

# Computer and Network Security

## Lecture 24: Anonymity & Censorship

COMP-5370/6370  
Fall 2025





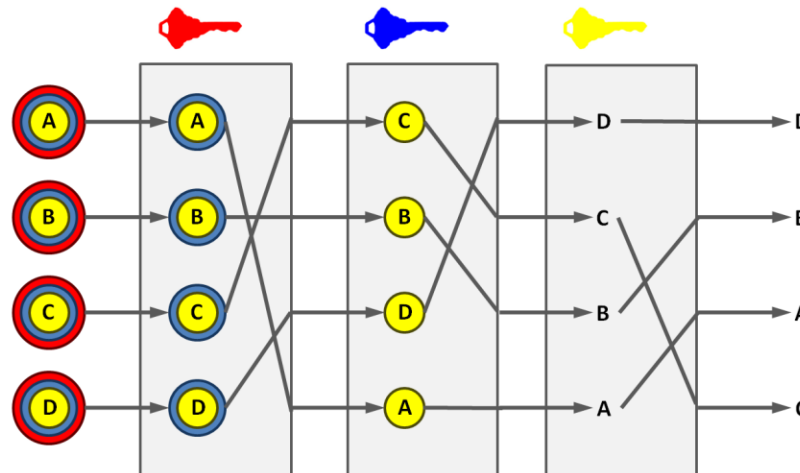
A **Virtual Private Network (VPN)** is a *logical* concept through which a remote client appears on the local network by use of a multiplexed secure channel.

- Many different protocols can be used
- IKE+IPSec is a common implementation
- Can connect two remote-networks as 1
- Can be used on a client-server construction

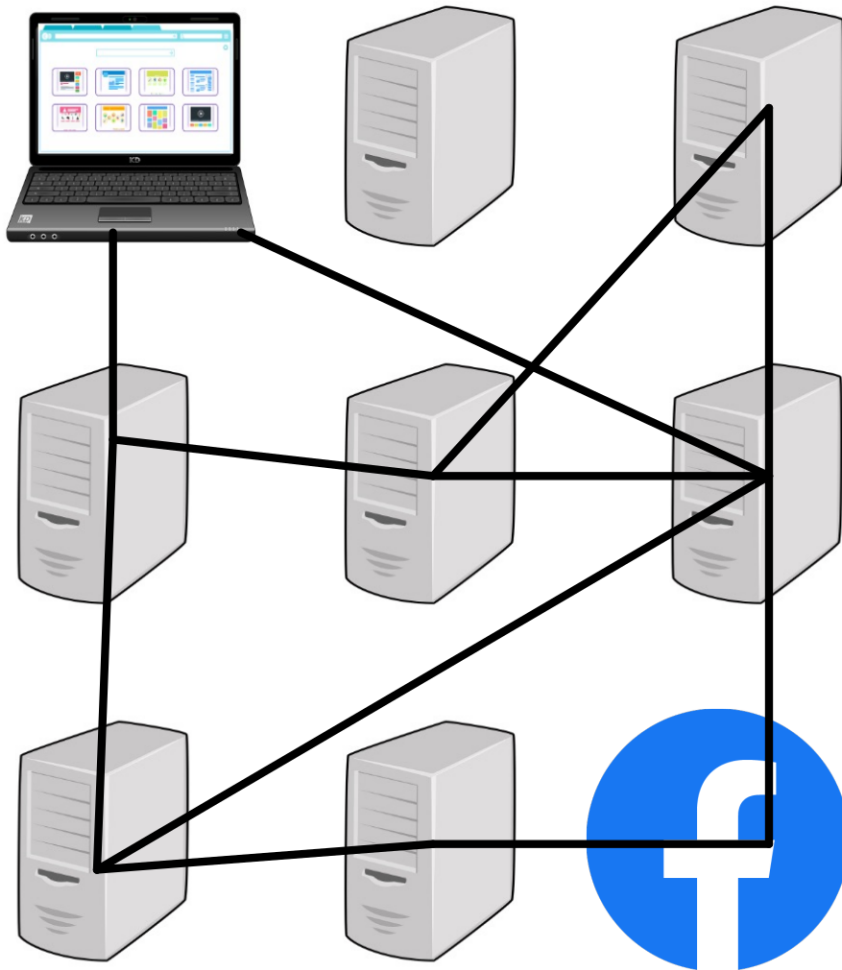
# Mix Networks



**Mix Networks (Mix-Nets)** are a type of high-latency anonymous network which relies on bounces among nodes with other messages for protections.

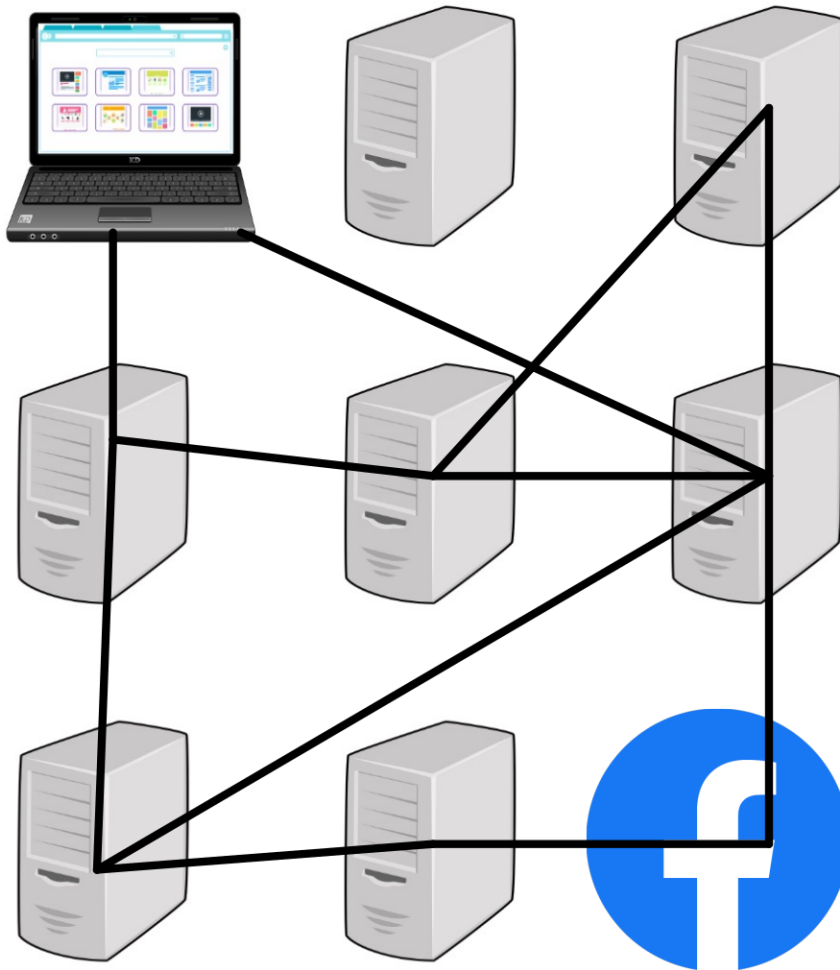


# Mix-Nets



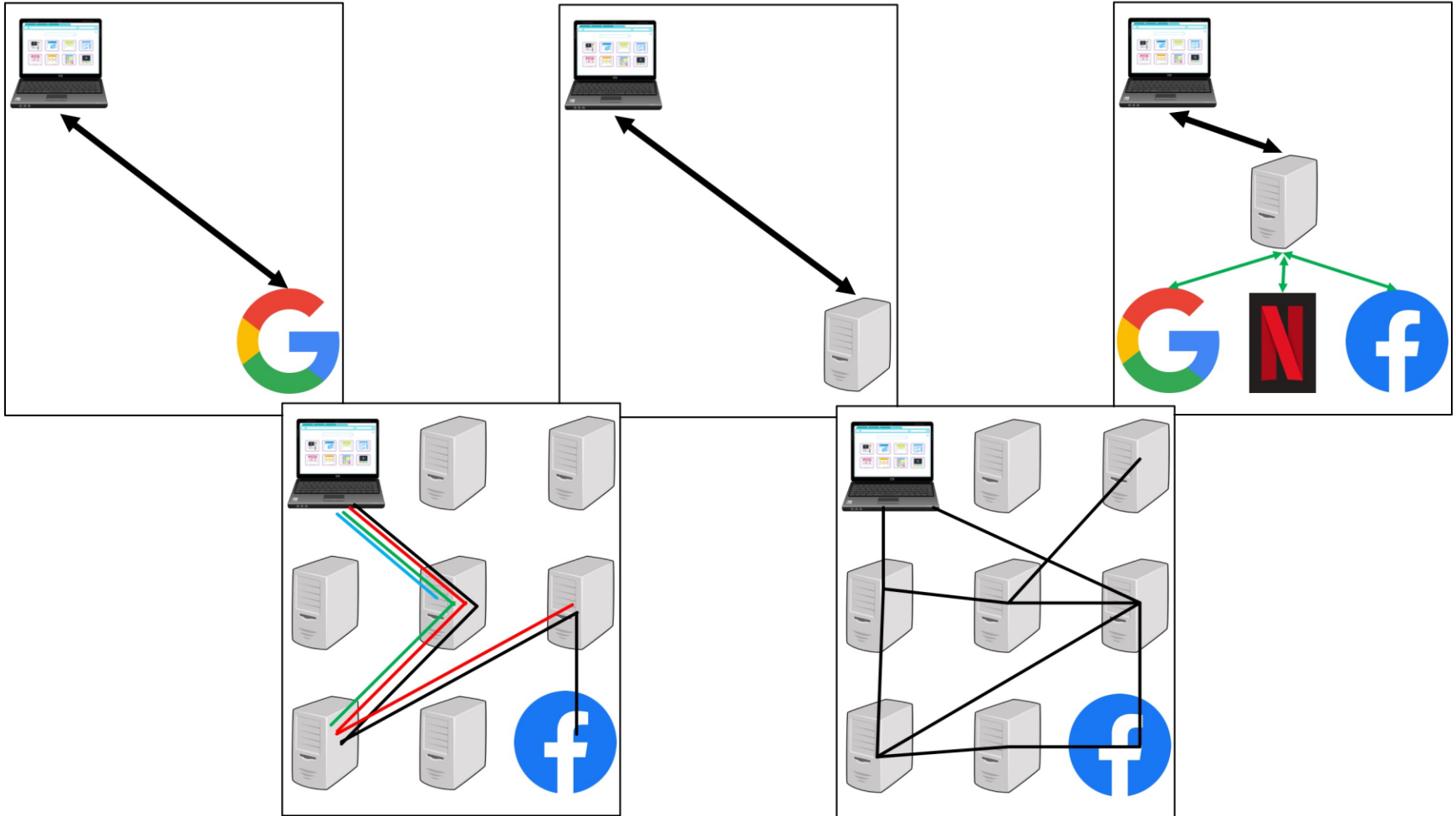
- Client sends message to network
- Nodes delay random amount of time
- Nodes sends random selection of nodes
- Repeat

# Mix-Net Downsides



- Extremely Slow
- Require large networks and high through-put
- Non-linear scaling

# Different Protocols for Different Needs



# Censorship



**Censorship** is the suppression of access to information that is deemed harmful for the perceived advancement of the *greater good*.



**What are examples  
data/information which SHOULD  
or SHOULD NOT be censored?**

# OK to Censor?



## Widely Accepted

- Pornography (setting)
- Abusive Content
- Malicious C2 nodes

## Widely Rejected

- Negative publicity
- Scientific research
- Different opinions

## More Complicated

- Culturally insensitive content
- Intentionally fake/misleading content
- Anything not yet approved
  - White-list instead of black-list

# Censorship



**Censorship** is the suppression of access to information that is deemed harmful for the perceived advancement of the *greater good*.

- Sometimes called “network interference” to avoid the connotation of “censorship”
- Often associated with *authoritarian* actors but goals and approaches are common

# Anonymity



**Anonymity** is the *concept* that any piece of information can not be tied to a real-world identity which it describes.

- Lots and lots of trade-offs when adding

# Anonymity



**Anonymity** is the *concept* that any piece of information can not be tied to a real-world identity which it describes.

- Lots and lots of trade-offs when adding
- Lots of techniques but many are far-less useful than they appear



**Anonymity** is the inability to connect an actor's actions to their identity

**Is that a good thing?**

- Prevents retaliation for actions
- Prevents holding accountable for actions
- Allows speech that is forbidden

# Censorship



**Censorship** is the suppression of access to information that is deemed harmful for the perceived advancement of the *greater good*.

- Sometimes called “network interference” to avoid the connotation of “censorship”
- Often associated with *authoritarian* actors but goals and approaches are common



# **Where does censorship exist in the real-world?**

- Who is the censor?
- Who is being censored?
- What is being censored?

# Censors are Rational Actors

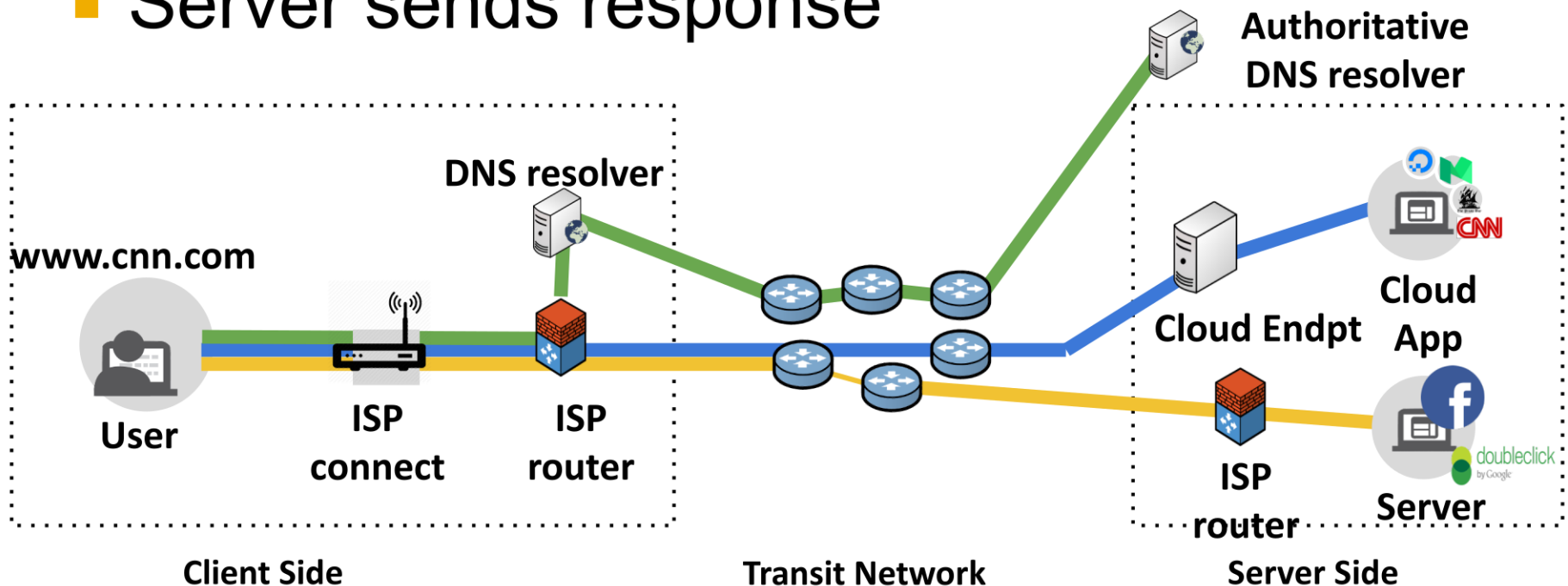


- In almost all cases, censors understand how their actions will be perceived
  - By those who are censored
  - By the censor's "peers"
- Censorship still exists because the censors decide that the *trade-off* is worth the optics & dislike



# How to Fetch a Website

- User types `www.cnn.com`
- Dereferences to an IP via DNS
- Browser makes request
- Server sends response



# Client-Side Compliance



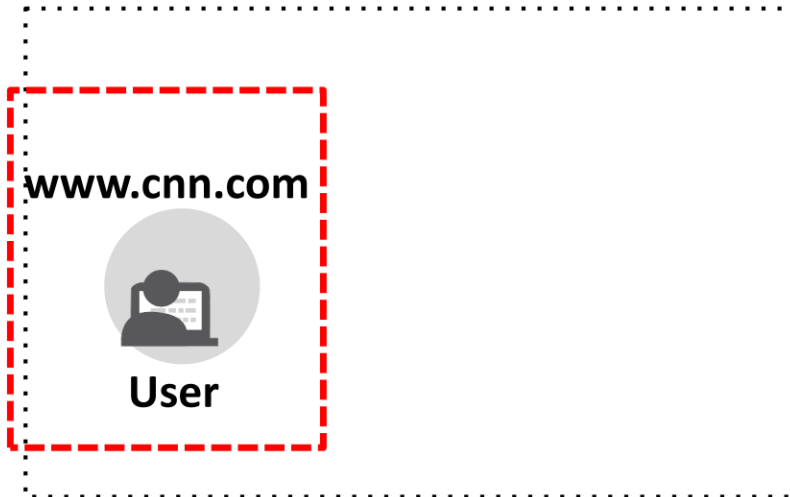
- Software installed on user-device to block access to content



# How to Fetch a Website

- User types `www.cnn.com`
- ~~Dereferences to an IP via DNS~~
- ~~Browser makes request~~
- ~~Server sends response~~

OS  
rejects



Client Side

# Client-Side Compliance



- Software installed on user-device to block access to content
- Easy to implement and easy to defeat
  - Don't install
  - Uninstall
  - Mimic
  - ...

# Infrastructure Compliance



Table 2. ASes that contain filtering devices

| AS Number       | AS Name                    | Number of Filtering Interfaces |
|-----------------|----------------------------|--------------------------------|
| Border ASes     |                            | 481                            |
| 4134            | CHINANET-BACKBONE          | 374                            |
| 4812            | CHINANET-SH-AP             | 9                              |
| 4837            | CHINA169-BACKBONE CNCGROUP | 82                             |
| 9929            | CNCNET-CN                  | 4                              |
| 4538            | ERX-CERNET-BKB             | 4                              |
| 9808            | CMNET-GD                   | 5                              |
| 9394            | CRNET                      | 3                              |
| Non-border ASes |                            | 14                             |
| 23650           | CHINANET-JS-AS-AP          | 4                              |
| 17785           | CHINATELECOM-HA-AS-AP      | 4                              |
| 37943           | CNNIC-GIANT                | 3                              |
| 38356           | TIMENET                    | 1                              |
| 17633           | CHINATELECOM-SD-AS-AP      | 1                              |
| 4813            | BACKBONE-GUANGDONG-AP      | 1                              |

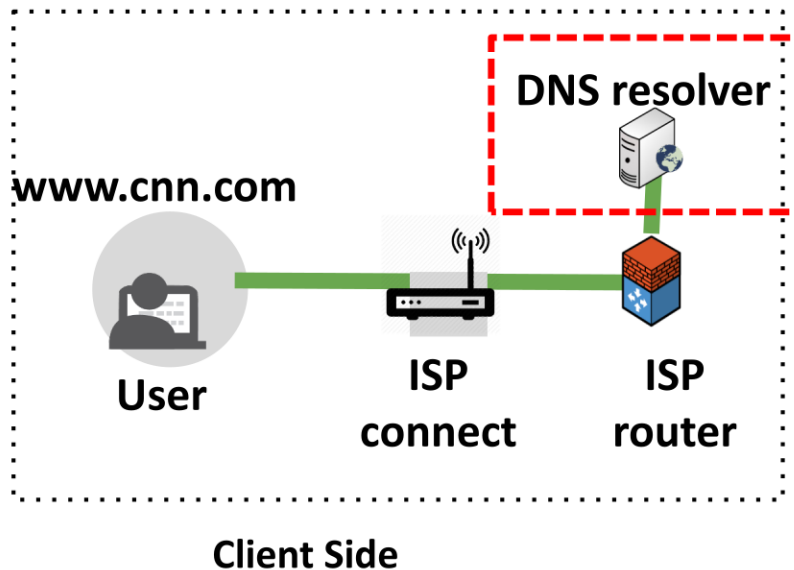
- Require ISP and telco-providers to censor traffic
- Censor creates requirements and delegate enforcement
  - *I don't care how you do it but you must not allow access to ...*



# How to Fetch a Website

- User types `www.cnn.com`
- Dereferences to an IP via DNS
- ~~■ Browser makes request~~
- ~~■ Server sends response~~

ISP gives  
wrong IP



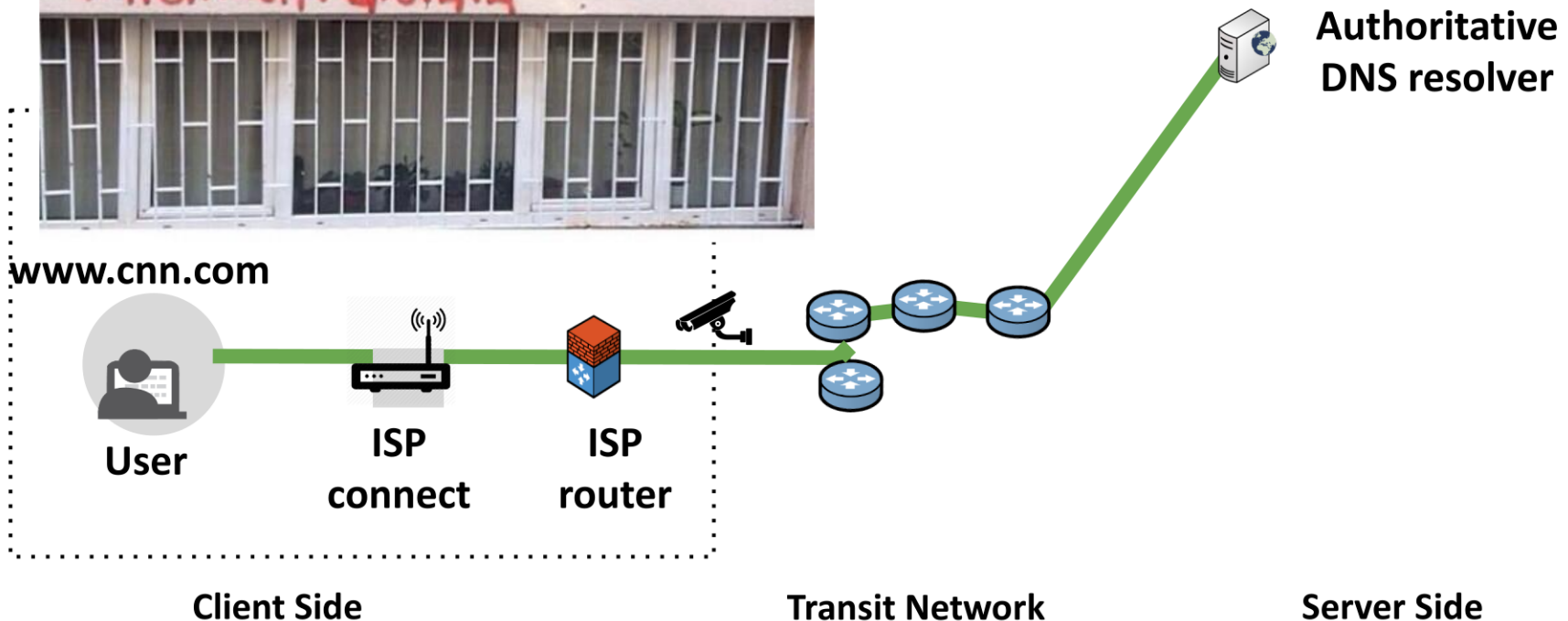
## Thou Shalt Not Allow:

- `*.cnn.com`
- `*.google.com`
- `*.facebook.com`
- ...

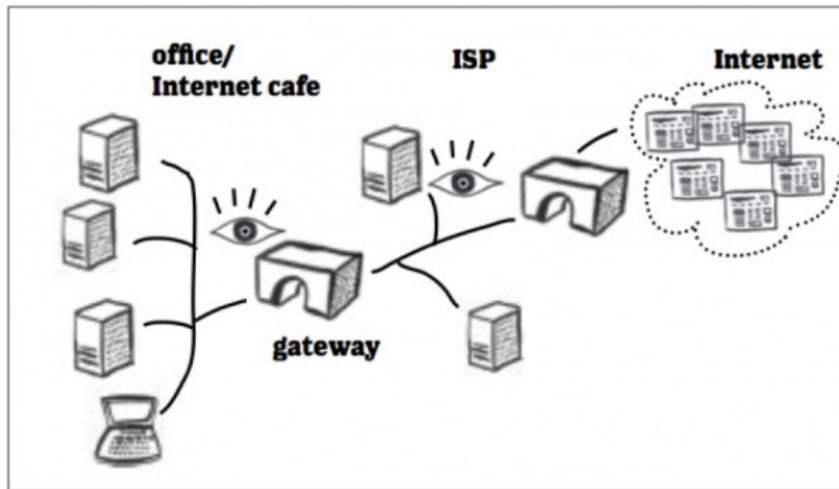
# Trusted DNS Servers



- Manually configure DNS to non-censored server directly

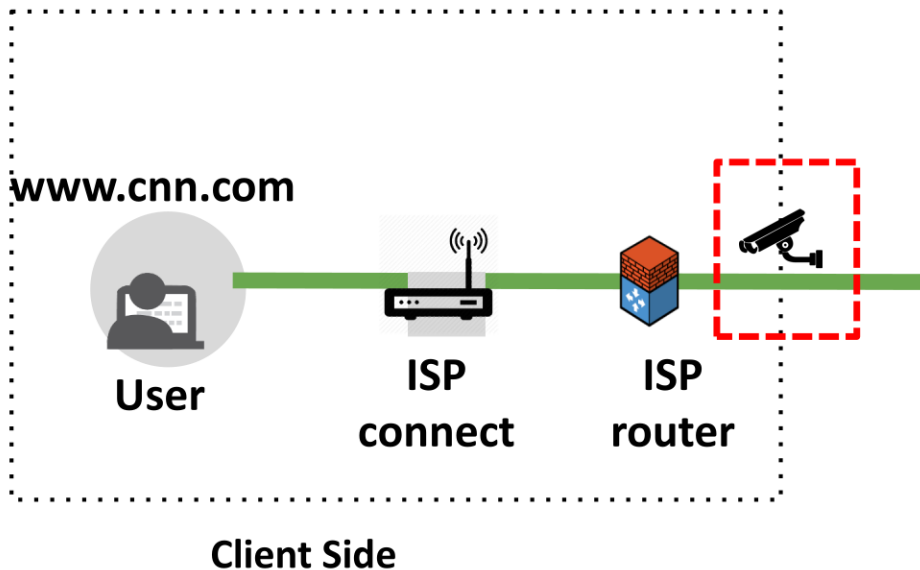
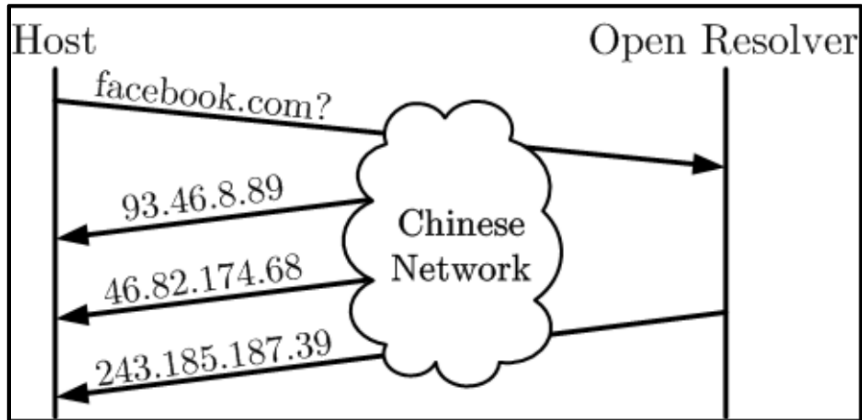


# Infrastructure Enforcement



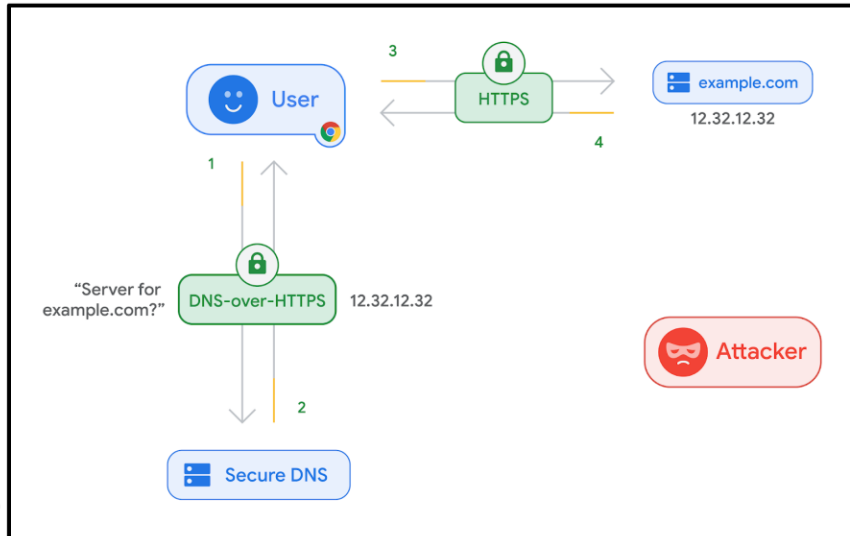
- Require ISP and telco-providers to provide on-path access
- Censor deploys own implementation to block access

# DNS Injection

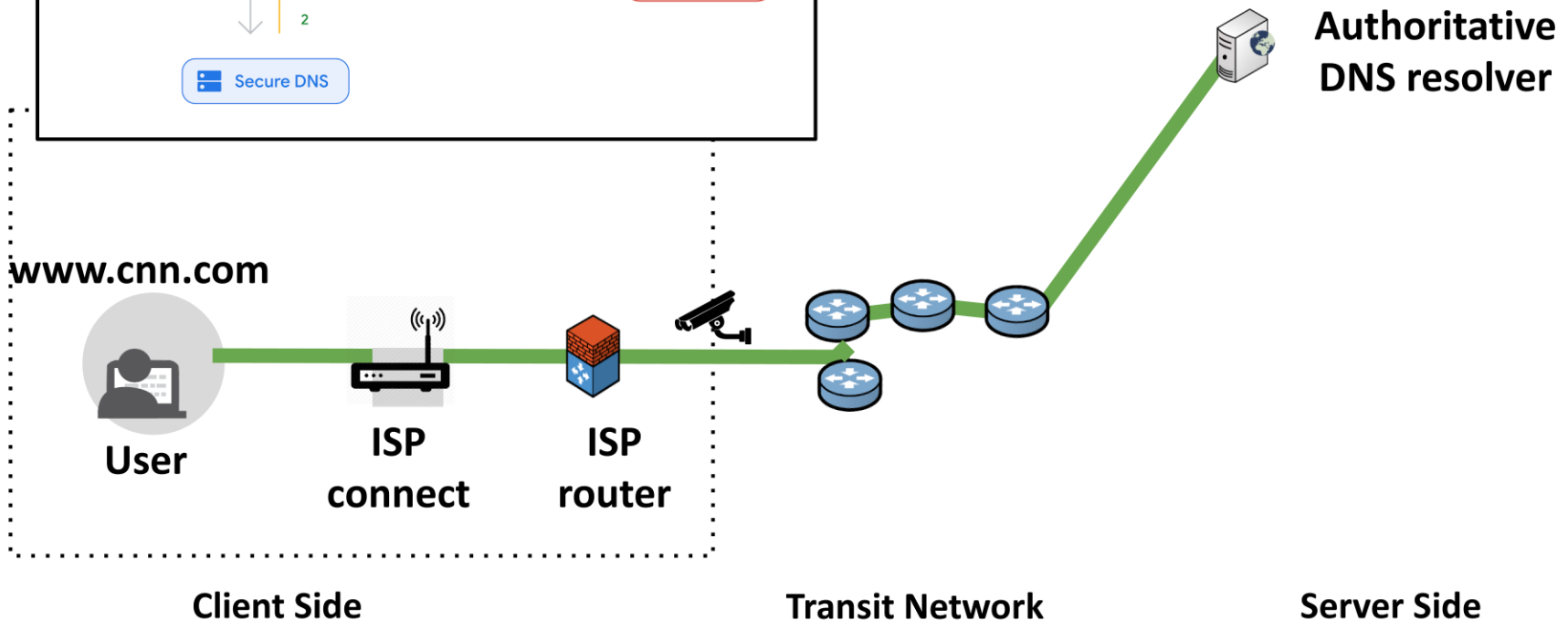


- Censor looks for DNS req in outbound traffic
  - Destined for honest DNS server
- Censor injects fake DNS responses
- Real response is ignored when arrives

# DNS over HTTPS



- Wrap DNS protocol inside HTTPS channel



# Deep Packet Inspection



**Deep Packet Inspection (DPI)** is a network component that is able to monitor traffic for signs of *deemed-harmful* content.

- DPI is an IDS/IPS used specifically for censorship
- Arbitrarily advanced logic to trigger

## Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a network *monitoring* component that is able to *watch* for signs of maliciousness.

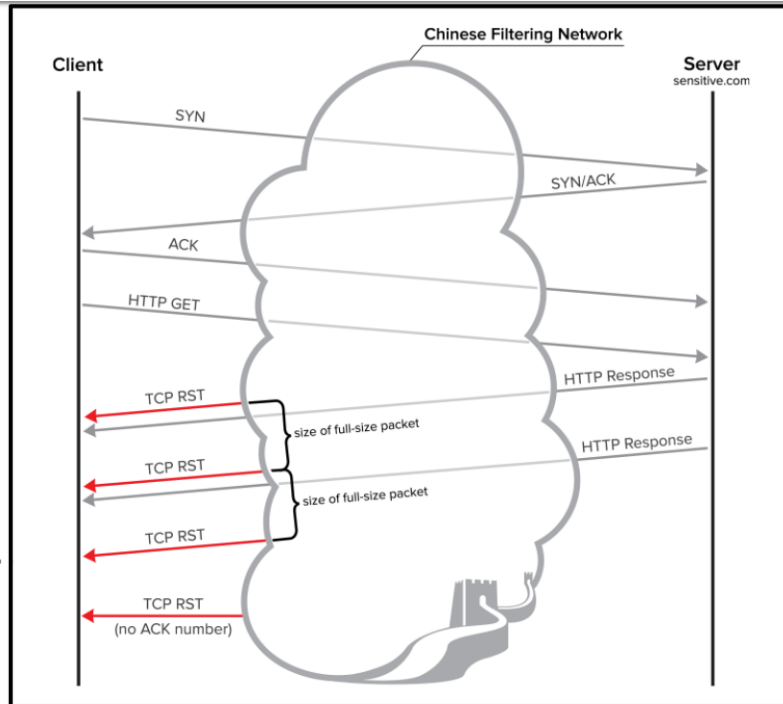
- Capable of granular and complex rules
  - Beyond L2/L3 (IP/TCP) headers
  - “Deep Packet Inspection” (DPI)
- Capable of pattern/regex matching
- Capable of searching for multi-flow patterns



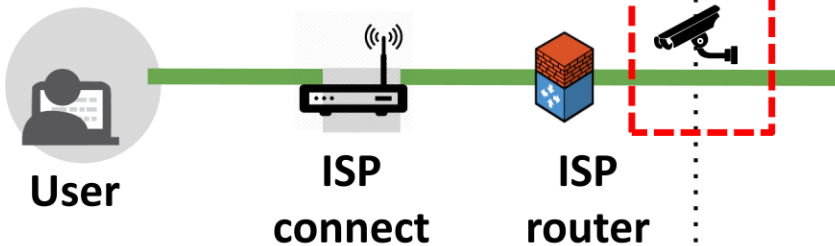
# Common DPI Triggers

- Search for banned domains/IPs
- Search for banned content
  - Words, phrases, images, etc
- Search for traffic fingerprints
  - Timing of requests
  - Packet-flow rate/size
  - Inter-flow correlations (fetching dependencies)
- Search for illogical characteristics
  - Side-channels to fake interactions

# TCP Injection



www.cnn.com



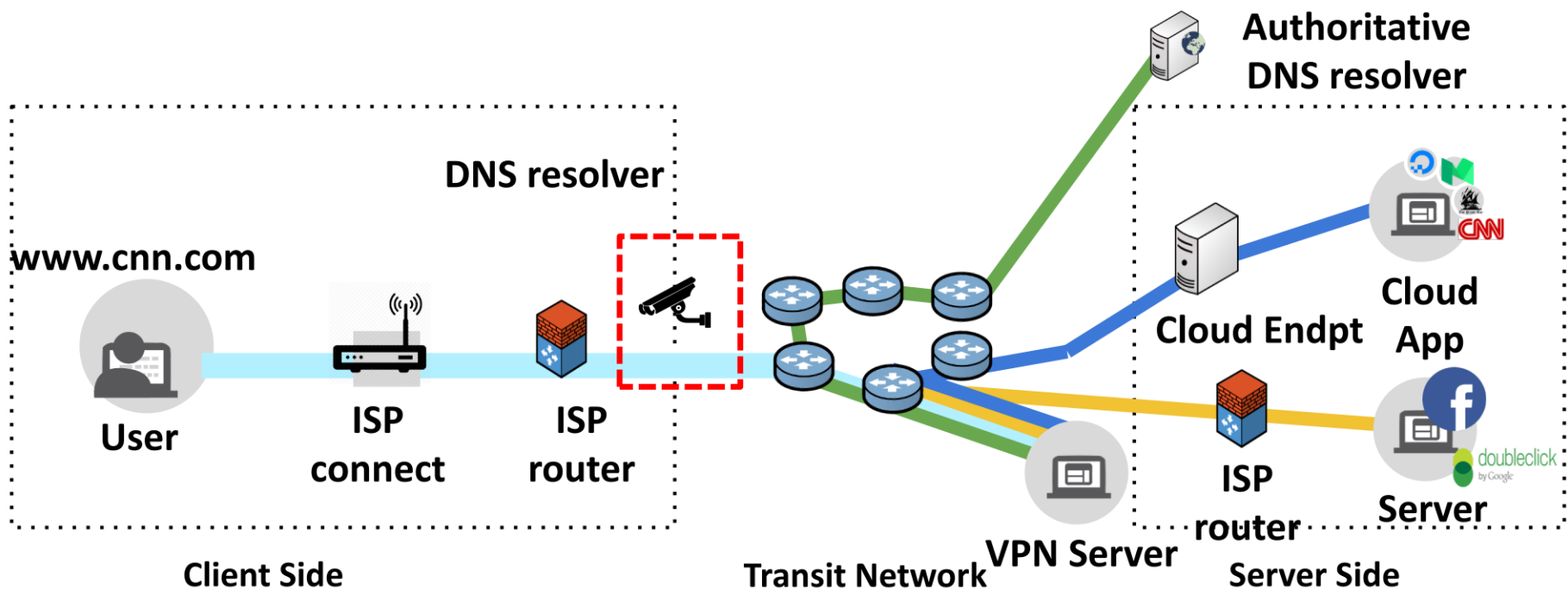
Client Side

- Censor looks for DPI triggers in outbound traffic
- Censor injects fake TCP RST packets
- Client thinks RST from server and closes connection

# Secure Channel Encapsulation



- DPI much less useful w/ encrypted traffic
  - TLS/VPN/etc.



# TLS Interception



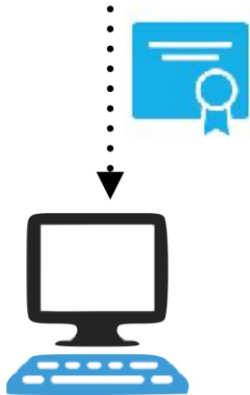
**TLS Interception** is an *explicit* mechanism to Man-in-the-Middle (MitM) TLS/HTTPS connections in order to monitor contents.

- Estimated 5-10% of TLS connections

# TLS Interception



Administrator installs  
root certificate on client



# TLS Interception



Certificate Manager

Your Certificates

People

Servers

Authorities

You have certificates on file that identify these certificate authorities

| Certificate Name                     | Security Device      |
|--------------------------------------|----------------------|
| AC Camerfirma S.A.                   |                      |
| Chambers of Commerce Root - 2008     | Builtin Object Token |
| Global Chambersign Root - 2008       | Builtin Object Token |
| AC Camerfirma SA CIF A82743287       |                      |
| Camerfirma Chambers of Commerce R... | Builtin Object Token |
| Camerfirma Global Chambersign Root   | Builtin Object Token |
| ACCV                                 |                      |
| ACCVRAIZ1                            | Builtin Object Token |
| Actalis S.p.A./03358520967           |                      |
| Actalis Authentication Root CA       | Builtin Object Token |

View...

Edit Trust...

Import...

Export...

Delete or D...

Keychains

login

Local Items

System

System Roots

Category

All Items

Passwords

Secure Notes

My Certificates

Keys

Certificates

Certificate

VRK Gov. Root CA

Root certificate authority

Expires: Monday, December 18, 2023 at 07:51:08 CST

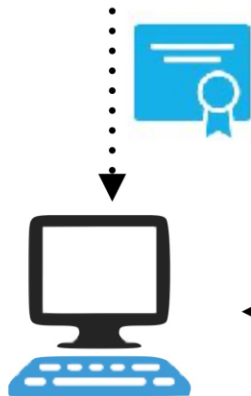
This certificate is valid

| Name                             | Kind        | Expires                      | Keychain     |
|----------------------------------|-------------|------------------------------|--------------|
| AAA Certificate Services         | certificate | Dec 31, 2028 at 5:59:59...   | System Roots |
| AC RAIZ FNMT-RCM                 | certificate | Dec 31, 2029 at 6:00:00...   | System Roots |
| Actalis Authentication Root CA   | certificate | Sep 22, 2030 at 6:22:02...   | System Roots |
| AddTrust Class 1 CA Root         | certificate | May 30, 2020 at 5:38:31...   | System Roots |
| AddTrust External CA Root        | certificate | May 30, 2020 at 5:48:38...   | System Roots |
| Admin-Root-CA                    | certificate | Nov 10, 2021 at 1:51:07 AM   | System Roots |
| AffirmTrust Commercial           | certificate | Dec 31, 2030 at 8:06:06...   | System Roots |
| AffirmTrust Networking           | certificate | Dec 31, 2030 at 8:08:24...   | System Roots |
| AffirmTrust Premium              | certificate | Dec 31, 2040 at 8:10:36...   | System Roots |
| AffirmTrust Premium ECC          | certificate | Dec 31, 2040 at 8:20:24...   | System Roots |
| Amazon Root CA 1                 | certificate | Jan 16, 2038 at 6:00:00...   | System Roots |
| Amazon Root CA 2                 | certificate | May 25, 2040 at 7:00:00...   | System Roots |
| Amazon Root CA 3                 | certificate | May 25, 2040 at 7:00:00...   | System Roots |
| Amazon Root CA 4                 | certificate | May 25, 2040 at 7:00:00...   | System Roots |
| ANF Global Root CA               | certificate | Jun 05, 2033 at 12:45:38...  | System Roots |
| Apple Root CA                    | certificate | Feb 09, 2035 at 3:40:36...   | System Roots |
| Apple Root CA - G2               | certificate | Apr 30, 2039 at 1:10:09 PM   | System Roots |
| Apple Root CA - G3               | certificate | Apr 30, 2039 at 1:19:06 P... | System Roots |
| Apple Root Certificate Authority | certificate | Feb 09, 2025 at 6:18:14...   | System Roots |
| ApplicationCA2 Root              | certificate | Mar 12, 2033 at 9:00:00...   | System Roots |
| Atos TrustedRoot 2011            | certificate | Dec 31, 2030 at 5:59:59...   | System Roots |
| Autoridad de...nal CIF A62634068 | certificate | Dec 31, 2030 at 2:38:15...   | System Roots |
| Autoridad de...Estado Venezolano | certificate | Dec 17, 2030 at 5:59:59...   | System Roots |

# TLS Interception



Administrator installs  
root certificate on client



Middlebox generates  
new certificate for client



TLS





# Intermediate Certificate

# Root Certificate

qKQ  
eLF  
fsc  
MBO  
Egy

Subject Name \_\_\_\_\_  
Country US  
State/Province New Jersey  
Locality Jersey City  
Organization The USERTRUST Network  
Common Name USERTrust RSA Certification Authority

112  
+WJ  
5jB  
h1P  
RCR  
Smy  
eoC  
nrK  
oJ8  
OJR  
---

Issuer Name \_\_\_\_\_  
Country US  
State/Province New Jersey  
Locality Jersey City  
Organization The USERTRUST Network  
Common Name USERTrust RSA Certification Authority



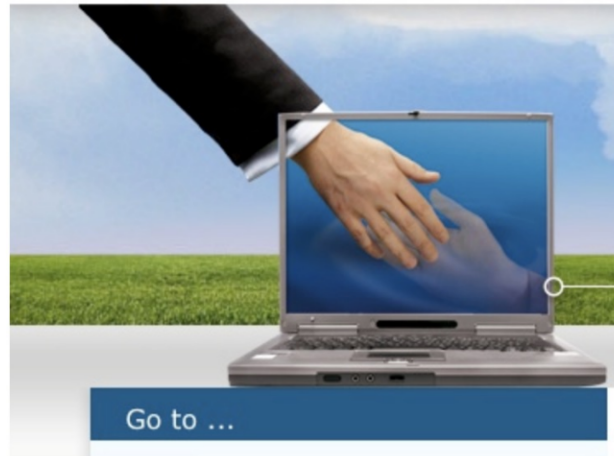
# Compromised Root CA



WIRED

SUBSCRIBE

## DigiNotar Files for Bankruptcy in Wake of Devastating Hack



A Dutch certificate authority that suffered a major hack attack this summer has been unable to recover from the blow and filed for bankruptcy this week.

# Compromised Root Chain



## Leaf Certificate

```
-----BEGIN CERTIFICATE-----
MIIFjCCBHKgAwIBAgIQMarm4TPRa4oupkXTLQJKBtANBgkqhkiG9w0BAQwFADCB
MQswCQYDVQGEwJVUzELMAKGA1UEBmCTUkxZjAQBgNVBACTCUFIbBcmJvcjES
MBAGA1UEChMJSW50ZXJzJzYyMREwDwYDQGEwJbJkNvbWV1bWVjZmFMB0GA1UEAxMw
SW50b21tb24uLmF1bnB1bnR1cnZlciBDQTAeFw0xNzA0MTgwMDAwMDAwMDAwMDAwMDAw
MzU5NTlaMjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MDAw
dHkx
EQYI
AQER
fhRE
Hxqg
2Atg
dOAK
Ngbr
d49s
MA4G
BwME
AQU
L2N
Y3Jz
KwYE
b20v
L2N
S1b3
OF4h
umSW
jCmc
W2be
8bs9
-----
```

|                     |                                  |
|---------------------|----------------------------------|
| Subject Name        |                                  |
| Country             | US                               |
| State/Province      | Alabama                          |
| Locality            | Auburn University                |
| Organization        | 300 Lem Morrison Drive           |
| Organizational Unit | Auburn University                |
| Common Name         | Office of Information Technology |
| Issuer Name         |                                  |
| Country             | US                               |
| State/Province      | MI                               |
| Locality            | Ann Arbor                        |
| Organization        | Internet2                        |
| Organizational Unit | InCommon                         |
| Common Name         | InCommon RSA Server CA           |

## Intermediate Certificate

```
-----BEGIN CERTIFICATE-----
MIIF3jCCBKAQAwIBAgIQAF1tMPyjj1GoG7xkdjUdLTANBgkqhkiG9w0BAQwFADCB
iDELMAKGA1UEBmCVVMeXZARBgNVBACTCk5ldyBkZXJzZXkxZDASBgNVBACTC0pl
cnNleSBDAxR5MR4wHAYDVQQKEVUaGUGVFNULRSVNUIE5ldHdvcmxkLjAeBgNV
BAMTJVVTRVJUCnZvdCBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkwHicCNMTQx
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MDAw
dHkx
EQYI
AQER
fhRE
Hxqg
2Atg
dOAK
Ngbr
d49s
MA4G
BwME
AQU
L2N
Y3Jz
KwYE
b20v
L2N
S1b3
OF4h
umSW
jCmc
W2be
8bs9
-----
```

|                     |                                       |
|---------------------|---------------------------------------|
| Subject Name        |                                       |
| Country             | US                                    |
| State/Province      | MI                                    |
| Locality            | Ann Arbor                             |
| Organization        | Internet2                             |
| Organizational Unit | InCommon                              |
| Common Name         | InCommon RSA Server CA                |
| Issuer Name         |                                       |
| Country             | US                                    |
| State/Province      | New Jersey                            |
| Locality            | Jersey City                           |
| Organization        | The USERTRUST Network                 |
| Common Name         | USERTrust RSA Certification Authority |

## Root Certificate

```
-----BEGIN CERTIFICATE-----
MIIF+TCCA+GgAwIBAgIQRYDQ+oVGGn4XoWQckYRjdBANBgkqhkiG9w0BAQwFADCB
iDELMAKGA1UEBmCVVMeXZARBgNVBACTCk5ldyBkZXJzZXkxZDASBgNVBACTC0pl
cnNleSBDAxR5MR4wHAYDVQQKEVUaGUGVFNULRSVNUIE5ldHdvcmxkLjAeBgNV
BAMTJVVTRVJUCnZvdCBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkwHicCNMTQx
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MDAw
dHkx
EQYI
AQER
fhRE
Hxqg
2Atg
dOAK
Ngbr
d49s
MA4G
BwME
AQU
L2N
Y3Jz
KwYE
b20v
L2N
S1b3
OF4h
umSW
jCmc
W2be
8bs9
-----
```

|                |                                       |
|----------------|---------------------------------------|
| Subject Name   |                                       |
| Country        | US                                    |
| State/Province | New Jersey                            |
| Locality       | Jersey City                           |
| Organization   | The USERTRUST Network                 |
| Common Name    | USERTrust RSA Certification Authority |
| Issuer Name    |                                       |
| Country        | US                                    |
| State/Province | New Jersey                            |
| Locality       | Jersey City                           |
| Organization   | The USERTRUST Network                 |
| Common Name    | USERTrust RSA Certification Authority |

## Malicious Leaf

```
-----BEGIN CERTIFICATE-----
MIIFjCCBHKgAwIBAgIQMarm4TPRa4oupkXTLQJKBtANBgkqhkiG9w0BAQwFADCB
MQswCQYDVQGEwJVUzELMAKGA1UEBmCTUkxZjAQBgNVBACTCUFIbBcmJvcjES
MBAGA1UEChMJSW50ZXJzJzYyMREwDwYDQGEwJbJkNvbWV1bWVjZmFMB0GA1UEAxMw
SW50b21tb24uLmF1bnB1bnR1cnZlciBDQTAeFw0xNzA0MTgwMDAwMDAwMDAwMDAwMDAw
MzU5NTlaMjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MDAw
dHkx
EQYI
AQER
fhRE
Hxqg
2Atg
dOAK
Ngbr
d49s
MA4G
BwME
AQU
L2N
Y3Jz
KwYE
b20v
L2N
S1b3
OF4h
umSW
jCmc
W2be
8bs9
-----
```

|                     |                        |
|---------------------|------------------------|
| Subject Name        |                        |
| Country             | US                     |
| State/Province      | Alabama                |
| Locality            | Auburn University      |
| Organization        | 300 Lem Morrison Drive |
| Organizational Unit | Auburn University      |

## Malicious Intermediate

```
-----BEGIN CERTIFICATE-----
MIIF3jCCBKAQAwIBAgIQAF1tMPyjj1GoG7xkdjUdLTANBgkqhkiG9w0BAQwFADCB
iDELMAKGA1UEBmCVVMeXZARBgNVBACTCk5ldyBkZXJzZXkxZDASBgNVBACTC0pl
cnNleSBDAxR5MR4wHAYDVQQKEVUaGUGVFNULRSVNUIE5ldHdvcmxkLjAeBgNV
BAMTJVVTRVJUCnZvdCBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkwHicCNMTQx
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
MDAw
dHkx
EQYI
AQER
fhRE
Hxqg
2Atg
dOAK
Ngbr
d49s
MA4G
BwME
AQU
L2N
Y3Jz
KwYE
b20v
L2N
S1b3
OF4h
umSW
jCmc
W2be
8bs9
-----
```

|                     |                        |
|---------------------|------------------------|
| Subject Name        |                        |
| Country             | US                     |
| State/Province      | MI                     |
| Locality            | Ann Arbor              |
| Organization        | Internet2              |
| Organizational Unit | InCommon               |
| Common Name         | InCommon RSA Server CA |

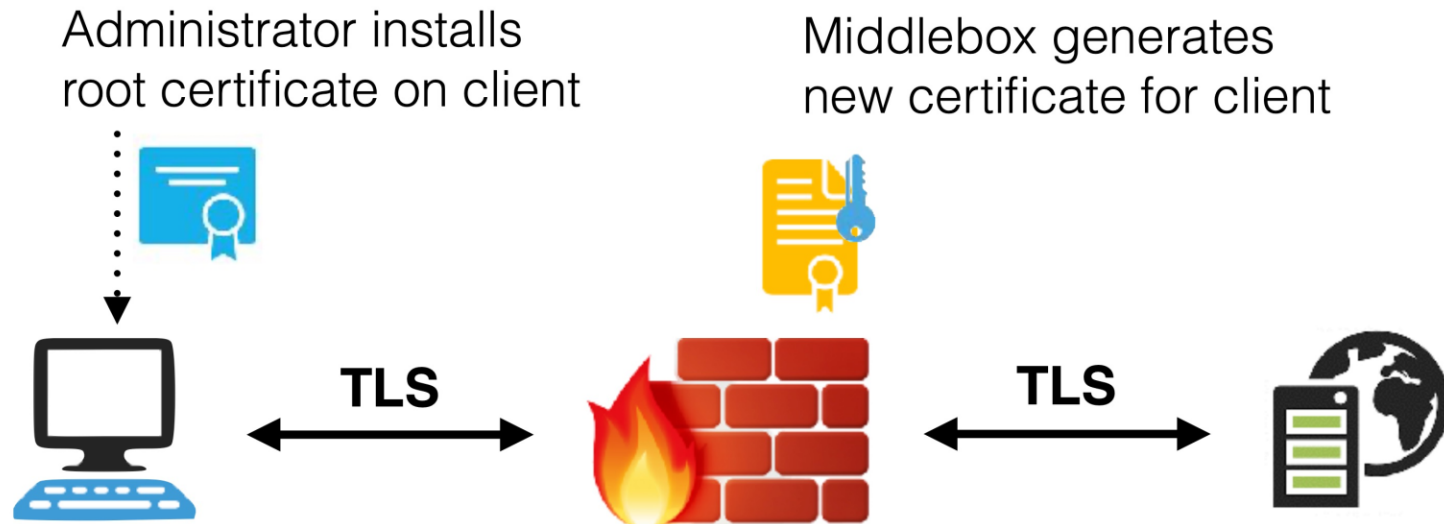
COMPROMISED



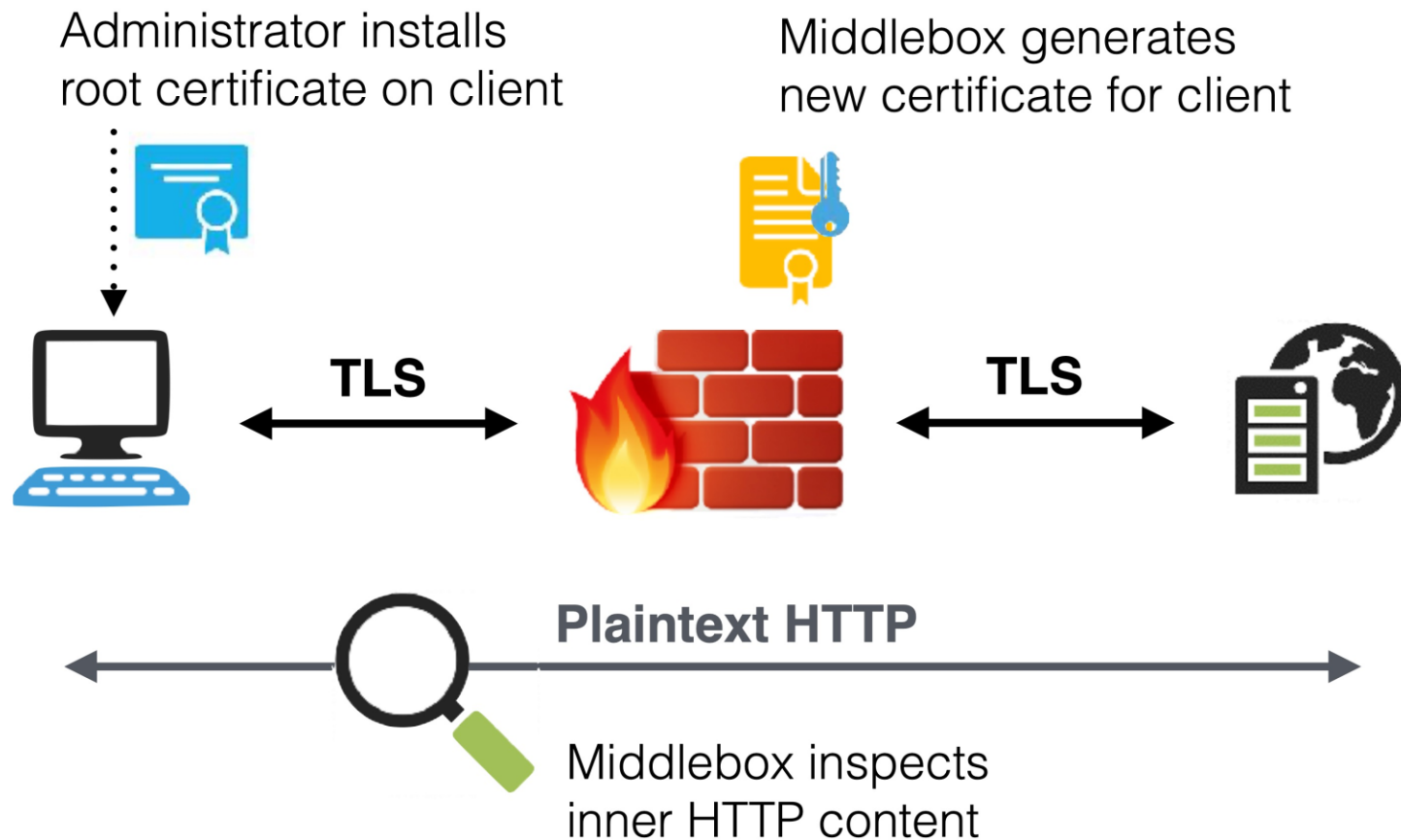
# Root Certificate

|       |                |                        |
|-------|----------------|------------------------|
| MDAg  | Subject Name   |                        |
| dhKc  |                |                        |
| FOV7  | Country        | US                     |
| AQEF  |                |                        |
| fHrF  |                | 36849                  |
| lhxqe |                |                        |
| ZK5c  | State/Province | Alabama                |
| dON4  |                |                        |
| Ngbr  | Locality       | Auburn University      |
| d49s  |                |                        |
| MA4E  |                | 300 Lem Morrison Drive |
| BwHc  |                |                        |
| BOUE  | Organization   | Auburn University      |

# TLS Interception



# TLS Interception



# TLS Interception



**TLS Interception** is an *explicit* mechanism to Man-in-the-Middle (MitM) TLS/HTTPS connections in order to monitor contents.

- Estimated 5-10% of TLS connections
- Often ***claims*** to be a security defense
- More often it ***creates vulnerabilities*** in otherwise secure interactions

# Impact of TLS Interception



| TLS Security             | Increased Security | Same Security | Decreased Security | Severely Broken |
|--------------------------|--------------------|---------------|--------------------|-----------------|
| Client Security Products | 0/20               | 2/20          | 18/20              | 10/20           |
| Middleboxes              | 0/12               | 1/12          | 6/12               | 5/12            |

# Impact of TLS Interception



| TLS Security             | Increased Security | Same Security | Decreased Security | Severely Broken |
|--------------------------|--------------------|---------------|--------------------|-----------------|
| Client Security Products | 0/20               | 2/20          | 18/20              | 10/20           |
| Middleboxes              | 0/12               | 1/12          | 6/12               | 5/12            |

## The Security Impact of HTTPS Interception

Zakir Durumeric<sup>\*∇</sup>, Zane Ma<sup>†</sup>, Drew Springall<sup>\*</sup>, Richard Barnes<sup>‡</sup>, Nick Sullivan<sup>§</sup>,  
Elie Bursztein<sup>¶</sup>, Michael Bailey<sup>†</sup>, J. Alex Halderman<sup>\*</sup>, Vern Paxson<sup>||∇</sup>

<sup>\*</sup> University of Michigan   <sup>†</sup> University of Illinois Urbana-Champaign   <sup>‡</sup> Mozilla   <sup>§</sup> Cloudflare  
<sup>¶</sup> Google   <sup>||</sup> University of California Berkeley   <sup>∇</sup> International Computer Science Institute

# Impact of TLS Interception



| Product                  | OS  | Browser MITM |        |         |        | Grade | Validates Certificates | Modern Ciphers | TLS Version | Grading Notes             |
|--------------------------|-----|--------------|--------|---------|--------|-------|------------------------|----------------|-------------|---------------------------|
|                          |     | IE           | Chrome | Firefox | Safari |       |                        |                |             |                           |
| Avast ...                | Win | ●            | ○      | ○       | ●      | A*    | ✓                      | ✓              | 1.2         | Mirrors client ciphers    |
| AV 11                    | Mac | ●            | ○      | ○       | ●      | F     | ✓                      | ✓              | 1.2         | Advertises DES            |
| AVG ...                  | Win | ●            | ●      | ○       | ●      | C     | ✓                      | ✓              | 1.2         | Advertises RC4            |
| Bitdefender ...          | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ○              | 1.2         | RC4, 768-bit D-H          |
| Internet Security 2016   | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ○              | 1.2         | RC4, 768-bit D-H          |
| Total Security Plus 2016 | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ○              | 1.2         | RC4, 768-bit D-H          |
| AV Plus 2015-16          | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ○              | 1.2         | RC4, 768-bit D-H          |
| Bullguard ...            | Win | ●            | ●      | ●       | ●      | A*    | ✓                      | ✓              | 1.2         | Mirrors client ciphers    |
| Internet Security 16     | Win | ●            | ●      | ●       | ●      | F     | ✓                      | ✓              | 1.0         | Advertises DES            |
| CYBERSitter ...          | Win | ●            | ●      | ●       | ●      | F     | ✗                      | ✗              | 1.2         | No cert. validation, DES  |
| Dr. Web ...              | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ○              | 1.2         | RC4, FREAK                |
| Security Space 11        | Mac | ●            | ●      | ●       | ●      | F     | ✓                      | ✗              | 1.0         | Export ciphers, DES, RC2  |
| Dr. Web 11 for OS X      | Win | ●            | ●      | ●       | ●      | F     | ○                      | ○              | 1.2         | Broken cert. validation   |
| ESET ...                 | Win | ●            | ●      | ●       | ●      | F     | ○                      | ○              | 1.2         | Broken cert. validation   |
| NOD32 AV 9               | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ✓              | 1.2         | CRIME vulnerability       |
| Kaspersky ...            | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ✓              | 1.2         | CRIME vulnerability       |
| Internet Security 16     | Win | ●            | ●      | ●       | ●      | C     | ✓                      | ✓              | 1.2         | CRIME vulnerability       |
| Total Security 16        | Mac | ●            | ●      | ●       | ●      | C     | ✓                      | ✓              | 1.2         | 768-bit D-H               |
| Internet Security 16     | Win | ●            | ●      | ●       | ●      | F     | ○                      | ✗              | 1.0         | Broken cert. validation   |
| KinderGate ...           | Win | ●            | ●      | ●       | ●      | F     | ✓                      | ✓              | 1.2         | Anonymous ciphers         |
| Parental Control 3       | Mac | ●            | ●      | ●       | ●      | F     | ✓                      | ✓              | 1.2         | Anonymous ciphers         |
| Net Nanny ...            | Win | ●            | ●      | ●       | ●      | F     | ✓                      | ✓              | 1.2         | Anonymous ciphers         |
| Net Nanny 7              | Mac | ●            | ●      | ●       | ●      | F     | ✓                      | ✓              | 1.2         | Anonymous ciphers         |
| PC Pandora ...           | Win | ●            | ○      | ○       | ○      | F     | ✗                      | ✗              | 1.0         | No certificate validation |
| PC Pandora 7             | Win | ●            | ○      | ○       | ○      | F     | ✗                      | ✗              | 1.0         | No certificate validation |
| Quostodio ...            | Mac | ●            | ●      | ●       | ●      | F     | ✓                      | ✓              | 1.2         | Advertises DES            |
| Parental Control 2015    | Mac | ●            | ●      | ●       | ●      | F     | ✓                      | ✓              | 1.2         | Advertises DES            |

Fig. 4: **Security of Client-side Interception Software**—We evaluate and fingerprint popular products, finding that products from twelve vendors intercept connections.<sup>2</sup> In all but two cases, security. \*Mirrors browser ciphers.



| Product                        | Grade | Validates Certificates | Modern Ciphers | Advertises RC4 | TLS Version | Grading Notes                 |
|--------------------------------|-------|------------------------|----------------|----------------|-------------|-------------------------------|
| A10 vThunder SSL Insight       | F     | ✓                      | ✓              | Yes            | 1.2         | Advertises export ciphers     |
| Blue Coat ProxySG 6642         | A*    | ✓                      | ✓              | No             | 1.2         | Mirrors client ciphers        |
| Barracuda 610Vx Web Filter     | C     | ✓                      | ✗              | Yes            | 1.0         | Vulnerable to Logjam attack   |
| Checkpoint Threat Prevention   | F     | ✓                      | ✗              | Yes            | 1.0         | Allows expired certificates   |
| Cisco IronPort Web Security    | F     | ✓                      | ✓              | Yes            | 1.2         | Advertises export ciphers     |
| Forcepoint TRITON AP-WEB Cloud | C     | ✓                      | ✓              | No             | 1.2         | Accepts RC4 ciphers           |
| Fortinet FortiGate 5.4.0       | C     | ✓                      | ✓              | No             | 1.2         | Vulnerable to Logjam attack   |
| Juniper SRX Forward SSL Proxy  | C     | ✓                      | ✗              | Yes            | 1.2         | Advertises RC4 ciphers        |
| Microsoft Threat Mgmt. Gateway | F     | ✗                      | ✗              | Yes            | SSLv2       | No certificate validation     |
| Sophos SSL Inspection          | C     | ✓                      | ✓              | Yes            | 1.2         | Advertises RC4 ciphers        |
| Untangle NG Firewall           | C     | ✓                      | ✗              | Yes            | 1.2         | Advertises RC4 ciphers        |
| WebTitan Gateway               | F     | ✗                      | ✓              | Yes            | 1.2         | Broken certificate validation |

Fig. 3: **Security of TLS Interception Middleboxes**—We evaluate popular network middleboxes that act as TLS interception proxies. We find that nearly all reduce connection security and five introduce severe vulnerabilities. \*Mirrors browser ciphers.



**Why would censors inject traffic  
(DNS responses/TCP RSTs/etc)  
instead of intercepting traffic?**

Inline DPI+blocking is expensive  
and delays *approved* content.

# Censors are Rational Actors



- In almost all cases, censors understand how their actions will be perceived
  - By those who are impacted
  - By other governments/companies
- Censorship still exists because the censors decide that the negative aspects are acceptable due to the advantages.

# Censorship Avoidance



**Censorship avoidance** is intentionally designing, building, using, and maintaining systems whose goal is explicitly to give users ability to bypass local censorship.

- Attempts to modify the censor's trade-off
  - Increase the negative impacts of blocking
  - Decrease the user-effort to avoid

# Censorship Avoidance



**Censorship avoidance** is intentionally designing, building, using, and maintaining systems whose goal is explicitly to give users ability to bypass local censorship.

- Attempts to modify the censor's trade-off
  - Increase the negative impacts of blocking
  - Decrease the user-effort to avoid
- Will never be 100% successful but that's OK
  - **Just need to cross trade-off boundary**



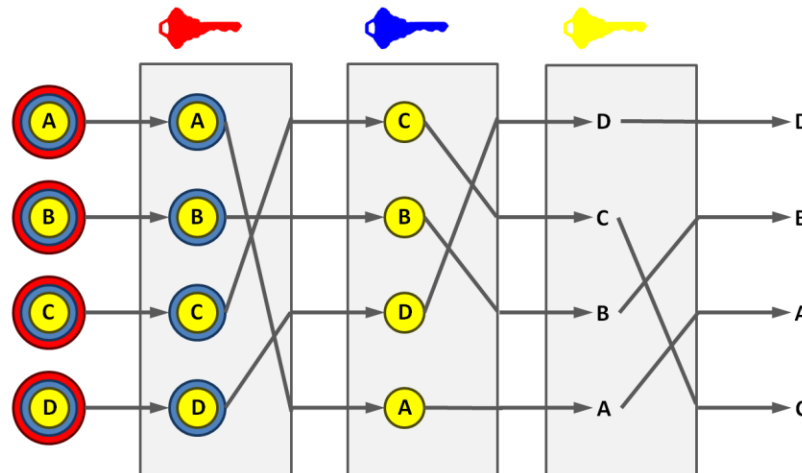
A **Virtual Private Network (VPN)** is a *logical* concept through which a remote client appears on the local network by use of a multiplexed secure channel.

- Many different protocols can be used
- IKE+IPSec is a common implementation
- Can connect two remote-networks as 1
- Can be used on a client-server construction

# Mix Networks



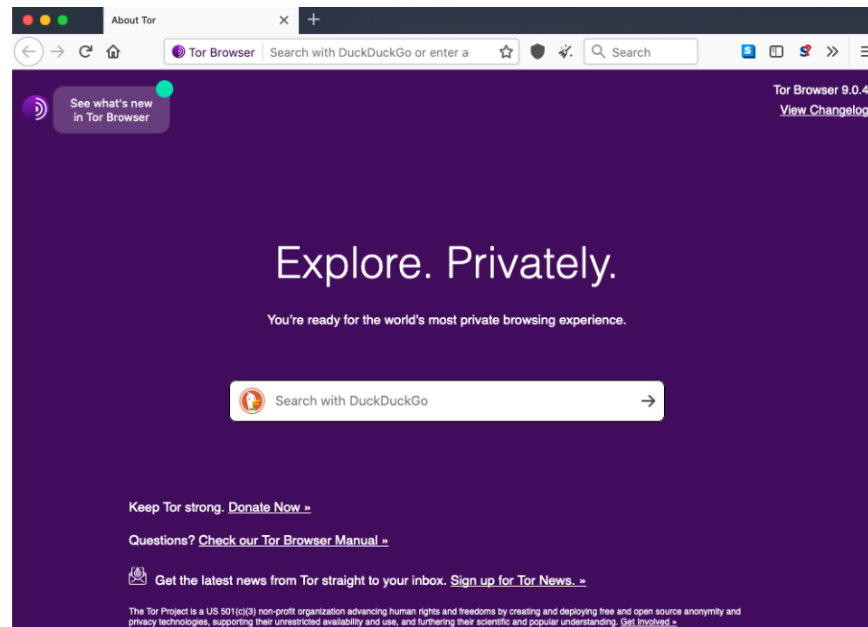
**Mix Networks (Mix-Nets)** are a type of high-latency anonymous network which relies on bounces among nodes with other messages for protections.

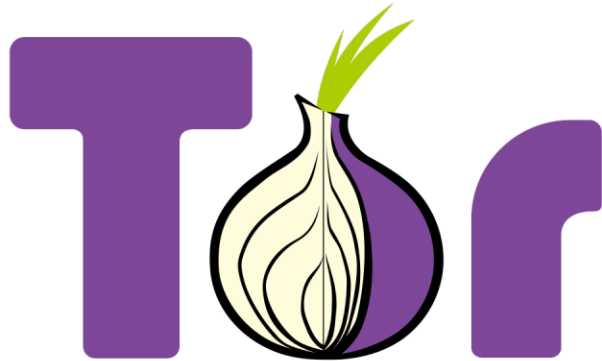


# The Onion Router (Tor)

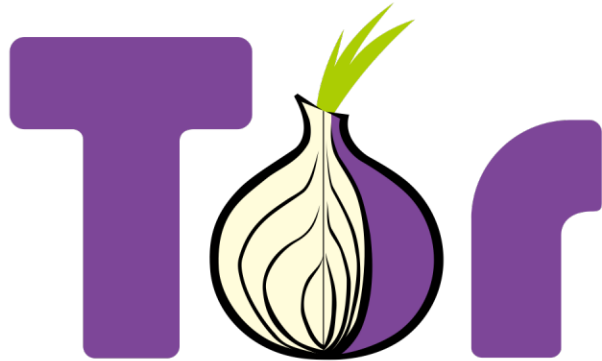


**The Onion Router (Tor)** network is a privacy- and anonymity-centric, volunteer-run communications network.





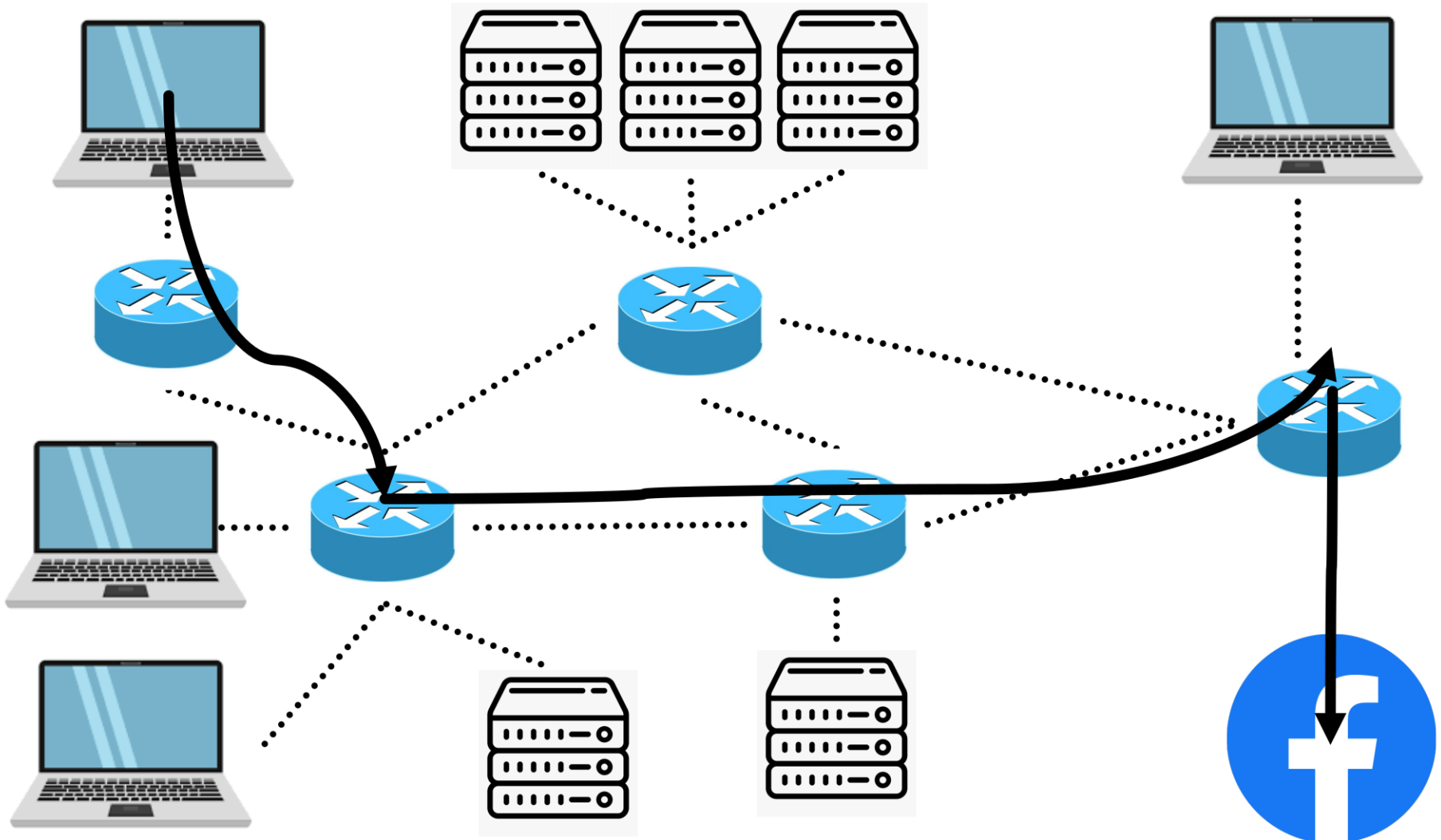
- Started by DoD's Naval Research Lab
- “Low-latency” Secure Channel
- *Overlay network*



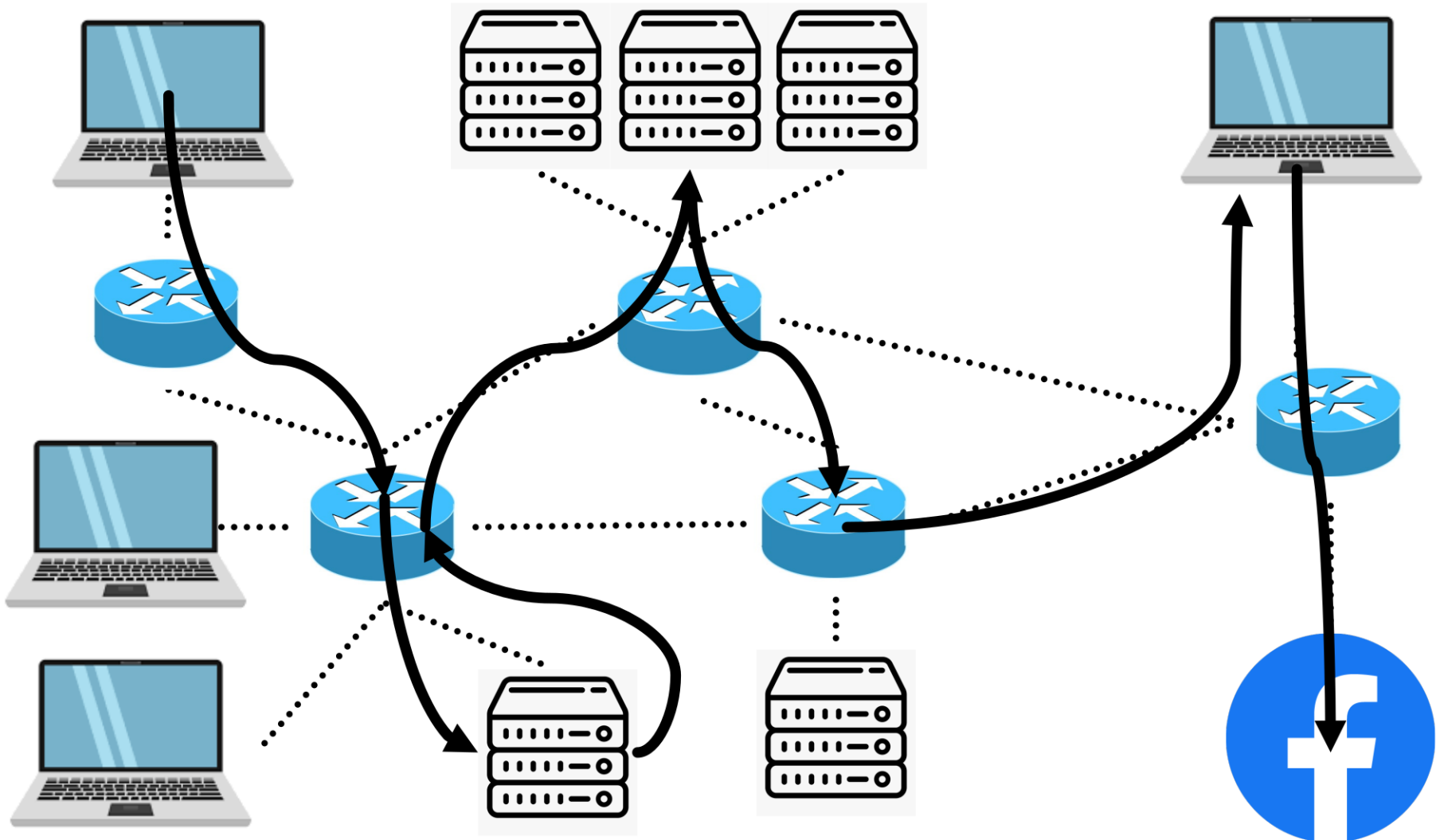
- Started by DoD's Naval Research Lab
- “Low-latency” Secure Channel
- *Overlay network*
- Used by *good guys*
- Used by *bad guys*

|                |                  |
|----------------|------------------|
| Journalists    | Drug Dealers     |
| Hackers        | Terrorists       |
| Activists      | Researchers      |
| Whistleblowers | Mil/Intel Agents |
| Pedophiles     | Normal People    |

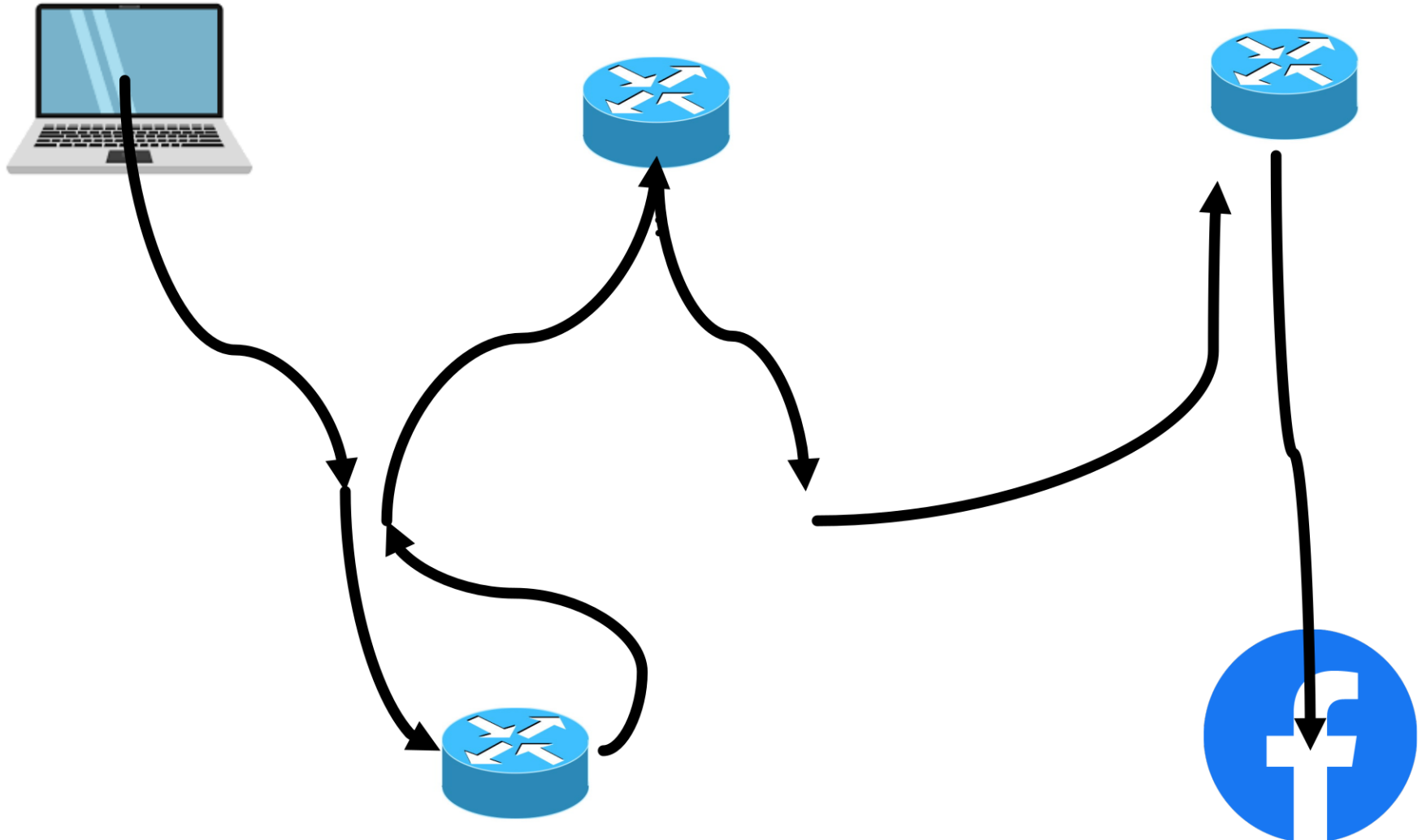
# "Normal" Network



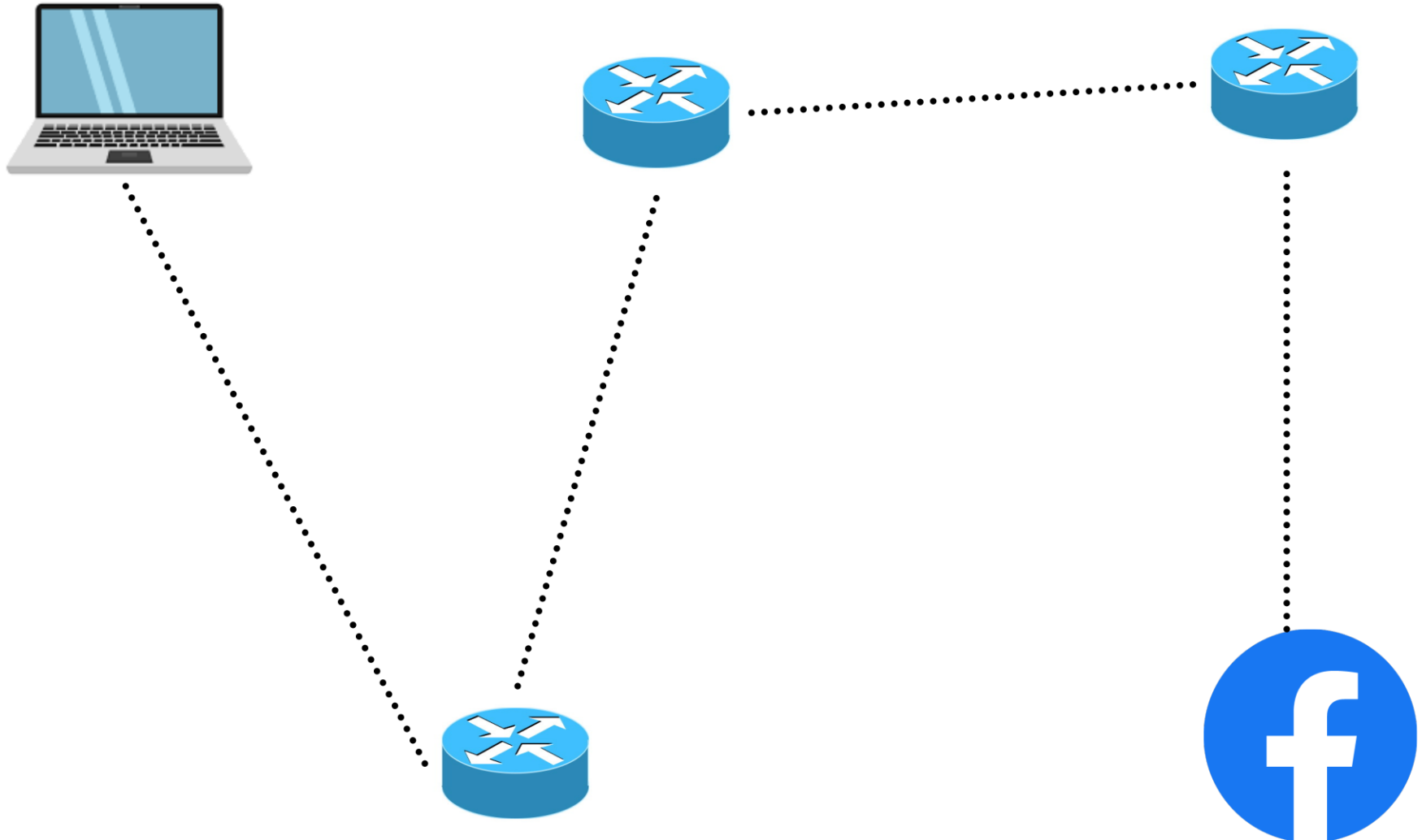
# "Overlay" Network



# "Overlay" Network



# "Overlay" Network

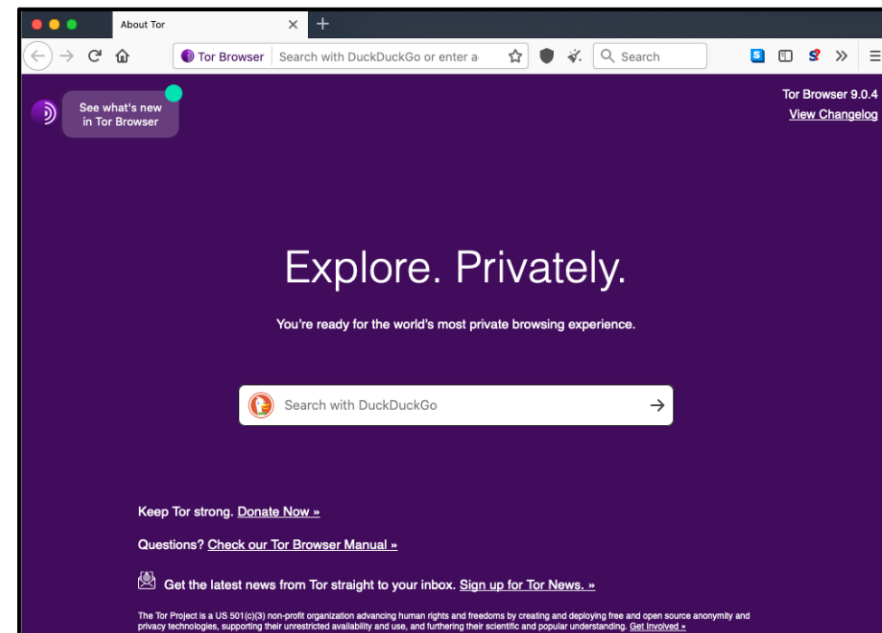


# Tor Browser



By default, users access Tor through a forked version of the Firefox web browser with numerous special-purpose patches.

- Use exactly as would Firefox/Chrome/etc
- 100% traffic routed over Tor network
- Cutting-edge privacy protections



# Computer and Network Security

## Lecture 24: Anonymity & Censorship

COMP-5370/6370  
Fall 2025

