Proxies, VPNs and Tor

What is hidden to some, is revealed to others.

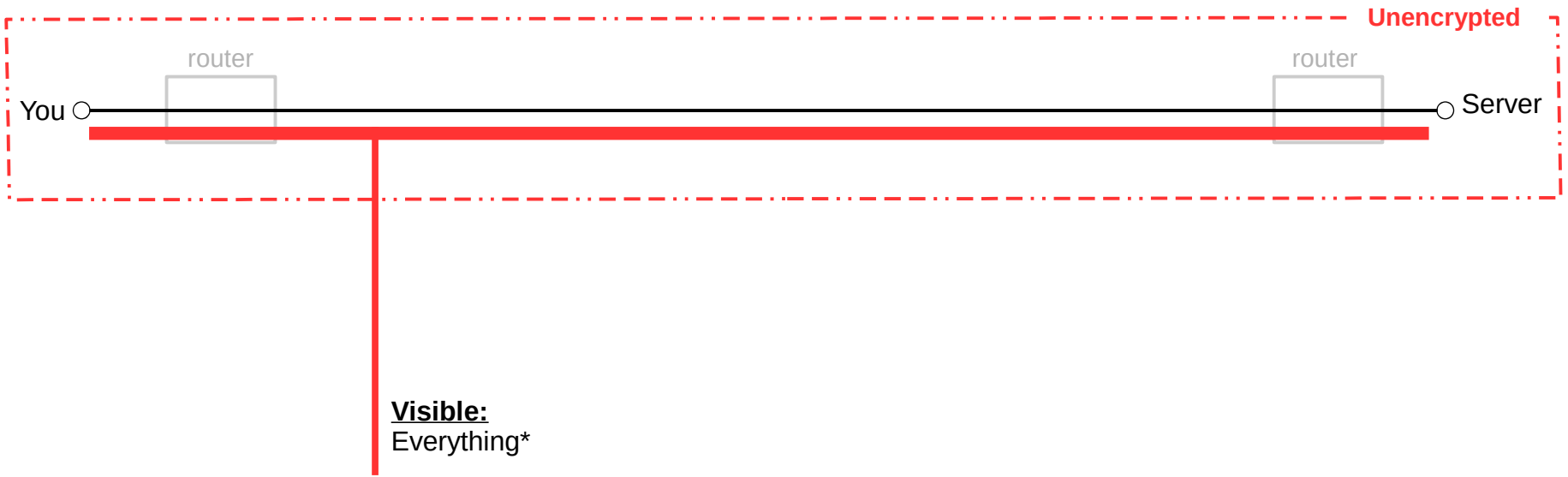
Tim Sammut, @t1msammut
15 July 2015

Objectives

- Understand the differences
- Know when to use each
- Be mindful of challenges and pitfalls

Direct Communications

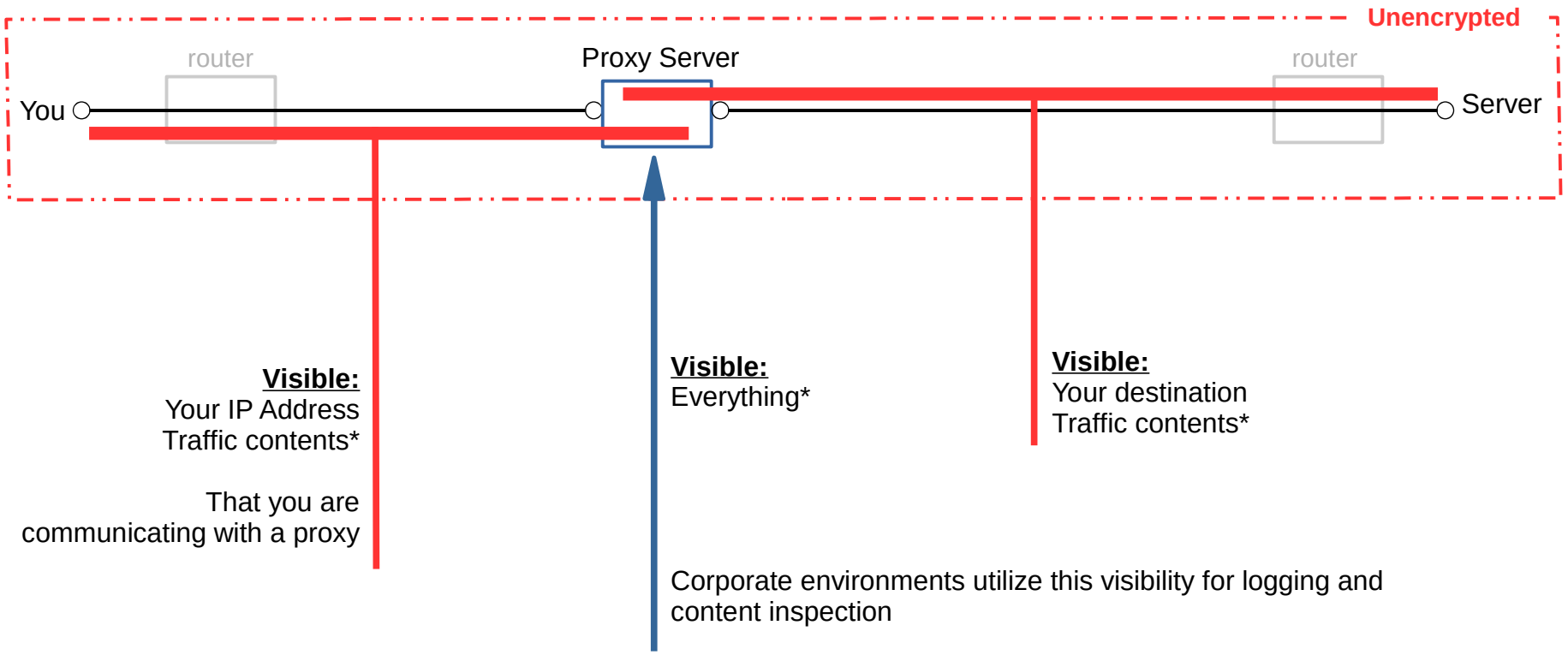
No precautions taken



** Ignores application-level encryption*

Proxy Servers

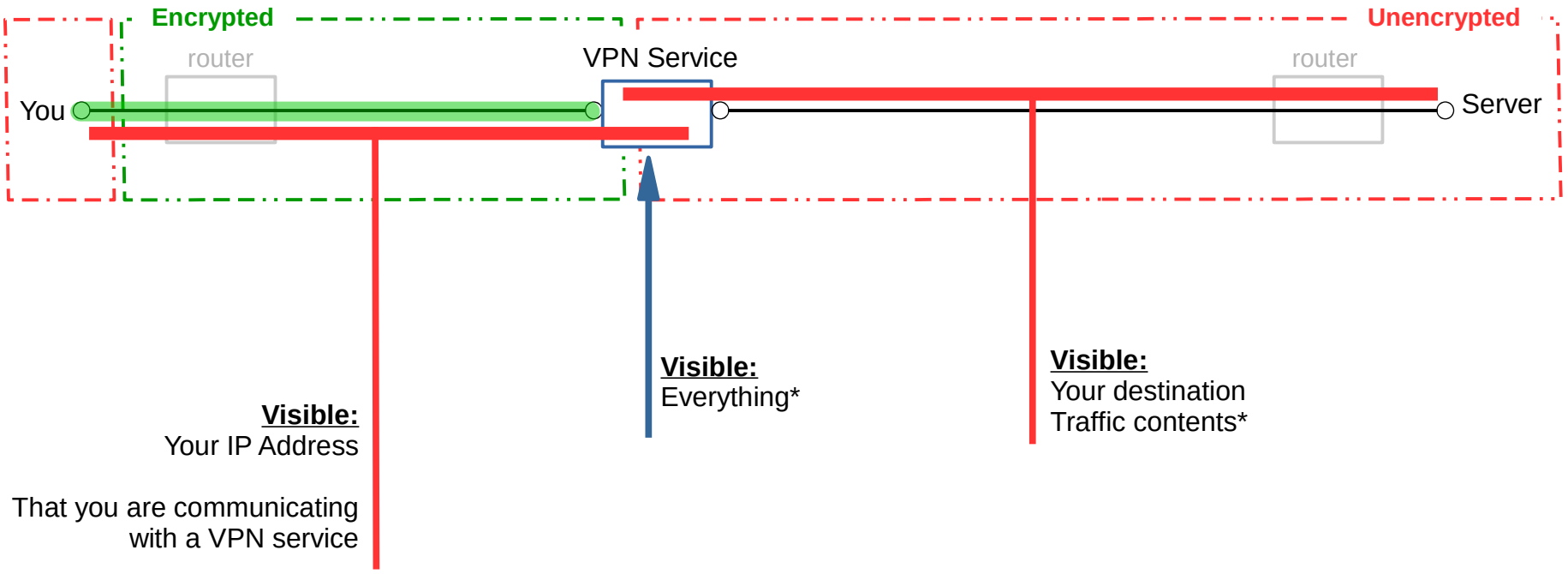
Generally unencrypted communications through an intermediary



* *Ignores application-level encryption*

VPN Services – Internet

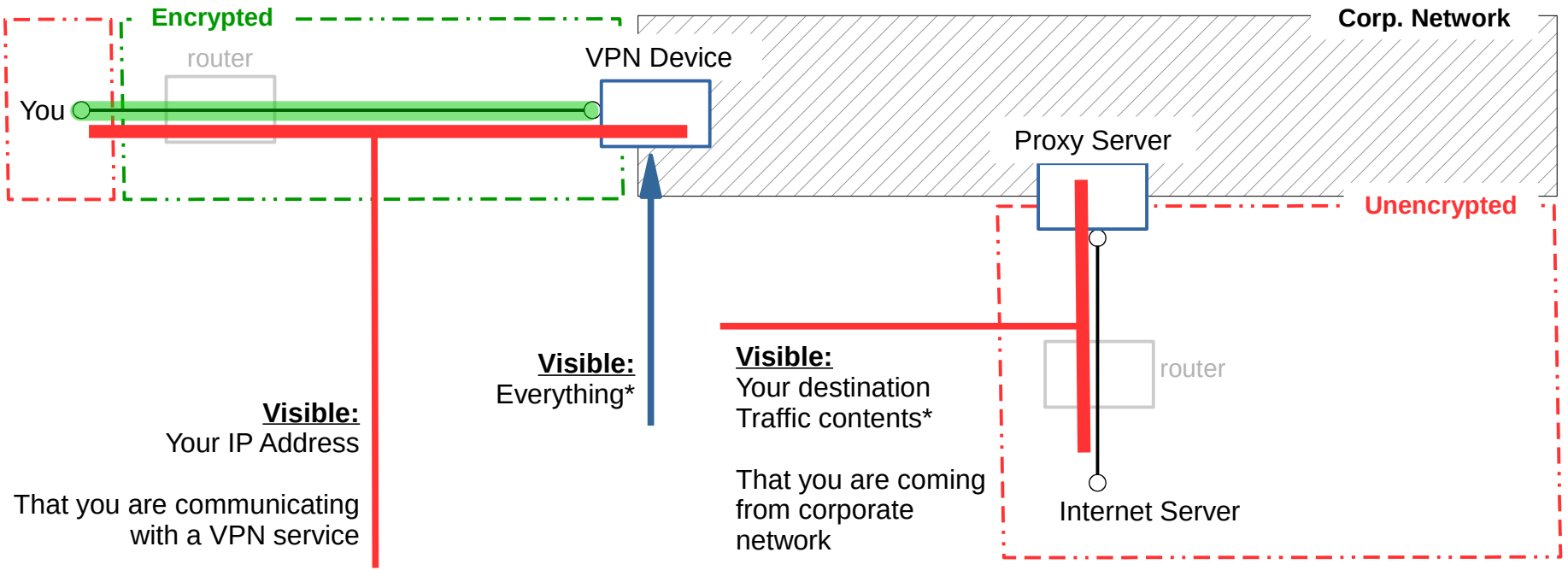
Encrypted tunnel to “trusted” location



* *Ignores application-level encryption*

VPN Services – Corporate

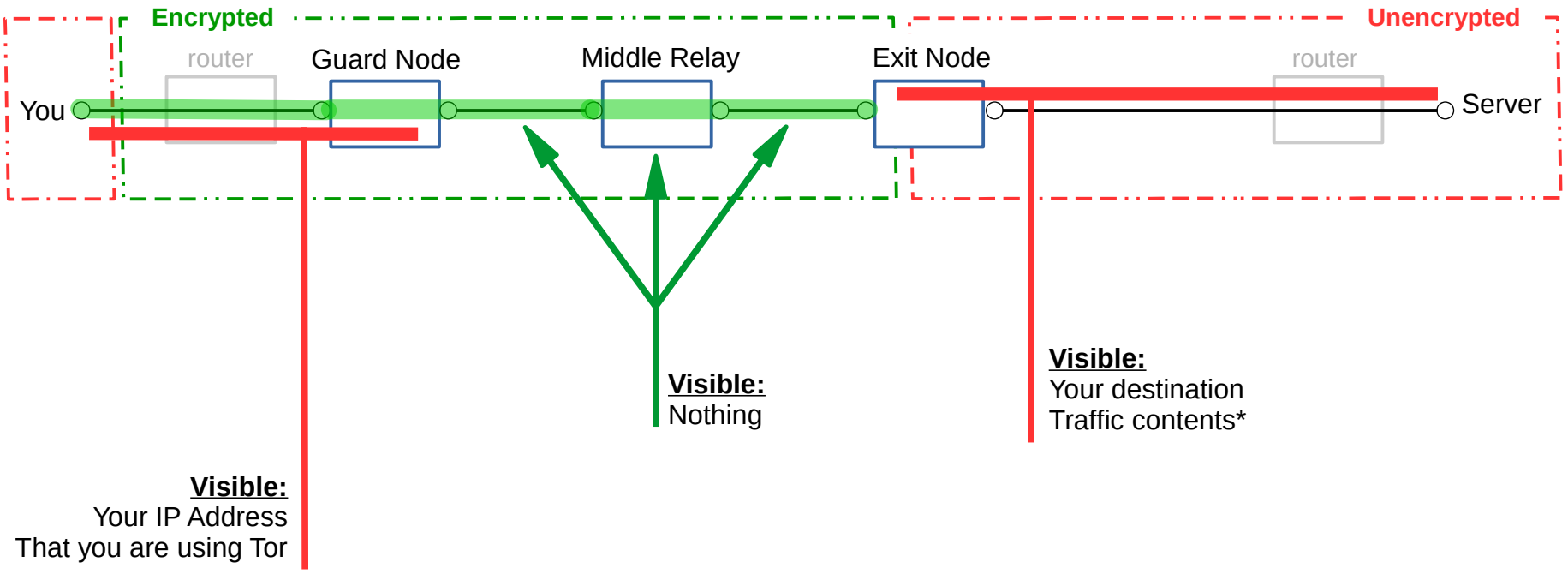
Encrypted tunnel to a typical corporate network



* *Ignores application-level encryption*

Tor

Anonymization and near-side encryption

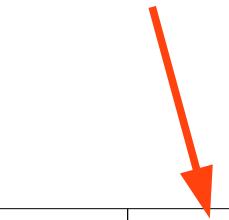


* *Ignores application-level encryption*

Use the right tool for the job.

And know no one tool can completely protect you.

Tor Browser Bundle



	Direct	Proxy	VPN	Tor	HTTPS	TBB
Censorship evasion		+	++	+++	+	+++
Make yourself appear elsewhere		+	++	+		+
Near-end encryption			++	+++	++	+++
Far-end encryption					++	
End-to-end encryption					++	
Anonymity		+	+	++		+++
Privacy		---	-	+	+	+++
Speed	+++	+	++	--		--

We know governments monitor us.

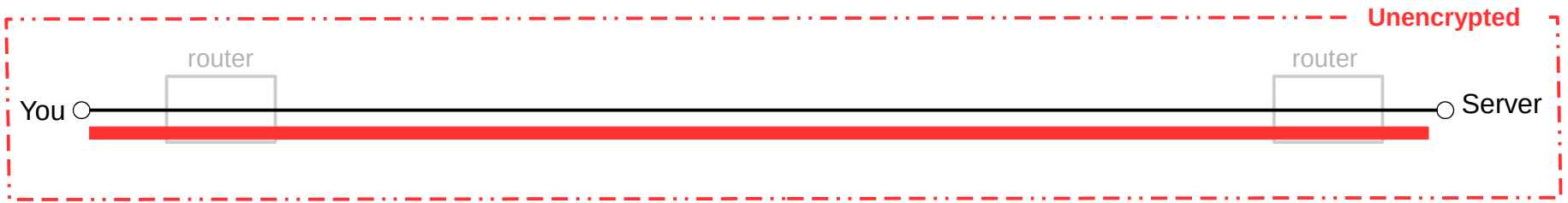
What about proxy, VPN and Tor operators?

What about governments leveraging these network locations with a high-density of “secretive” users?

Every network is untrusted—act accordingly.

Direct Communications

Pitfalls and Recommendations



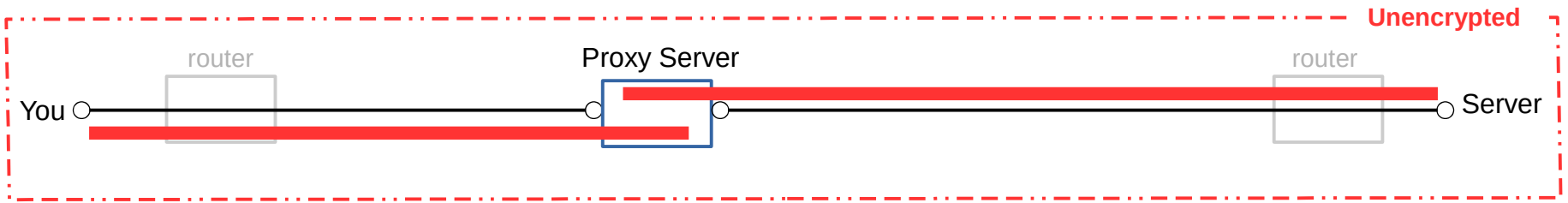
If...

- You're using a secure and robust protocol
- You're not facing censorship
- Your network traffic will not trigger ramifications

...a direct connection may actually be the best option

Proxy Servers

Pitfalls and Recommendations



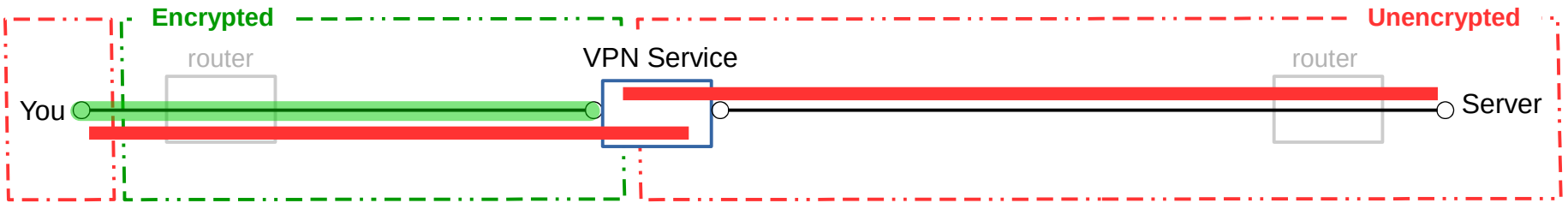
	Direct	Proxy	VPN	Tor	HTTPS	TBB
Censorship evasion		+	++	+++	+	+++
Make yourself appear elsewhere		+	++	+		+
Near-end encryption			++	+++	++	+++
Far-end encryption					++	
End-to-end encryption					++	
Anonymity		+	+	++		+++
Privacy		---	-	+	+	+++

Outside of “corporate” environments, unless you have a very specific need, just don't use proxies.

VPNs are nearly-free, much less risky, and have stronger benefits.

VPN Services – Internet

Pitfalls and Recommendations



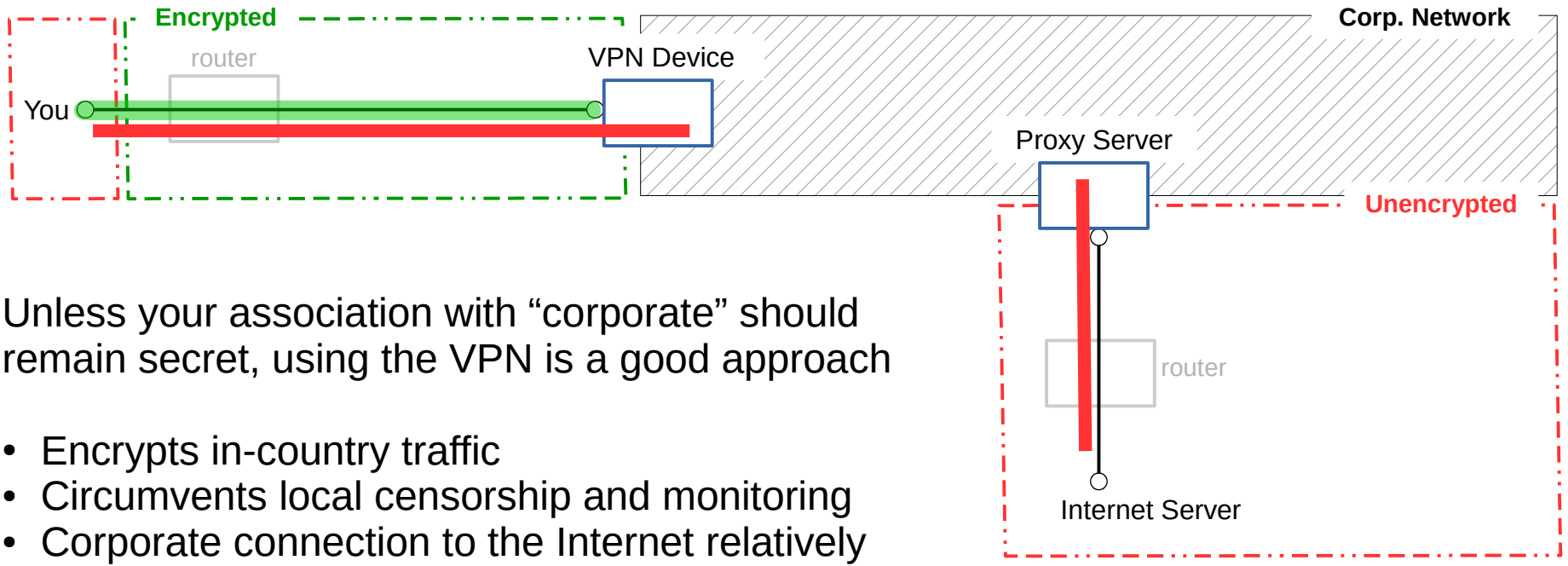
If the task does not require anonymity and Tor is just too slow, VPNs are an option.

Very critical to select a reputable provider.

- Do they have a privacy policy?
- What geographies are they in?
- What governments have jurisdiction?
- Will their VPN client expose you to security issues?

VPN Services – Corporate

Pitfalls and Recommendations



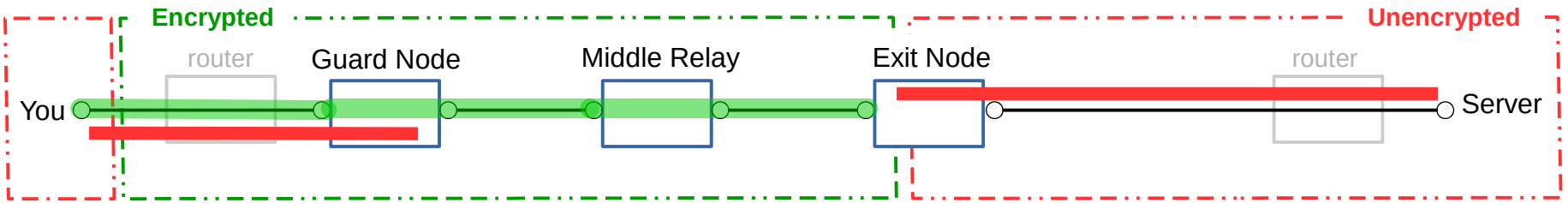
Unless your association with “corporate” should remain secret, using the VPN is a good approach

- Encrypts in-country traffic
- Circumvents local censorship and monitoring
- Corporate connection to the Internet relatively trusted

Make sure you are actually connected!

Tor

Pitfalls and Recommendations



Real online anonymity is very difficult. If you require it you must use Tor Browser Bundle (TBB) or TAILS.

Don't do anything that would provide a link to your identity

- Don't connect to any site or service you use without TBB or TAILS
- If your use of Tor is a one-time occurrence, consider using TAILS from an unfamiliar location

Recommendations

- Treat every network as untrusted
- Use secure protocols everywhere
- To evade censorship and monitoring, use Tor together with secure protocols

Thank you.