Hardening a SAS® Installation on a multi tier installation on Linux

Jan Bigalke

Allianz

Environment

- IT Sicherheitsgesetz 24.07.2015

  Mindeststandards zur IT-Sicherheit
- OWASP

  The Open Web Application Security Project
- FIPS Federal Information Processing Standard

  https://en.wikipedia.org/wiki/FIPS_140-2

Scope in this presentation

Important but not covered:

- social engineering
- key loggers (attack of the workplace)
- vulnerabilities in the operating system
- security process frameworks

Risk management

- It’s a continuous process

Allianz

OWASP Top 10 – 2010 (old)	OWASP Top 10 – 2013 (New)
2010-A1 – Injection	2013-A1 – Injection
2010-A2 – Cross Site Scripting (XSS)	2013-A2 – Broken Authentication and Session Management
2010-A3 – Broken Authentication and Session Management	2013-A3 – Cross Site Scripting (XSS)
2010-A4 – Insecure Direct Object References	2013-A4 – Insecure Direct Object References
2010-A5 – Cross Site Request Forgery (CSRF)	2013-A5 – Security Misconfiguration
2010-A6 – Security Misconfiguration	2013-A6 – Sensitive Data Exposure
2010-A7 – Insecure Cryptographic Storage	2013-A7 – Missing Function Level Access Control
2010-A8 – Failure to Restrict URL Access	2013-A8 – Cross-Site Request Forgery (CSRF)
2010-A9 – Insufficient Transport Layer Protection	2013-A9 – Using Known Vulnerable Components (NEW)
2010-A10 – Unvalidated Redirects and Forwards (NEW)	2013-A10 – Unvalidated Redirects and Forwards
3 Primary Changes:	▪ Merged: 2010-A7 and 2010-A9 -> 2013-A6
▪ Added New 2013-A9: Using Known Vulnerable Components	▪ 2010-A8 broadened to 2013-A7

OWASP The Open Web Application Security Project

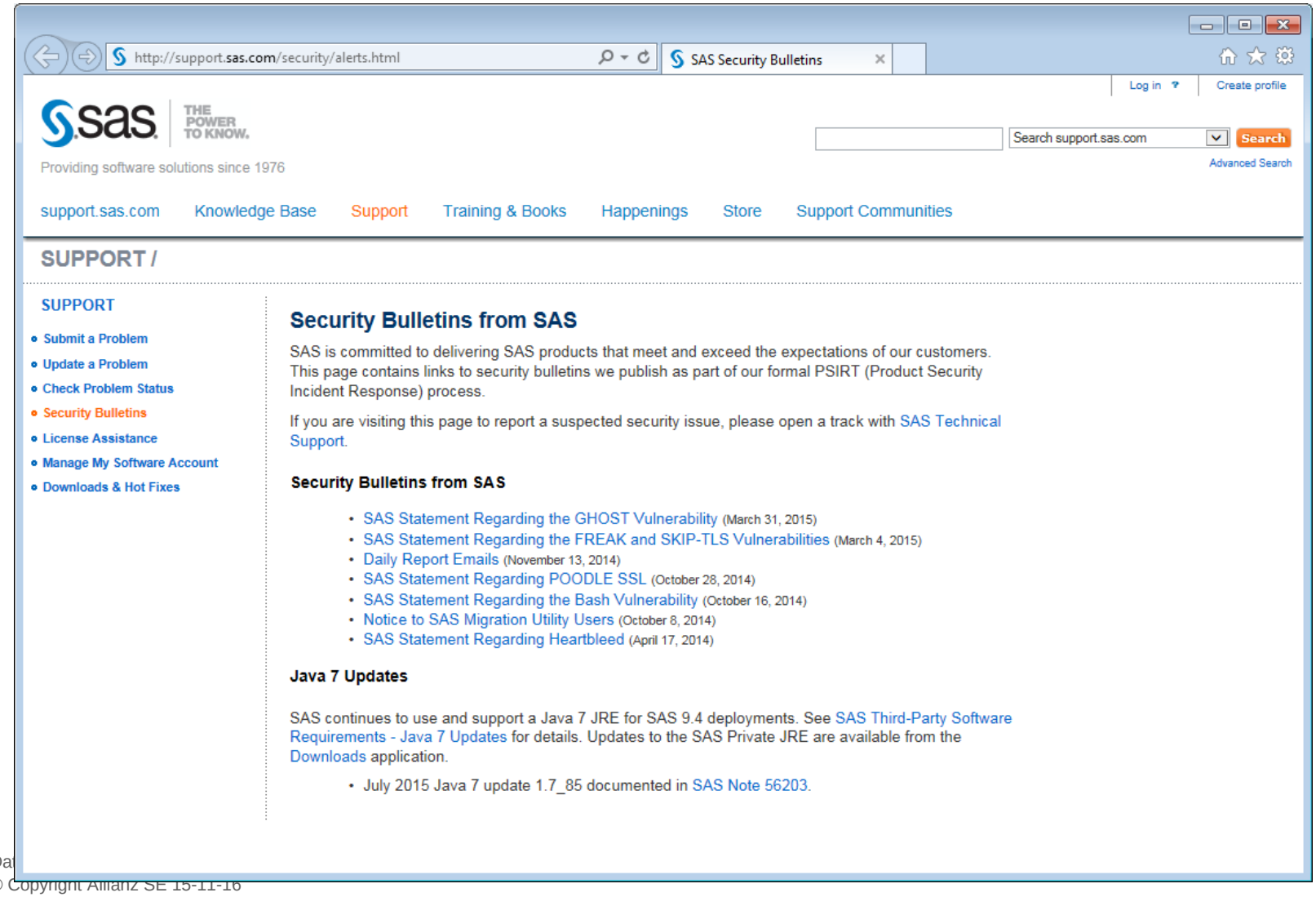
The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

Link: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Control
A8: Cross Site Request Forgery (CSRF)
A9 : Using Known Vulnerable Components
A10: Unvalidated Redirects and Forwards

Patch management

http://support.sas.com/security/alerts.html



Hotfix -> Patch management

http://ftp.sas.com/techsup/download/hotfix/HF2/94_whats_new.html

Problem Note *56481:* OpenSSL vulnerabilities exist in the SAS® 9.4 Web Server (OpenSSL advisories through 9th July 2015)

http://support.sas.com/kb/56/481.html

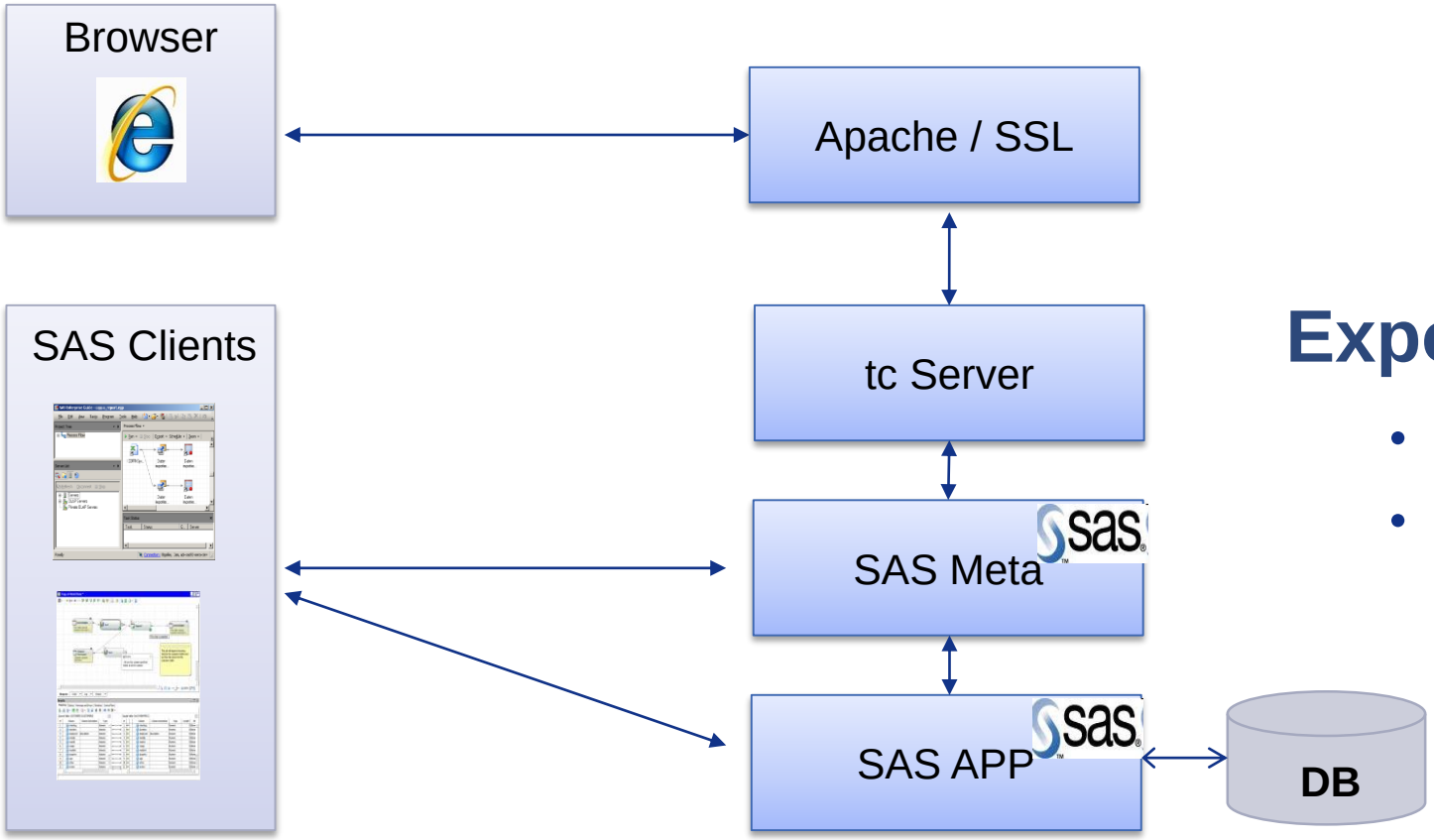
Problem Note *56385:* OpenSSL security vulnerabilities (11 Jun 2015 and 9 Jul 2015) exist in the Secure Sockets Layer (SSL) capability in SAS® Foundation products

http://support.sas.com/kb/56/385.html

Problem Note *53245:* OpenSSL security vulnerabilities (05 Jun 2014) exist in SAS/SECURE™ software

http://support.sas.com/kb/53/245.html

SAS infrastructure



Exposure:

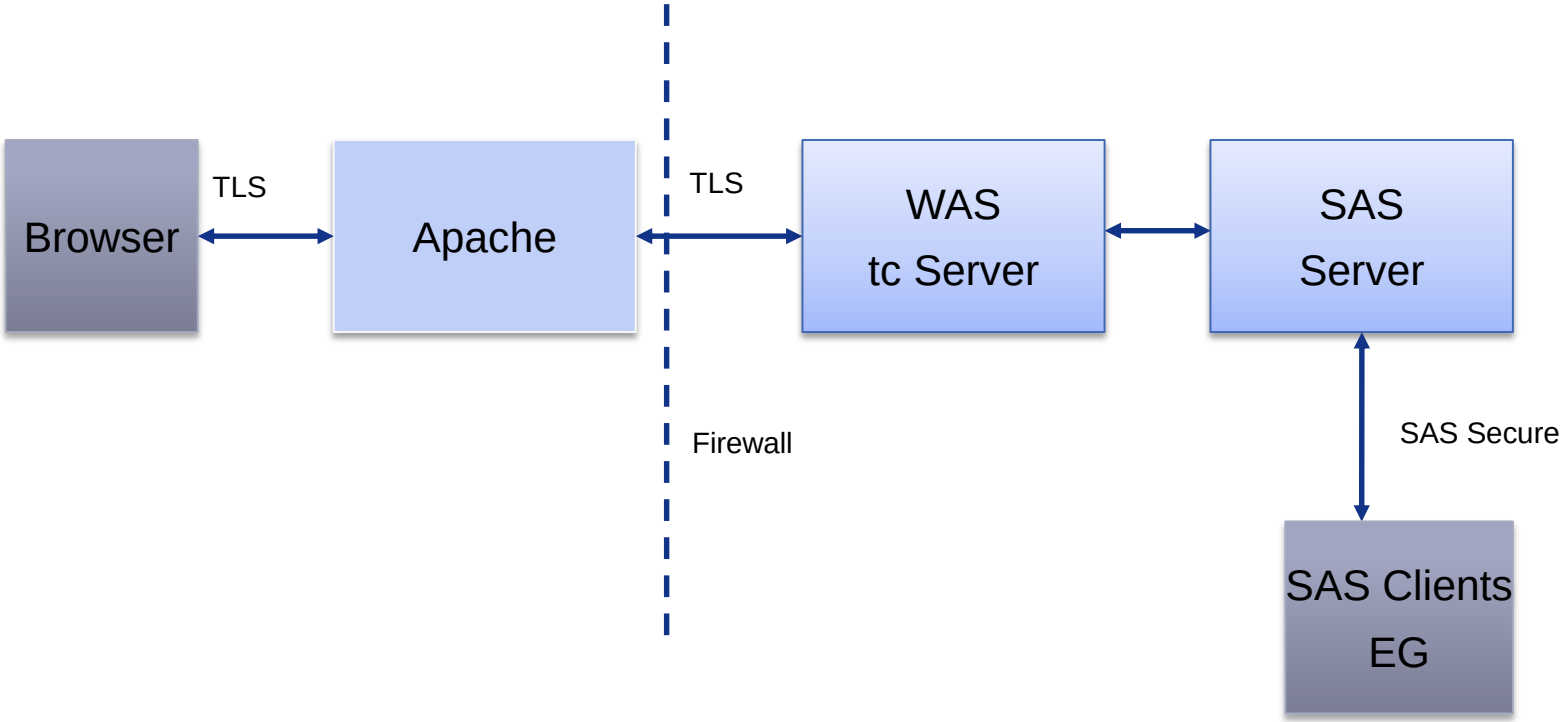
- **Credentials**
- **Data**

Security requirements

similar requirements like FIPS 140-2

SSL handshake protocol: TLS 1.0

http://support.sas.com/resources/papers/proceedings12/358-2012.pdf



Credentials protection

Google Declares War on Passwords (www.wired.com 01/18/13)

Passwords only are insecure ..

two factor authentication (like token, smart cards,..)

impact on SAS

default authentication provider metadata server with user/password

no passwords for SAS (single sign on)

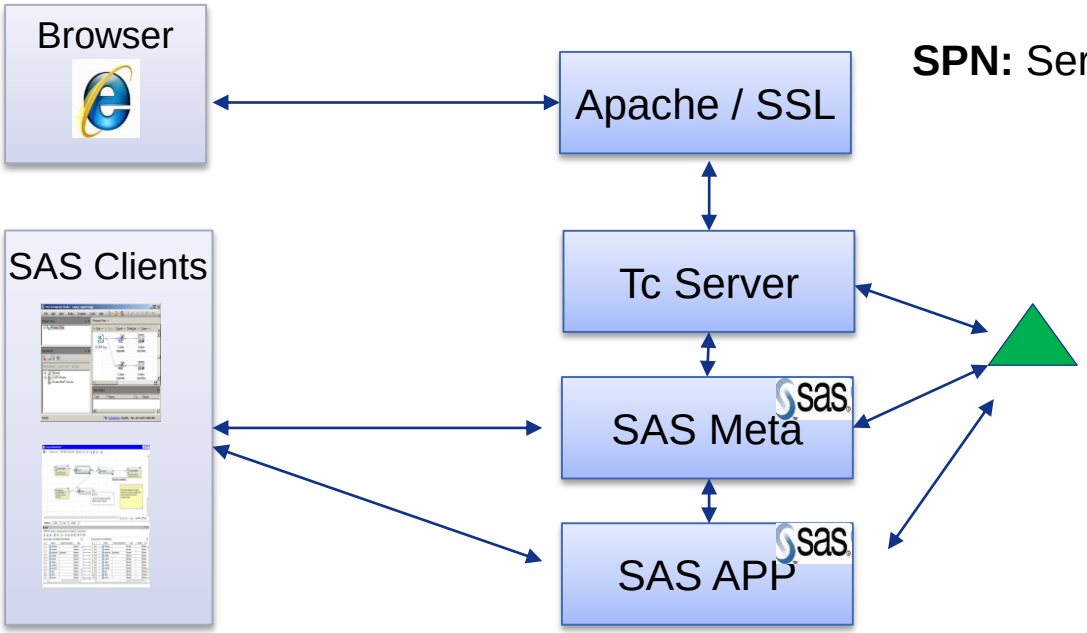
delegate the authentication to the underlying components

SSO (replacement for username/password)

Web/Client Single Sign On

Kerberos (ticket based)

same authentication provider for Web and SAS Clients



SPN: Service principal name in active directory

1. SPN URL: HTTP/domain.net@domain

2. SPN : SAS/meta.dnsname.net@domain

3. SPN : SAS/app.dnsname.net@domain

Encryption of communication

encryption of connections

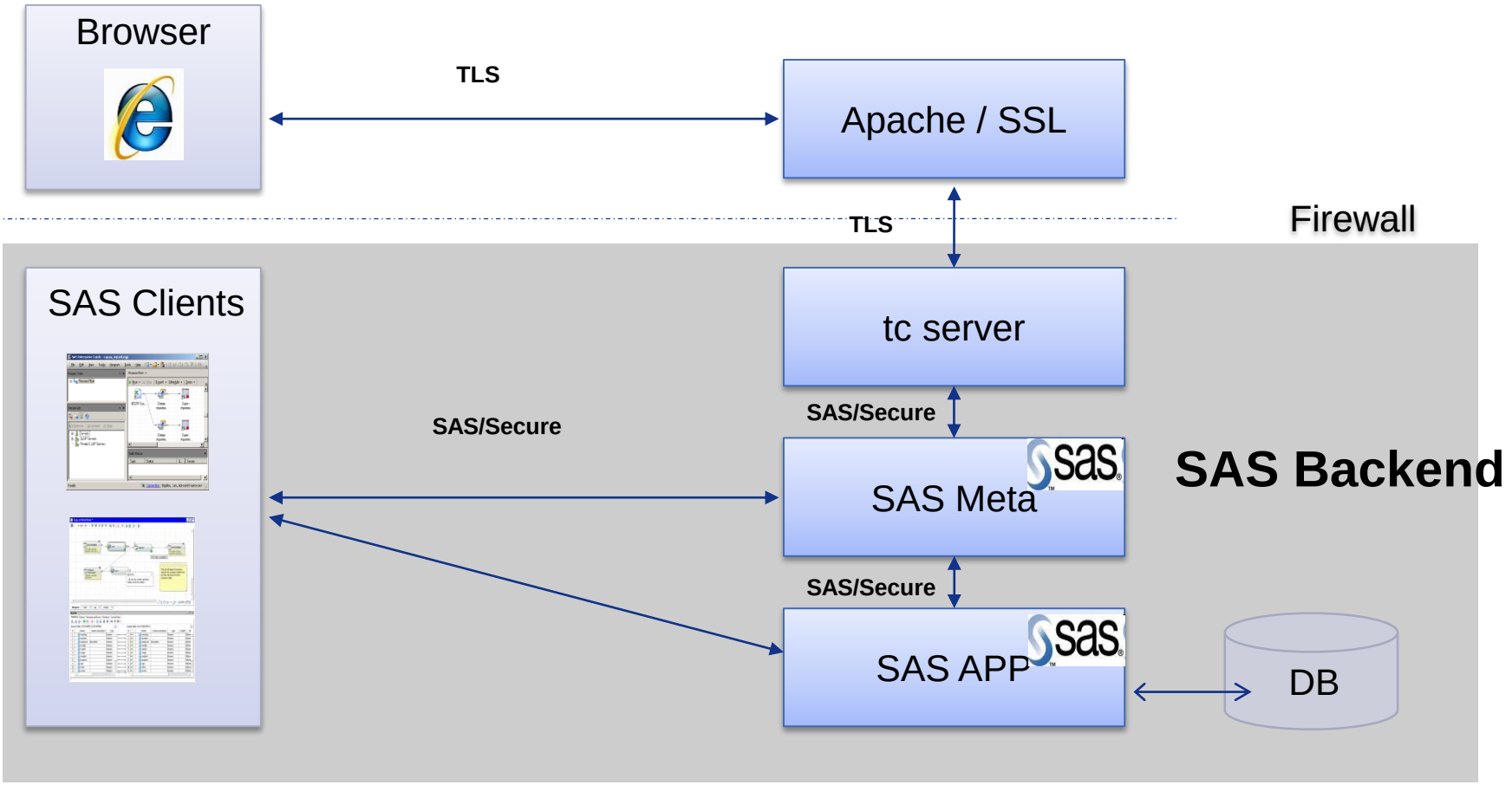
- (data classification, requirements)
- firewall to protect the backend Servers

Web TLS 1.0 (SSL 3.1) Transport Layer Security

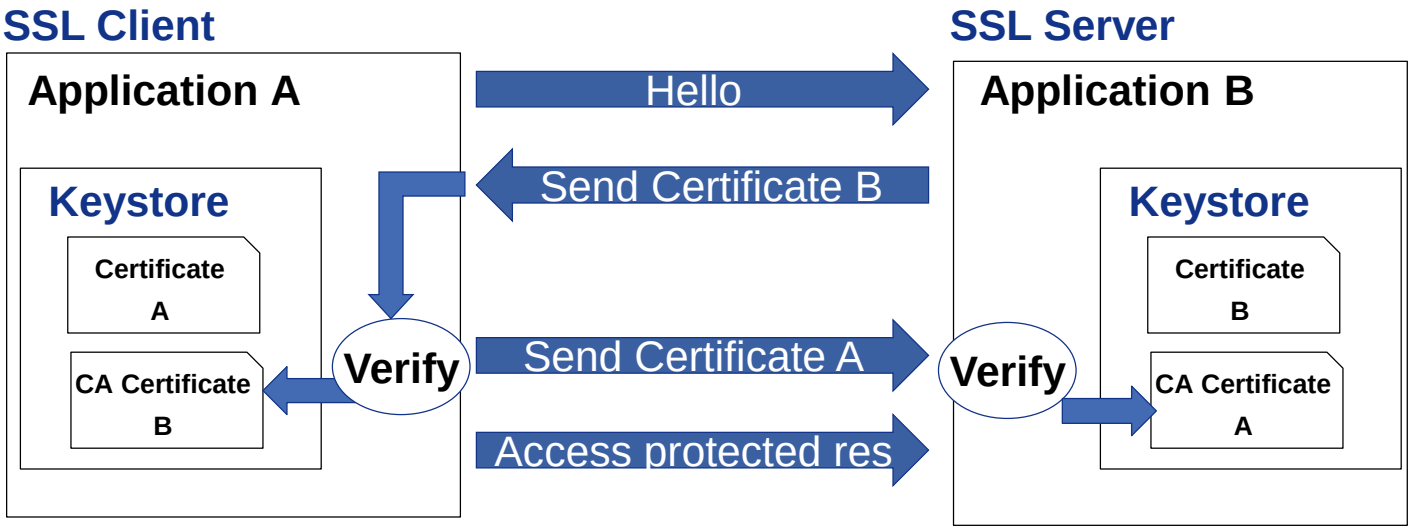
SAS Clients (SAS/Secure™) included since SAS 9.4

- SAS System Option -encryptfips -netencryptalgorithm aes;
- FIPS 140-2 compliant encryption algorithms are used

Reverse proxy and firewall

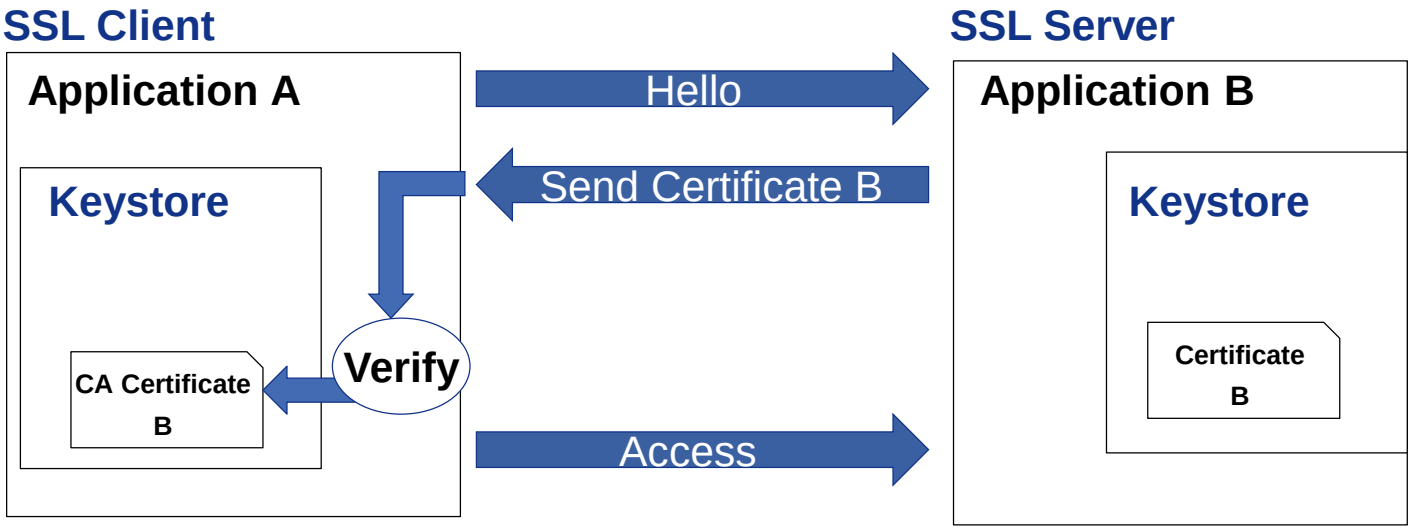


SSL (two way SSL)



1. A client requests access to a protected resource.
2. The server presents its certificate to the client.
3. The client verifies the server's certificate.
4. If successful, the client sends its certificate to the server.
5. The server verifies the client's credentials.
6. If successful, the server grants access to the protected resource requested by the client.

one way SSL

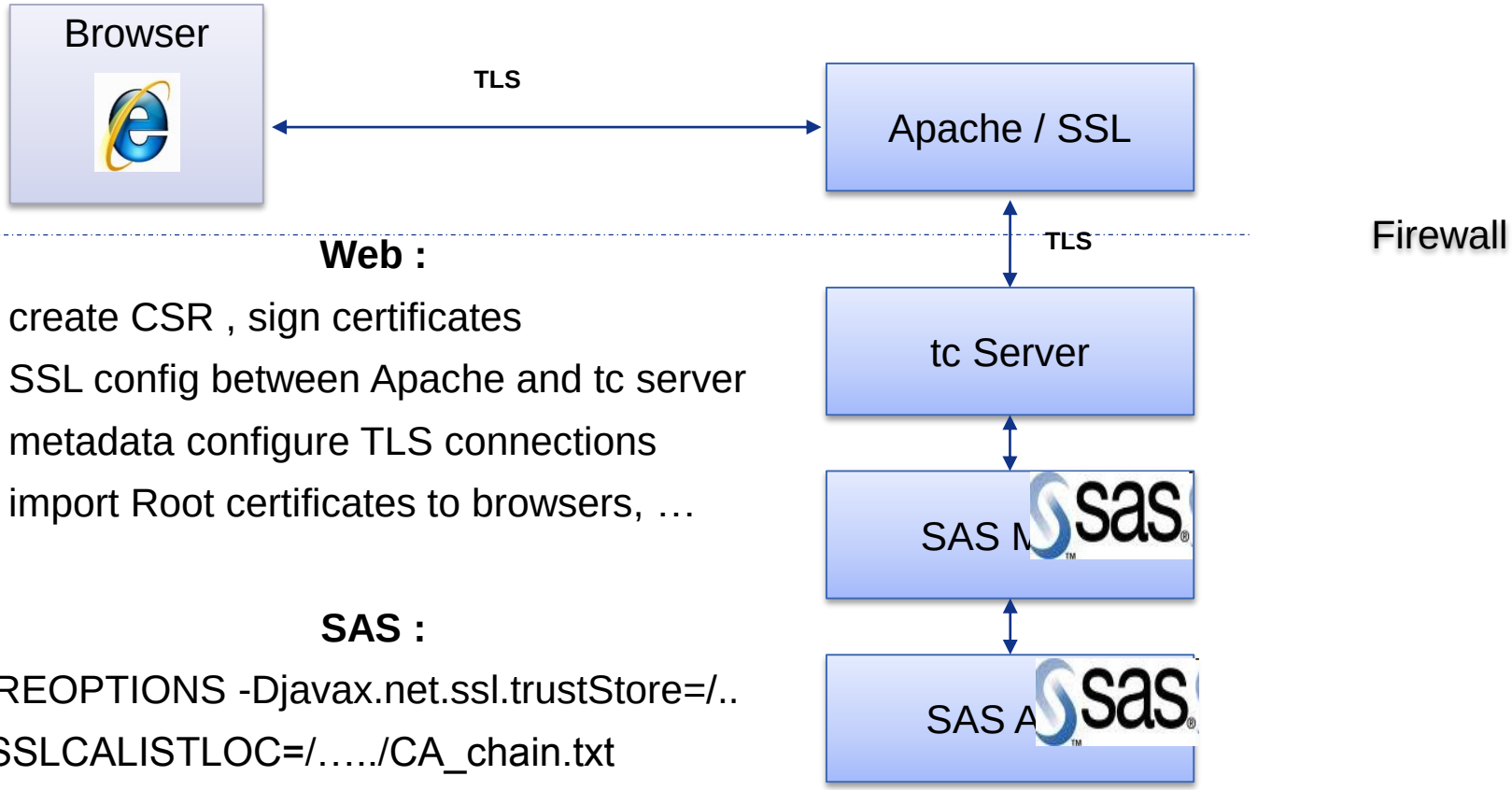


In such mode,

the SSL-client application is not verified by the SSL-server application.

Only the server is verified

SAS infrastructure TLS configuration



Web :

- create CSR , sign certificates
- SSL config between Apache and tc server
- metadata configure TLS connections
- import Root certificates to browsers, …

SAS :

JREOPTIONS -Djavax.net.ssl.trustStore=/..

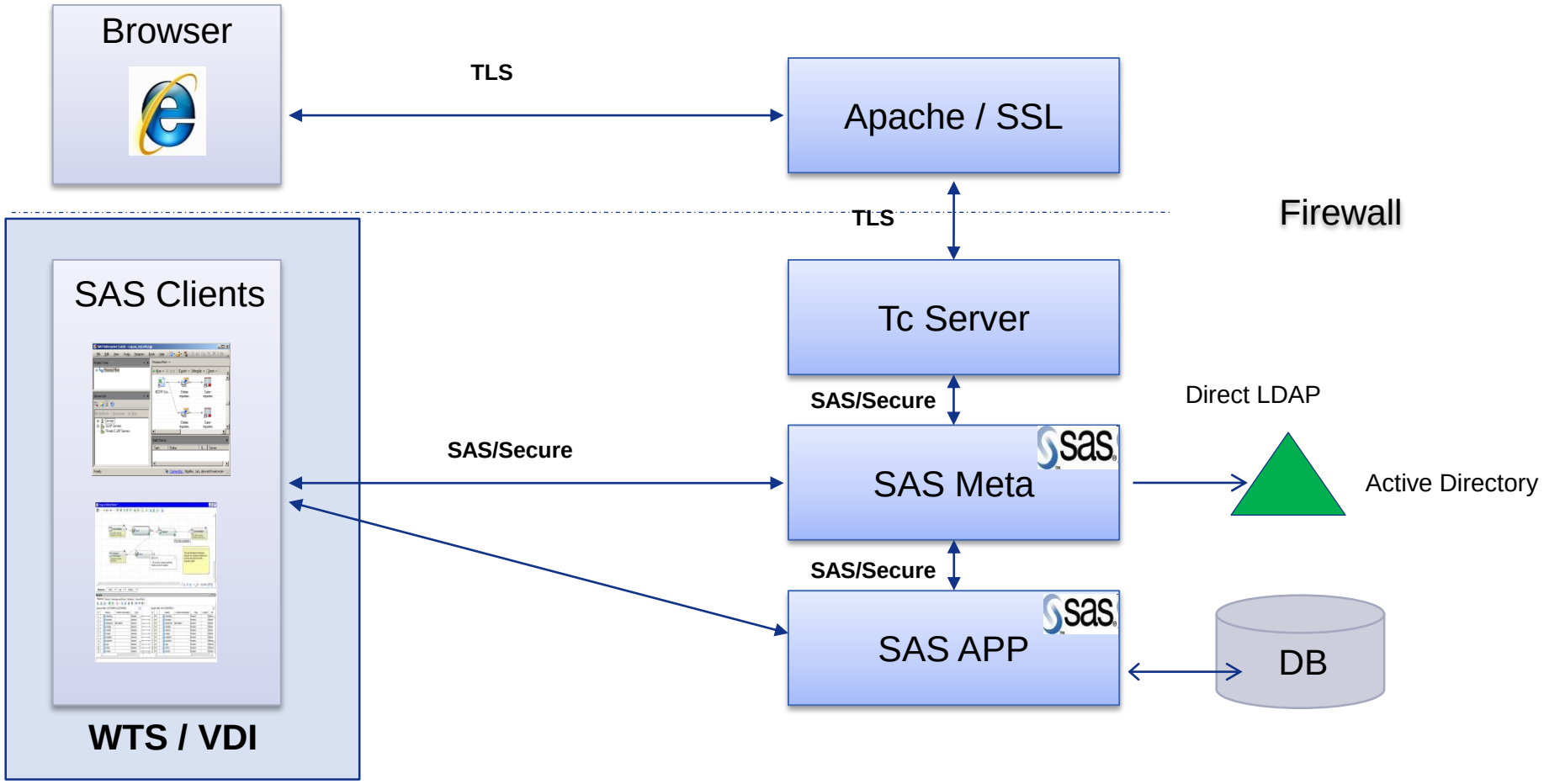
-SSLCALISTLOC=/…../CA_chain.txt

SAS Clients :

- import Root certificates(e.g. java keystore,)

SAS 9.4 Install Guide documentation

SAS infrastructure clients



Conclusion

Vulnerability:

credentials

data

Improve security:

Patch management

SSO to reduce the need for entering credentials

Encryption for the communication channels

TLS and SAS Secure

penetration testing (open web application security project OWASP)