)

→ 被允許的請求 (CD=90), DSTPORT & DSTIP 欄位具有意義。在此情況下, SOCKS server 會取得一個用來等待傳入連線的 socket, 並把該 socket 的 port & IP 分別填入回覆中的 DSTPORT & DSTIP 傳回 Client。若回覆中的 DSTIP 為 0, Client 並應將其替換為它所連接之 SOCKS server 的 IP address。

When SOCKS Server 成功接收到来自 Application server 的预期連線, 会 Reply Second 封包, SOCKS Server 会检查連線來源主机的 IP address 是否與 client 在 BIND 請求中指定的 DSTIP 相符。若相符, 回覆 90, ebe, 91.

SOCK 4



SOCK 44

• SOCK4A: SOCK4 Protocol 的簡易擴充
⇒ 4A 旨在讓那些無法解析所有網域名稱的主機也能使用 SOCKS.

* 封包格式

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

4

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

4A

- ① 對 4A 來說, 若 Client 無法將目標主機的網域名稱解析成 IP address, 它應將 DSTIP 的前三位元組設為 0, 最後一個字元為非 0。Ex.: 0.0.0.1
- ② 在 USERID 結尾的 NULL 之後, Client 必須在封包中附上目標主機的網域名稱, 並以另一個 NULL 結尾。

SOCKS

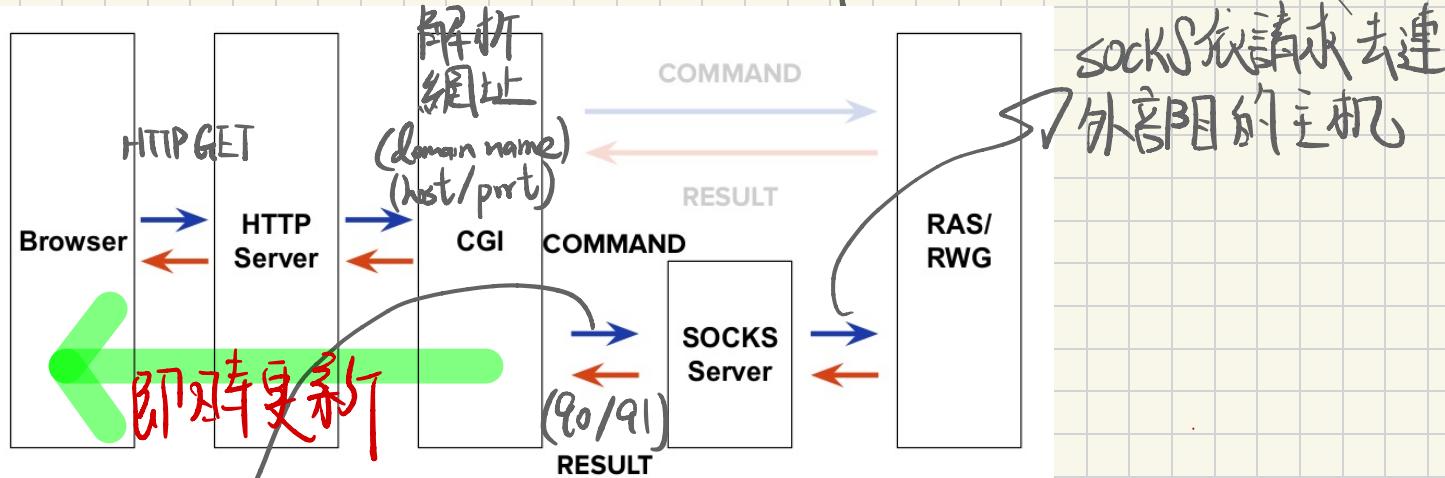
- **Free**
- de facto standard proxying package on the Internet.
- **Generic**
 - So, no intelligent logging or access control
- **Only works with TCP**
 - For UDP, use UDP Packet Relayer
- **Very popular**
- Components:
 - SOCKS Server
 - SOCKS client library for UNIX machines
 - ▶ e.g., Rconnect() for connect(), change Makefile
 - SOCKS-ified versions of several standard programs like FTP and Telnet.

C

G

T

CGI是在這之間扮演的角色？



依 Query string 解析到目標 host/port，主動連線到 SOCKS，送 Request.

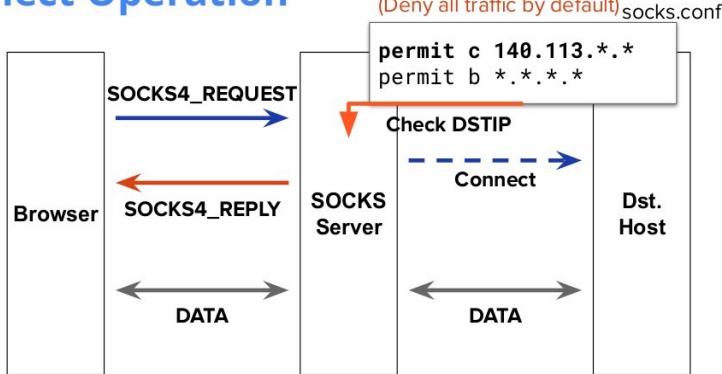
CGI (Common Gateway Interface)

是一種讓 Web server 能夠執行外部程式 (如 C 程式、Python 腳本、Perl 等) 的標準介面，這些程式通常用來產生動態網頁內容！

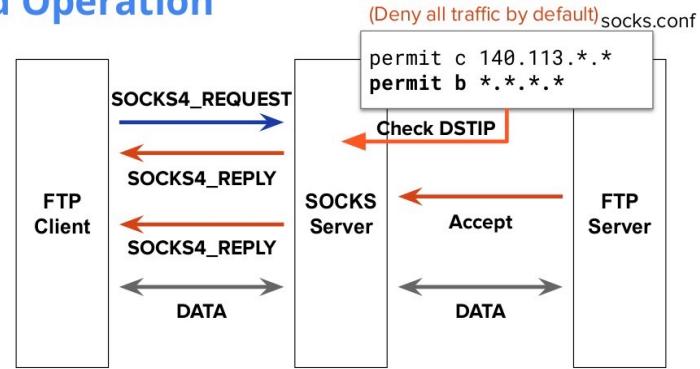
firewall

Firewall II

Connect Operation



Bind Operation



→ 寫一個 xx.conf 的規則檔，以 permit 為關鍵詞，b & c 代表 bind & connect 來解析。

- permit c 140.113.*.* 表示允許 Connect 140.113 網域。
- permit b *.*.*.* 表示允許啟動 BIND

