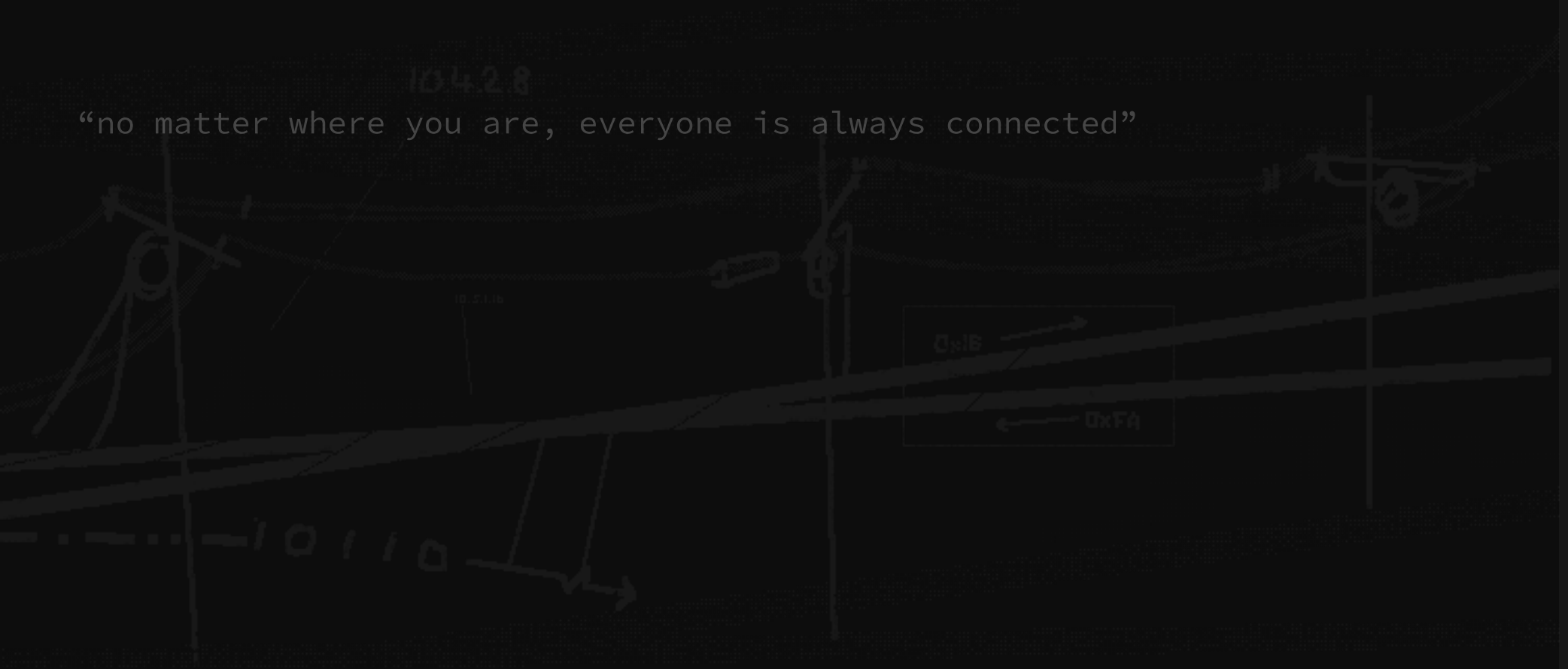
“no matter where you are, everyone is always connected”

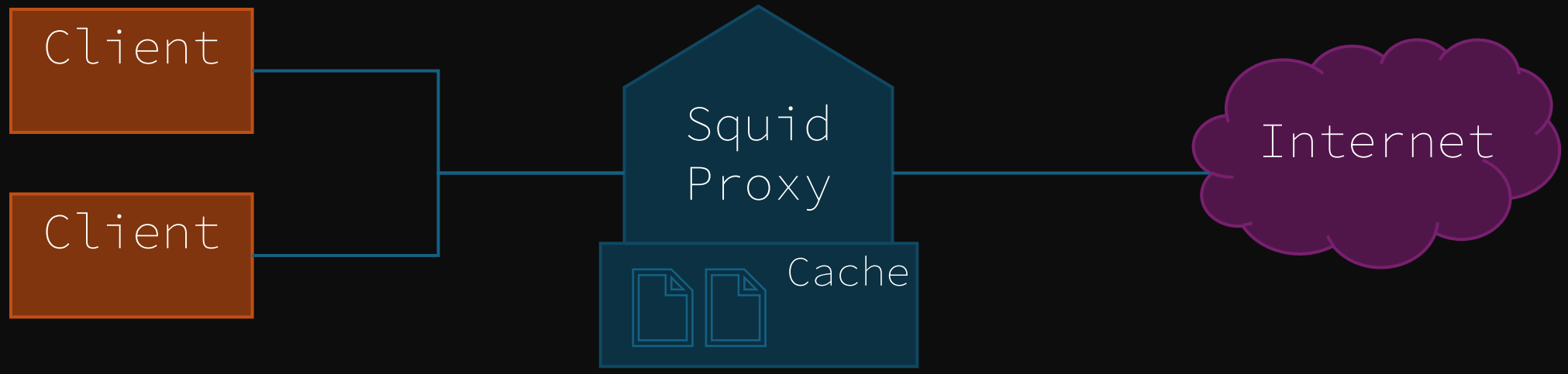
15



Squid Proxy

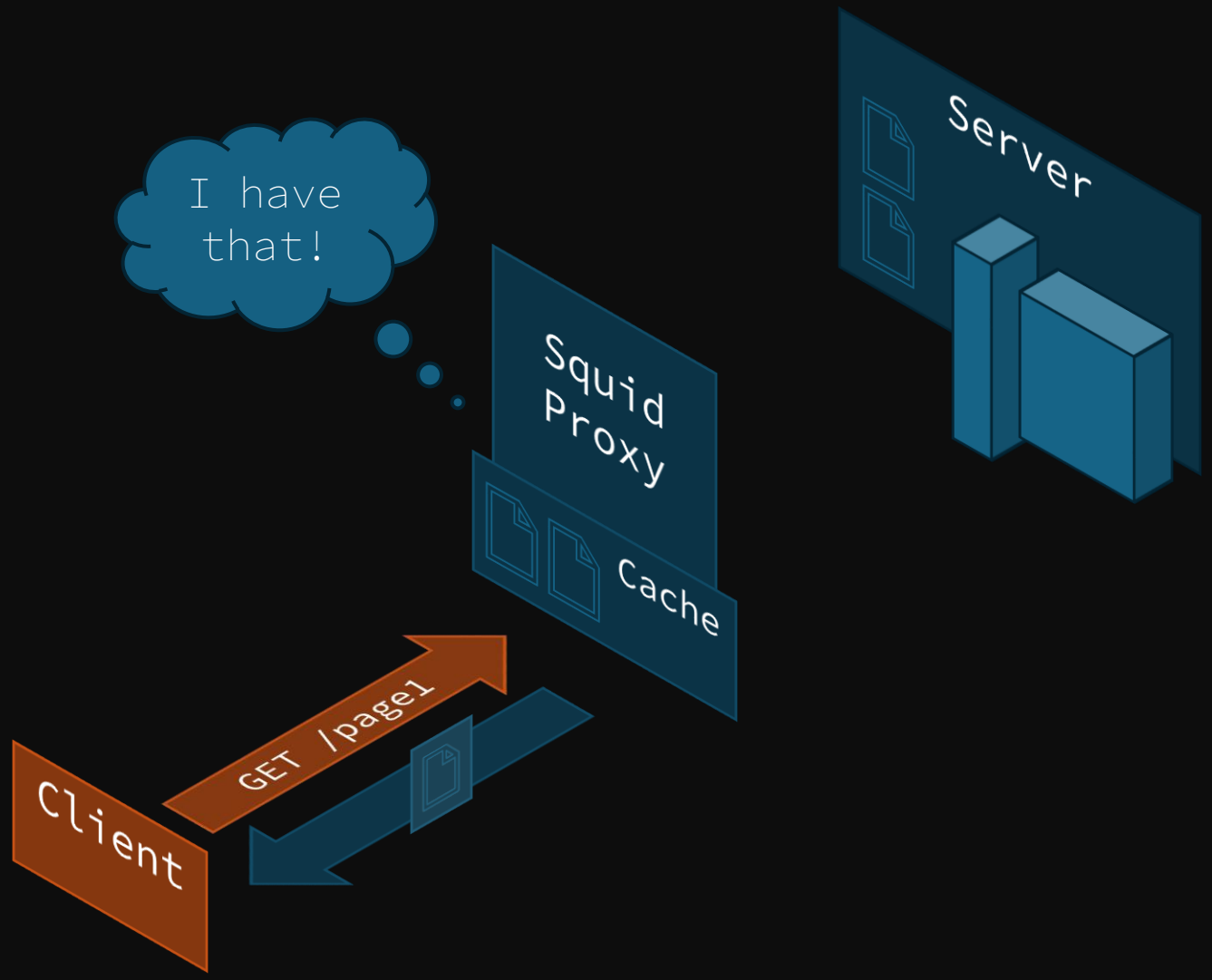
What is Squid?

Squid is a proxy server for web services such as HTTP(S). It acts as an intermediary between a server and client. It caches requests, saving a copy of the request on the server. If the same request is made, it gives the copy instead of sending the new request, improving efficiency.



What Makes Caching Important?

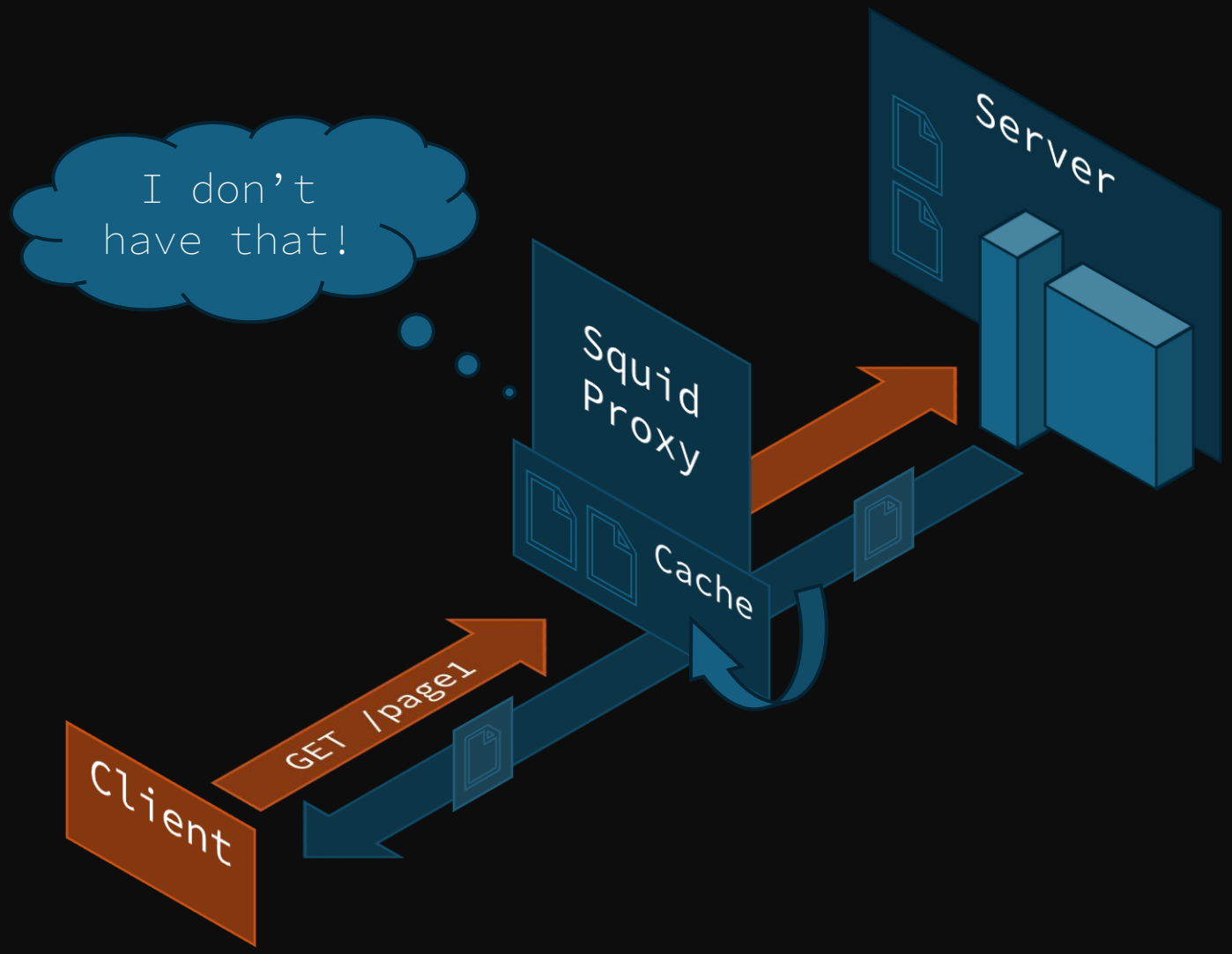
Let’s say you install a Squid Proxy server in front of your Apache web server in a setup called a “reverse proxy”. If the proxy receives a request for a page already in its cache, it has no need to contact the server.



What Makes Caching Important?

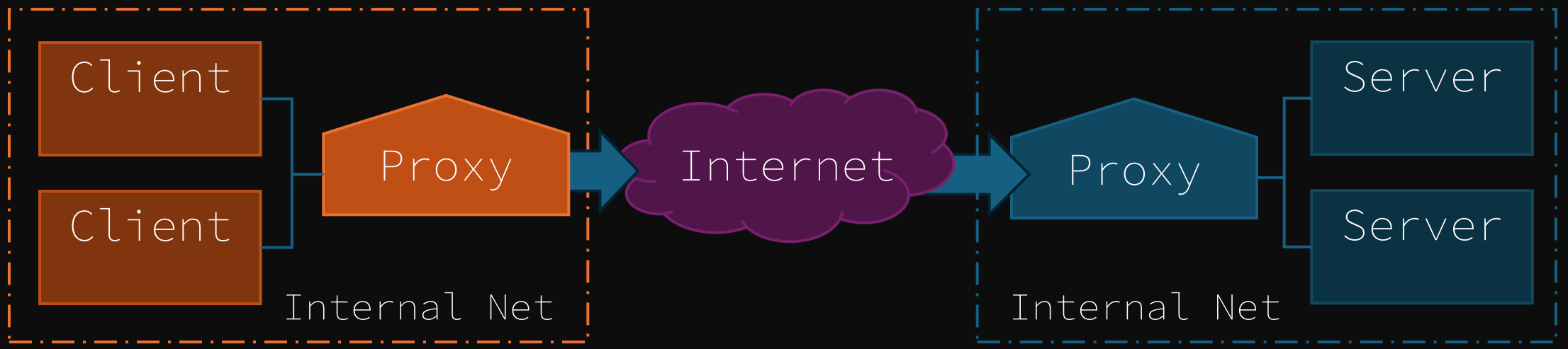
If a request is made that isn't cached already, Squid will pass on your request to the server before sending it back to you.

The proxy may also store that in the cache so it can be reused.



Forward Proxy vs. Reverse Proxy

A forward proxy typically is placed “in front of the clients” and enforces policies before sending off traffic to servers/the Internet.



A reverse proxy typically is placed “in front of the servers” and handles requests and regulates traffic before feeding it into the server.

Secure Configuration

in file */etc/squid/squid.conf*

```
httpd_suppress_version_string on
```

Squid shows the version information by default in the Server header.

To prevent this, add or change the following line to

/etc/squid/squid.conf

Secure Configuration

in file */etc/squid/squid.conf*

```
via off
```

The via header reveals information about the proxy server including hostname and version.

To prevent this, add or change the following line to

/etc/squid/squid.conf

Secure Configuration

in file */etc/squid/squid.conf*

```
reply_header_access X-Cache deny all

reply_header_access X-Cache-Lookup
   deny all
```

The X-Cache and X-Cache-Lookup headers reveal information about the cache behavior on the proxy (i.e. if cache for request was found).

To prevent this, add or change the following line to

/etc/squid/squid.conf

Secure Configuration

in file */etc/squid/squid.conf*

```
follow_x_forwarded_for allow
   localhost
follow_x_forwarded_for deny all
request_header_access X-Forwarded-For
   deny all
```

For inbound requests, follow_x_forwarded_for allows you to find a client's actual ip address using the header. Changes could have been made to the header before reaching squid, so it is not recommended.

To prevent this, add or change the following line.

Secure Configuration

in file */etc/squid/squid.conf*

```
forwarded_for delete
request_header_access X-Forwarded-For
   deny all
```

For outbound requests, forwarded_for allows you to add a client's actual ip to the request to transmit.

To prevent this, add or change the following line.

Secure Configuration

in file */etc/squid/squid.conf*

```
acl Safe_ports port 80
acl Safe_ports port 443

acl Safe_methods method GET POST
   OPTIONS CONNECT
```

You should only allow the following HTTP methods through the proxy when used as a “forward proxy”

To set this, add or change the following line.

Secure Configuration

in file */etc/squid/squid.conf*

```
acl Safe_ports port 80
acl Safe_ports port 443

acl Safe_methods method GET POST
   OPTIONS CONNECT
```

You should only allow the following HTTP methods through the proxy when used as a “forward proxy”

To set this, add or change the following line.