Internet Privacy Options

Networking

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 19 June 2014
Common/Reports/internet-privacy-options.tex, r892

Acronyms and Abbreviations

IP	Internet Protocol
ISP	Internet Service Provider
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over SSL
SSL	Secure Sockets Layer (same as TLS)
TCP	Transmission Control Protocol
TLS	Transport Layer Security (same as SSL)
Tor	The Onion Router
VPN	Virtual Private Network

Contents

What is the Internet?

Network

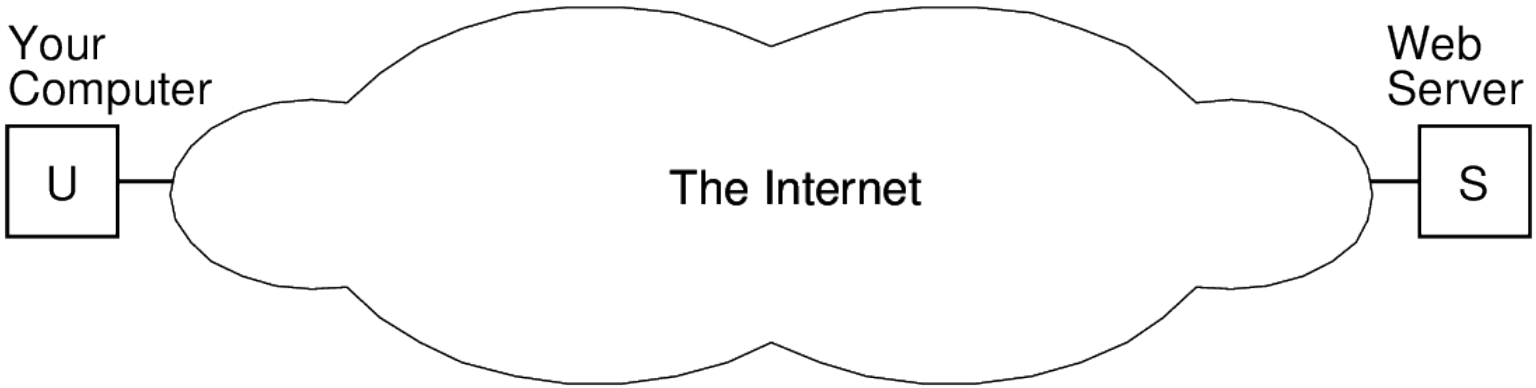
Collection of computer networks connected together using routers, where hosts and routers communicate using the Internet Protocol

- Access networks: connect to core networks; home, company LAN, mobile networks
- Core networks: connect to access networks and other core networks; run by ISPs, telecom companies

Applications

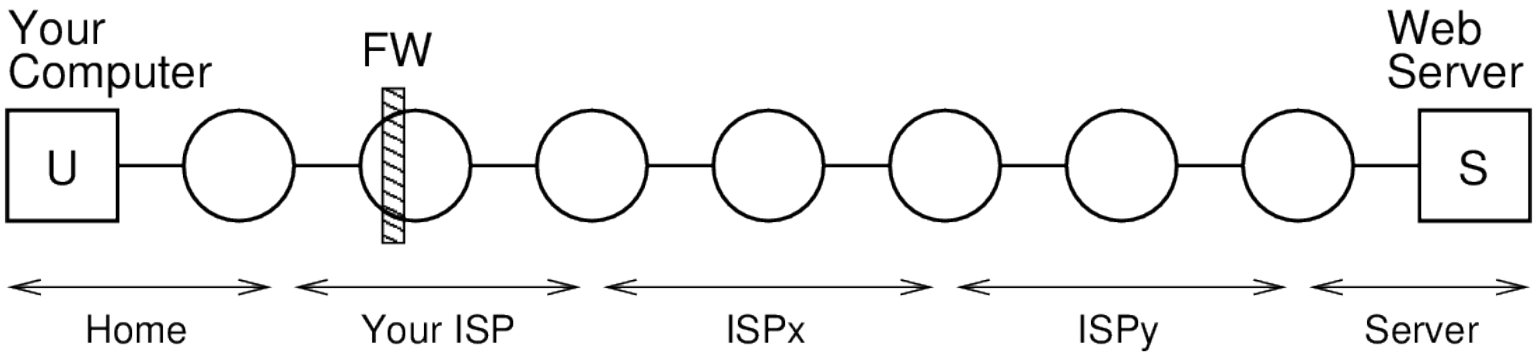
- Web browsing, email, instant messaging, voice and video calls, collaboration, audio/video streaming, games, ...

What does the Internet look like?



The Internet allows your computer to communicate with another computer (a web server)

What does the Internet look like?



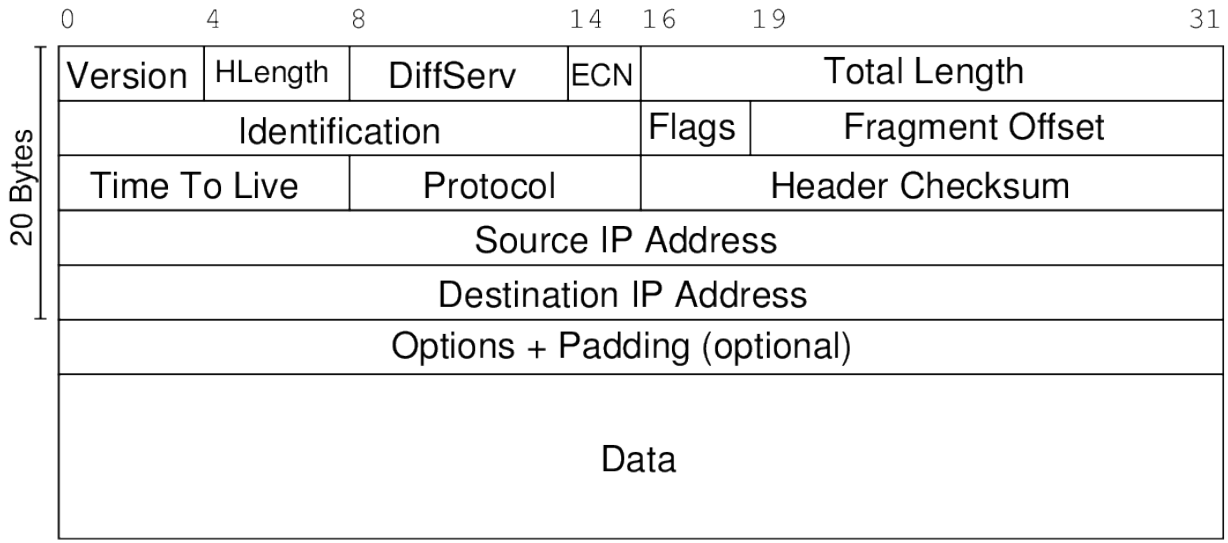
- Home computer connects via WiFi or LAN to ADSL router
- ADSL router connects via telephone cable to your ISPs router
- Your ISP connects to other ISPs and so on

How are computers identified in the Internet?

- IP addresses: 32 bits, often in dotted decimal notation
  - `106.187.46.22`, `61.91.8.94`, `203.131.209.82`
- Each host (computer, server) has a globally unique IP address
  - What about NAT and private addresses, e.g. `192.168.1.1`?
- Routers also have IP addresses
- Humans use domain names, e.g. `www.example.com`
- DNS maps domain name to IP address
  - `sandilands.info` → `106.187.46.22`
  - `ict.siit.tu.ac.th` → `203.131.209.82`

How does IP work?

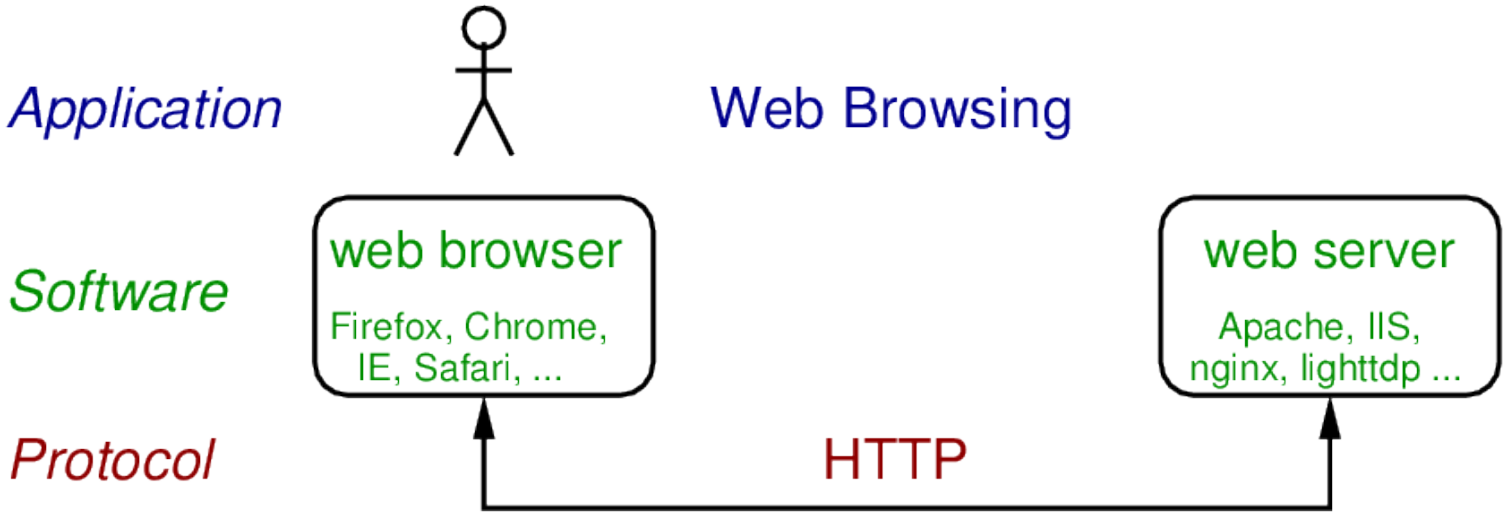
1. Your computer creates an IP packet
   - Source address: your computer; destination address: server



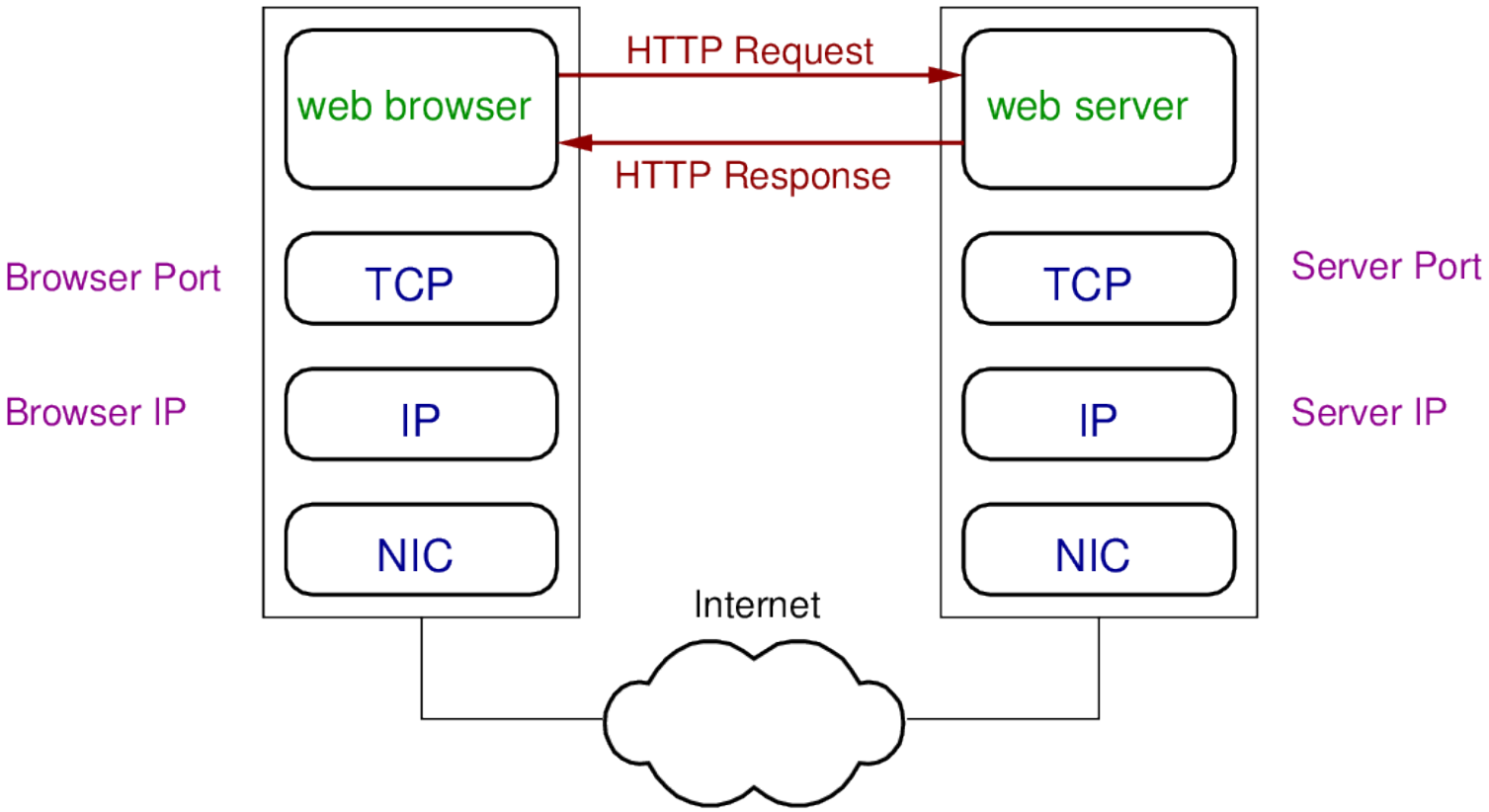
2. Sends IP packet to your local (default) router
3. Router forwards IP packet to next router, and so on
4. IP packet eventually arrives at destination

- Routing: finds the path of routers between source and destination, creates routing tables

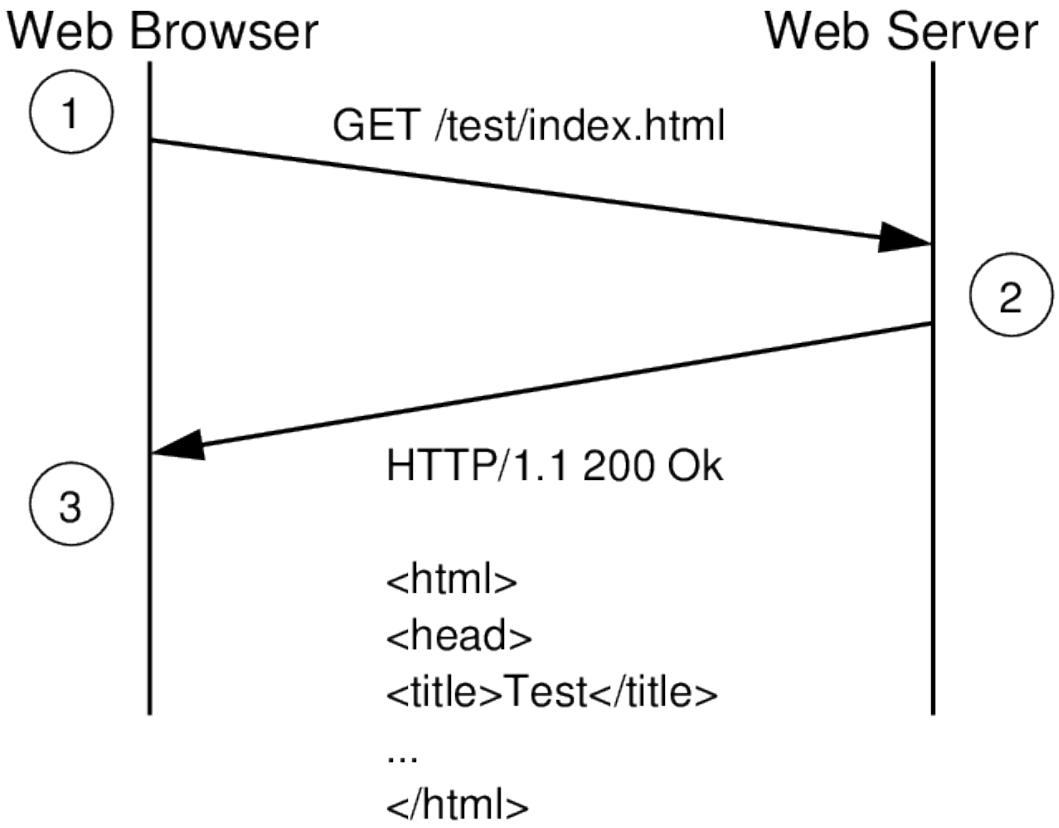
How does web browsing work?



How does web browsing work?



How does web browsing work?



Contents

Security in the Internet

- Internet security includes:
  - Confidentiality: keeping data secret (encryption)
  - User Authentication: ensuring the other entity is who they say they are (passwords, keys)
  - Data Integrity: ensuring fake/modified data is not accepted (encryption, signatures)
  - Privacy: keeping actions secret (?)
  - ...
- Terminology can be confusing:
  - Confidentiality = secrecy = data privacy
- Our focus: privacy of actions and confidentiality of data

Confidentiality and Privacy

Why keep data confidential?

- Competitors cannot steal your ideas and trade secrets
- Criminals cannot steal your money
- Employer/government/parents cannot see the information you are exchanging with others
- ...

Why keep actions private?

- Employer cannot determine you are looking for new job
- Whistle-blower cannot be identified
- People do not know your medical conditions
- Governments cannot determine if you are plotting against them
- ...

Some Common Requirements

Security

- I don't want anyone but the server to read my data
- I don't want others to know I am communicating with the server
  - During the communication
  - After the communication has taken place
- I don't want the server to be able to identify me
- I want to bypass blocks at a firewall

Convenience

- I want it free
- I want it easy to setup/use
- I want it to perform well

Contents

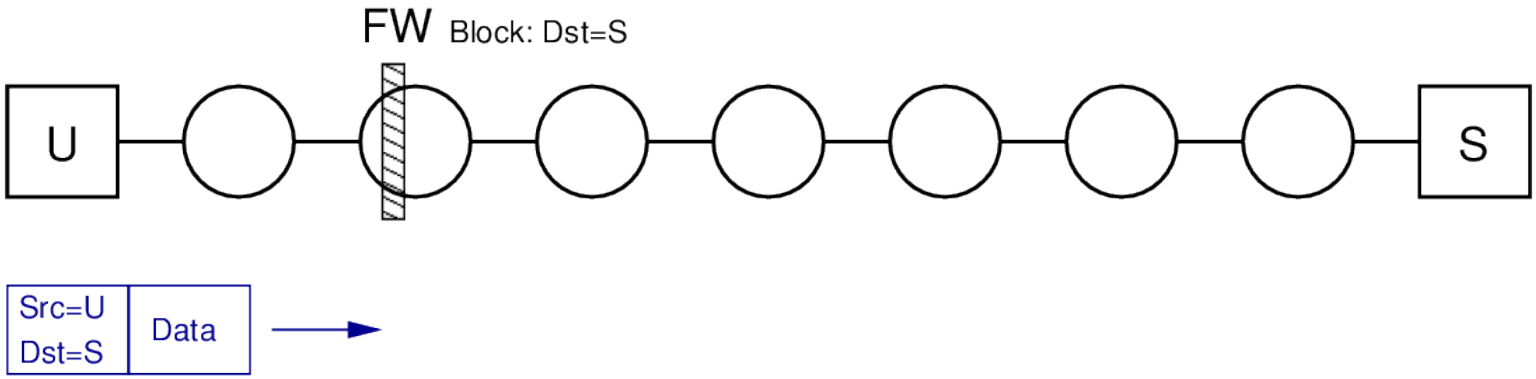
Assumptions

- Encryption algorithms are strong
- Path between you and a server is unpredictable, may change
- Computers (and users) uniquely identified by IP address
- Firewall blocks based on destination IP address

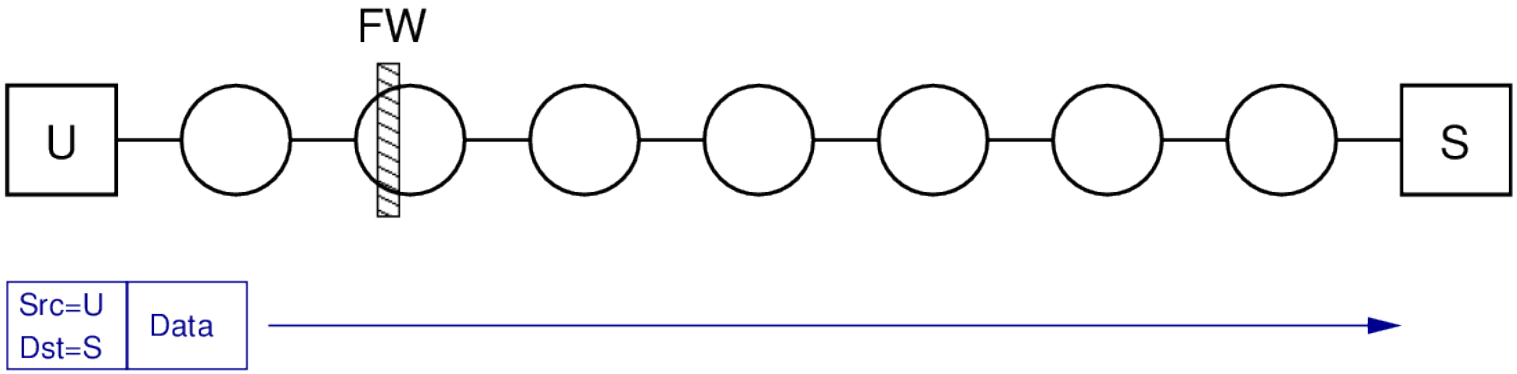
Notation and Terminology

U	You, your computer
S	(Web) Server (also *Srv*)
P	Proxy server
V	VPN server (also *VPN*)
E	Tor Exit Relay
T*x*	Tor Relay
FW	Firewall
Src	Source IP address
Dst	Destination IP address

Basic Browsing with HTTP (Firewall Enabled)



Basic Browsing with HTTP (No Firewall)



Firewall can see the server you are communicating with

Firewall can read the data

Server can identify you

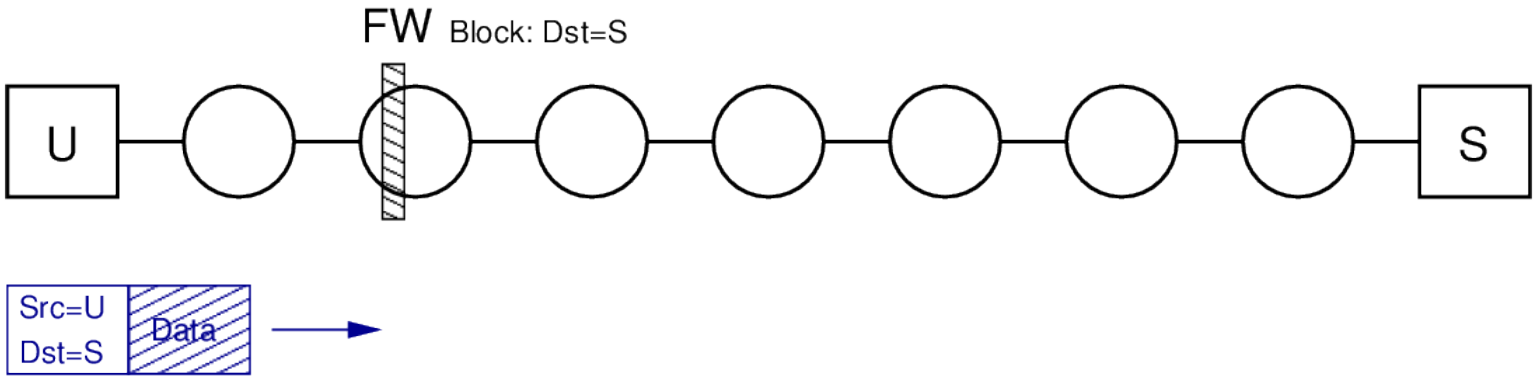
Others can see the server you are communicating with

Others can read the data

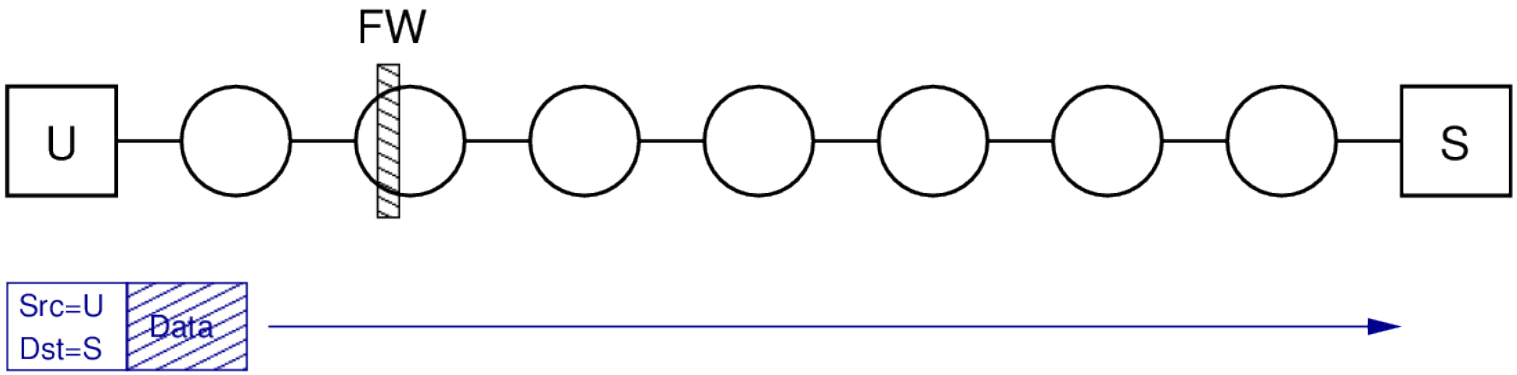
Confidentiality of Data when Browsing

- HTTPS: normal HTTP but using a secure transport (SSL/TLS)
- Encrypts data between browser and web server (both directions)
- Relies on certificates for distributing public key of web server
- Self-signed certificates or invalid certificates should not be trusted

Basic Browsing with HTTPS (Firewall Enabled)



Basic Browsing with HTTPS (No Firewall)



Firewall can see the server you are communicating with

Firewall cannot read the data

Server can identify you

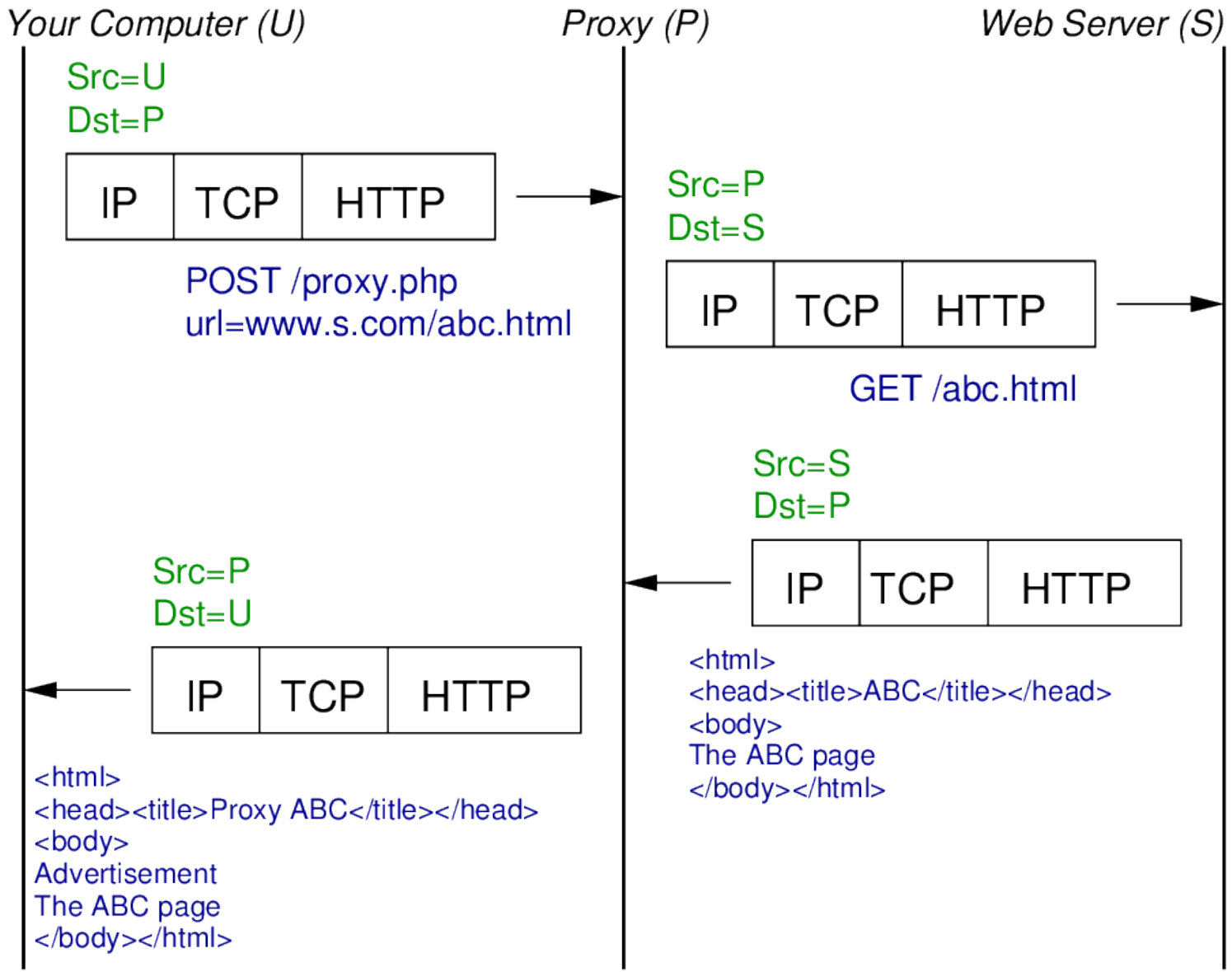
Others can see the server you are communicating with

Others cannot read the data

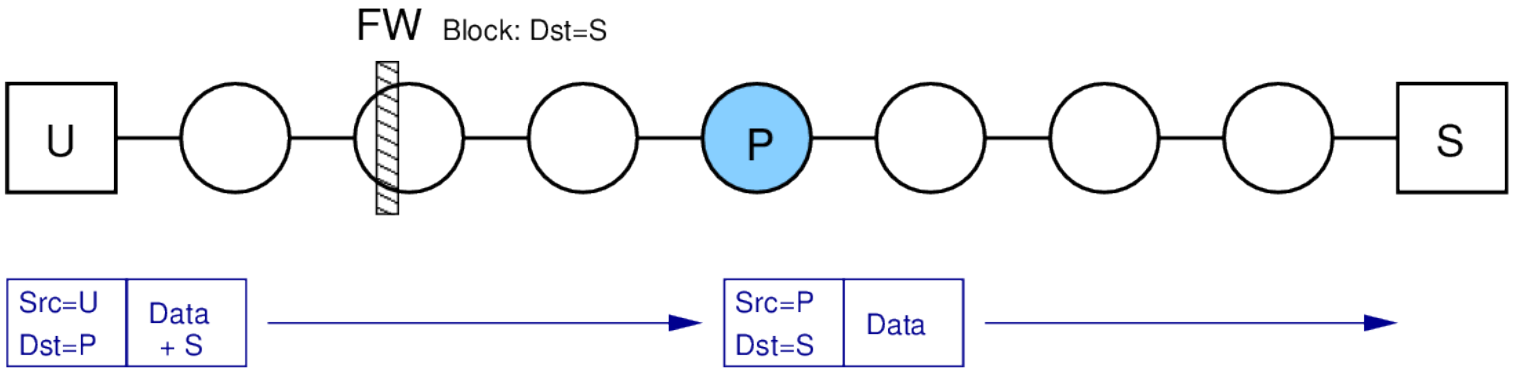
Web Proxy

- Website that sends HTTP request to web server on your behalf; HTTP response forwarded back to you
- Proxy web site provides form to enter URL of web server you want to visit
- Common usage models: free, ad-supported, pay per month

HTTP Exchange via Web Proxy



Proxy and HTTP



Firewall cannot easily see the server you are communicating with

Firewall can read the data

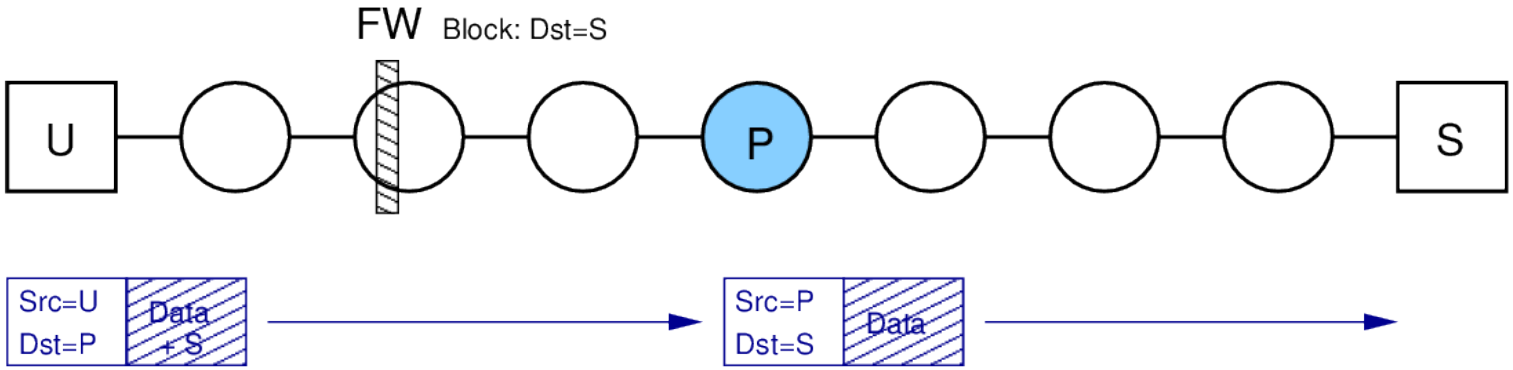
Server cannot identify you

Others cannot see the server you are communicating with

Others can read the data

Proxy can read data and knows who you are communicating with

Proxy and HTTPS



Proxy must decrypt then encrypt

Server cannot identify you

Firewall cannot easily see the server you are communicating with

Others cannot see the server you are communicating with

Firewall cannot read the data

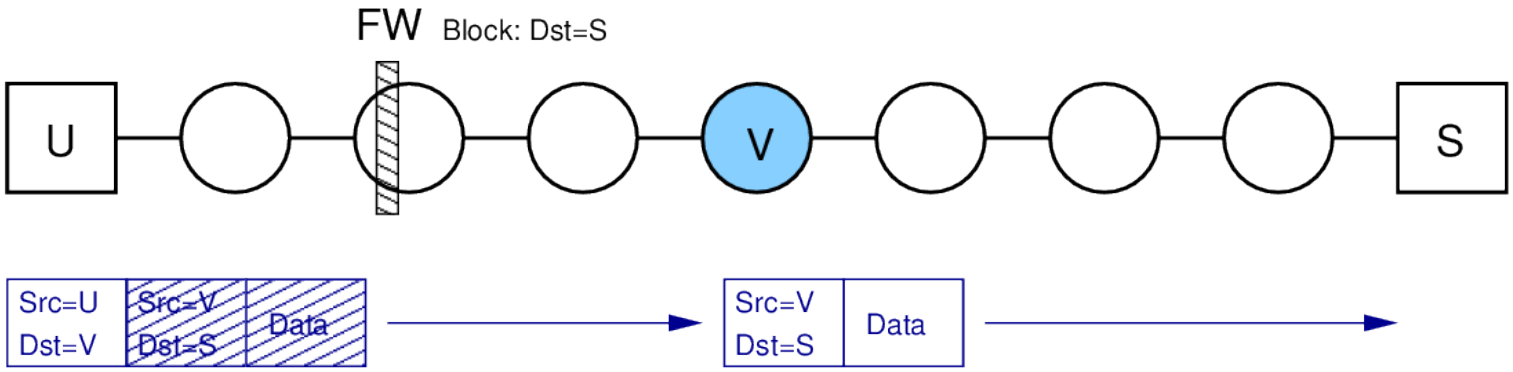
Others cannot read the data

Proxy can read data and knows who you are communicating with

Virtual Private Networks

- Tunnelling: packets at one layer are encapsulated into packets at the same or higher layer
- Encryption: tunnelling protocols usually also encrypt the inner packet
- Different VPN technologies:
  - Application layer: SSH (*)
  - Transport layer: TLS (OpenVPN)
  - Network layer: IPsec
  - Data link layer: PPTP, L2TP
- Create a virtual interface on your computer
  - (Inner) IP packets sent to virtual interface enter the tunnel
  - Tunnel encapsulates, encrypts the data and creates new (outer) IP packet
  - Outer IP packets sent via real interface

VPN and HTTP



Firewall cannot see the server you are communicating with

Server cannot identify you

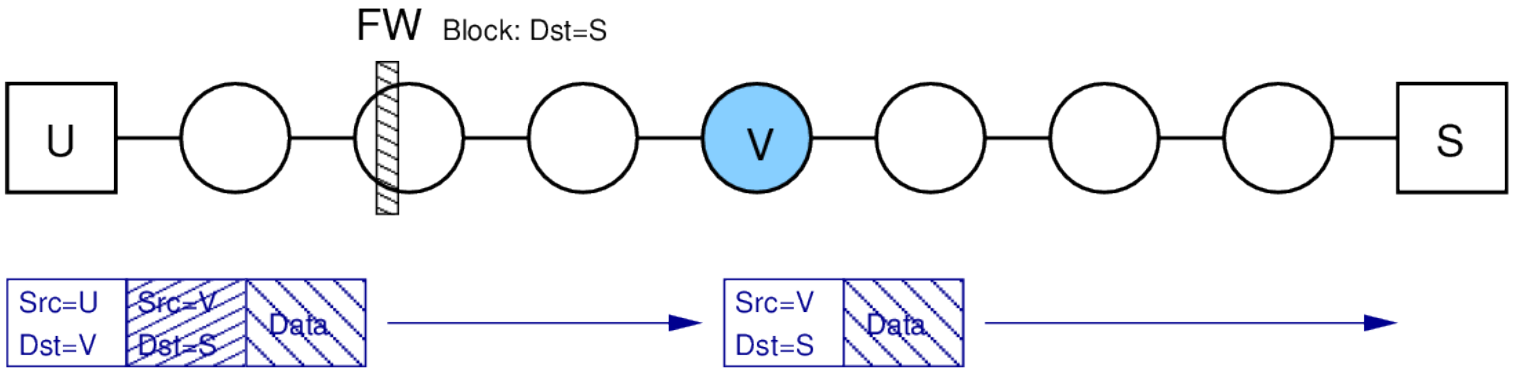
Others cannot see the server you are communicating with

Firewall cannot read the data

Others can read the data

VPN can read data and knows who you are communicating with

VPN and HTTPS



Server cannot identify you

Firewall cannot see the server you are communicating with

Others cannot see the server you are communicating with

Firewall cannot read the data

Others cannot read the data

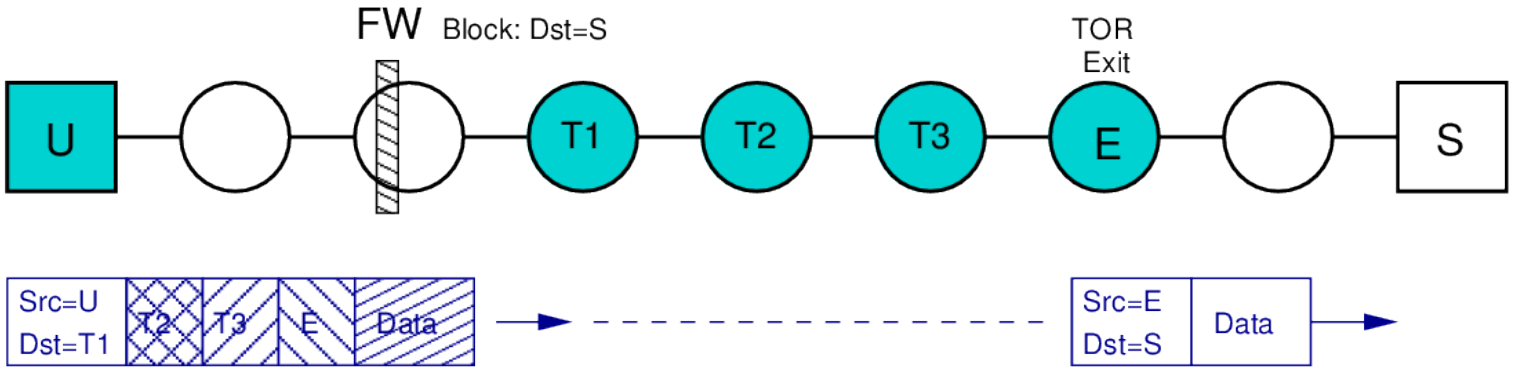
VPN cannot read the data

VPN knows who you are communicating with

Tor: The Onion Router

- Design for anonymous communications in public Internet
- Computers in Internet act as TOR relays
- Your computer selects set of relays to send via to reach TOR exit node
- SSL encryption used between each TOR node
- Keys exchanged so TOR node can decrypt receive packet and knows next TOR node to send to
- A TOR node only knows the previous TOR node and next TOR node in path
  - Doesn't know original source or final destination
- TOR exit node sends received packets across normal Internet

Tor and HTTP



Firewall cannot see the server you are communicating with

Server cannot identify you

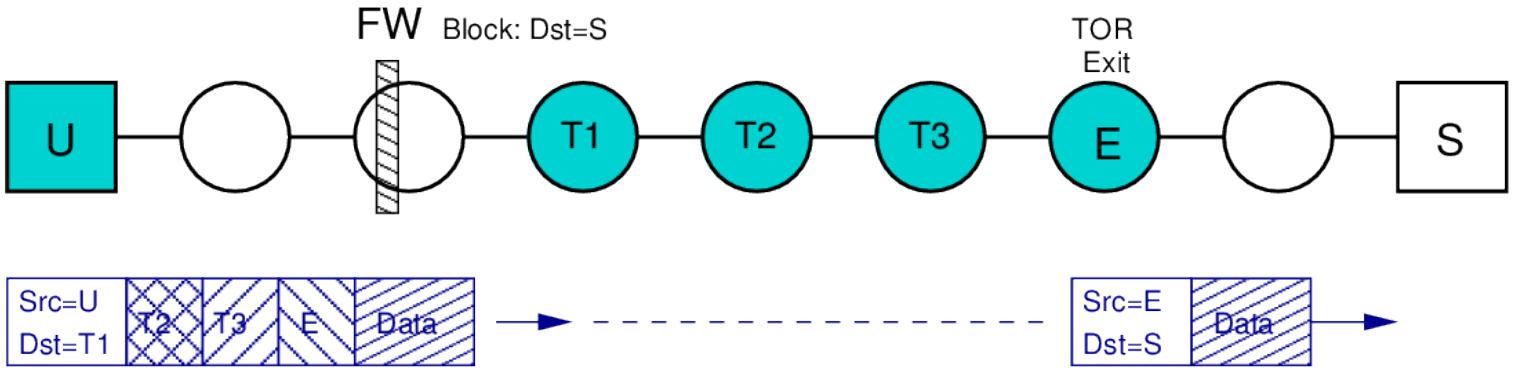
Others cannot see the server you are communicating with

Firewall cannot read the data

Others can read the data

TOR Exit node can read data
TOR Exit node does not know who you are communicating with

Tor and HTTPS



Server cannot identify you

Firewall cannot see the server
you are communicating with

Others cannot see the server
you are communicating with

Firewall cannot read the data

Others cannot read the data

TOR Exit node cannot read data
TOR Exit node does not know who you are communicating with

Comparison of Privacy Techniques

		Data Secrecy	Bypass Firewall	Network Privacy	Server Privacy	Log Analysis	Cost	Usage	Perf.
Basic	HTTP	✗	✗	✗	✗	ISP/Server	Free	Default	Best
	HTTPS	✓	✗	✗	✗				
Proxy	HTTP	✗	✓	✓ Proxy?	✓	ISP/Server + Proxy	Free Ads $2/mth	Browser	Depends on Proxy
	HTTPS	✗ Proxy?	✓	✓ Proxy?	✓				
VPN	HTTP	✓ You–VPN ✗ VPN–Srv	✓	✓ VPN?	✓	ISP/Server + VPN	Free Ads $5/mth	OS setup or software install	Depends on VPN
	HTTPS	✓	✓	✓ VPN?	✓				
TOR	HTTP	✓ You–Exit ✗ Exit–Srv	✓	✓	✓	?	Free	Software install	Depends on TOR nodes
	HTTPS	✓	✓	✓	✓				

Comparison of Tunnelling Protocols

	SSH	OpenVPN	PPTP	L2TP/IPsec
VPN Client Availability	App available for most OS's OpenSSH, PuTTY	OpenVPN app available for most (mobile) OS's	Built in most OS	Built in most OS
Application Support	Only works for some apps	All apps	All apps	All apps
VPN Server Setup	Easy to install	Complex setup, usage increasing	Easy setup, widely installed	Medium setup, widely installed
Encryption, Authentic.	Strong	Strong	Weak	Strong
Overhead, Processing	Medium	Low	Low	Medium
Protocols, Ports	TCP 22	UDP 1194 TCP 443	TCP 1723 GRE	UDP 50, 1701 IPsec

Contents

Network Address Translation (NAT)

- We assumed: computers uniquely identified by IP address
- Many access networks use NAT:
  - Computers assigned private IP address
  - Access network assigned single public (globally unique) IP address
  - NAT keeps maps private IP to unique public IP and port pairs
- Server privacy: NAT may help (server identifies your network, but not your specific computer)
- Network privacy: NAT operator often the entity trying to hide from
- Easy for NAT operator to identify you from your private IP

Firewalls and Deep Packet Inspection (DPI)

- We assumed: firewall blocks based on IP address only
- If your computer sends to an unblocked destination, can bypass firewall
- Firewalls may block based on other info: ports, protocols, application data
- If firewall "read" the HTTP GET Request or HTML in the HTTP Response, then it may block content even if IP is accepted
- Inspect the details of each packet can be very slow