ROSE-HULMAN INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

Day 27: Virtual Private Network

Slides modified from slides designed by Professor Kevin (Wenliang) Du

Outline

- Motivation
- Private Networks
- Requirements
- IP Tunneling
- SSL/TLS-based VPN

Private Networks

- Organization want to keep networks **private**

- Use private IP addresses
  - `10.0.0.0/8`, `192.168.0.0/16`

- Keep outsiders out of the network

Why Private Networks?

- Network in different locations can be “private”

- Firewall rules are used to keep undesired actors out

- But we need desired actors to still access private network areas

Requirements

- ❑ Allow legitimate users access private networks from the outside

- ❑ What do private networks guarantee?
  - Authentication
  - Protection (i.e., encryption)
  - Integrity No one can mess with your packets

- Authentication
- Encryption (privacy)

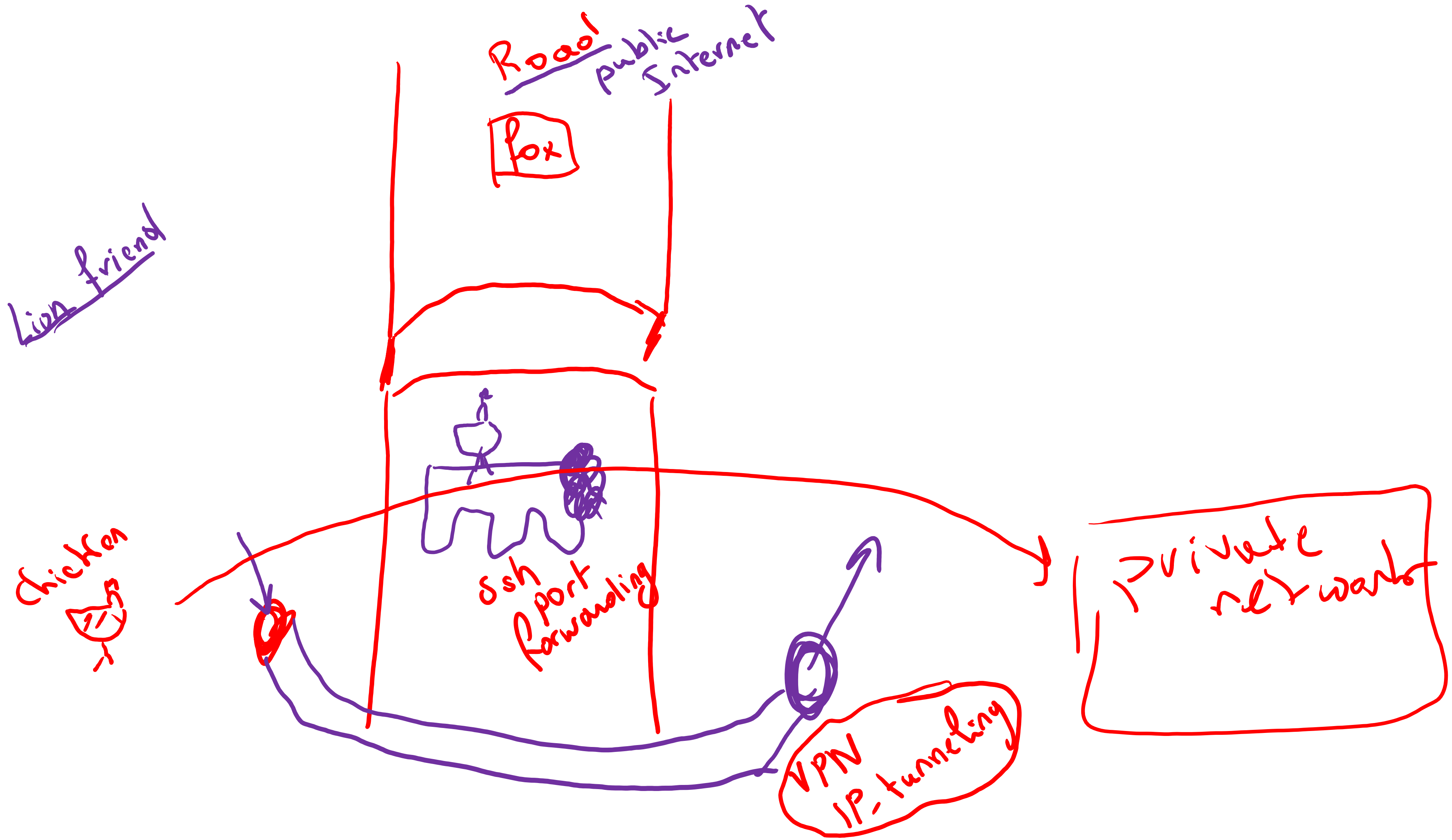
Goals

- ❑ Achieve **private properties** without being physically on location

- ❑ Be ***virtually* present** on premise

- ❑ Virtual Private Network (VPN)

The Chicken Analogy



Transparency

- We also want to achieve transparency

- Regardless of application support, data must be protected (e.g., chrome is not aware of the VPN)

How to send a packet from A to B **securely,** as if A and B were physically on the same network.

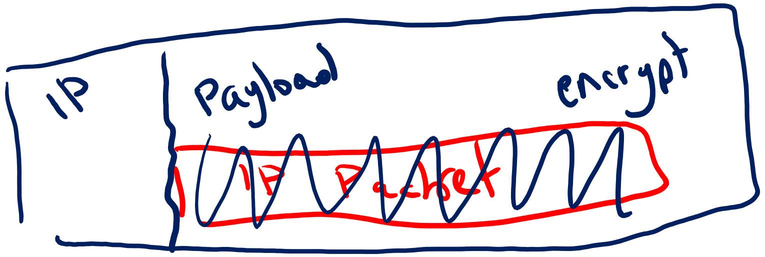
The Dilemma

- To achieve **transparency**, we must do protection at **the IP level**

- BUT, all fields of the IP packet (including the header) must be **encrypted**

- *Dilemma*: How to route an encrypted IP packet?

IP Tunneling

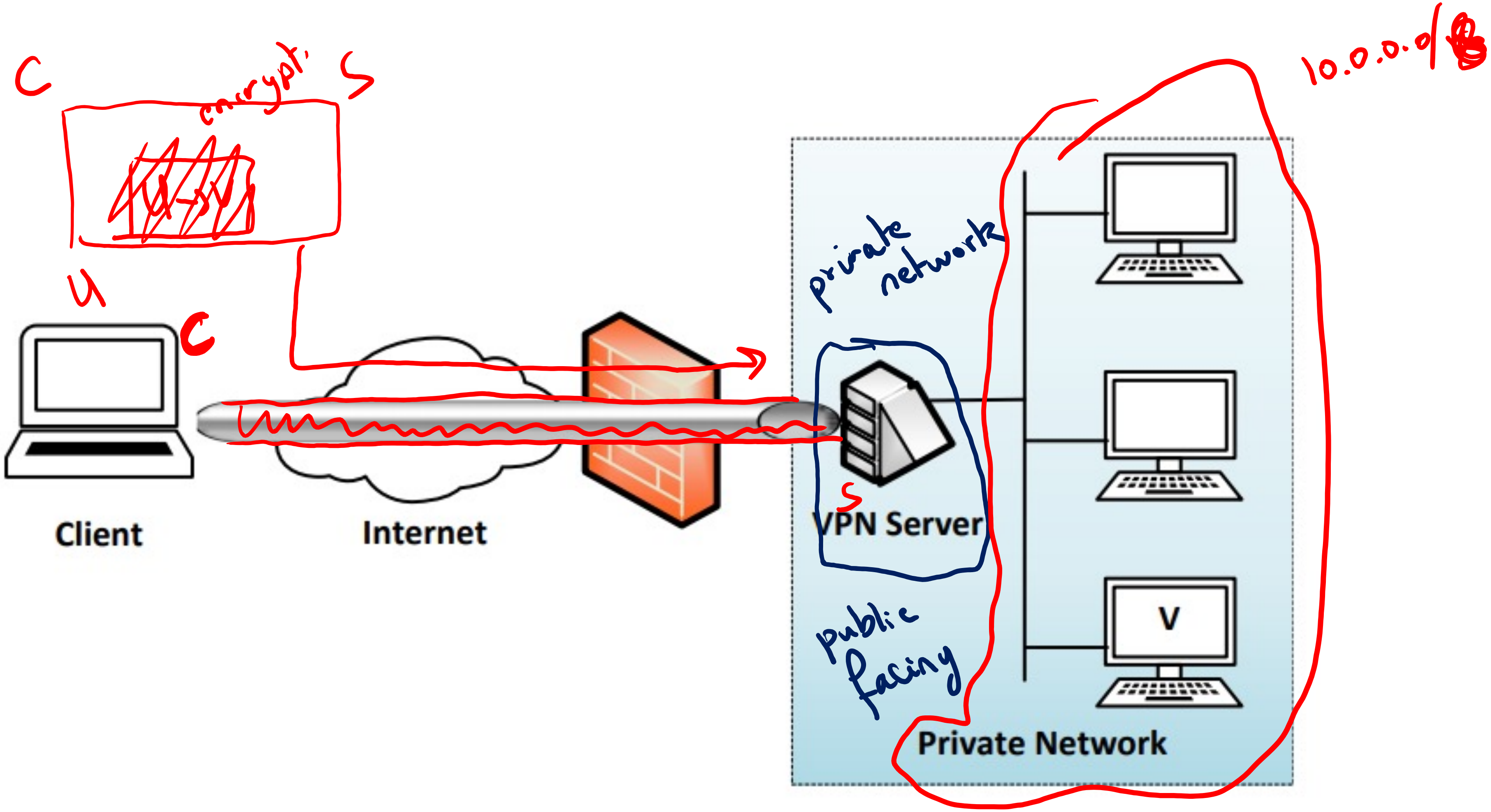


- ❑ **Encapsulate** encrypted packet inside IP packet

- ❑ Packets are encrypted before the start of the tunnel

- ❑ Packet are decrypted at the other end of the tunnel

IP Tunneling



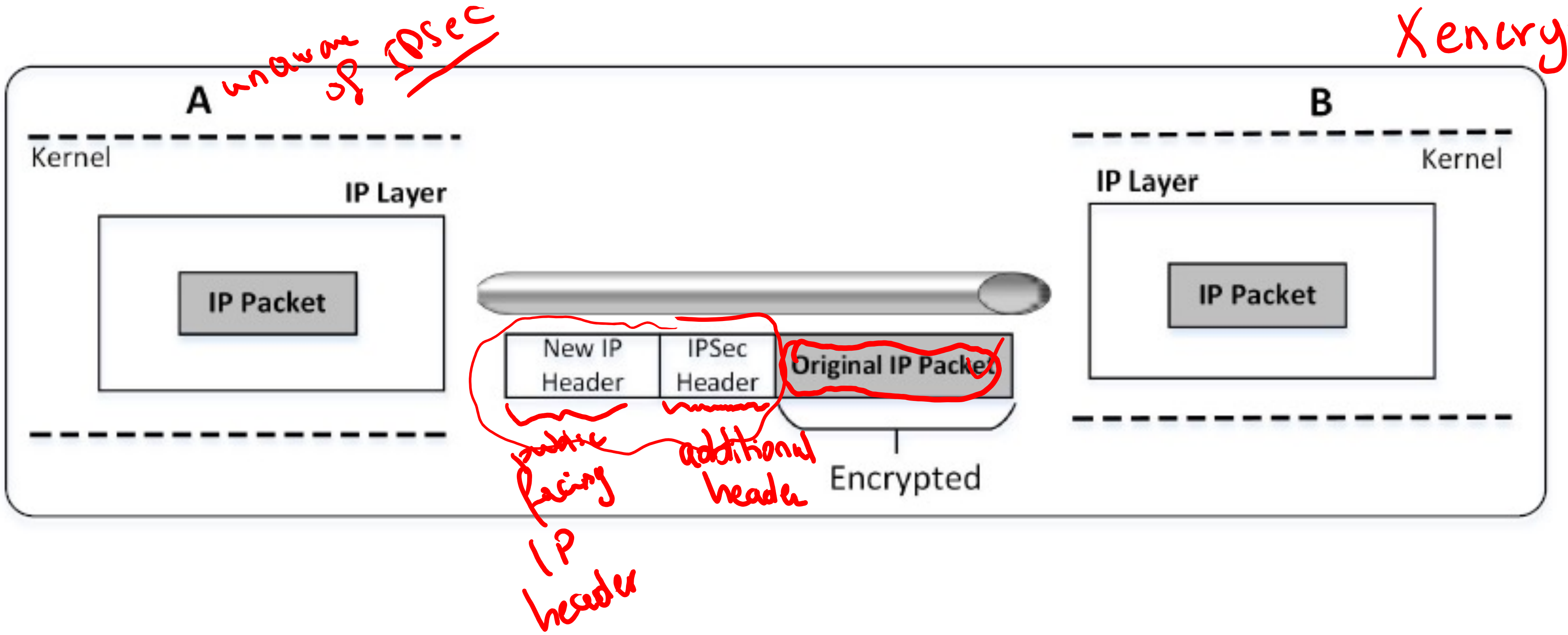
IPSec Tunneling

Inside of the kernel using IPSec

✓ transparency!

✗ Need system calls

✗ encryption is done in the kernel

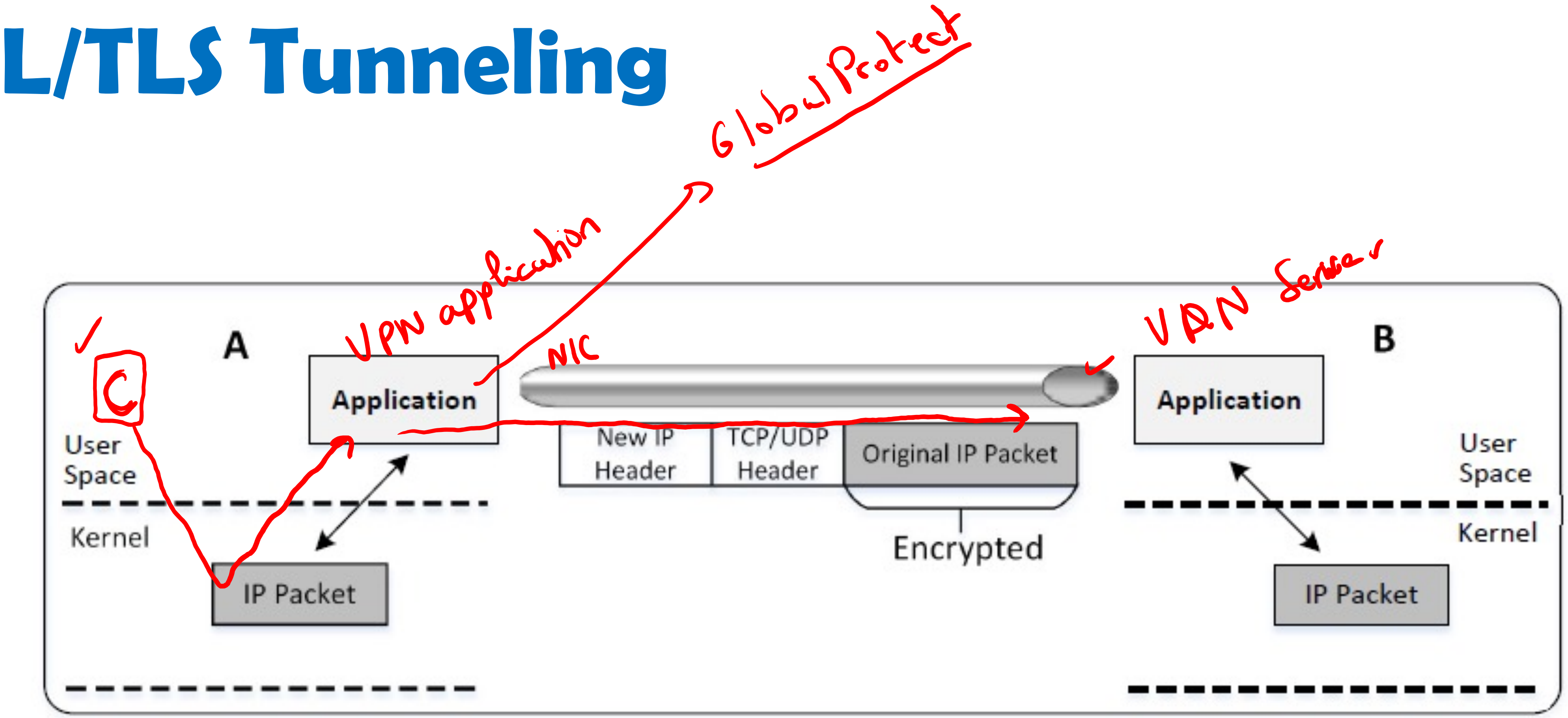


unaware of IPSec

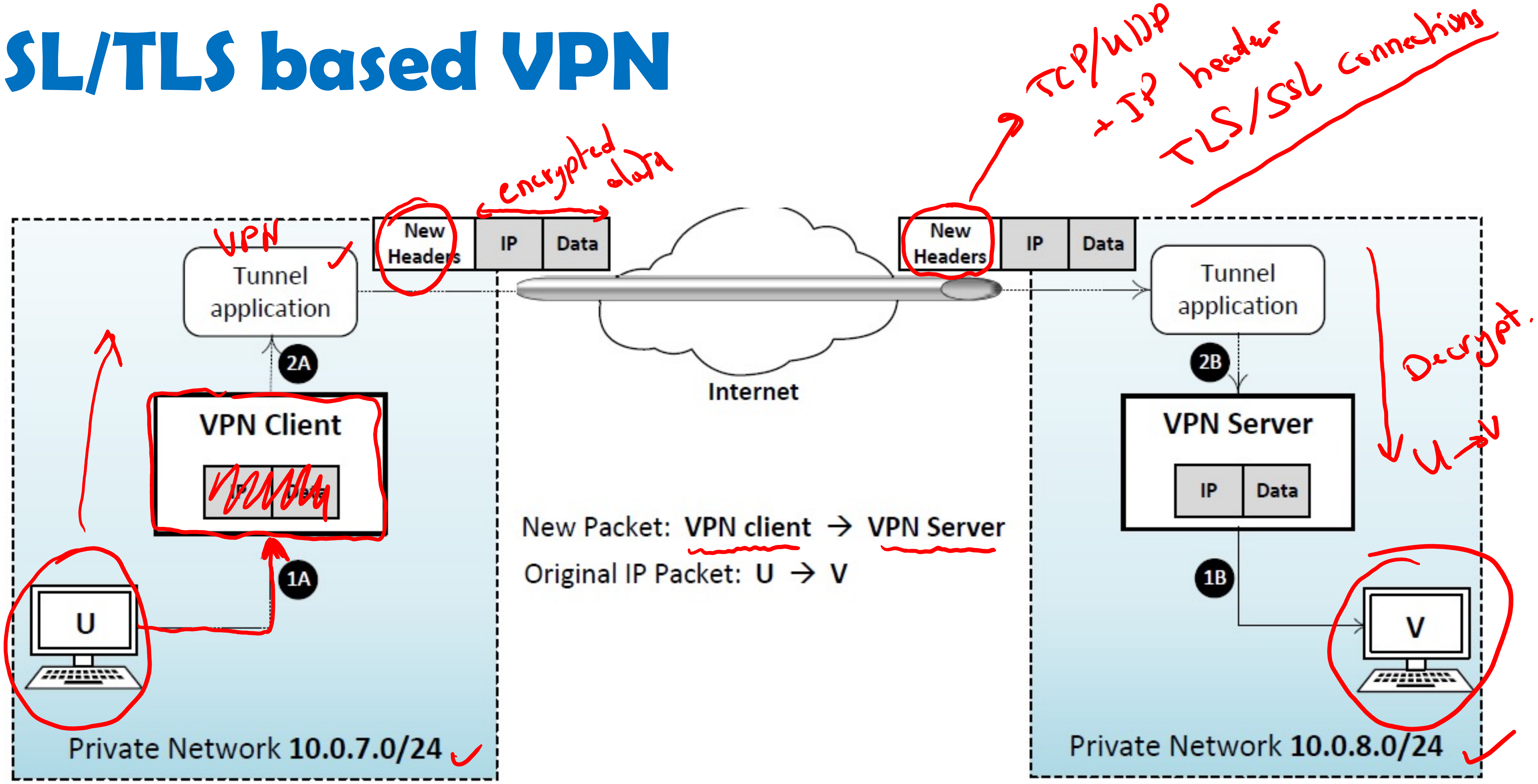
public facing IP header

additional header

SSL/TLS Tunneling



SSL/TLS based VPN



New Packet: VPN client → VPN Server

Original IP Packet: U → V

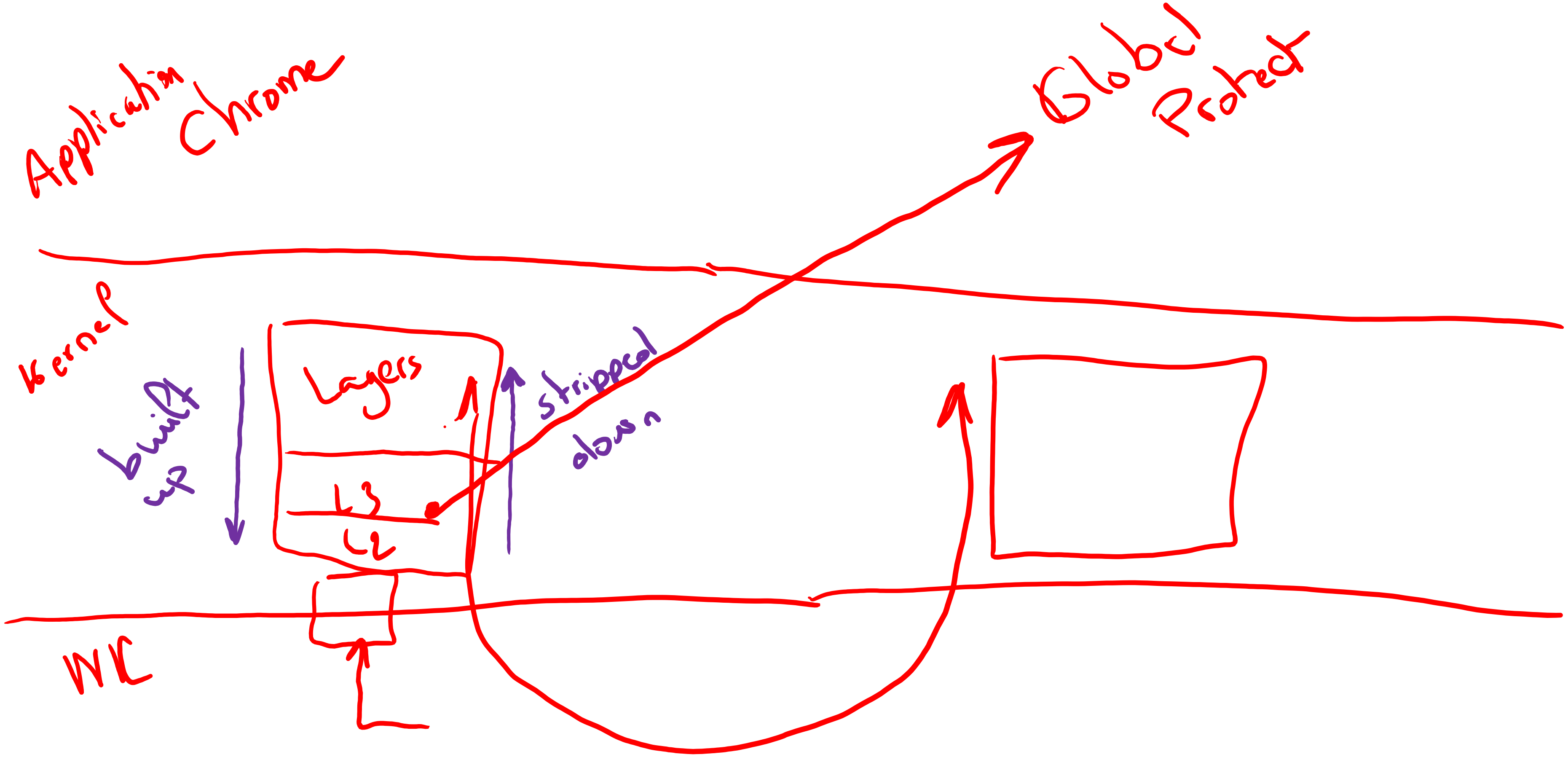
VPN Applications

- But how can an application grab a packet from the kernel?

- Sniffing only gets a copy of the packet

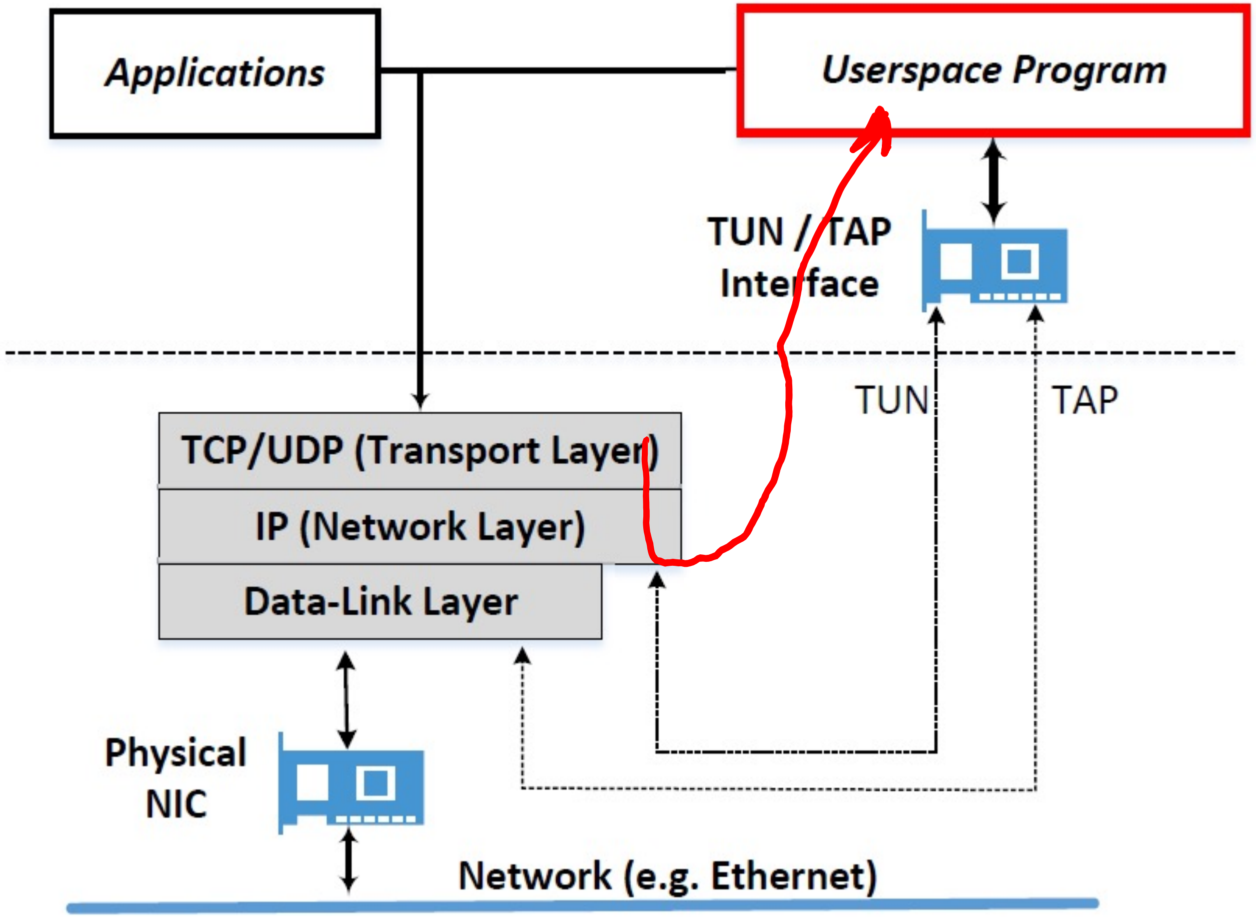
- We need to interject into the path of the packet ✓

How Applications Get Packets?



The Loopback Interface

Virtual Interfaces


Applications
Userspace Program
TUN / TAP
Interface
TUN
TAP
TCP/UDP (Transport Layer)
IP (Network Layer)
Data-Link Layer
Physical
NIC
Network (e.g. Ethernet)