Codaisseur

The Secure Web

SSL, Certificates, and Hostnames

What does this mean?

🤔 Why do we need SSL?

Encrypt data sent between client and server.

🤔 Why do we need a certificate?

Am I connected to the right server?

A Certificate Says:

- Company owns the domain
- Network traffic is encrypted

🤔 Who owns reader.codaisseur.com?

Ownership

- Has the root domain (codaisseur.com)
- Manages the DNS for that root domain
- Verified by a signing authority (CA)
- CA’s are trusted by browser vendors

Codaisseur

Certificate

-----BEGIN CERTIFICATE-----

MIIFXjCCBEagAwIBAgIRAL4eUiD500amUEJVQyNnr38wDQYJKoZIhvcNAQELBQAw

gZAxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO

BgNVBAcTB1NhbGZvcmQxGjAYBgNVBAoTEUNPTU9ETyBDQSBMaW1pdGVkMTYwNAYD

VQQDEy1DT01PRE8gUlNBIERvbWFpbiBWYWxpZGF0aW9uIFNIY3VyZSBTZXJ2ZXIg

Q0EwHhcNMTcwNzE4MDAwMDAwWhcNMTgwNzMxMjM1OTU5WjBfMSEwHwYDVQQLExhE

b21haW4gQ29udHJvbCBWYWxpZGF0ZWQxHTAbBgNVBAsTFFBvc2l0aXZlU1NMIFdp

....

sDx4/Q7lsTIMzt9WQeLJcJMzK9IQrQqrOmxxUx+Q6Mx1qA==

-----END CERTIFICATE-----

Codaisseur

Signed Certificate (by a CA)

-----BEGIN CERTIFICATE-----

MIIFXjCCBEagAwIBAgIRAL4eUiD500amUEJVQyNnr38wDQYJKoZIhvcNAQELBQAw

gZAxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO

BgNVBAcTB1NhbGZvcmQxGjAYBgNVBAoTEUNPTU9ETyBDQSBMaW1pdGVkMTYwNAYD

VQQDEy1DT01PRE8gUlNBIERvbWFpbiBWYWxpZGF0aW9uIFNIY3VyZSBTZXJ2ZXIg

Q0EwHhcNMTcwNzE4MDAwMDAwWhcNMTgwNzMxMjM1OTU5WjBfMSEwHwYDVQQLExhE

b21haW4gQ29udHJvbCBWYWxpZGF0ZWQxHTAbBgNVBAsTFFBvc2l0aXZlU1NMIFdp

....

sDx4/Q7lsTIMzt9WQeLJcJMzK9IQrQqrOmxxUx+Q6Mx1qA==

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU

...

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIFdDCCBFygAwIBAgIQJ2buVutJ846r13Ci/ITeljANBgkqhkiG9w0BAQwFADBv

...

-----END CERTIFICATE-----

Codaisseur

Certificate “Chain”

```
-----BEGIN CERTIFICATE-----
MIIFXjCCBEagAwIBAgIRAL4eUiD500amUEJVQyNnr38wDQYJKoZIhvcNAQELBQAw
gZAxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO
BgNVBAcTB1NhbGZvcmQxGjAYBgNVBAoTEUNPTU9ETyBDQSBMaW1pdGVkMTYwNAYD
VQQDEy1DT01PRE8gUlNBIERvbWFpbiBWYWxpZGF0aW9uIFNIY3VyZSBTZXJ2ZXIg
Q0EwHhcNMTcwNzE4MDAwMDAwWhcNMTgwNzMxMjM1OTU5WjBfMSEwHwYDVQQLExhE
b21haW4gQ29udHJvbCBWYWxpZGF0ZWQxHTAbBgNVBAsTFFBvc2l0aXZlU1NMIFdp
....
sDx4/Q7lsTIMzt9WQeLJcJMzK9IQrQqrOmxxUx+Q6Mx1qA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFdDCCBFygAwIBAgIQJ2buVutJ846r13Ci/ITeljANBgkqhkiG9w0BAQwFADBv
...
-----END CERTIFICATE-----
```

The certificate itself

The intermediate certificate

The root certificate

Creating a Certificate

```
openssl req -utf8 -nodes -sha256 -newkey rsa:2048 -keyout www.example.com.key -out www.example.com.csr
```

Creating a Certificate

- Create a Certificate Signing Request (CSR) and an encryption key
- Find a certificate vendor and provide the CSR
- Prove that you own the domain, entity exists, etc.
- Get a certificate
- Get the intermediate and root certificates from the vendor
- Provide your server with the certificates and the key file

Codaisseur

A Self-Signed Certificate

- Create a Certificate Signing Request (CSR) and an encryption key
- ~~Find a certificate vendor and provide the CSR~~
- Prove that you own the domain, entity exists, etc.
- Get a certificate
- ~~Get the intermediate and root certificates from the vendor~~
- Provide your server with the certificate~~s~~ and the key file
- **Accept that the certificate's authority is not trusted by browsers etc.**

🤔 Why would you use a self-signed certificate?

```
$ openssl \
  req -x509 \
  -newkey rsa:4096 \
  -keyout key.pem
  -out cert.pem \
  -days 365 \
  -nodes
```

🤔 Why would you NOT use a self-signed certificate?

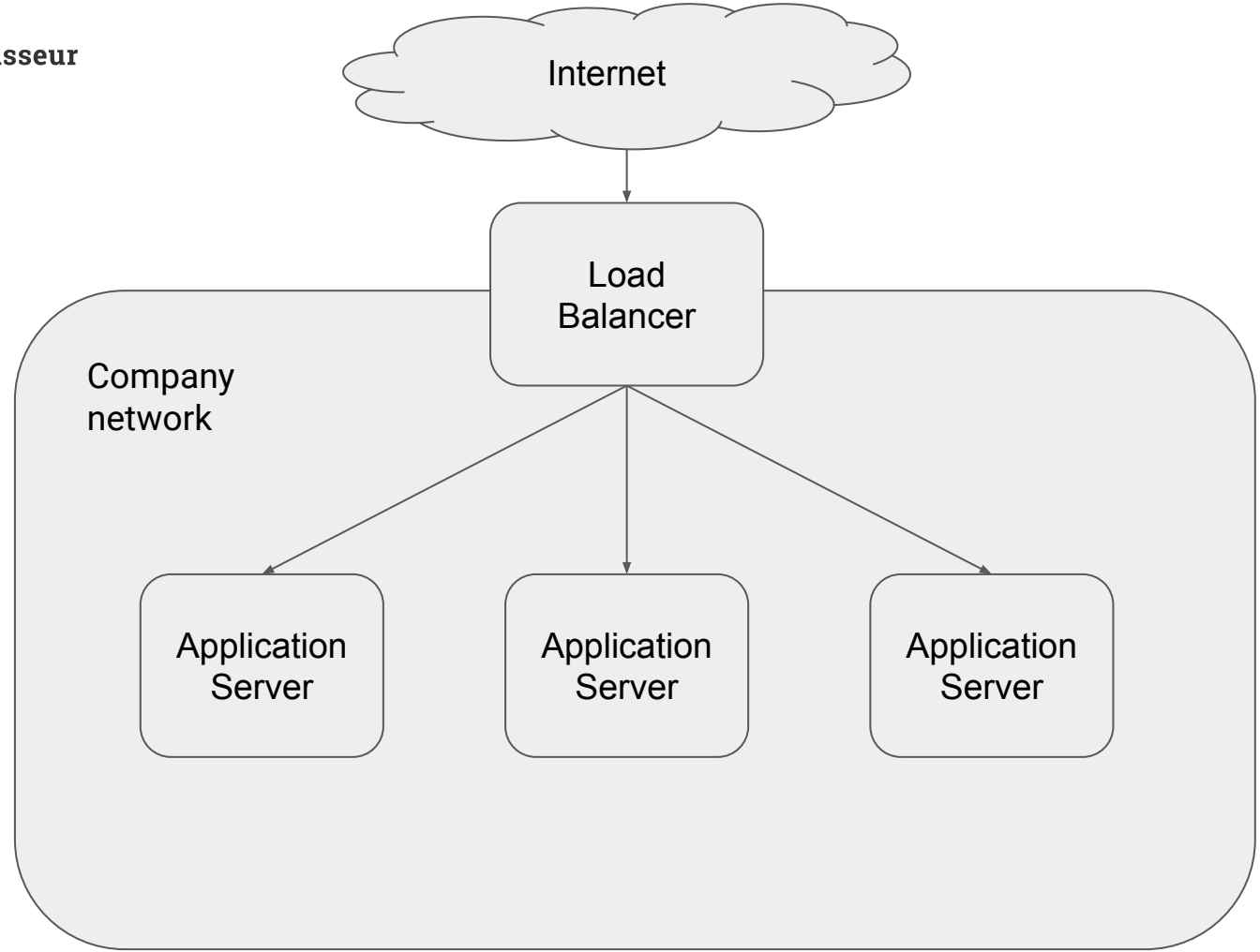
 Use LetsEncrypt instead

Common Practice

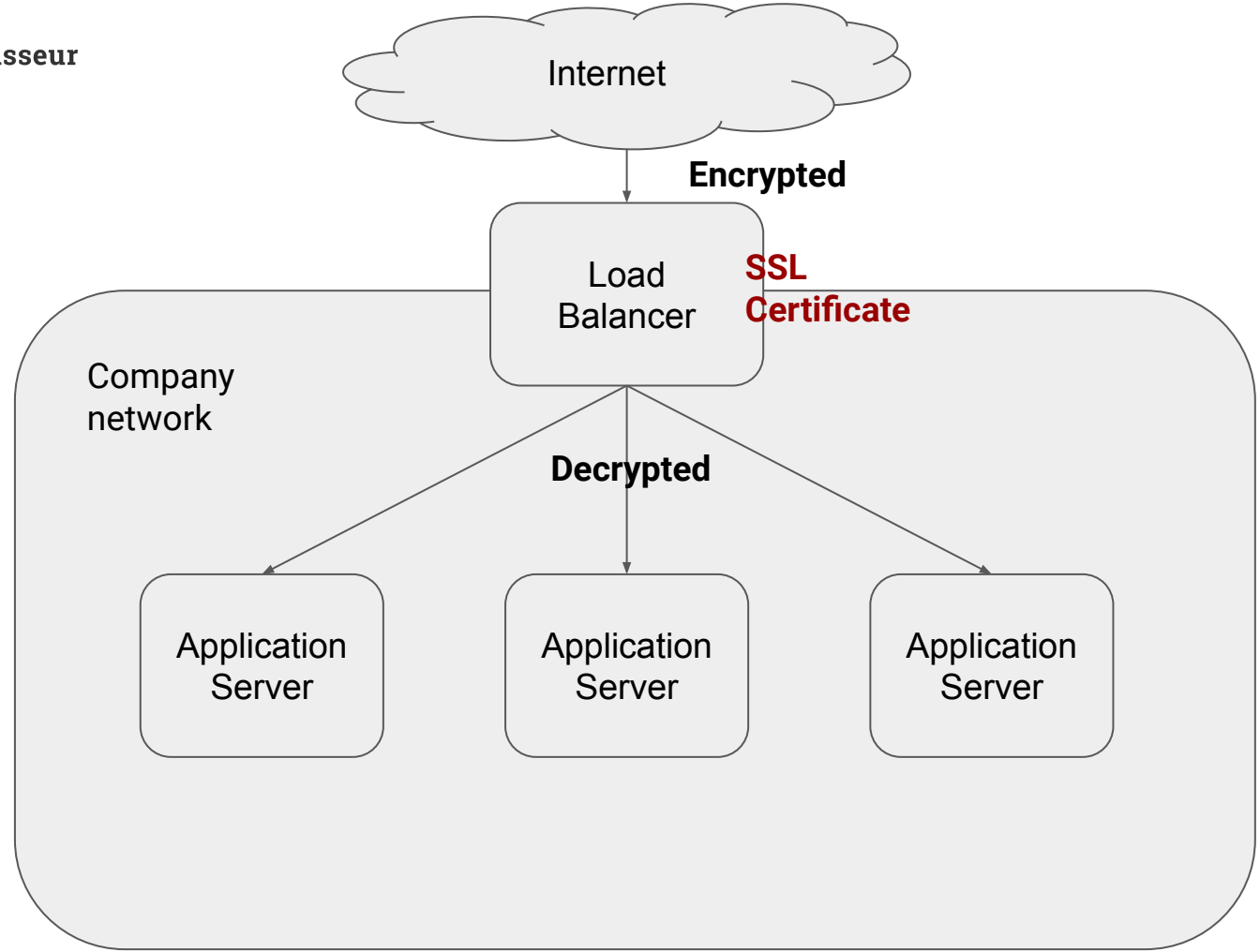
SSL Termination

Here is a typical setup

Codaisseur


Internet
Load Balancer
Company network
Application Server
Application Server
Application Server

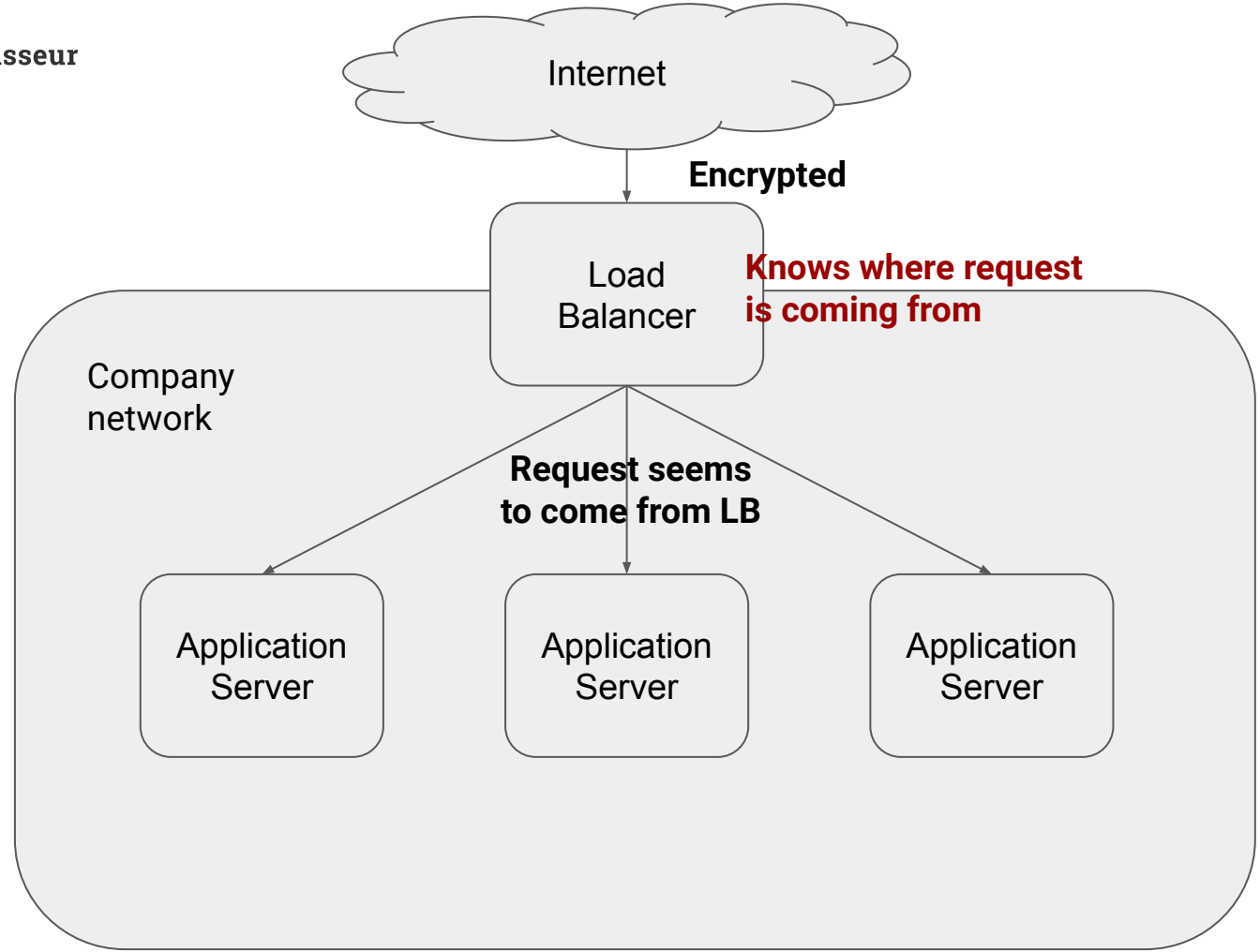
Codaisseur


Internet
Encrypted
Load Balancer
SSL Certificate
Company network
Decrypted
Application Server
Application Server
Application Server

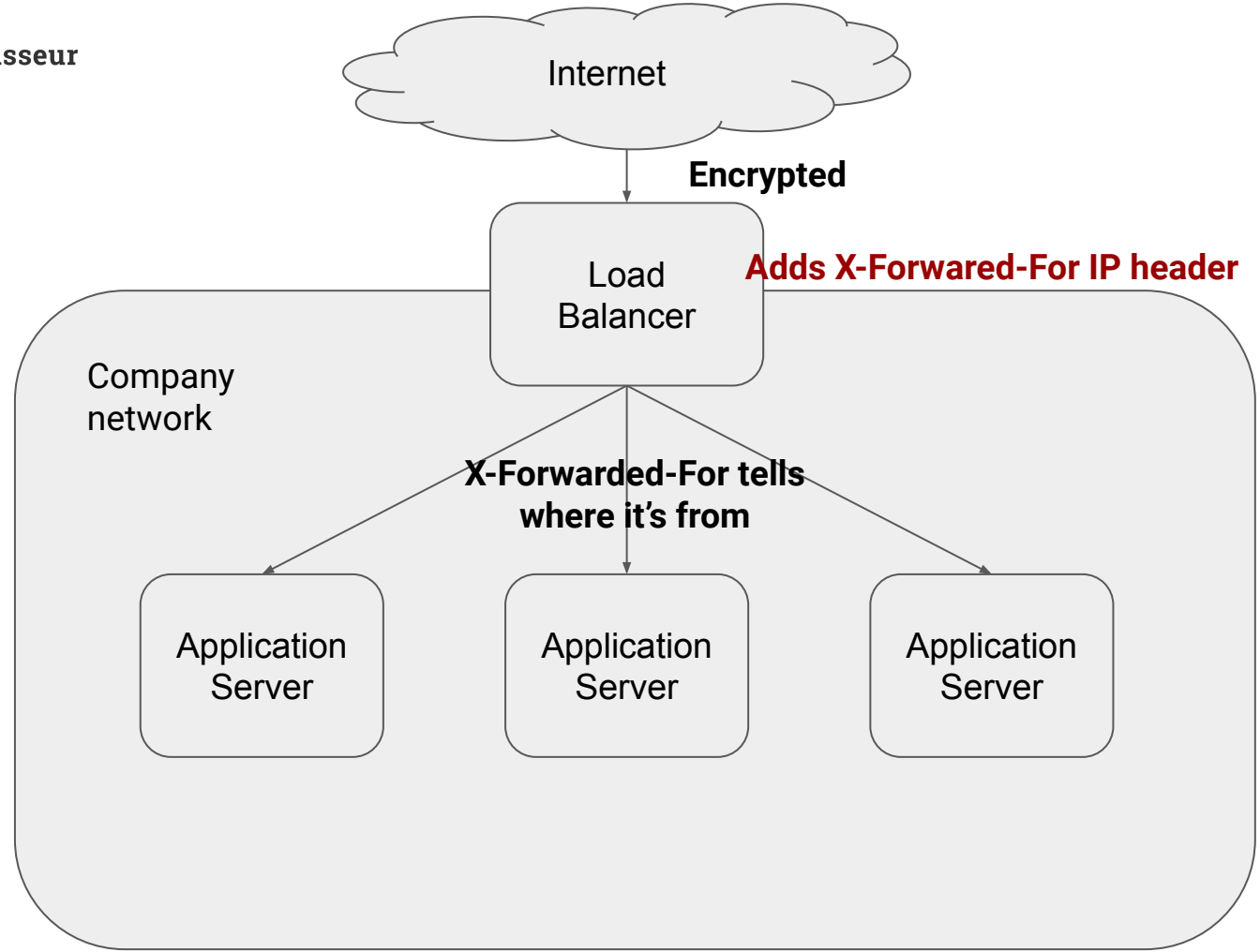
🤔 When might this turn into a security issue?

🤔 Why is this common practice?

Codaisseur


Internet
Encrypted
Load Balancer
Knows where request is coming from
Company network
Request seems to come from LB
Application Server
Application Server
Application Server

Codaisseur


Internet
Encrypted
Load Balancer
Adds X-Forwared-For IP header
Company network
X-Forwarded-For tells where it's from
Application Server
Application Server
Application Server

Also annoying: Wireshark is blind for SSL (try this)