

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

Jan Bigalke

## 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](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

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:	<ul style="list-style-type: none"> <li>▪ Merged: 2010-A7 and 2010-A9 -&gt; 2013-A6</li> </ul>
<ul style="list-style-type: none"> <li>▪ Added New 2013-A9: Using Known Vulnerable Components</li> </ul>	<ul style="list-style-type: none"> <li>▪ 2010-A8 broadened to 2013-A7</li> </ul>

# 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](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>



The screenshot shows a web browser window displaying the SAS Security Bulletins page. The browser's address bar shows the URL <http://support.sas.com/security/alerts.html>. The page header includes the SAS logo, the tagline "THE POWER TO KNOW", and a search bar. The main navigation menu includes links to "support.sas.com", "Knowledge Base", "Support", "Training & Books", "Happenings", "Store", and "Support Communities". The "SUPPORT /" section is active, and the "Security Bulletins from SAS" link is highlighted in the left sidebar. The main content area is titled "Security Bulletins from SAS" and contains the following text:

SAS is committed to delivering SAS products that meet and exceed the expectations of our customers. This page contains links to security bulletins we publish as part of our formal PSIRT (Product Security Incident Response) process.

If you are visiting this page to report a suspected security issue, please open a track with [SAS Technical Support](#).

**Security Bulletins from SAS**

- [SAS Statement Regarding the GHOST Vulnerability](#) (March 31, 2015)
- [SAS Statement Regarding the FREAK and SKIP-TLS Vulnerabilities](#) (March 4, 2015)
- [Daily Report Emails](#) (November 13, 2014)
- [SAS Statement Regarding POODLE SSL](#) (October 28, 2014)
- [SAS Statement Regarding the Bash Vulnerability](#) (October 16, 2014)
- [Notice to SAS Migration Utility Users](#) (October 8, 2014)
- [SAS Statement Regarding Heartbleed](#) (April 17, 2014)

**Java 7 Updates**

SAS continues to use and support a Java 7 JRE for SAS 9.4 deployments. See [SAS Third-Party Software Requirements - Java 7 Updates](#) for details. Updates to the SAS Private JRE are available from the [Downloads](#) application.

- July 2015 Java 7 update 1.7\_85 documented in [SAS Note 56203](#).

[http://ftp.sas.com/techsup/download/hotfix/HF2/94\\_whats\\_new.html](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)**

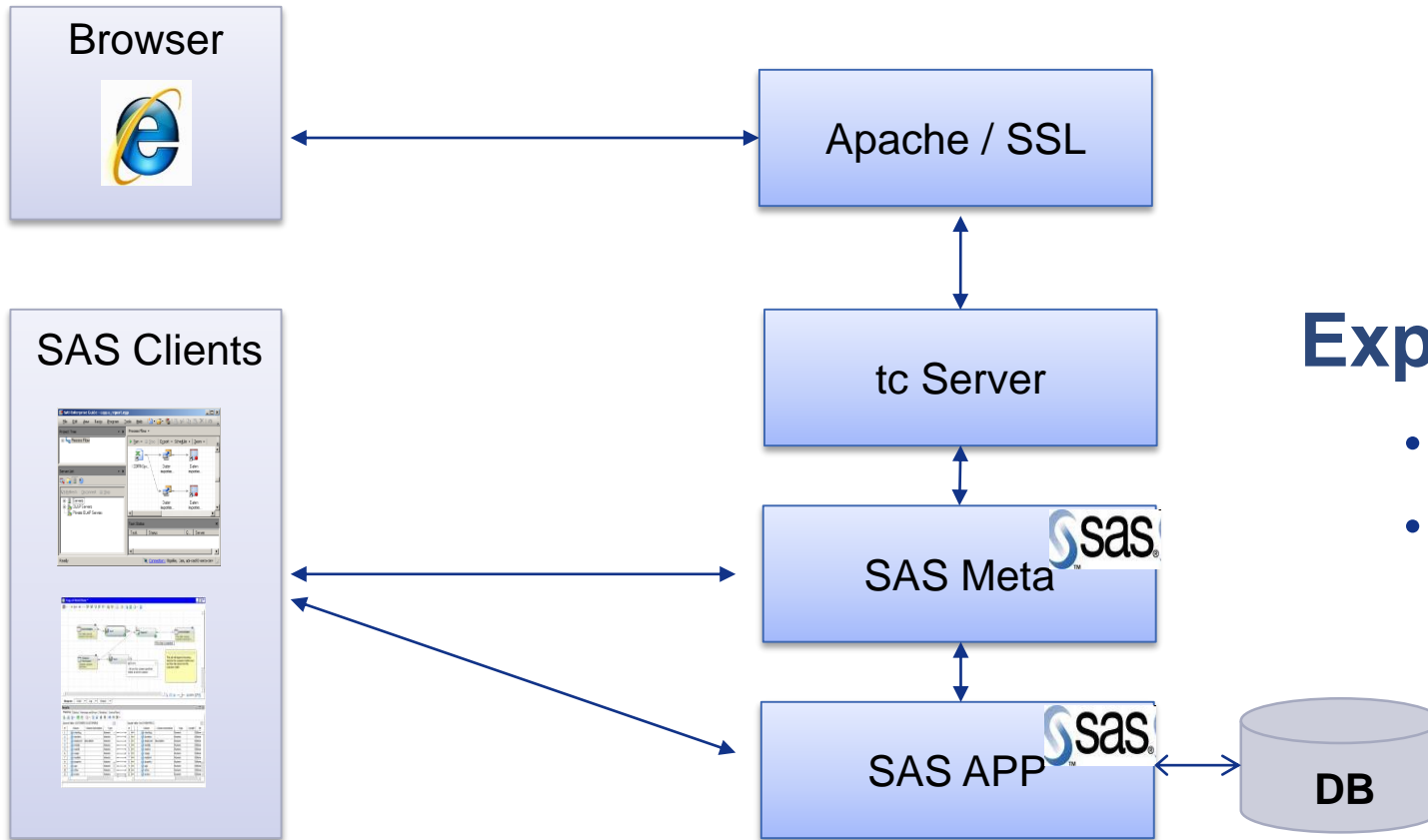
<http://support.sas.com/kb/56/481.html>

**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>



## Exposure:

- Credentials
- Data

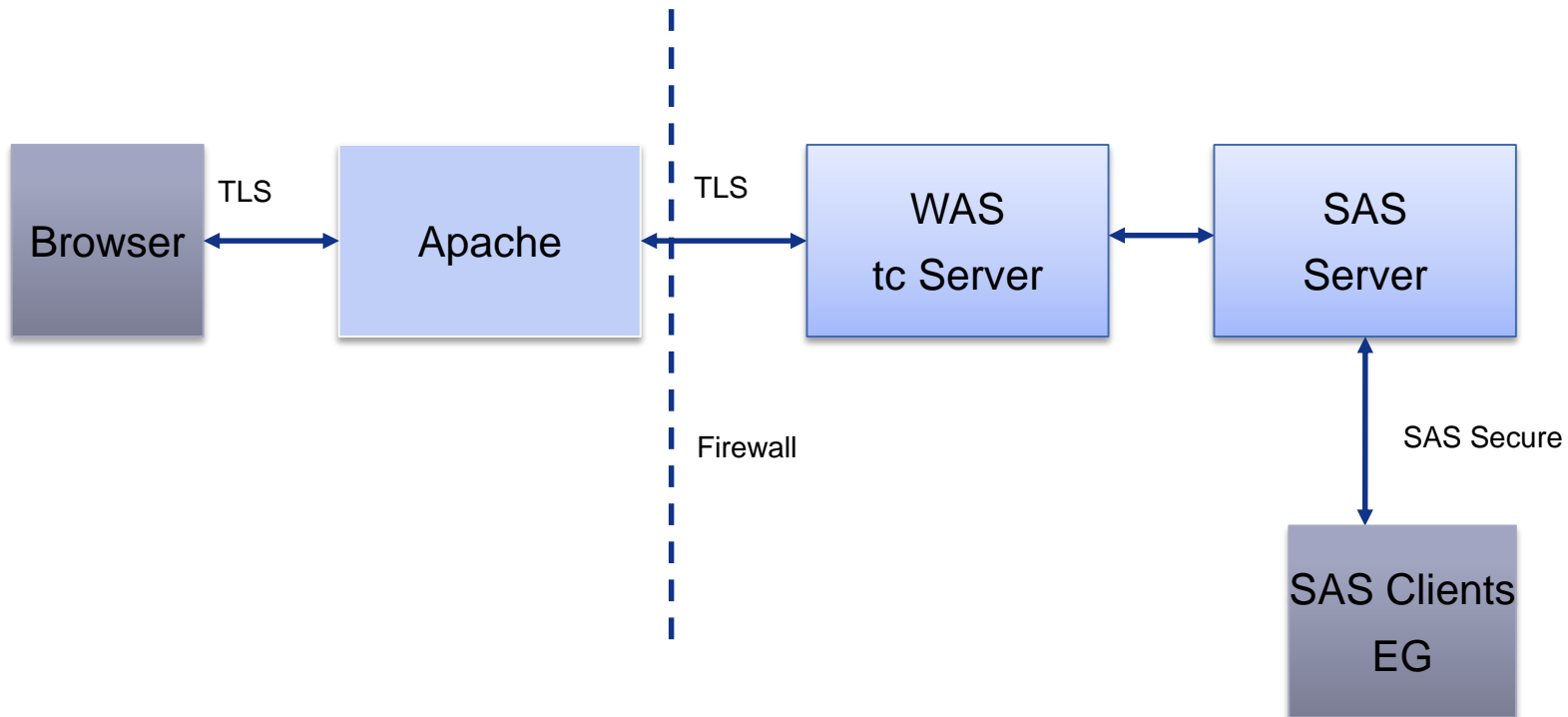


# Security requirements

## 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](http://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)

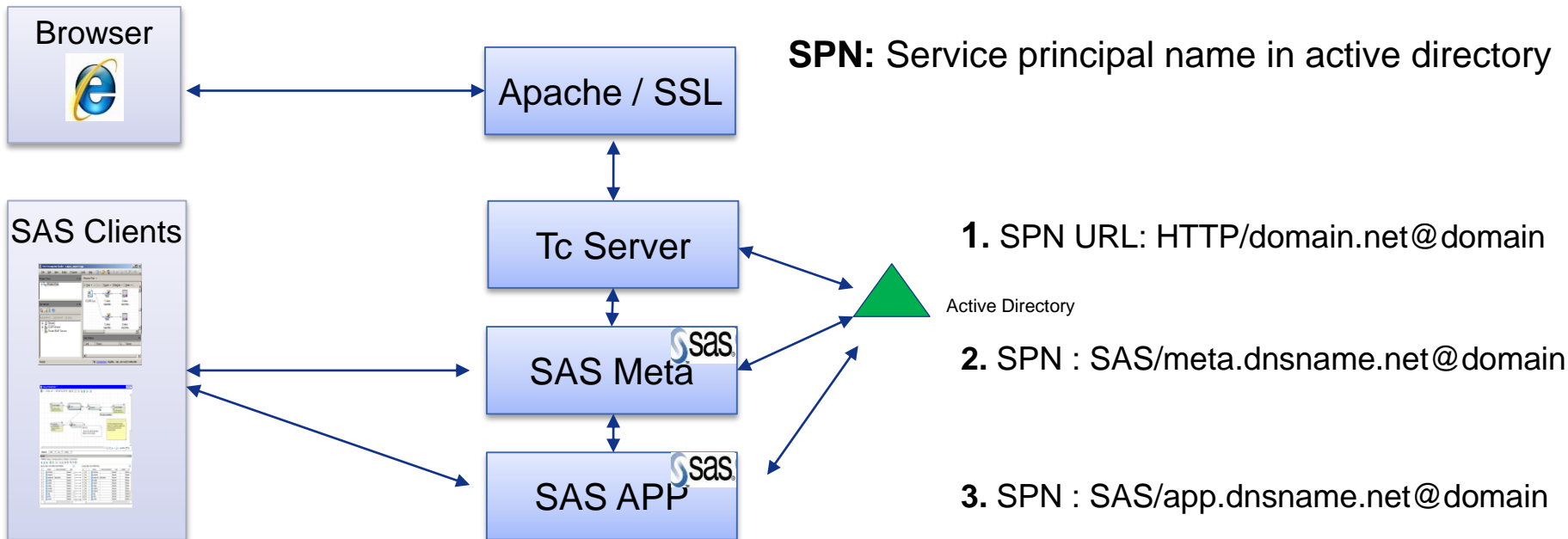
delegate the authentication to the underlying components

# SSO (replacement for username/password )

## Web/Client Single Sign On

Kerberos (ticket based)

same authentication provider for Web and SAS Clients



# Encryption of communication

## encryption of connections

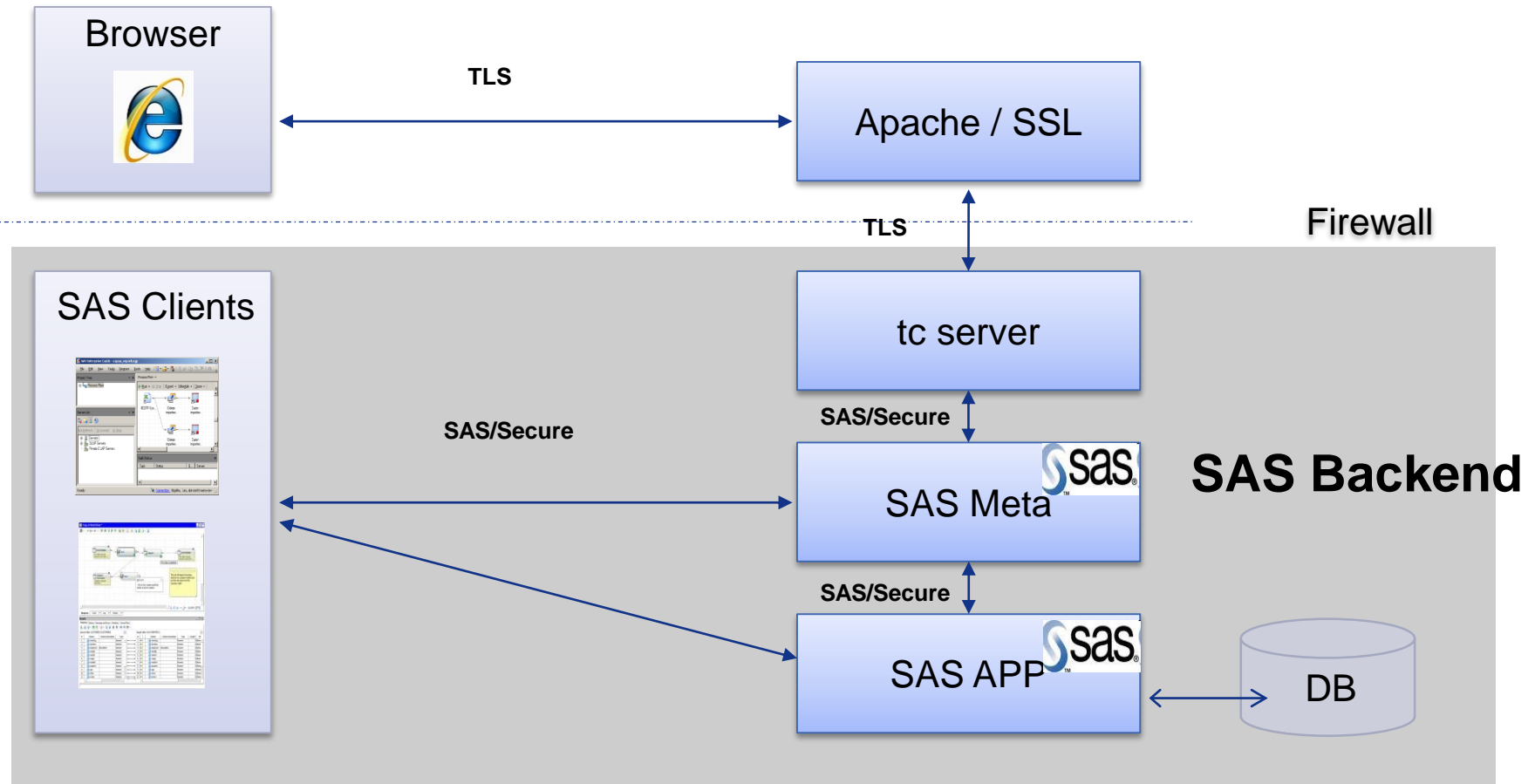
- (data classification, requirements )
- firewall to protect the backend Servers

## Web TLS 1.0 (SSL 3.1) Transport Layer Security

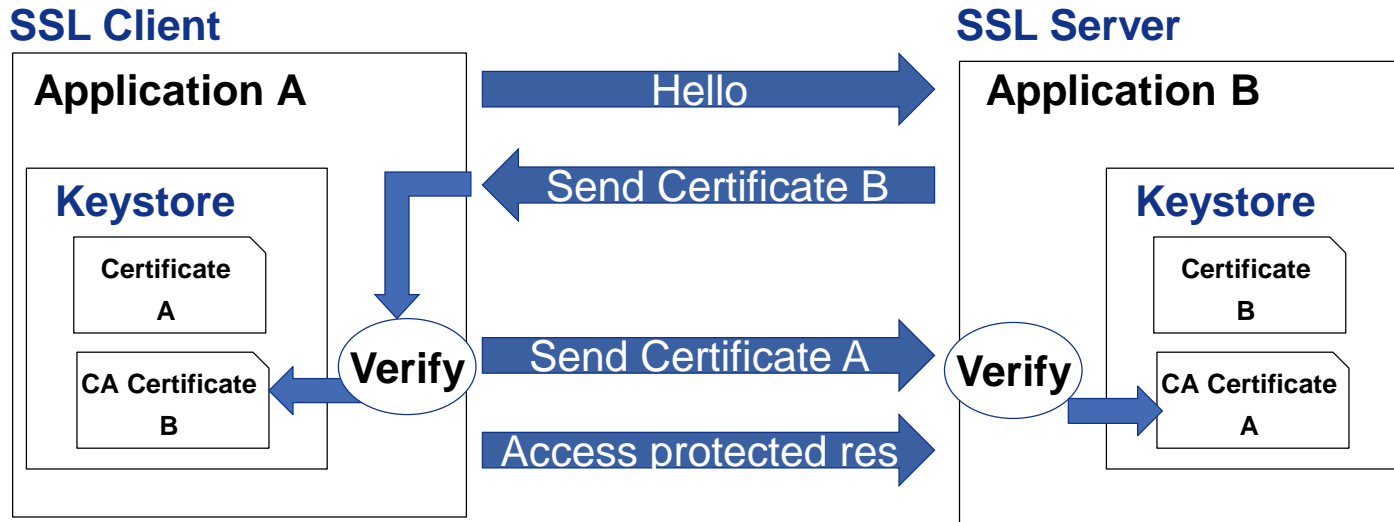
## SAS Clients (SAS/Secure™ ) included since SAS 9.4

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

# Reverse proxy and firewall

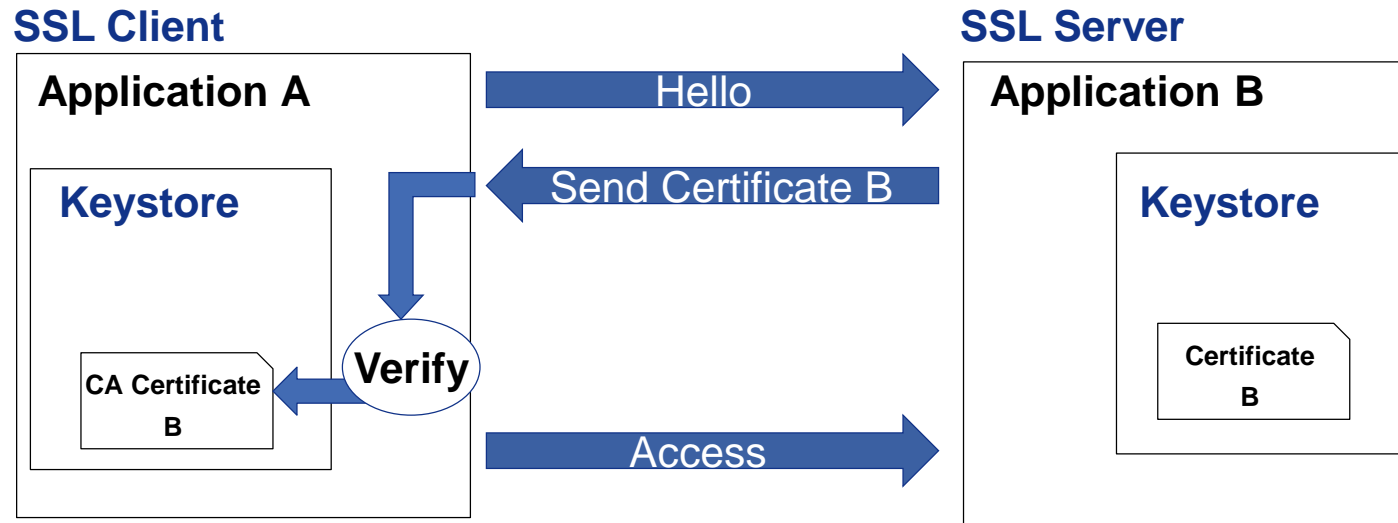


## SSL (two way SSL)



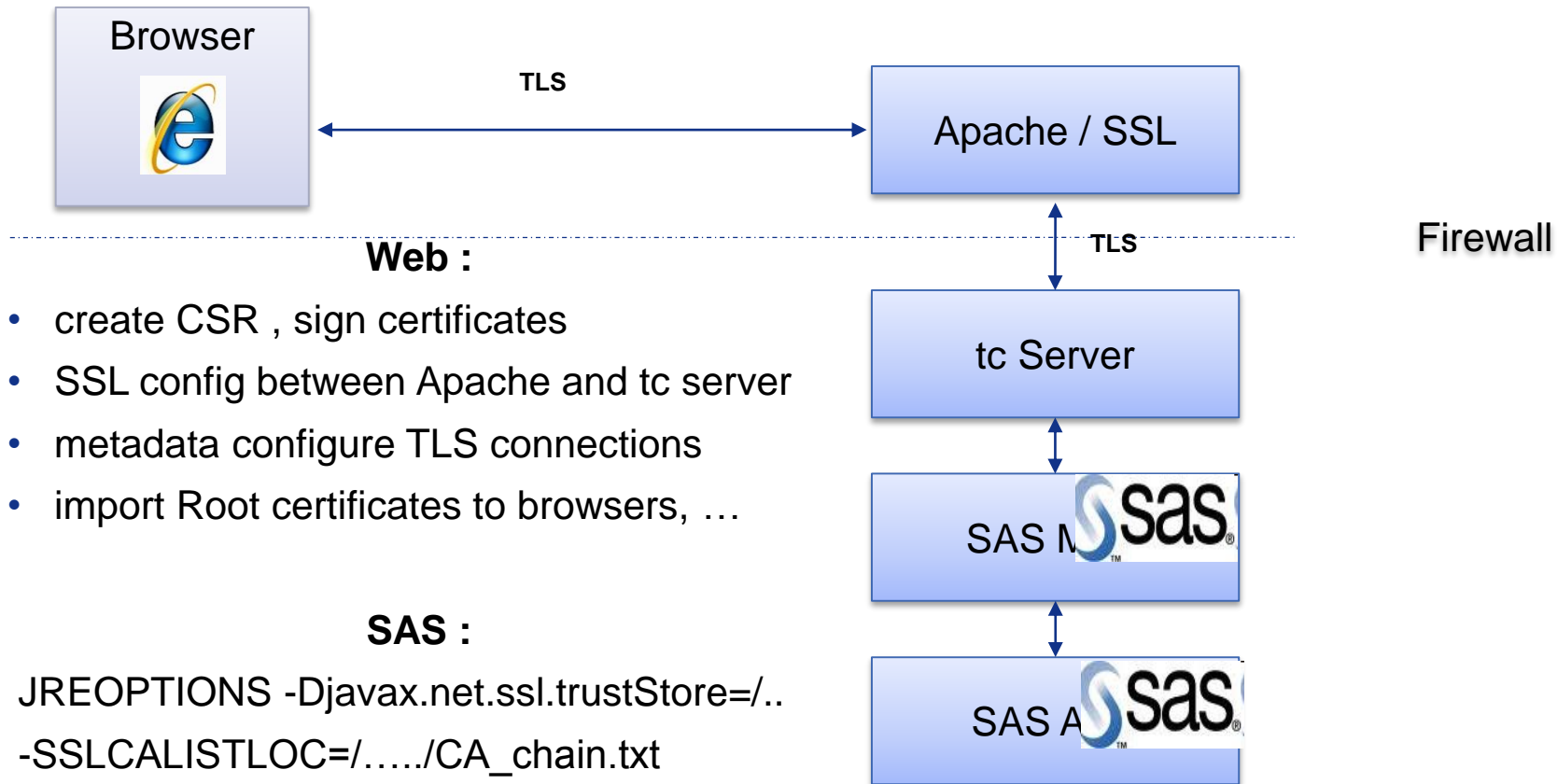
1. A client requests access to a protected resource.
2. The server presents its certificate to the client.
3. The client verifies the server's certificate.
4. If successful, the client sends its certificate to the server.
5. The server verifies the client's credentials.
6. If successful, the server grants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



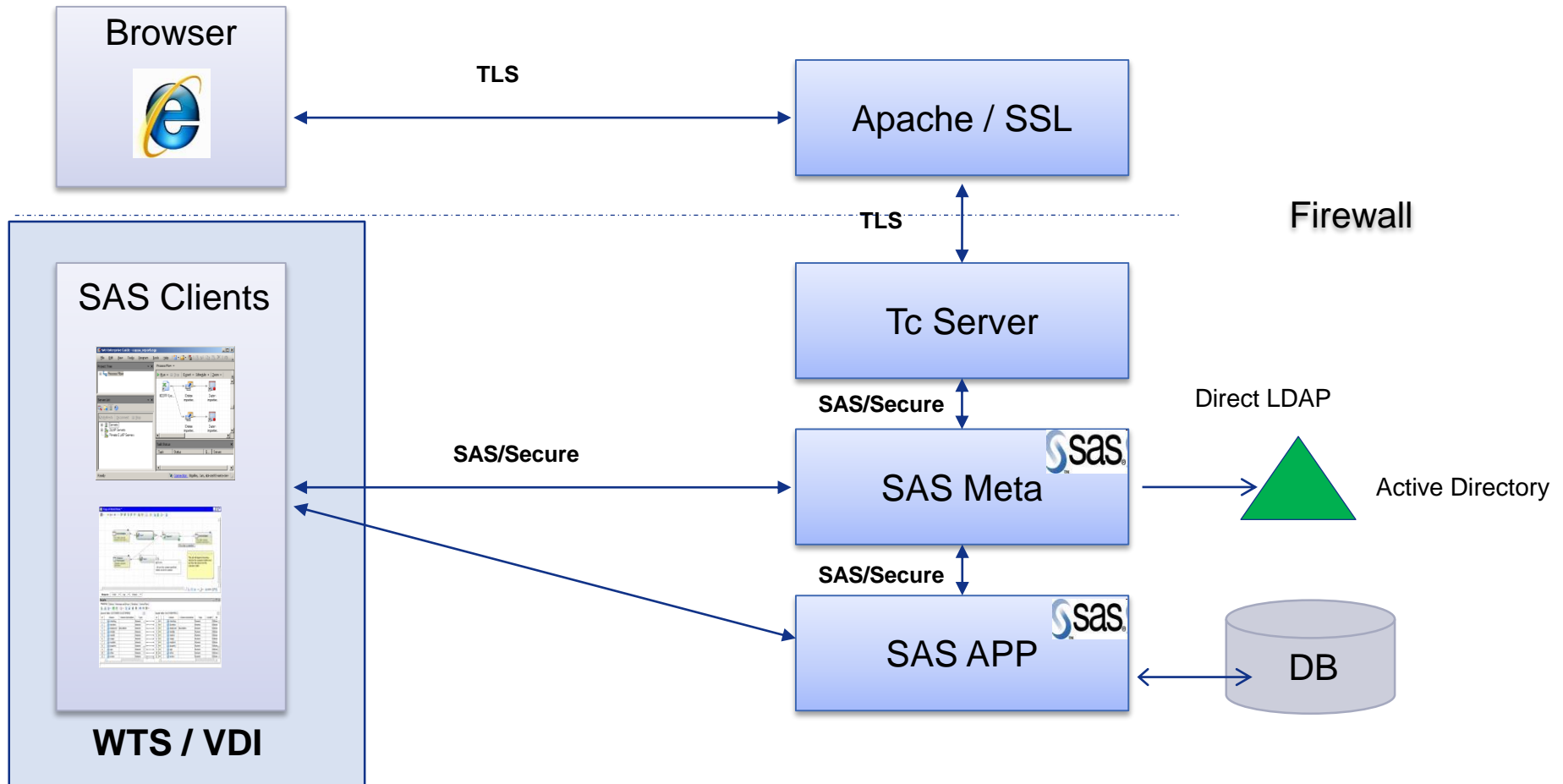
## SAS Clients :

- 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)