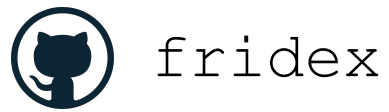


# AF\_KTLS

A Linux kernel TLS/DTLS module

Fridolín Pokorný  
fridolin@redhat.com



# What is TLS/DTLS?

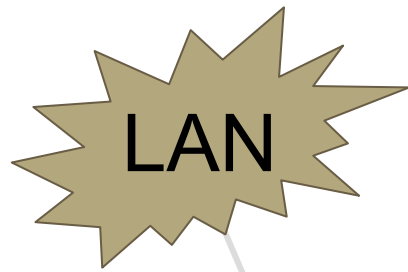
- (Datagram) Transport Layer Security
  - Secured Sockets Layer (SSL)
- version 1.2, draft 1.3
- GnuTLS, OpenSSL

# TLS/DTLS Protocols

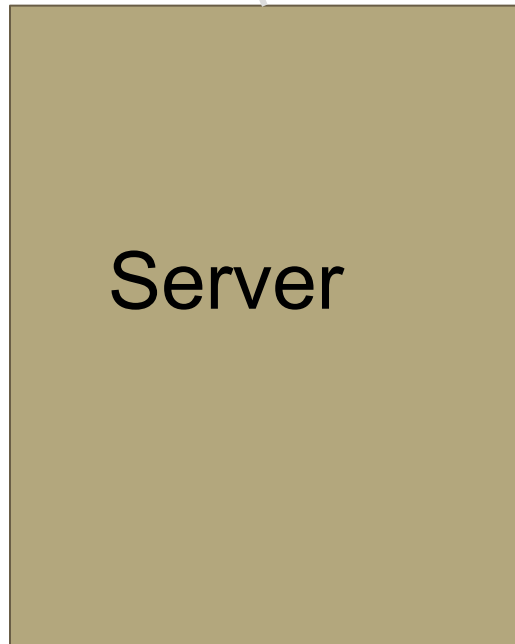
- Control layer and Record layer
- TLS
  - reliable underlying protocol (e.g. TCP)
- DTLS
  - unreliable underlying protocol (e.g. UDP)
  - additional information about state

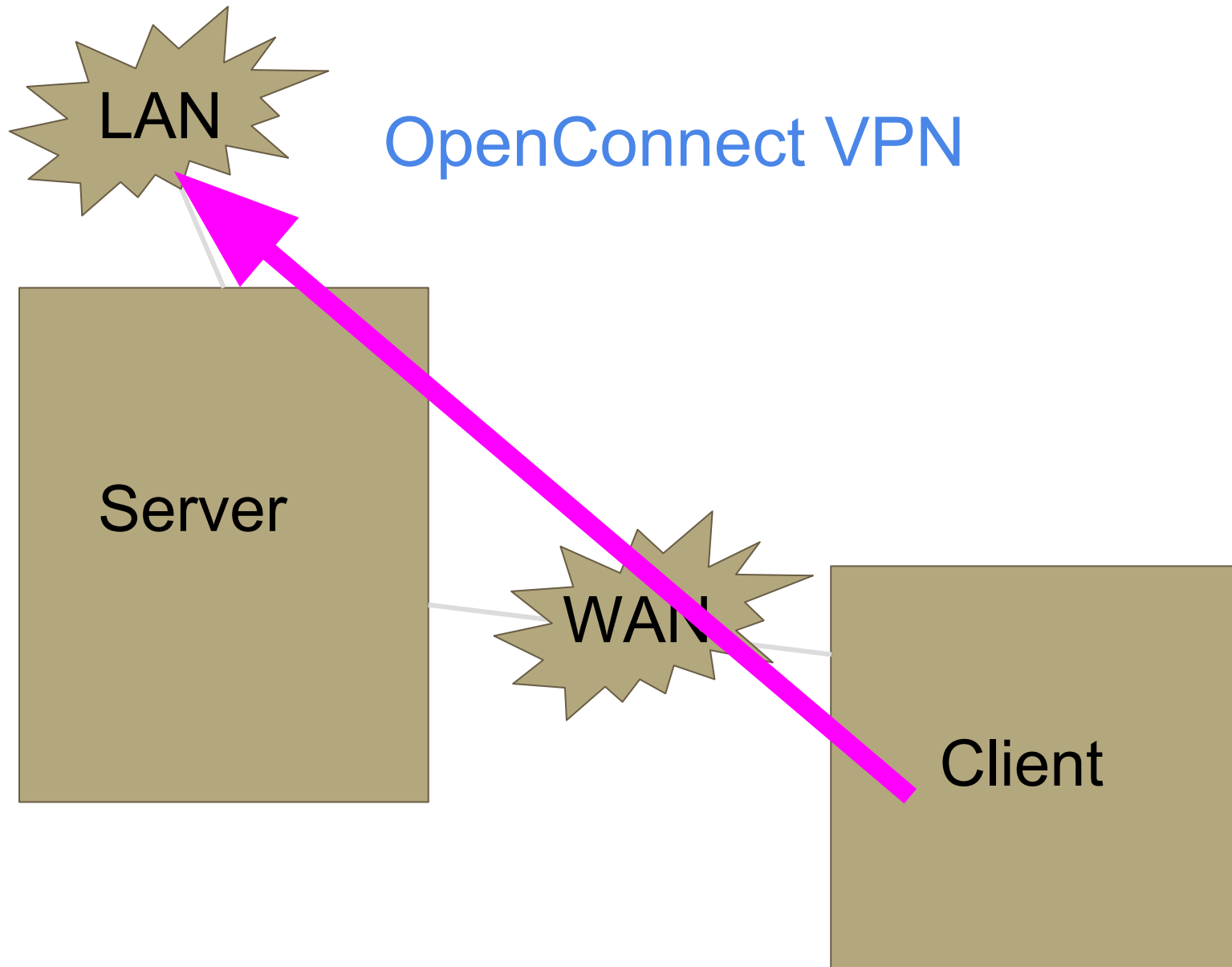
# TLS/DTLS Usage

- HTTPS, e-mail
- HAProxy
- SSL based VPNs
  - OpenConnect
  - CISCO AnyConnect

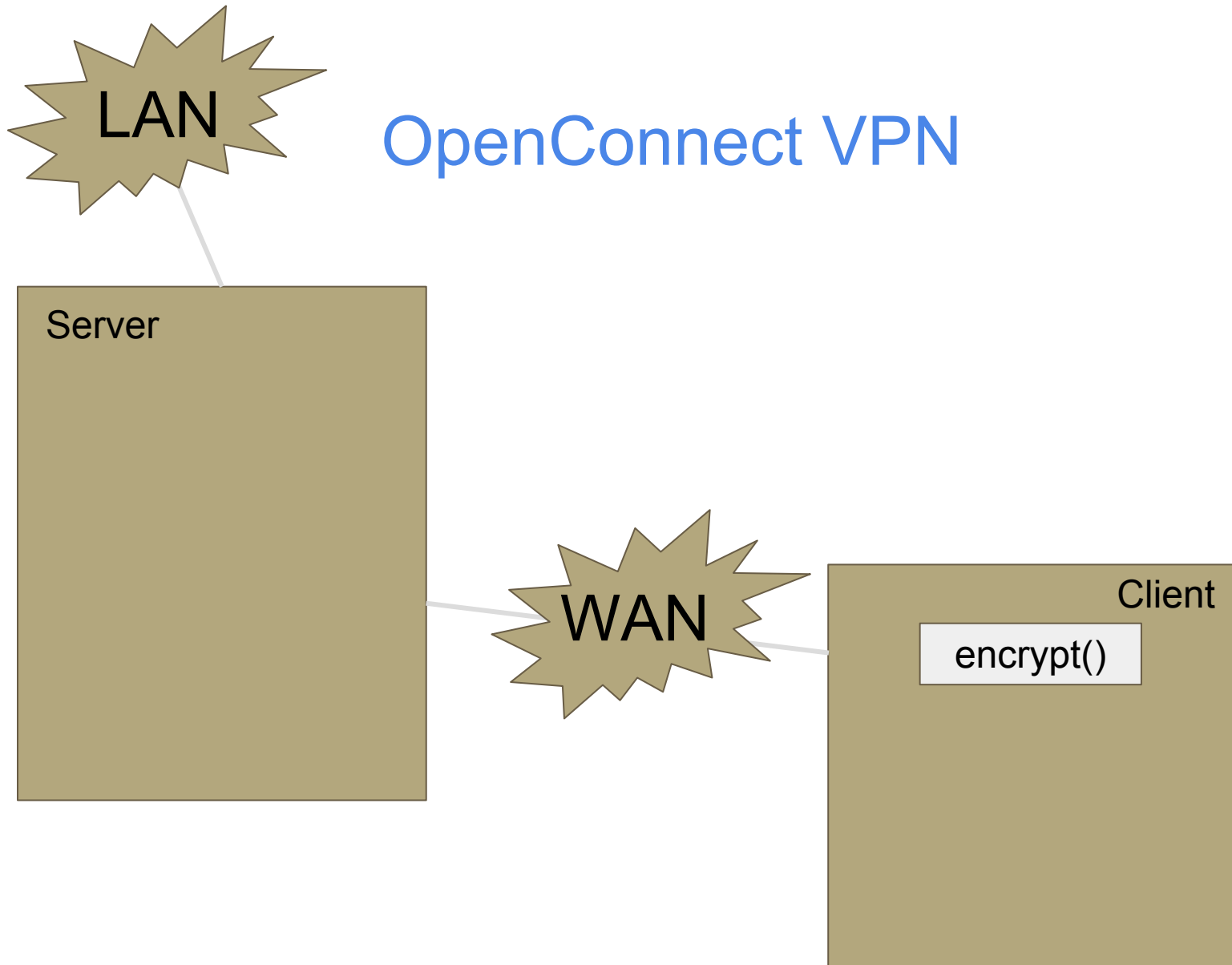


## OpenConnect VPN

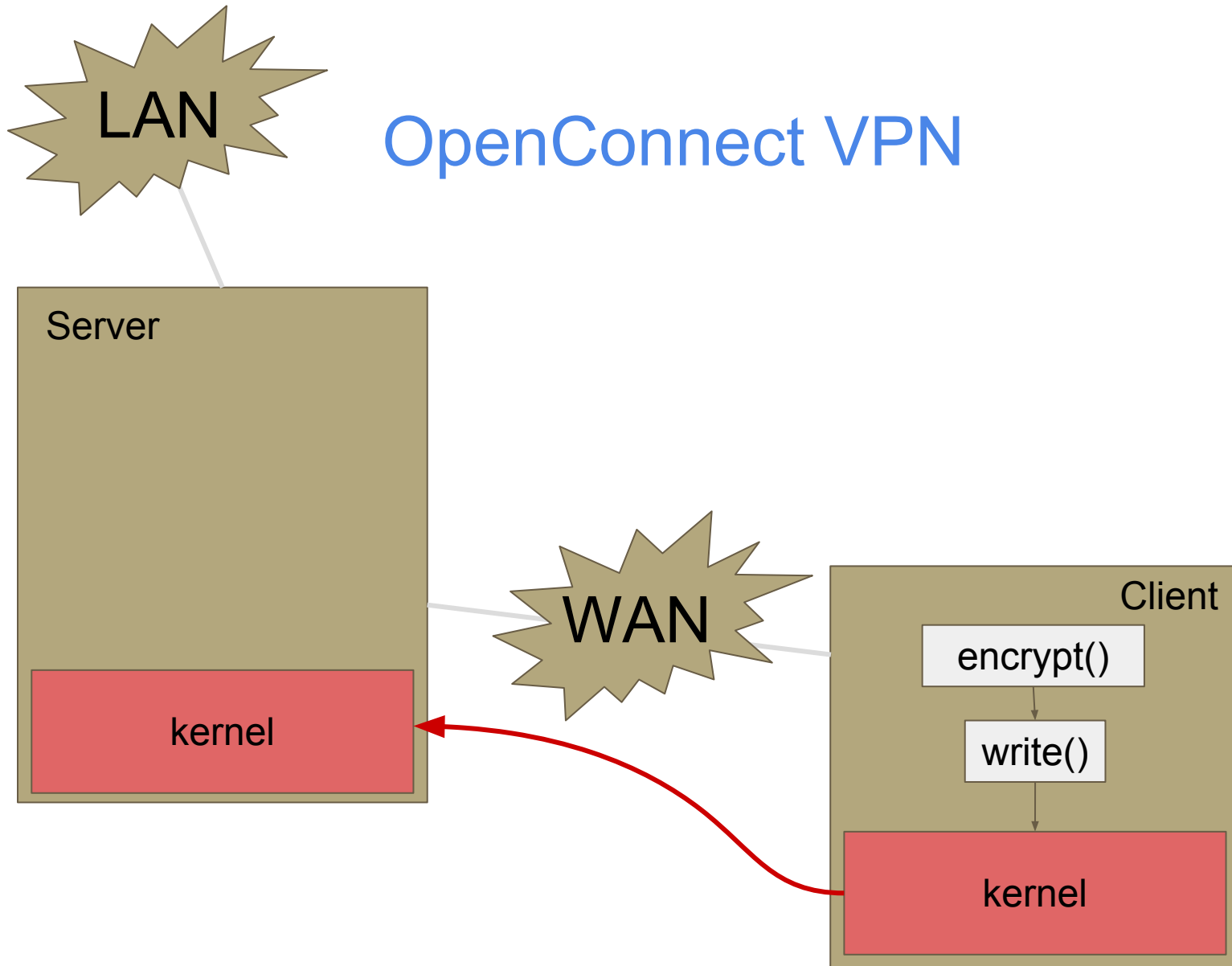




# OpenConnect VPN

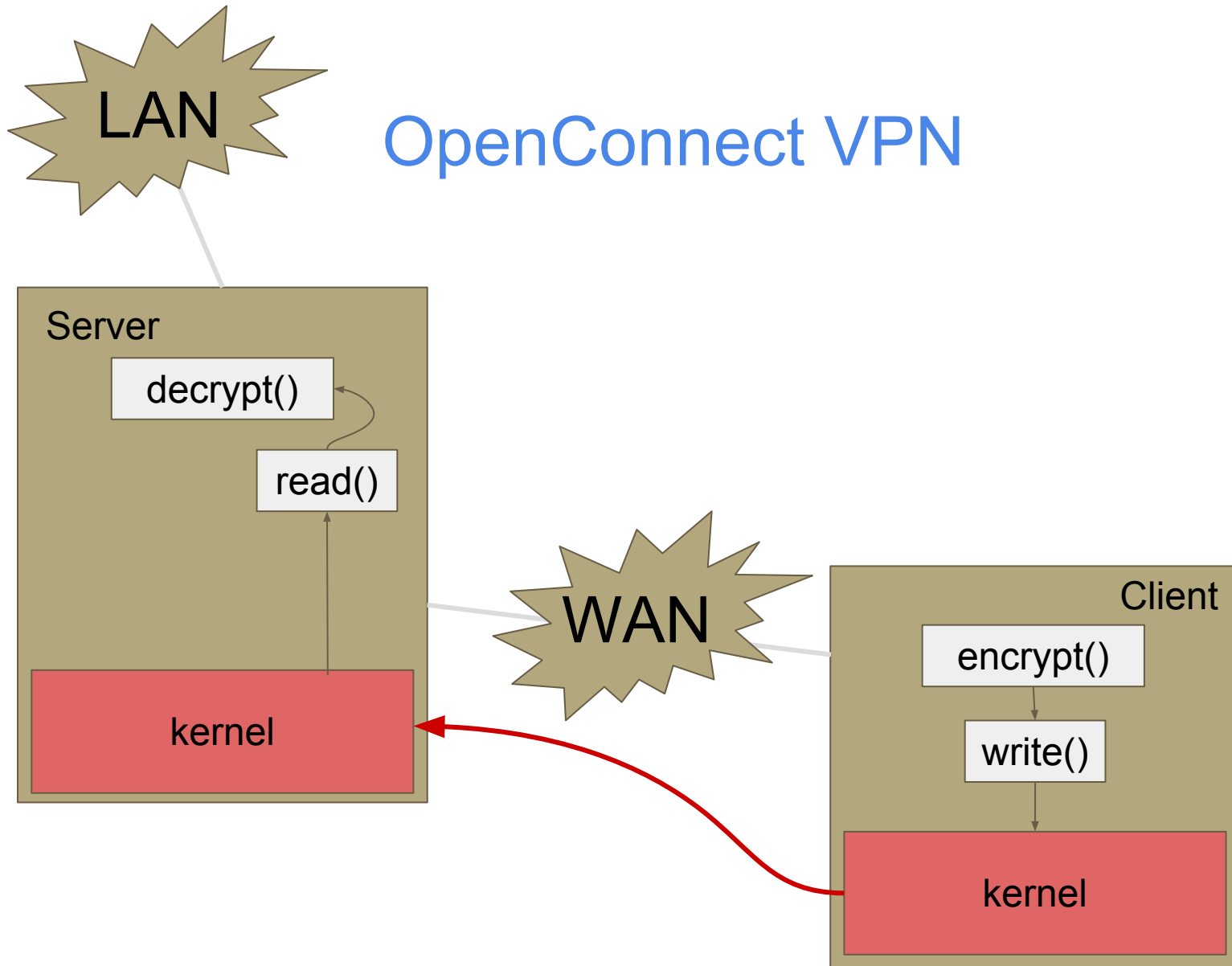


# OpenConnect VPN

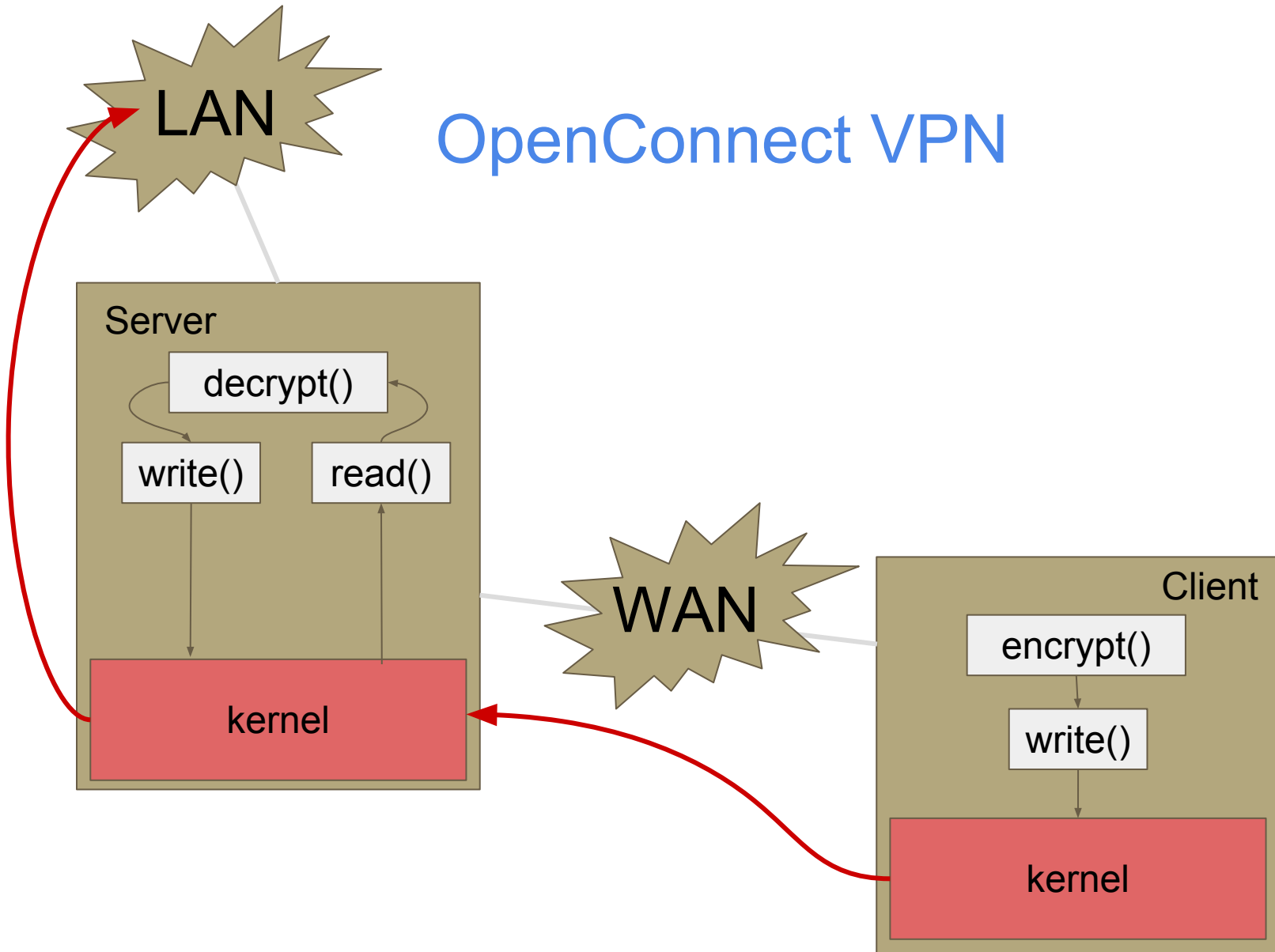




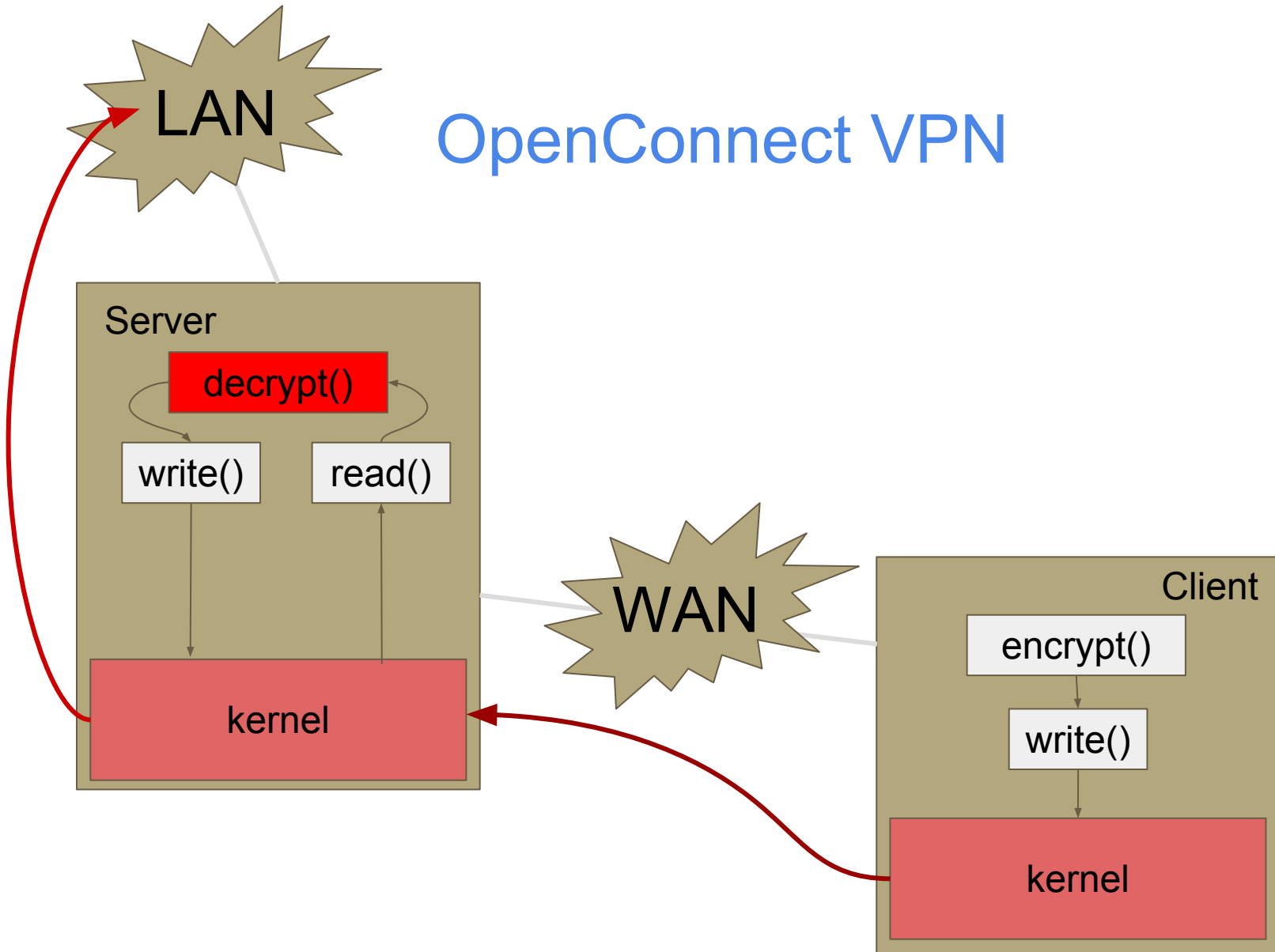
# OpenConnect VPN



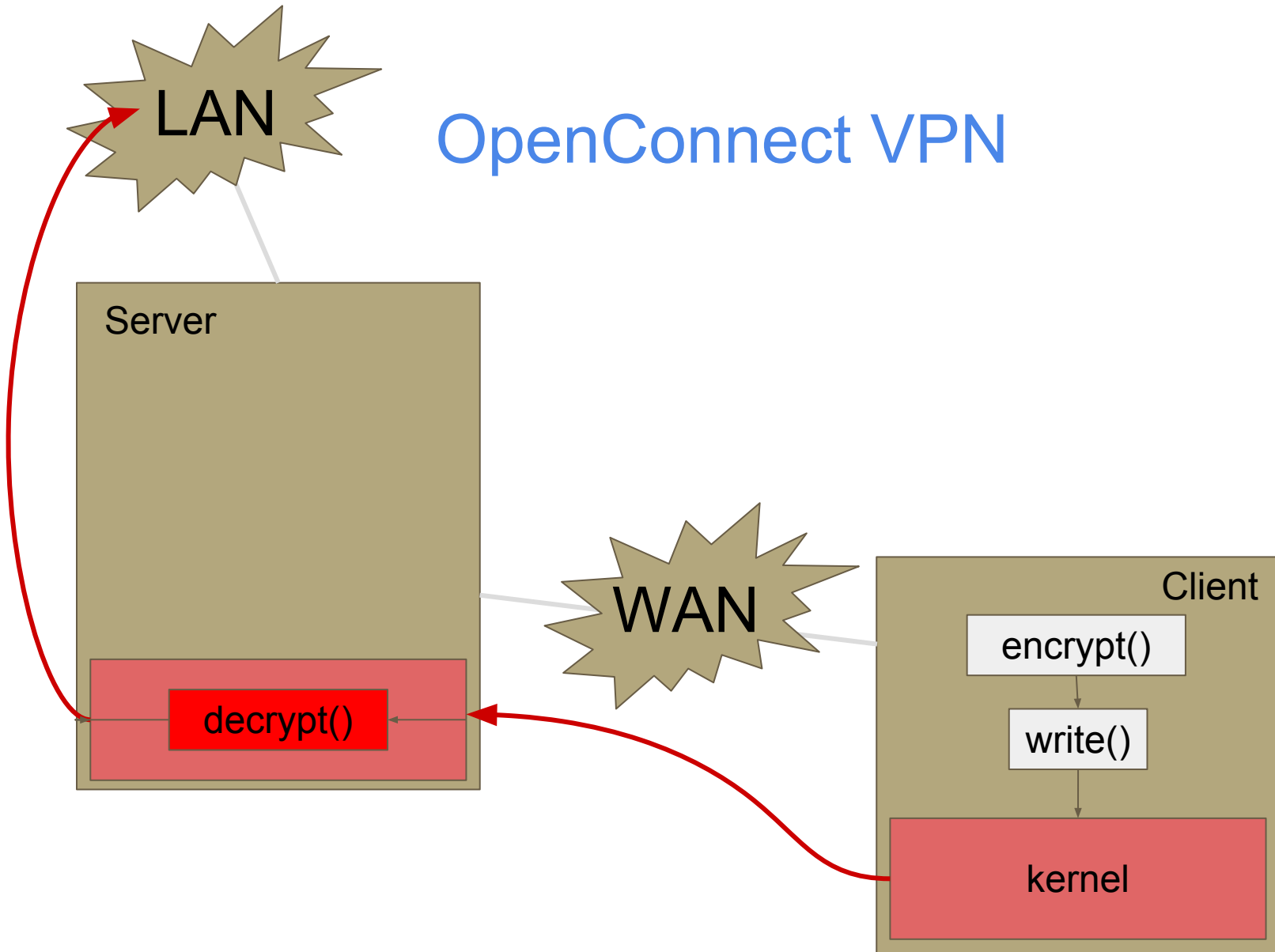
# OpenConnect VPN



# OpenConnect VPN

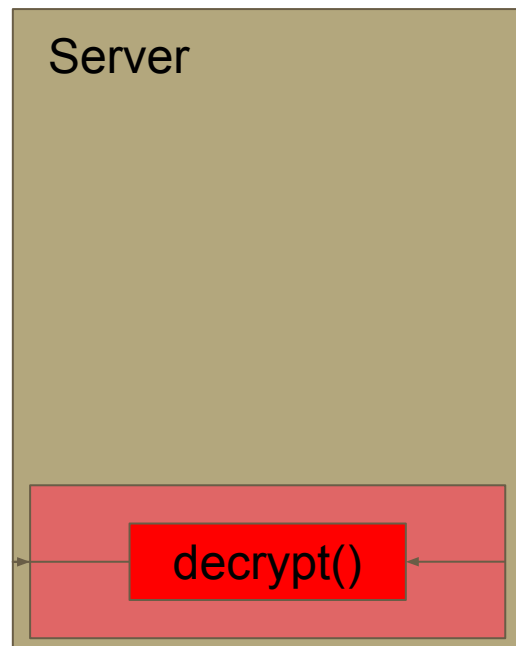


# OpenConnect VPN

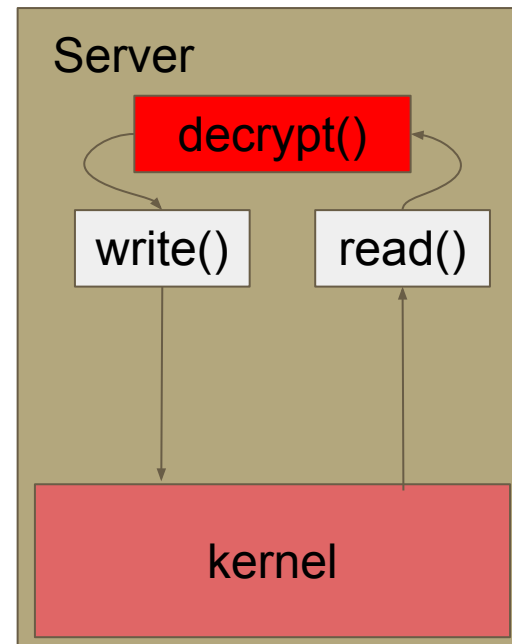


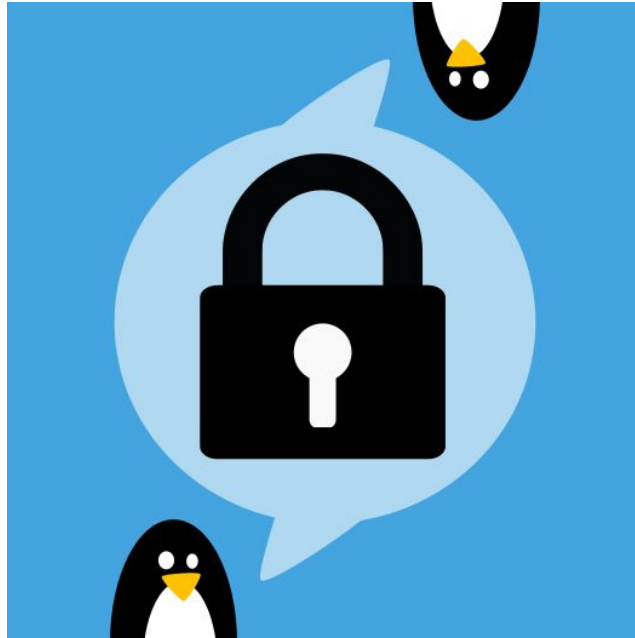
# Optimization

- saved 2 context switches, 2 copies

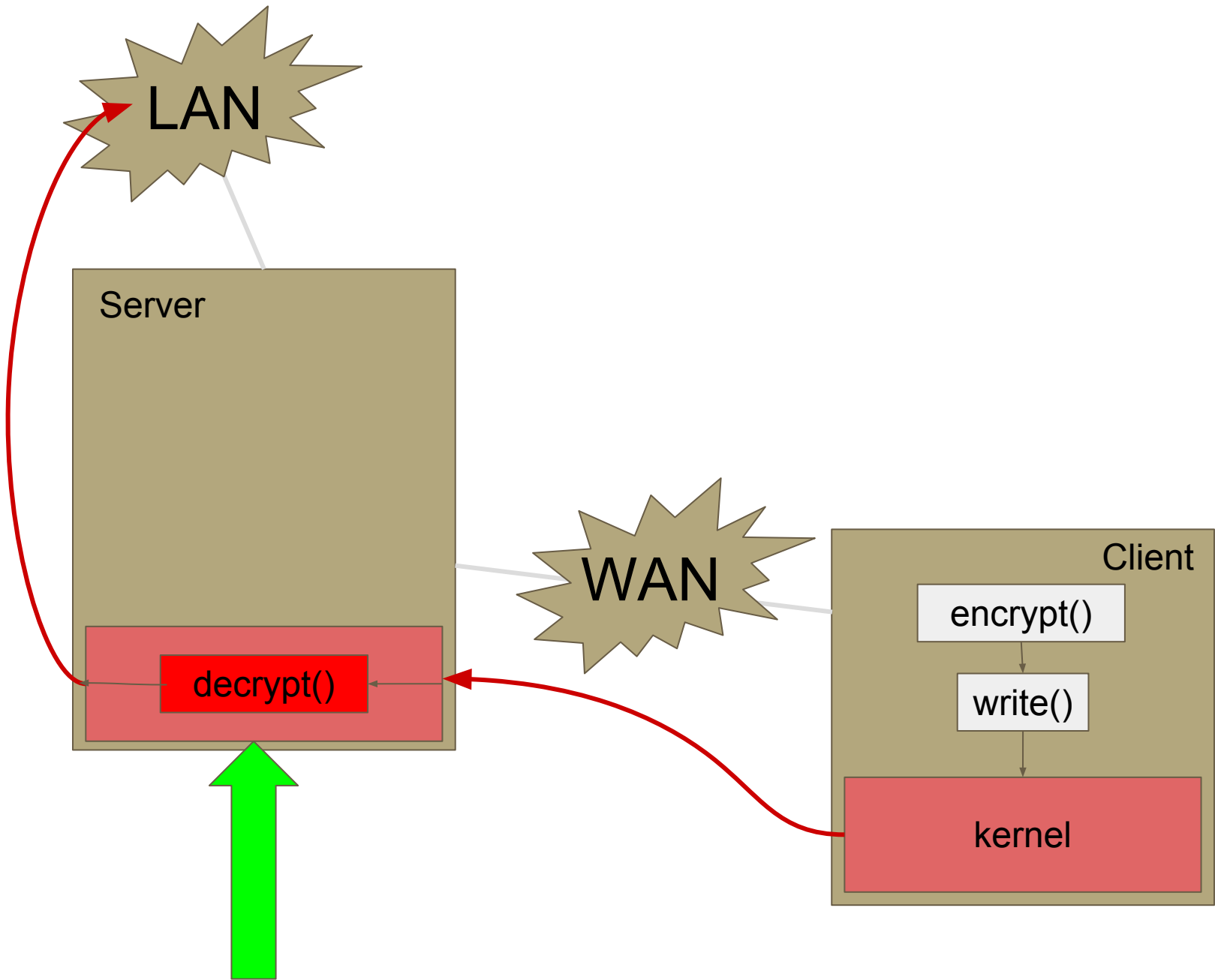


Vs.





AF\_KTLS



# AF\_KTLS

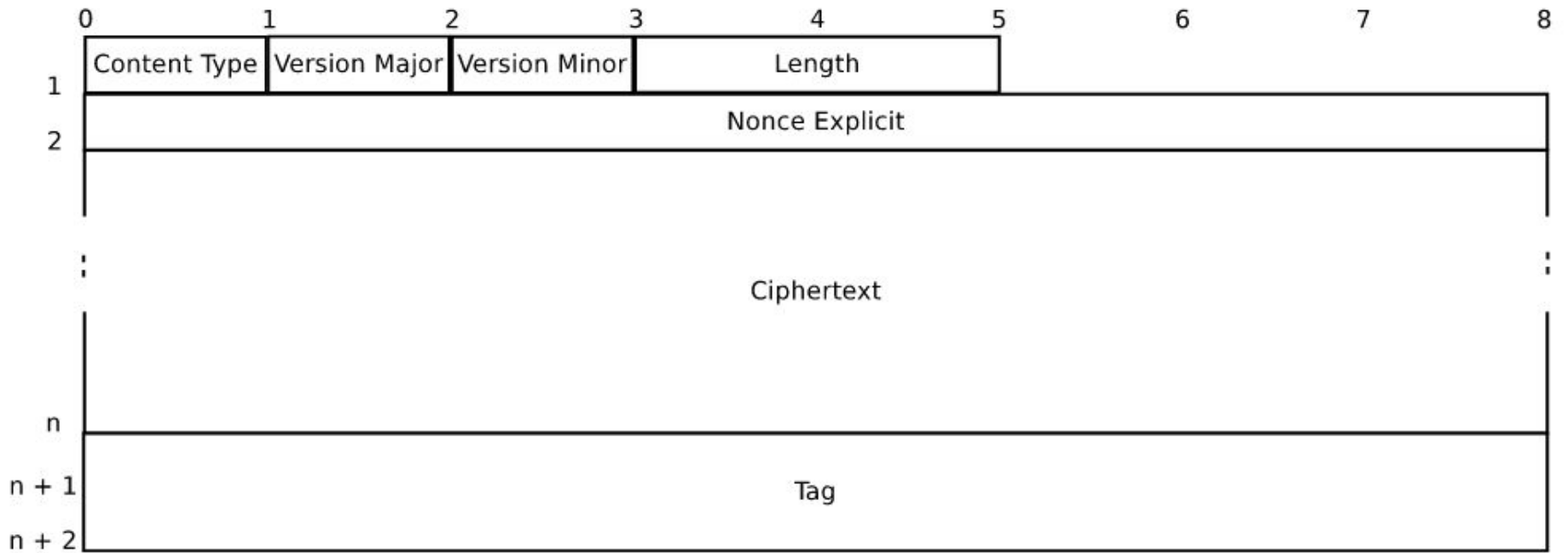
- new socket type AF\_KTLS
- TLS/DTLS record layer
- handshake in user space
- AES GCM
- socket operations
  - socket(2), bind(2), send(2), recv(2), ...



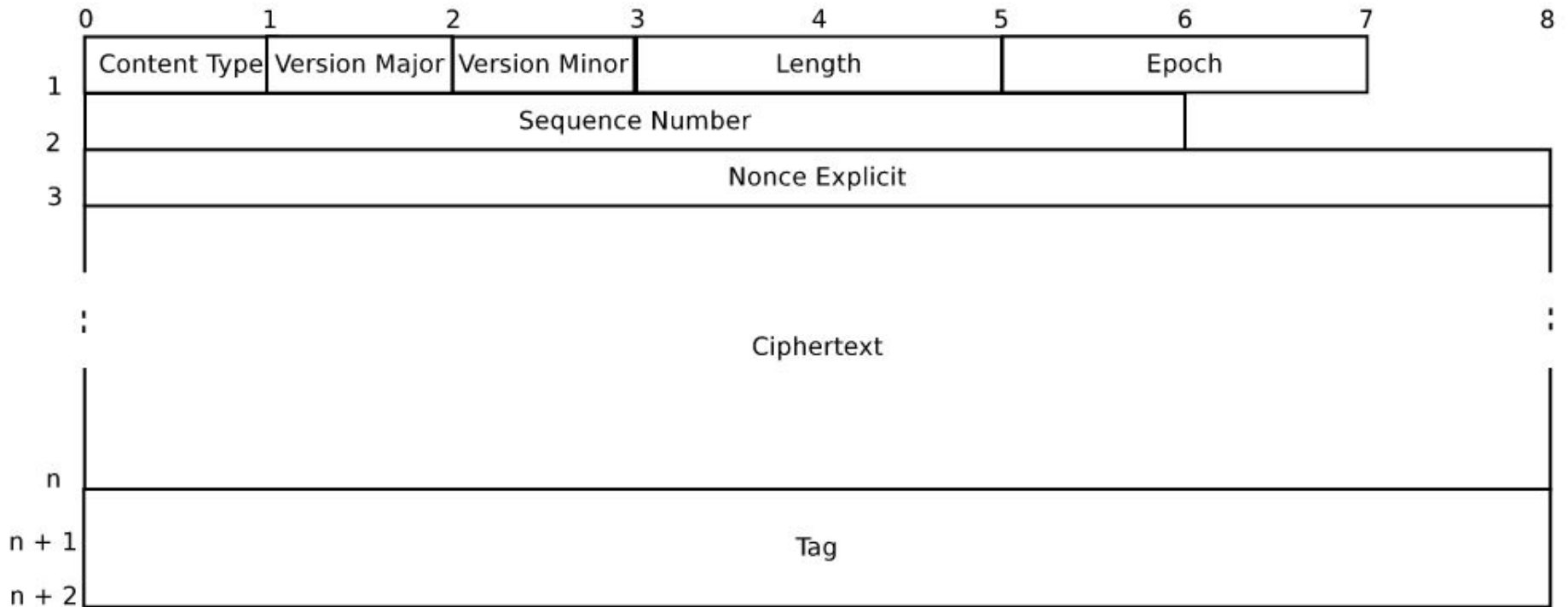
# Optimization

- 2 context switch
  - ideally, not possible
  - `sendfile(2)`, `splice(2)` ?
    - data in a pipe (kernel)
- 2 copies
  - data only in kernel space
- issues with padding

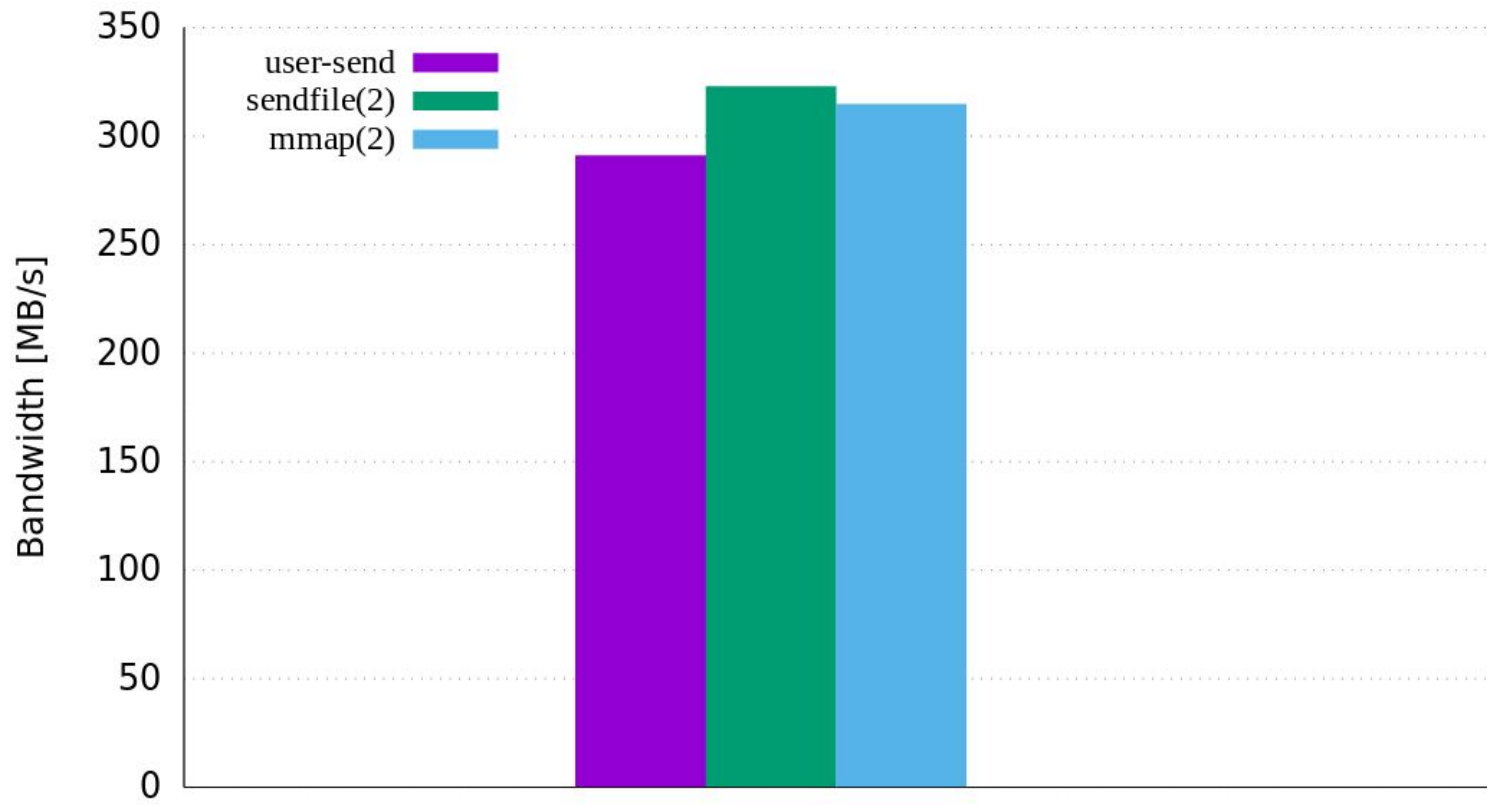
# TLS Record - AEAD ciphers



# DTLS Record - AEAD ciphers



# Optimization Results



## AF\_KTLS usages

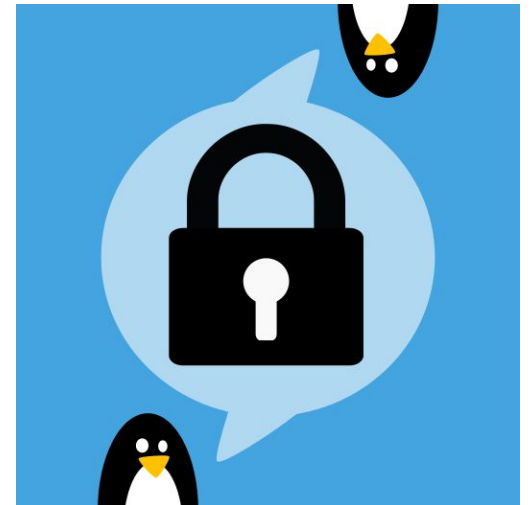
- OpenConnect VPN - TUN/TAP device support
- KCM
- Access raw data in kernel
  - Linux Socket Filtering
  - BCC
- NIC offloading

# TLS in kernel

- Solaris
  - ktls
- Netflix
  - BSD's sendfile(2) optimization
- Red Hat/Facebook
  - AF\_KTLS

# AF\_KTLS

<https://github.com/ktls>



# AF\_KTLS Questions?

- [\*\*https://github.com/ktls\*\*](https://github.com/ktls)
- [\*\*http://tinyurl.com/af-ktls\*\*](http://tinyurl.com/af-ktls)
- [\*\*http://netdevconf.org/1.2/session.html?dave-watson\*\*](http://netdevconf.org/1.2/session.html?dave-watson)