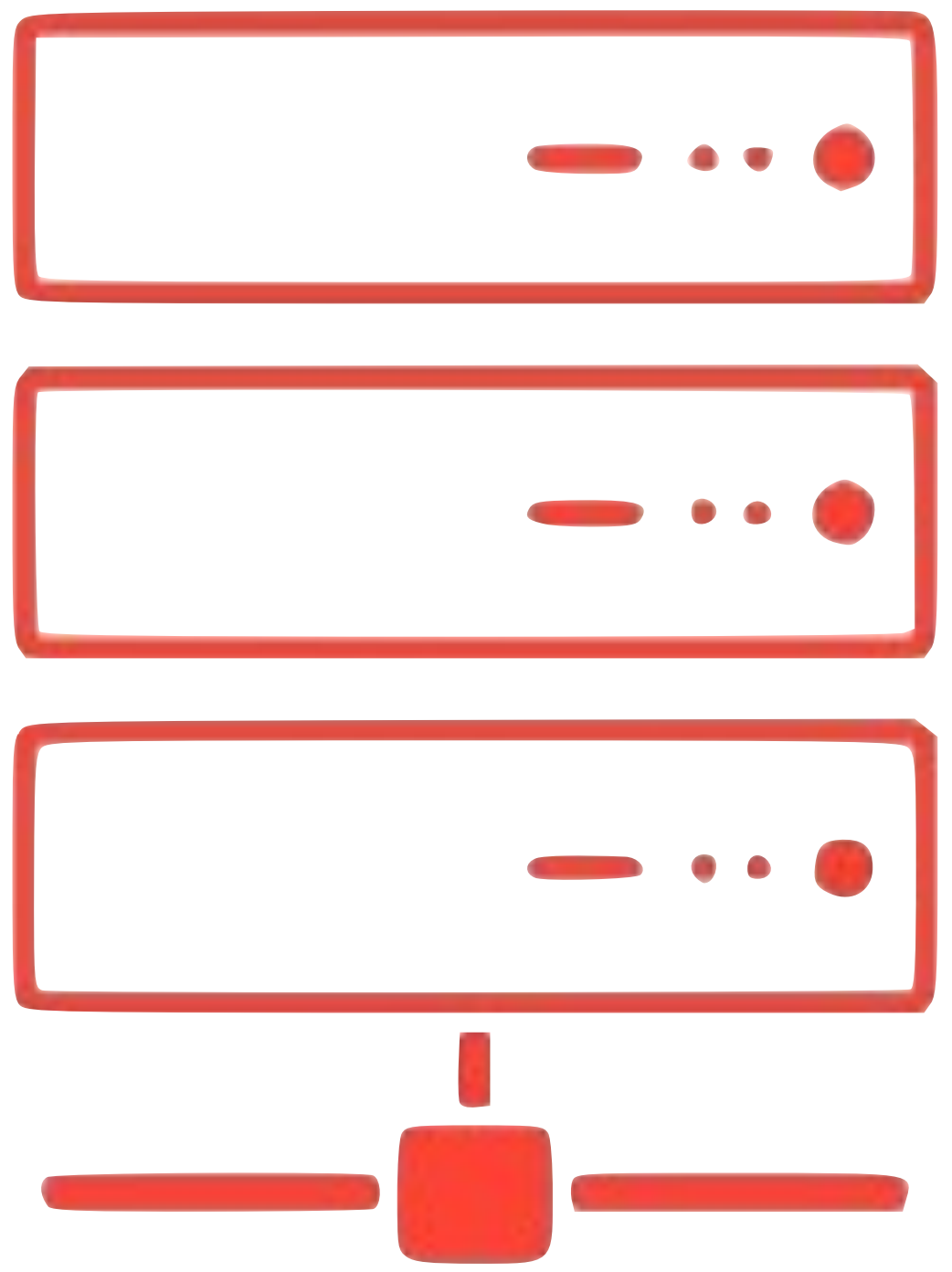
✓ HTTPS = HTTP + TLS

➡ TLS - Transport Layer Security (a.k.a SSL) provides

- **confidentiality :** end-to-end secure channel
- **integrity :** one-way authentication handshake

This how HTTPS works



example.com

HTTPS request

HTTPS response

Who are you?

I am example.com

This how HTTPS works

Who are you?

I am example.com

HTTPS request

HTTPS response

example.com

✓ **HTTPS = HTTP + TLS**

➡ TLS - Transport Layer Security (a.k.a SSL) provides

- **confidentiality :** end-to-end secure channel
- **integrity :** one-way authentication handshake

simplified and one-way authentication
TLS 1.2 (2008)