Help, the Internet is coming!
SAP Web Dispatcher and secure exposure

Tobias Lejczyk, Dr. Achim Braemer, SAP

PUBLIC

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

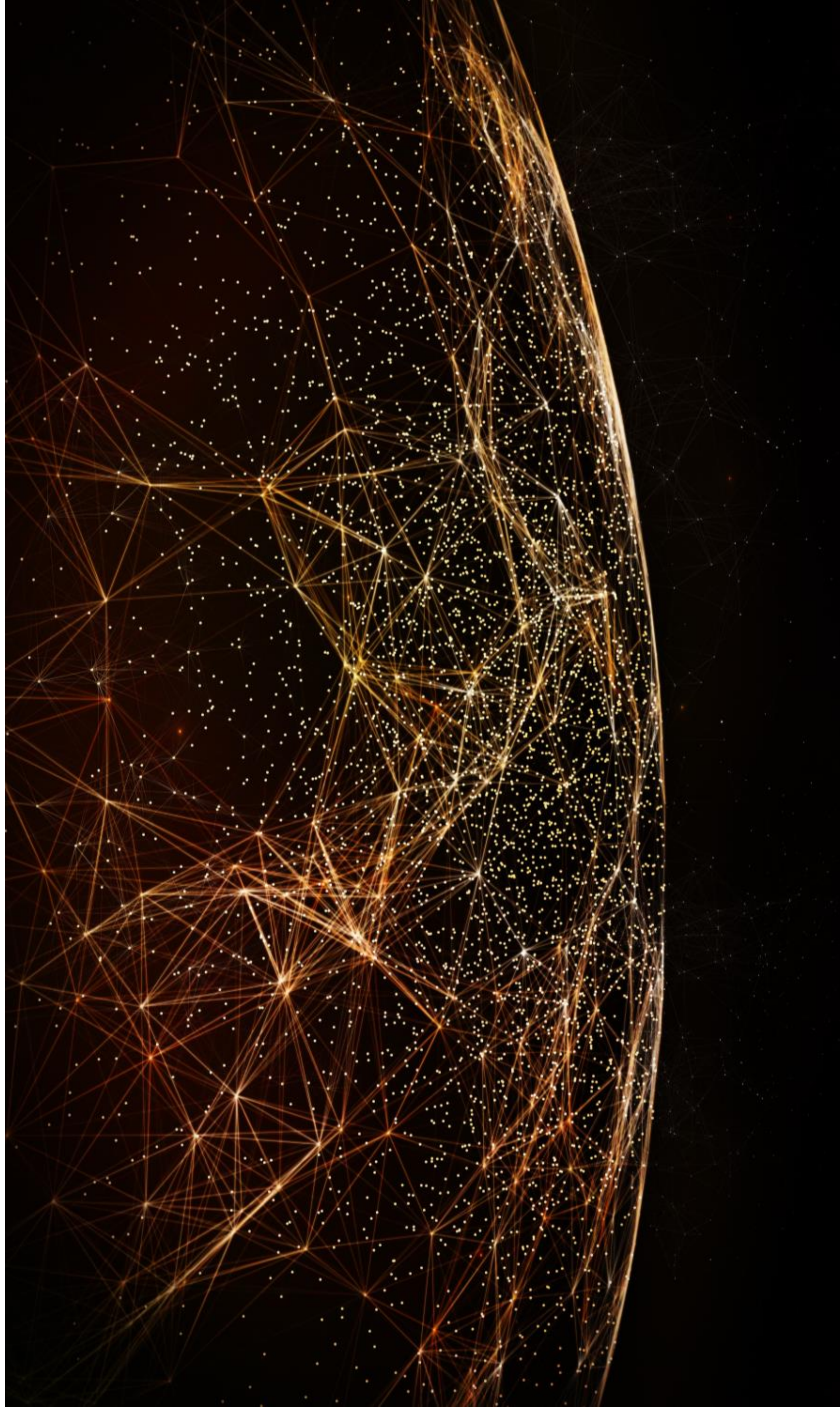
This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

The task

Enable Internet access to business system for

- Mobile devices
- External users
- Integration scenarios (machine to machine)



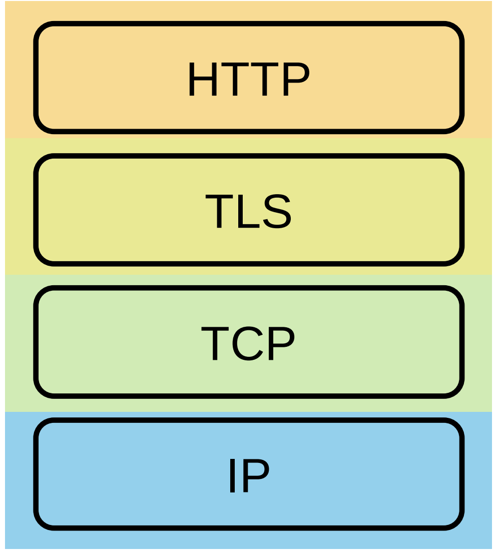
A journey in the dark

HTTP communication infrastructure

One protocol to rule them all

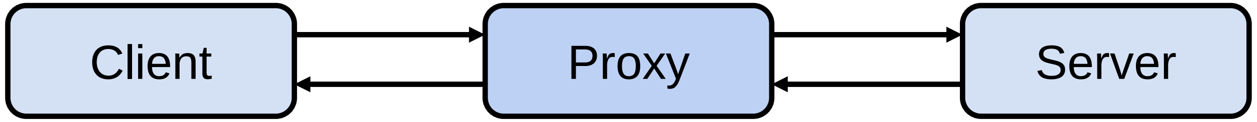
HTTP = **H**yper**t**ext **T**ransfer **P**rotocol

- Application layer protocol that enables communication between web servers and clients
- Was standardised by the Internet Engineering Task Force (IETF)
  RFC 7231
  https://datatracker.ietf.org/doc/html/rfc7231



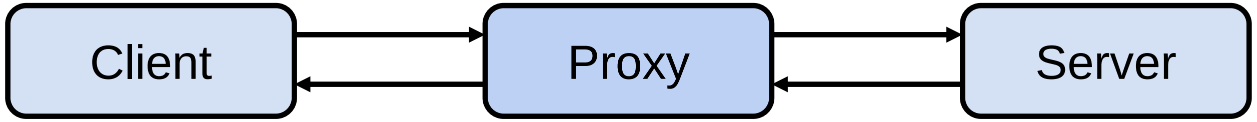
Proxy servers

- Intermediaries - handle traffic between clients and servers

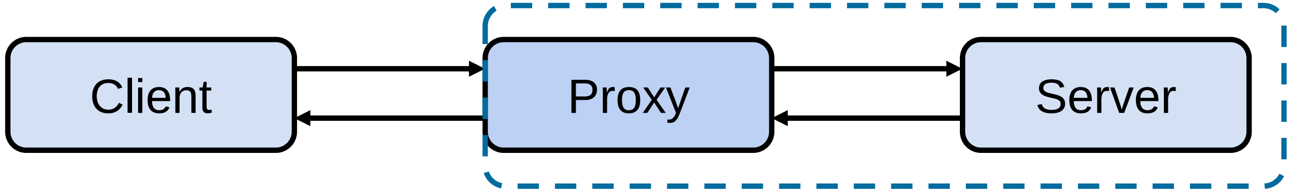


Proxy servers

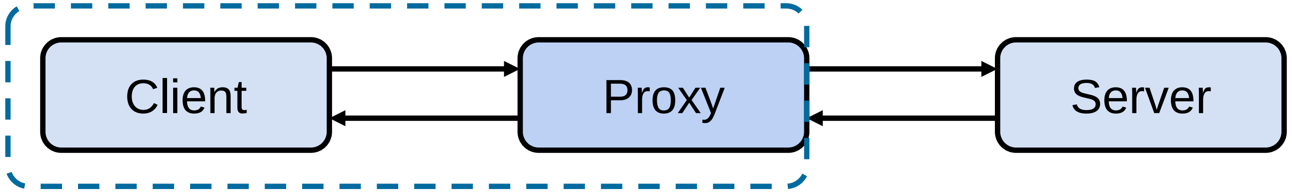
- Intermediaries - handle traffic between clients and servers



- Reverse proxies appear as servers to the client

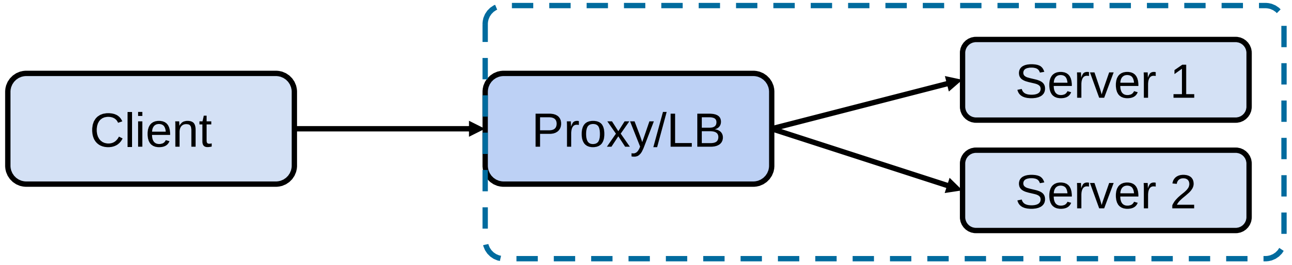


- Forward proxies forward traffic to another network

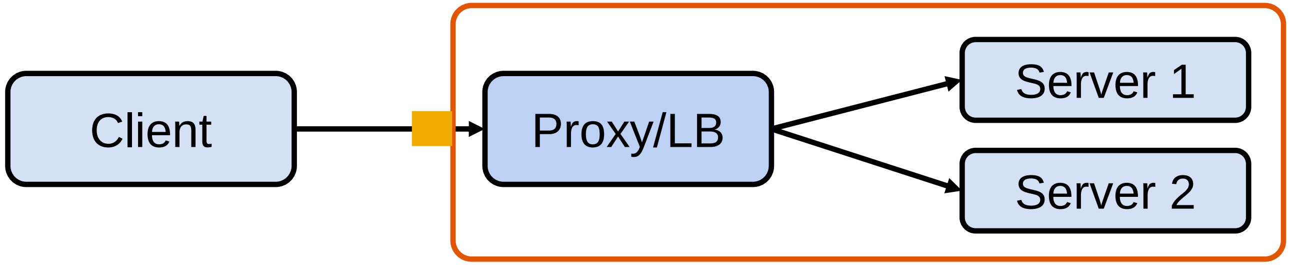


Reverse Proxies

- Loadbalancing

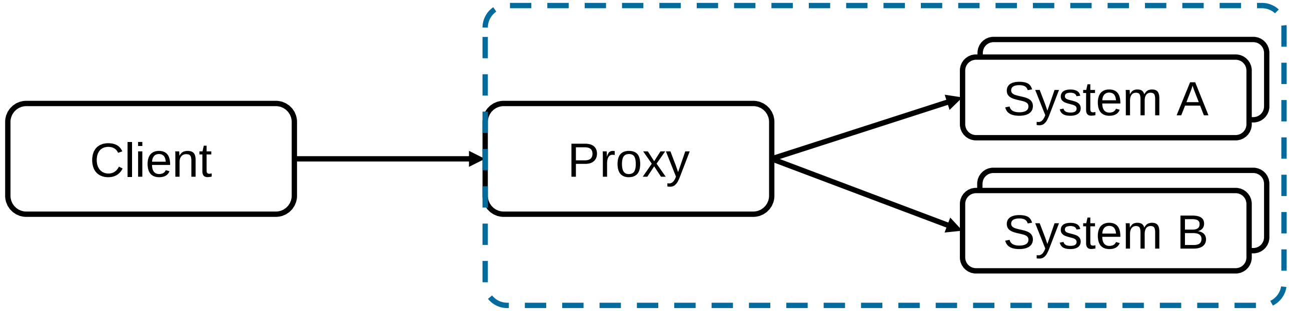


- Single Point of entry

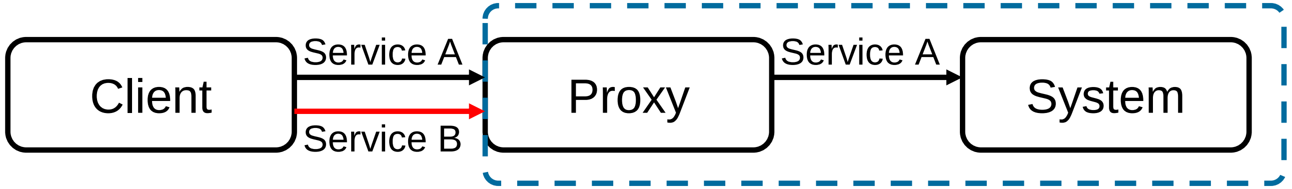


Reverse Proxies

- Traffic routing

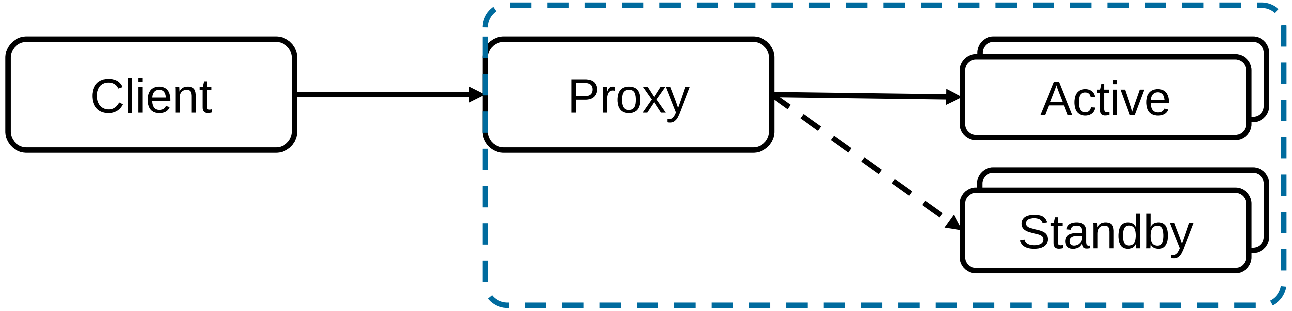


- Traffic filtering

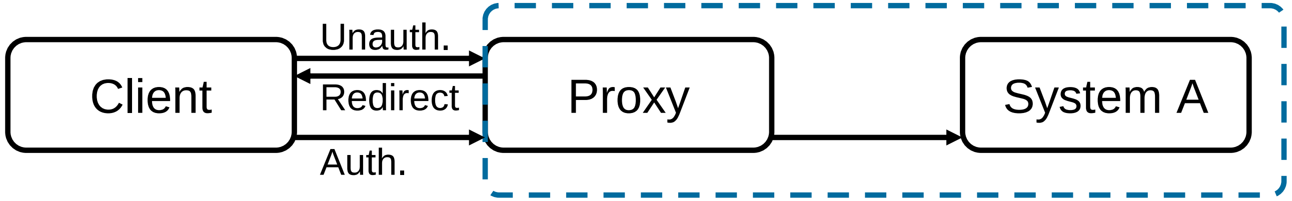


Reverse Proxies

- High availability

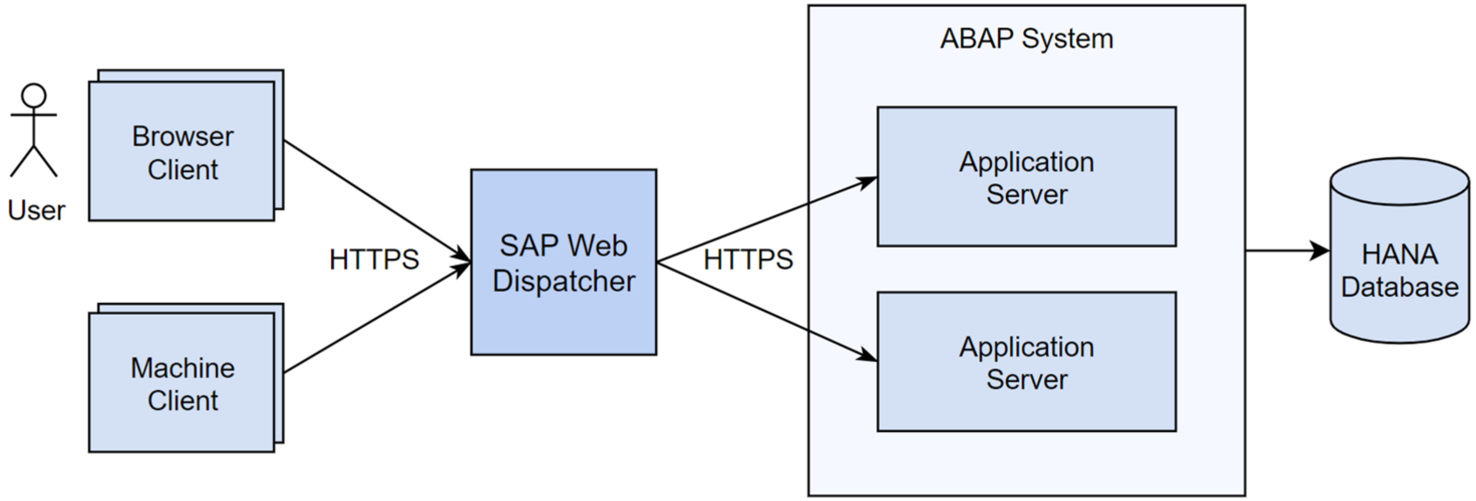


- (Pre-authentication)



SAP Web Dispatcher

- Software load balancer / Single Point of entry
- Reverse proxy
- Request router / filter
- By SAP for SAP systems (and others)

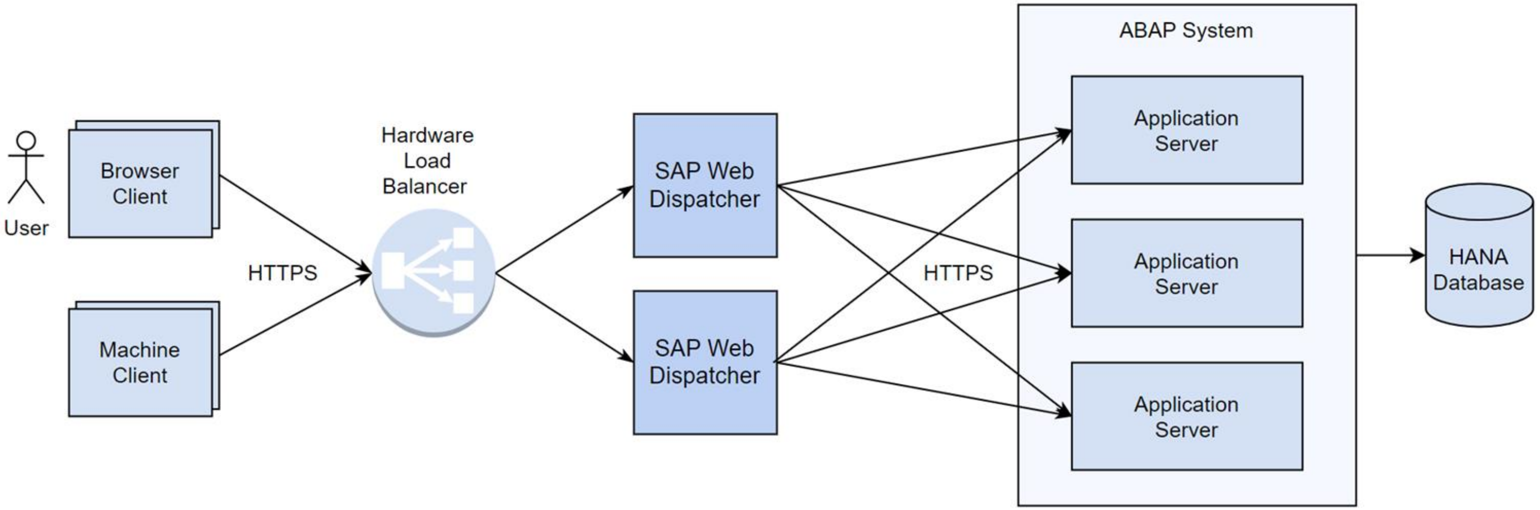


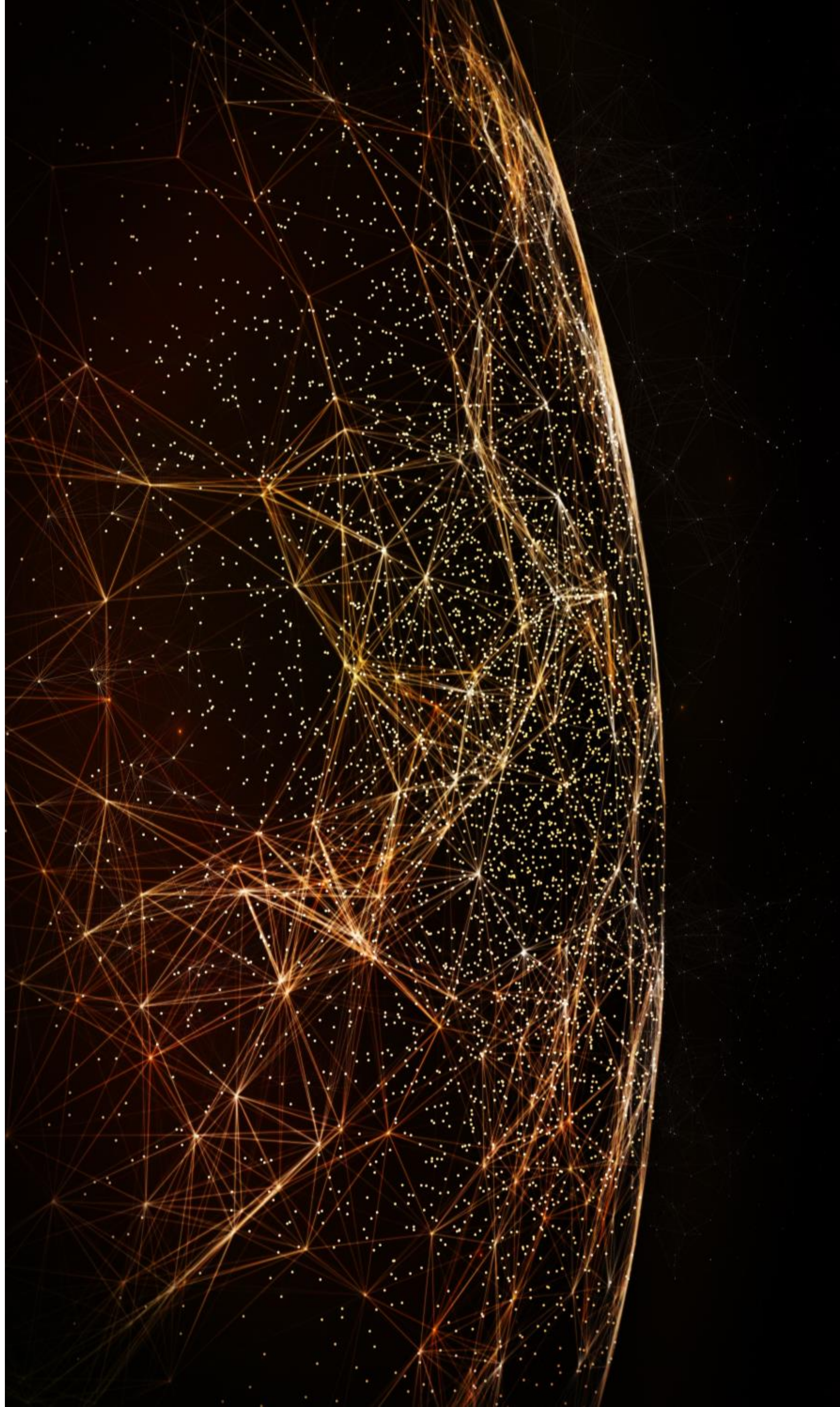
Exposing your S/4 to the Internet

Using SAP Web Dispatcher

The basic setup

Connect S/4 to the Internet using SAP Web Dispatcher





If high availability and high load are not relevant:
One Web Dispatcher without LB may be sufficient

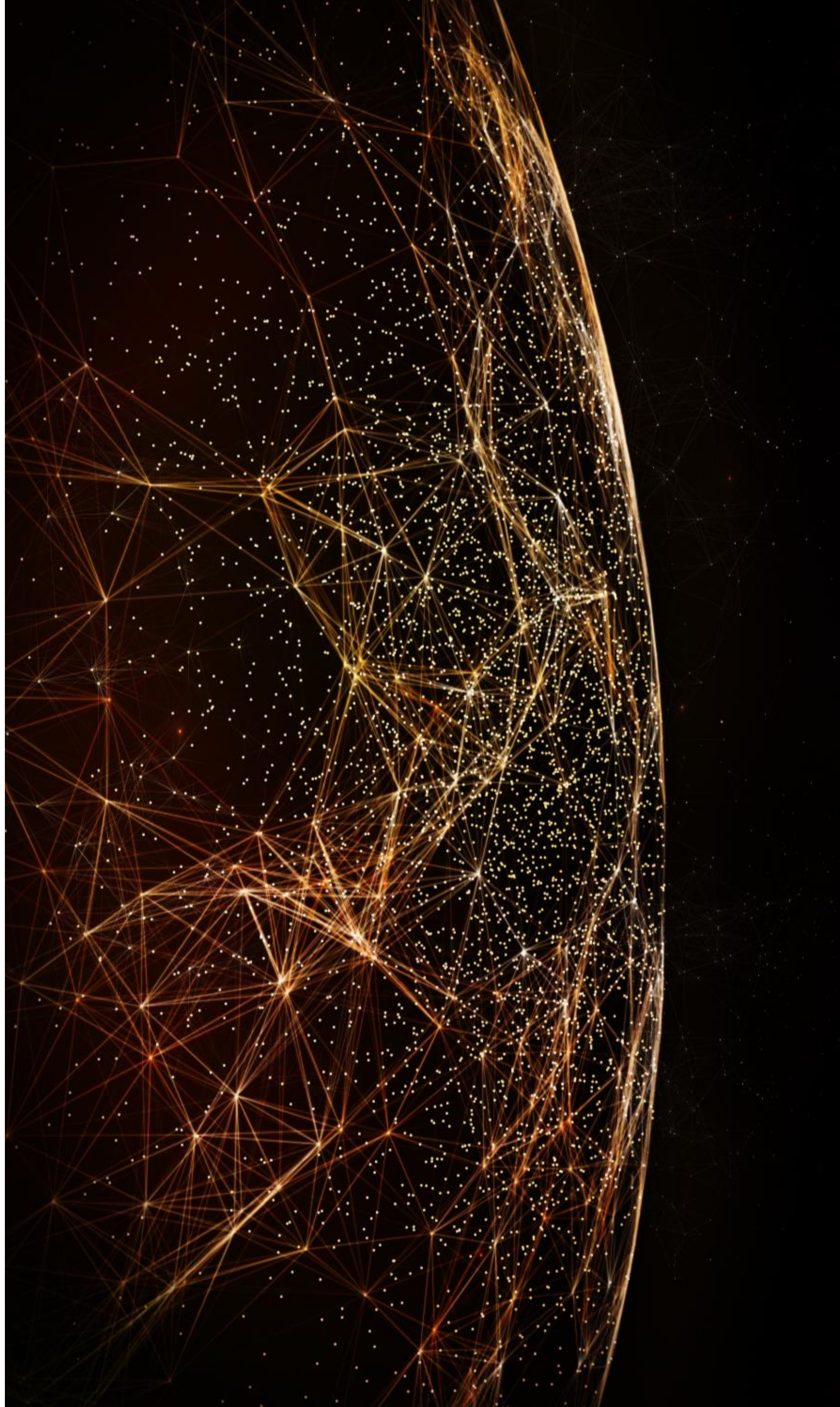
Protect against abusers from the Internet

Use secure authentication mechanisms

- Interactive login using IDP
  - MFA
  - Client certificates if possible
- Machine to machine
  - Client certificates if possible
  - IP filters if possible (few well-known communication partners)

Use SAP Web Dispatcher as request filter

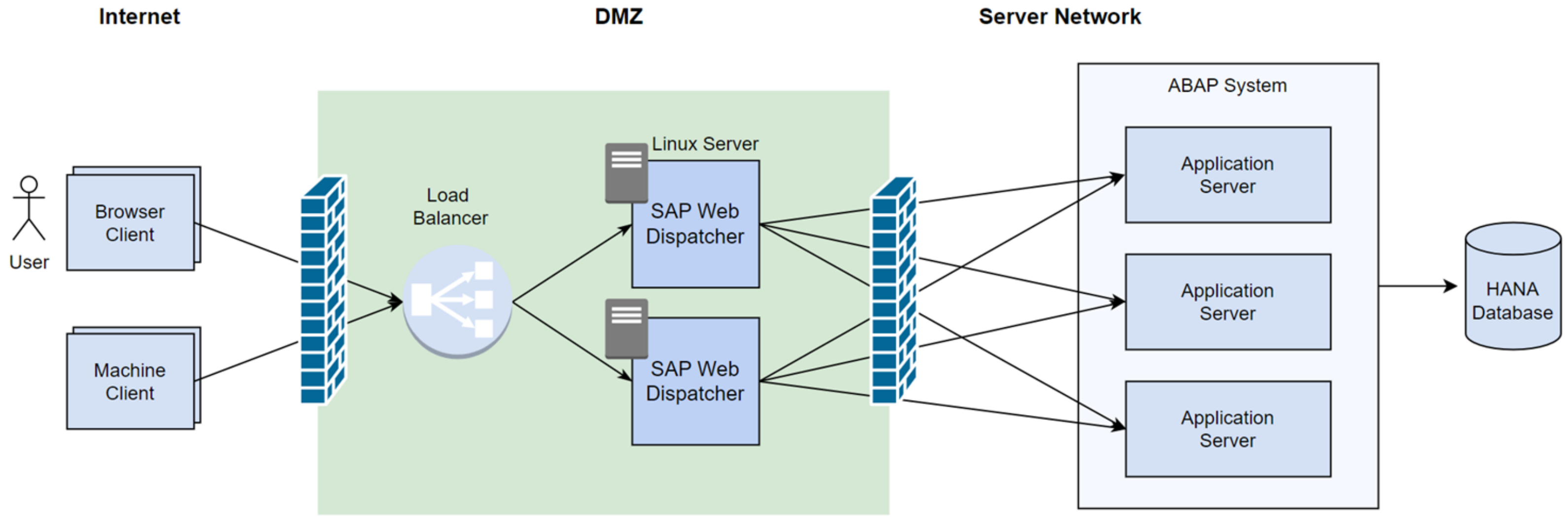
- HTTP protocol compliance
- Path prefix whitelisting
- Enforce client certificates
- IP filter

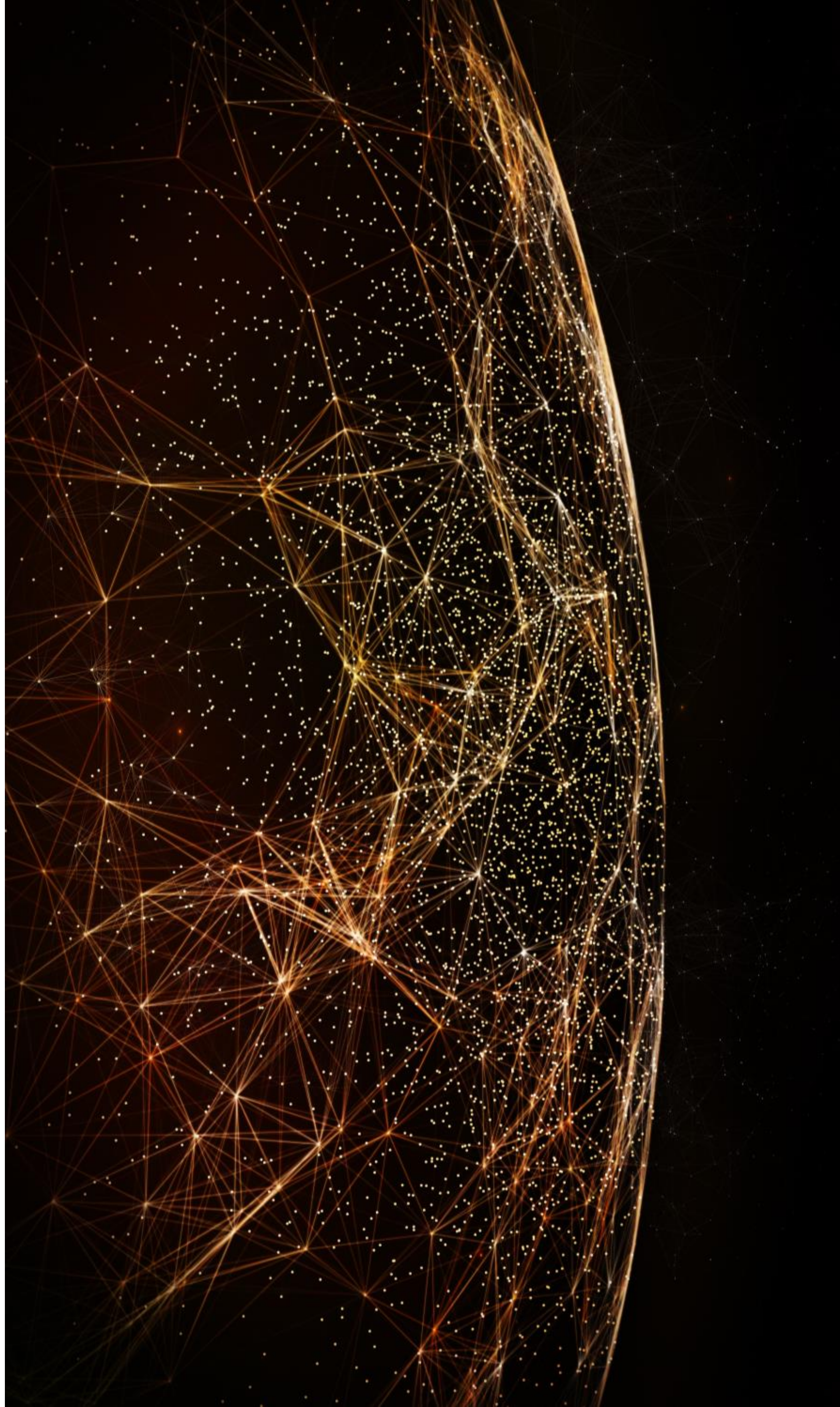


Secure network setup

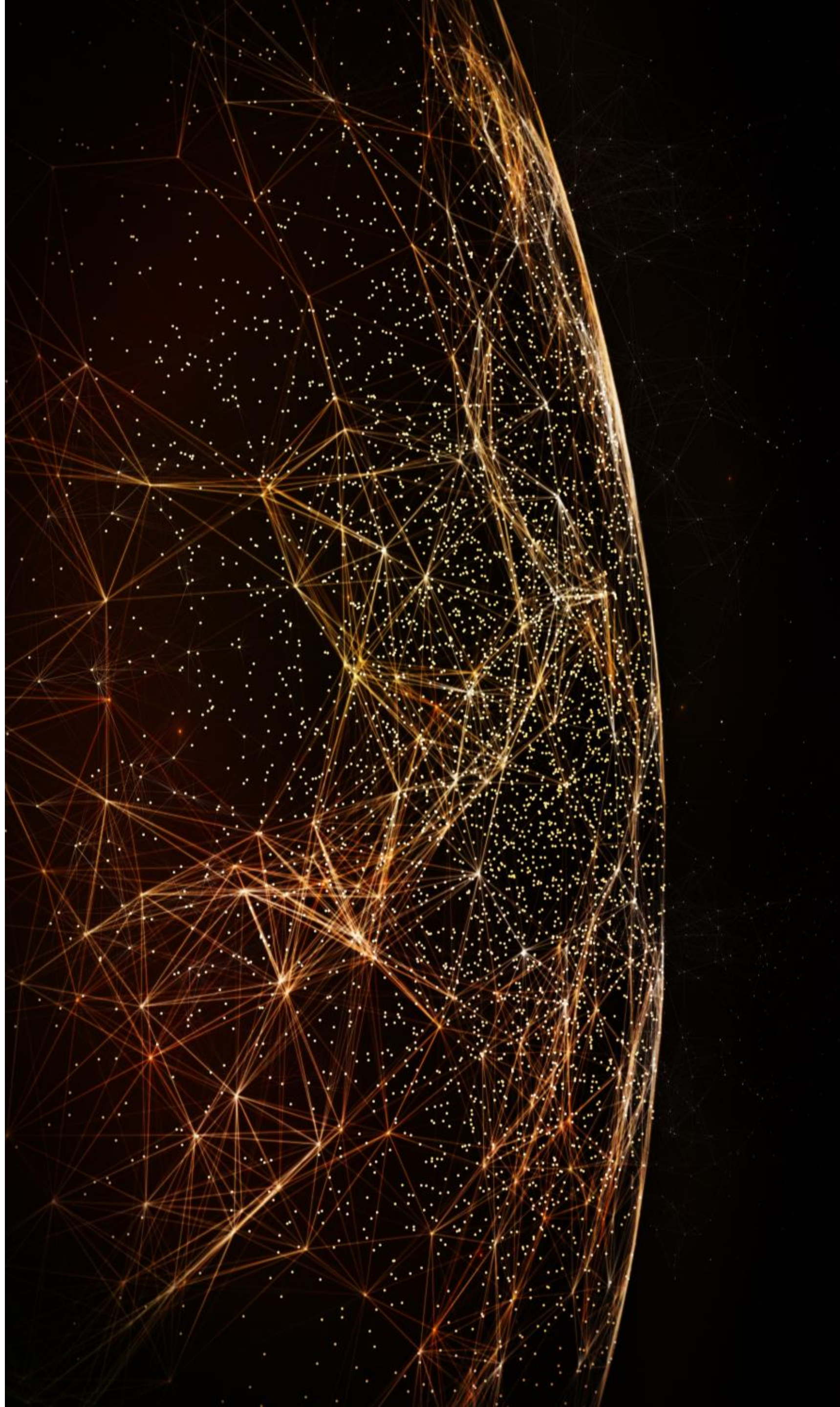
Place SAP Web Dispatcher in a "Demilitarized Zone" (DMZ)

- Recommended OS: Linux
- Host hardening goes without saying





Use a Web Application Firewall (WAF) or not?



Consider whether you need a WAF for SAP applications

- There is no WAF with explicit protection for the protocols used by SAP applications

- Standard WAF rulesets may do more harm than good
  - e.g [OWASP Core Rule Set]() (used by many WAFs) [blocks OData $batch]()

- SAP UI technologies are secure against OWASP top 10 attacks
  - Especially OData-based Fiori UIs use a completely different technology as normal Web applications
  - Recommendation: Use only SAP UI technologies, not homegrown

- However, some organizations require WAF in compliance rules

Avert Denial of Service (DoS) attacks

1) Against network infrastructure and LB

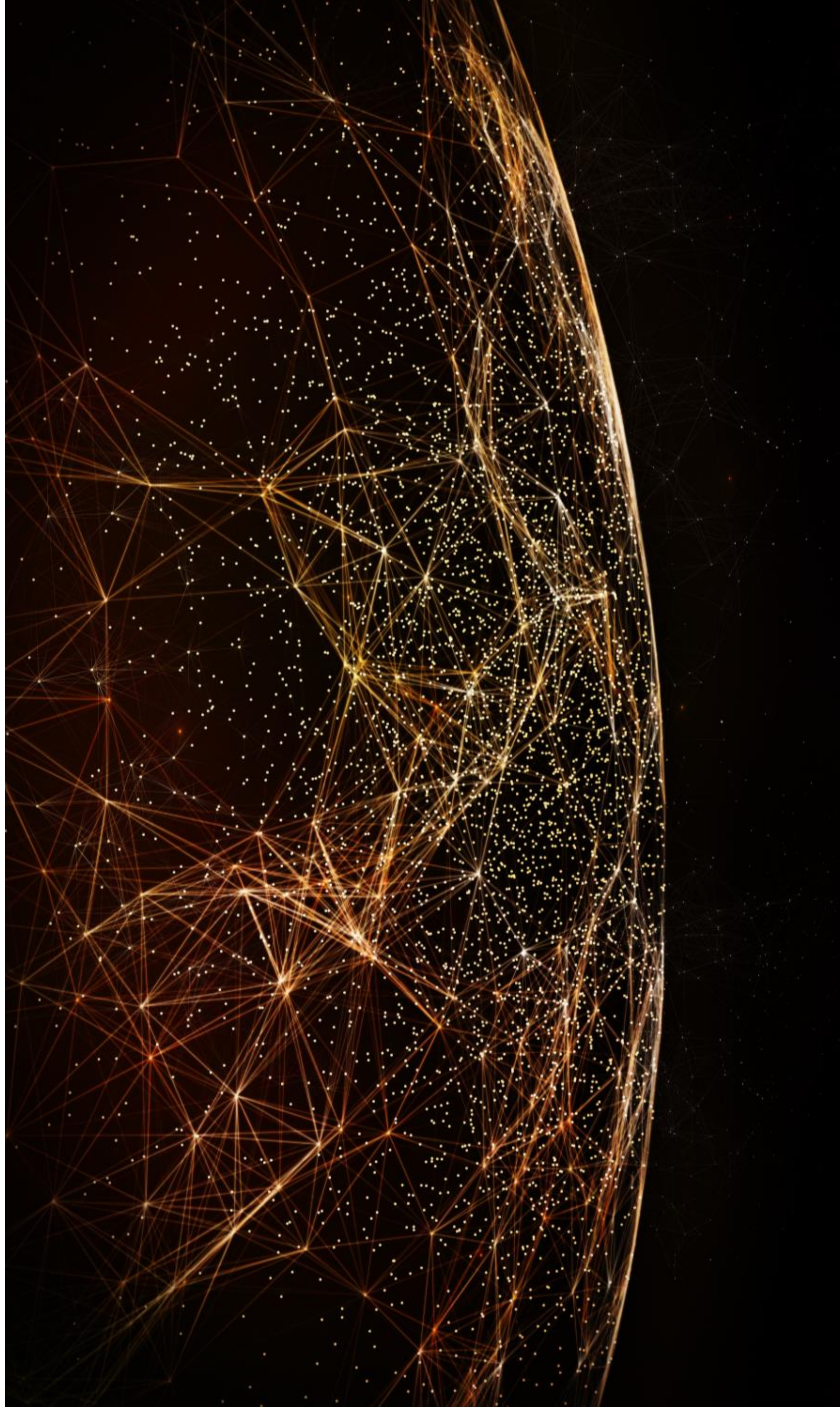
- Deploy DoS protection on network layer

2) Against SAP Web Dispatcher

- Configuration options see next slide

3) Against backend

- Use SAP Web Dispatcher to effectively protect your "crown jewels"
  See following slides

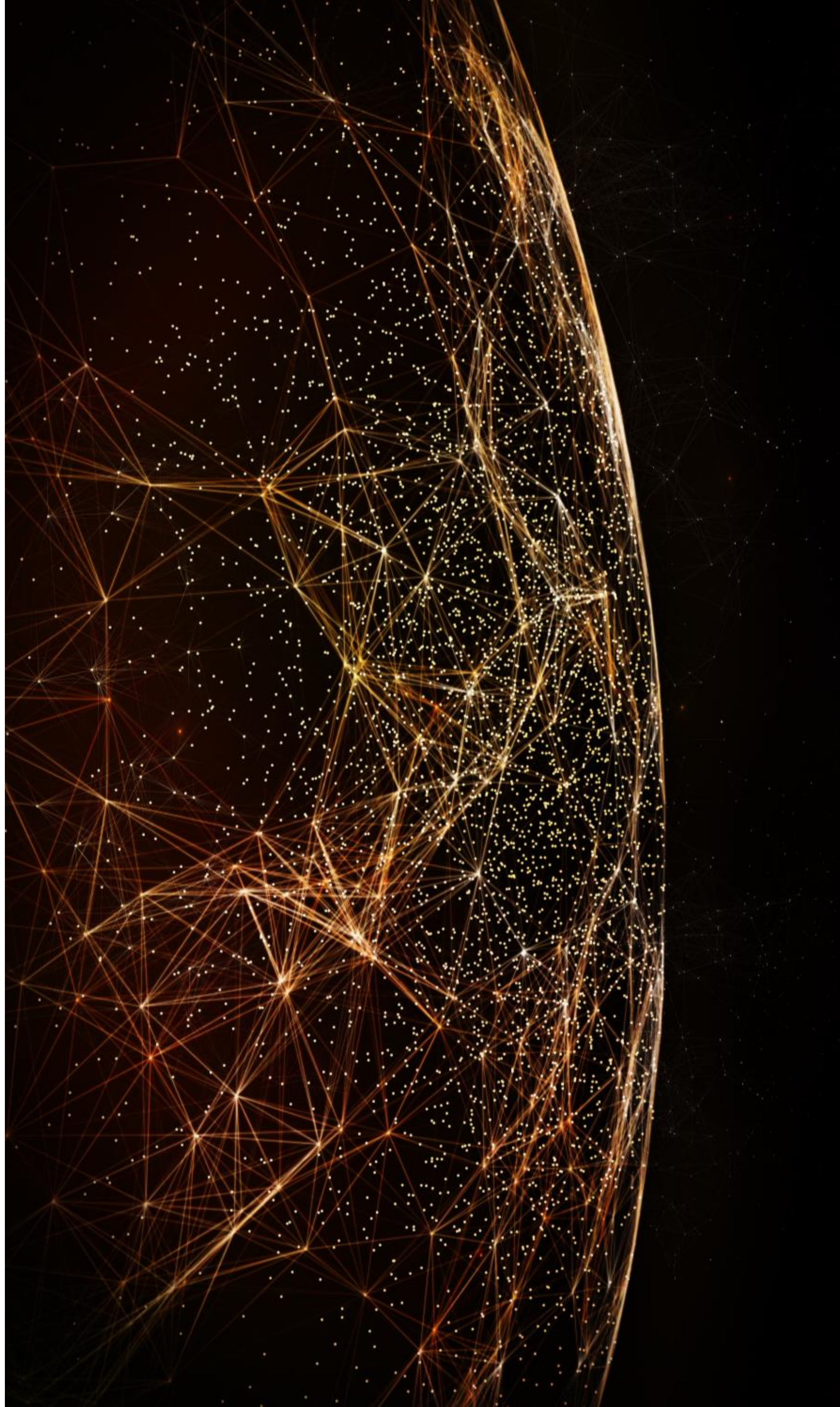


DoS protection of SAP Web Dispatcher

- Load Balancer throttling according to SAP Web Dispatcher sizing
  - Roughly 1000 request per second per CPU core
  - or connection limit as per WD configuration

- Limit Connections per Client IP
  - Difficult to tune with many clients over a single IP address
  - Tipp: use WARN and REJECT levels

- Configure protection against Slowloris Attacks
  - Also difficult to tune
  - Tipp: use WARN and REJECT levels



DoS protection of backend ABAP system

Separate critical business from Internet access

1) Expose only a subset of servers to the Internet

How to:

Create logon group, e.g. "INTERNET" (SMLG)

Create icm/HTTP/mod handler with one rule:

```
SetHeader X-SAP-WEBDISP-TARGET-GROUP-NO-REDISPATCH INTERNET
```

Now SAP Web Dispatcher sends requests only to servers in "INTERNET" group

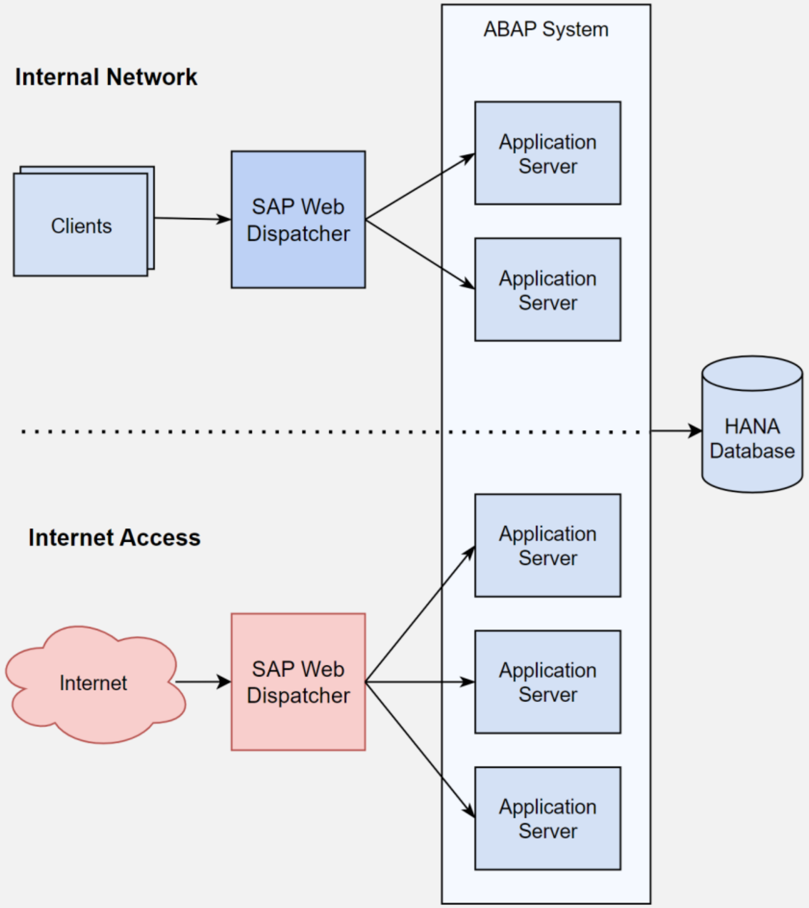
2) Limit the number of pending requests

How to:

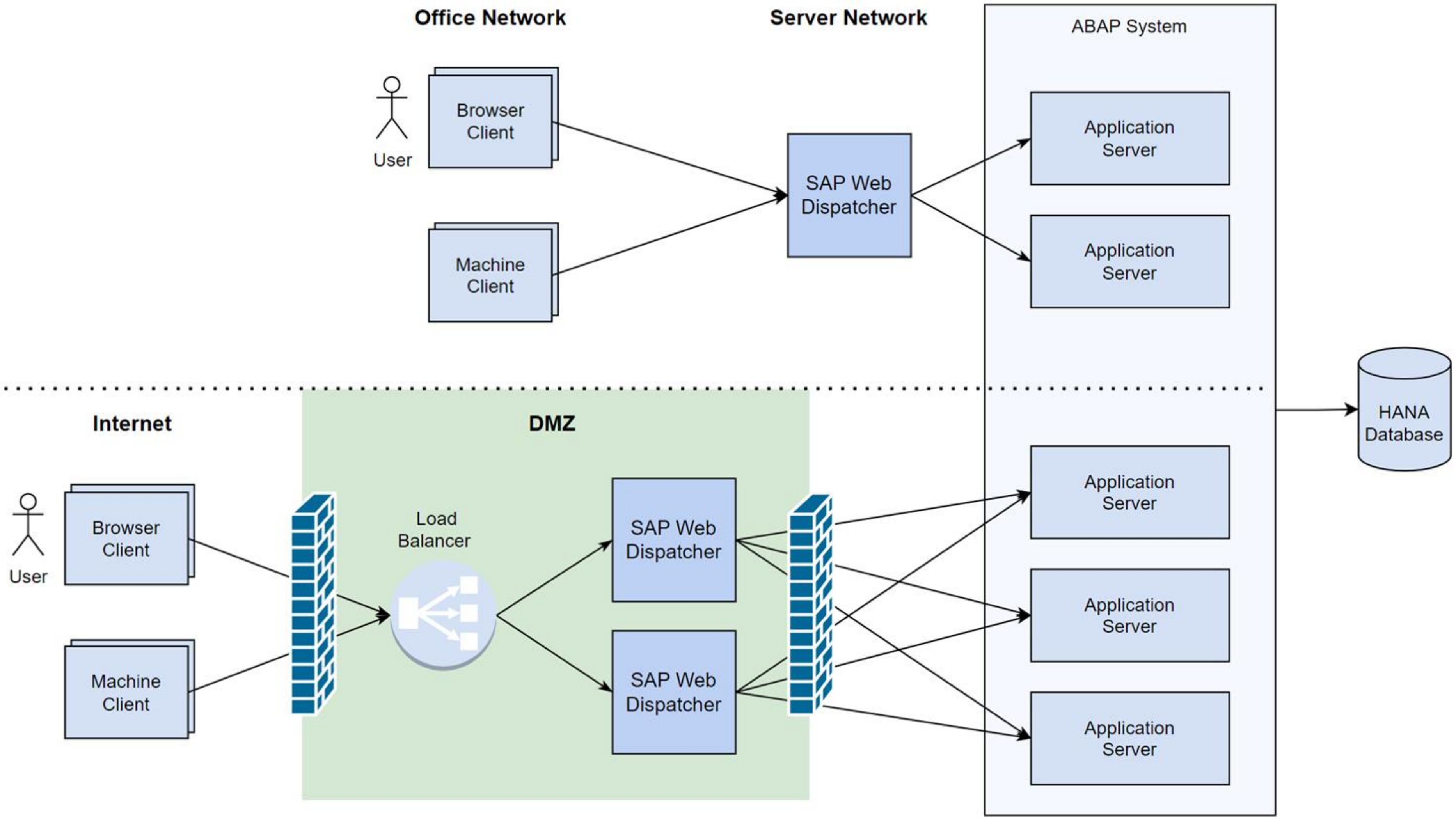
Configure Limit Concurrent Requests per System

in the Internet-facing SAP Web Dispatcher.

Avoids overload of work processes and database



Full picture



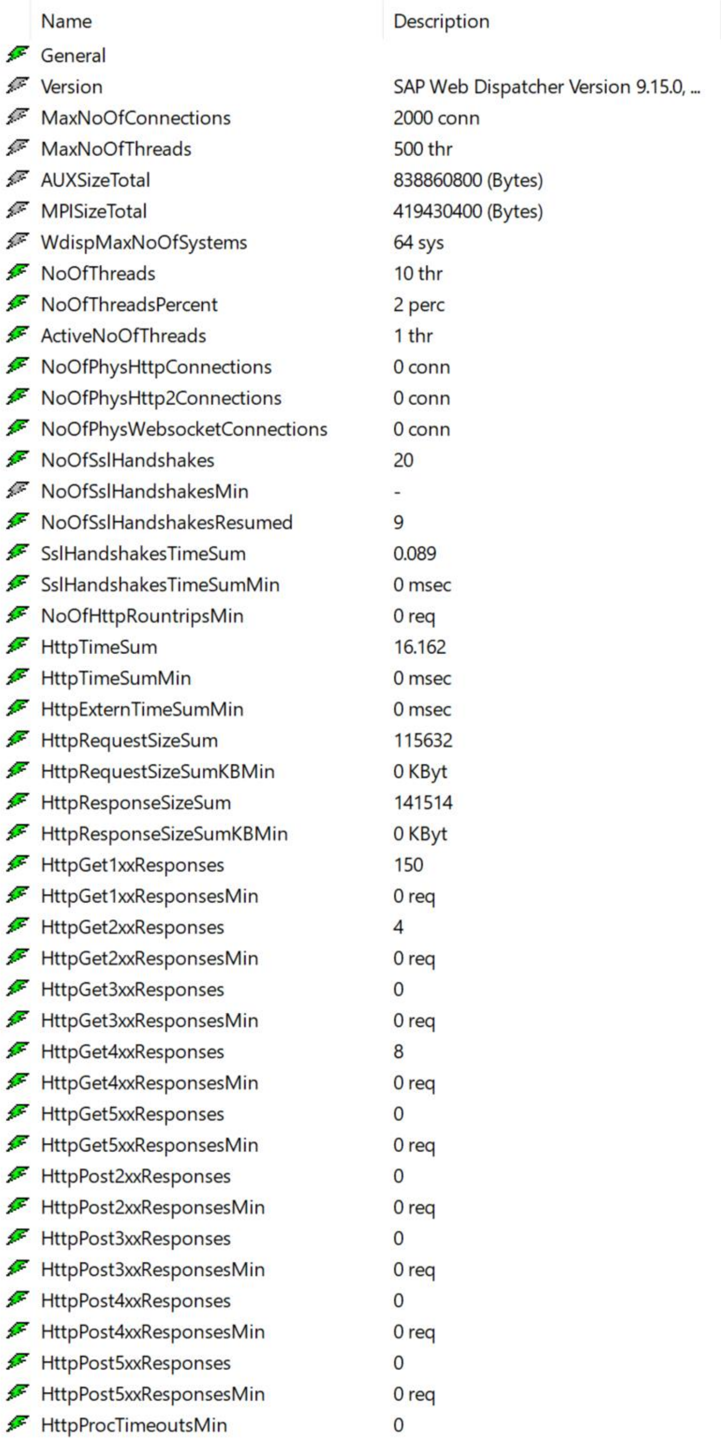
Last not least – Prepare for the worst

Monitor SAP Web Dispatcher and backend system

- Load monitoring
  - OS resources: CPU, network
  - CCMS metrics of Web Dispatcher
  - Web Dispatcher load statistics (webdisp-load-statistic* in work dir)
- Web Dispatcher security log
- HTTP log
- Security Information and Event Management (SIEM), e.g. SAP ETD

Security assessments

Create play-books for attack scenarios



Name	Description
General	
Version	SAP Web Dispatcher Version 9.15.0, ...
MaxNoOfConnections	2000 conn
MaxNoOfThreads	500 thr
AUXSizeTotal	838860800 (Bytes)
MPISizeTotal	419430400 (Bytes)
WdispMaxNoOfSystems	64 sys
NoOfThreads	10 thr
NoOfThreadsPercent	2 perc
ActiveNoOfThreads	1 thr
NoOfPhysHttpConnections	0 conn
NoOfPhysHttp2Connections	0 conn
NoOfPhysWebsocketConnections	0 conn
NoOfSslHandshakes	20
NoOfSslHandshakesMin	-
NoOfSslHandshakesResumed	9
SslHandshakesTimeSum	0.089
SslHandshakesTimeSumMin	0 msec
NoOfHttpRountripsMin	0 req
HttpTimeSum	16.162
HttpTimeSumMin	0 msec
HttpExternTimeSumMin	0 msec
HttpRequestSizeSum	115632
HttpRequestSizeSumKBMin	0 KByt
HttpResponseSizeSum	141514
HttpResponseSizeSumKBMin	0 KByt
HttpGet1xxResponses	150
HttpGet1xxResponsesMin	0 req
HttpGet2xxResponses	4
HttpGet2xxResponsesMin	0 req
HttpGet3xxResponses	0
HttpGet3xxResponsesMin	0 req
HttpGet4xxResponses	8
HttpGet4xxResponsesMin	0 req
HttpGet5xxResponses	0
HttpGet5xxResponsesMin	0 req
HttpPost2xxResponses	0
HttpPost2xxResponsesMin	0 req
HttpPost3xxResponses	0
HttpPost3xxResponsesMin	0 req
HttpPost4xxResponses	0
HttpPost4xxResponsesMin	0 req
HttpPost5xxResponses	0
HttpPost5xxResponsesMin	0 req
HttpProcTimeoutsMin	0

Thank you.

Contact information:

Tobias Lejczyk
Senior Technology Consultant
tobias.lejczyk@sap.com
+49 6227 7 79159

Dr. Achim Braemer
Chief Development Architect
Former SAP Web Dispatcher Product Owner
achim.braemer@sap.com

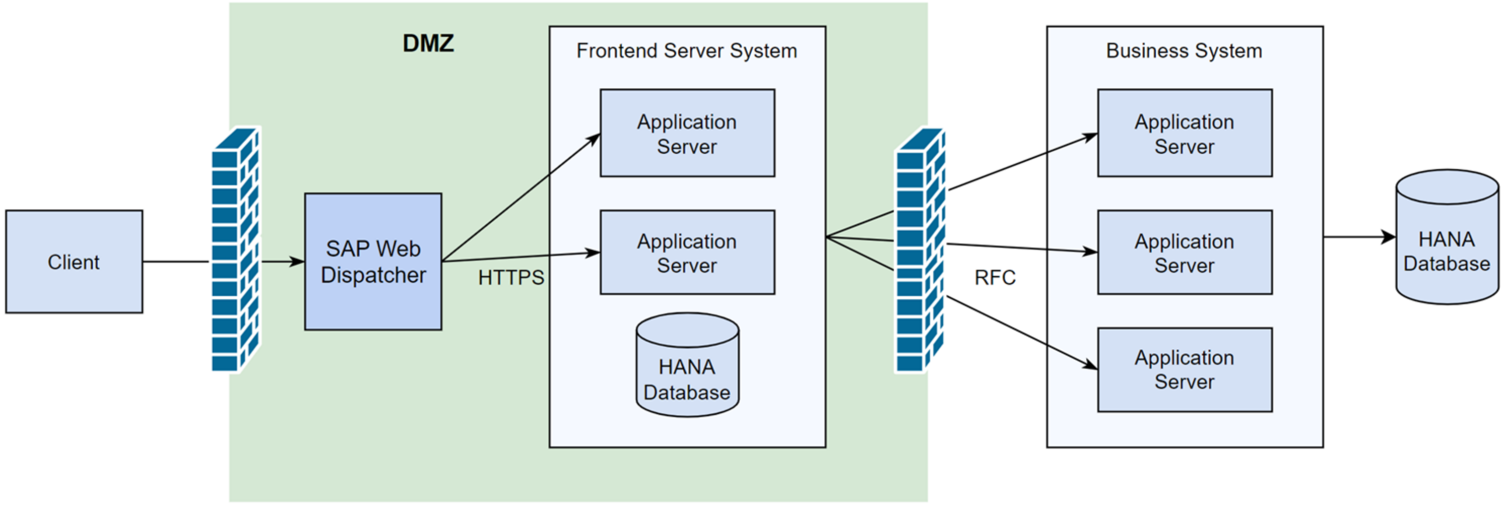
THE BEST RUN

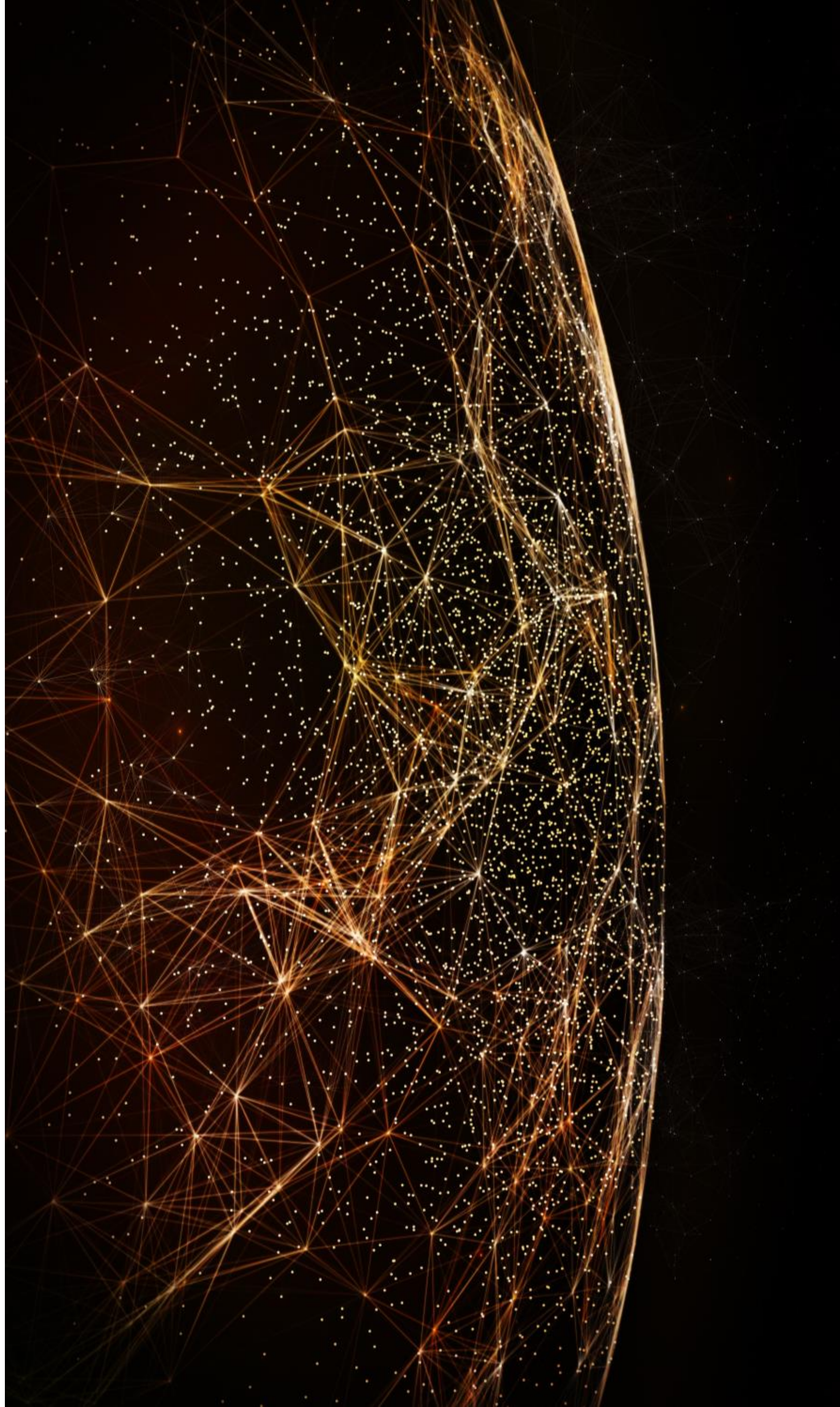
Appendix

Alternative security solution?
The Fiori Front-End Server

Standalone SAP Fiori Front-End Server can be installed in DMZ

- Forwards OData requests to backend wrapped in RFC protocol
  → Only works for Fiori apps
- Full S/4 foundation system with HANA DB, must be in sync with backend
- Great effort, questionable security benefit





How to forward the client IP address

SAP Web Dispatcher needs to know the client's IP address (for filtering, logging etc.)

Case 1: Load balancer acts on IP layer

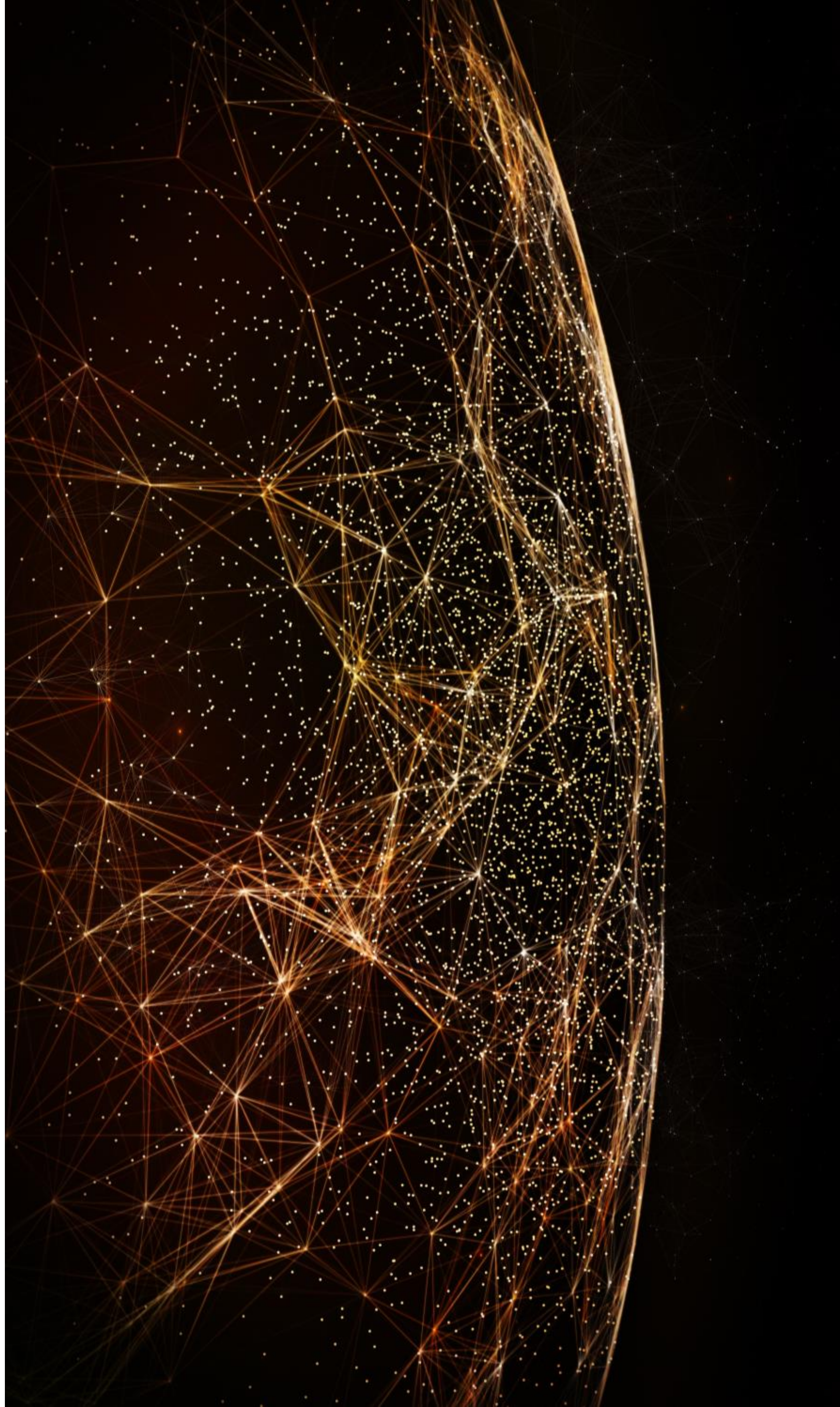
- Client IP is directly known in SAP Web Dispatcher

Case 2: Load balancer acts on TCP layer

- LB must support the PROXY protocol to forward the client IP

Case 3: Load balancer acts on HTTP layer (terminates TLS)

- Use `x-forwarded-for` or (better) the `true-client-ip` header

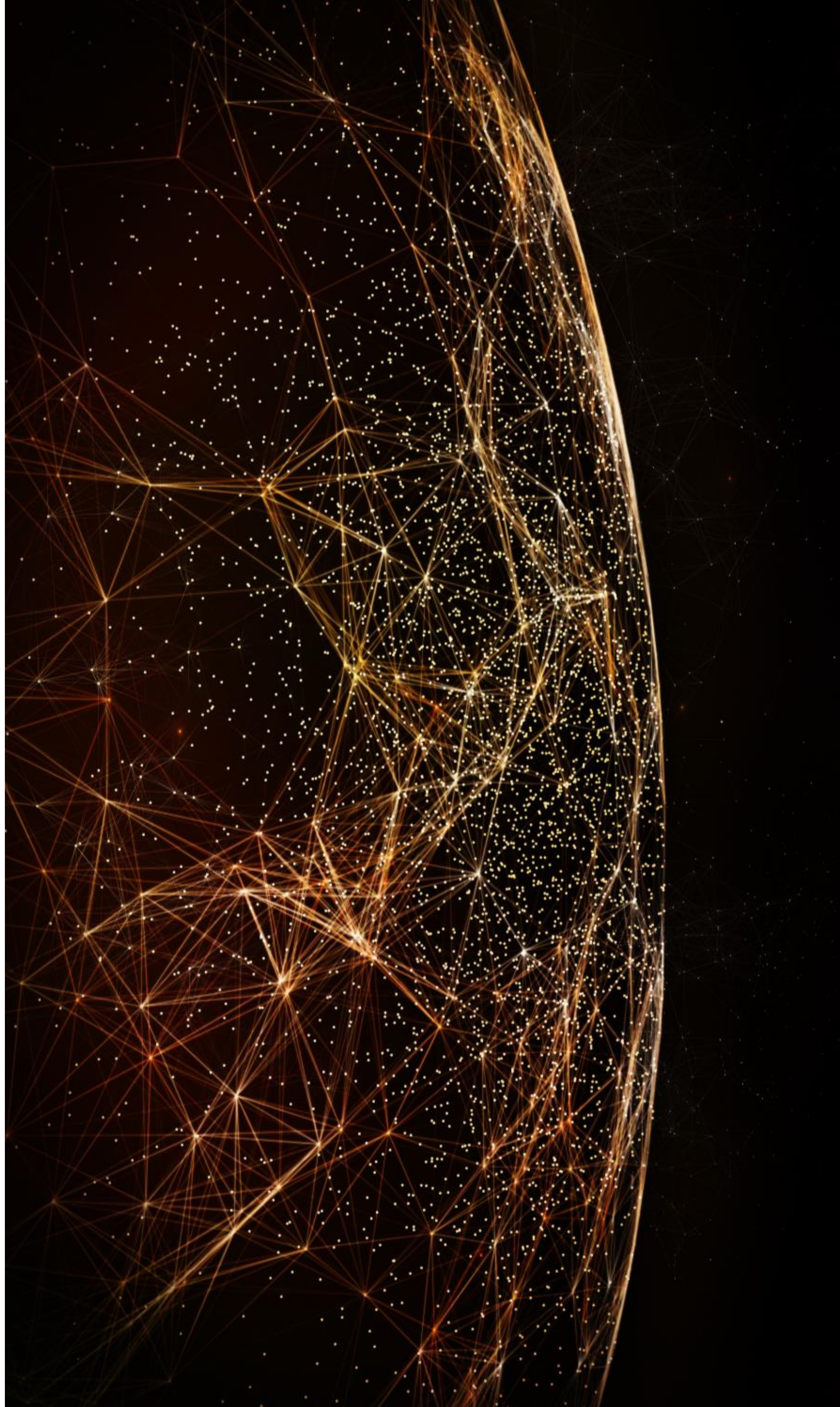


Configuration of the hardware load balancer

Chose where to terminate TLS:

- **In SAP Web Dispatcher**
  - Less resources in LB
  - Easier to configure
  - Client cert authentication & principal propagation much easier and more secure
    - Some LB have deficiencies that inhibit a secure setup for principal propagation

- **In the hardware load balancer**
  - Possible to use Web Application Firewall (WAF) and DoS protection integrated in LB (more on that later)



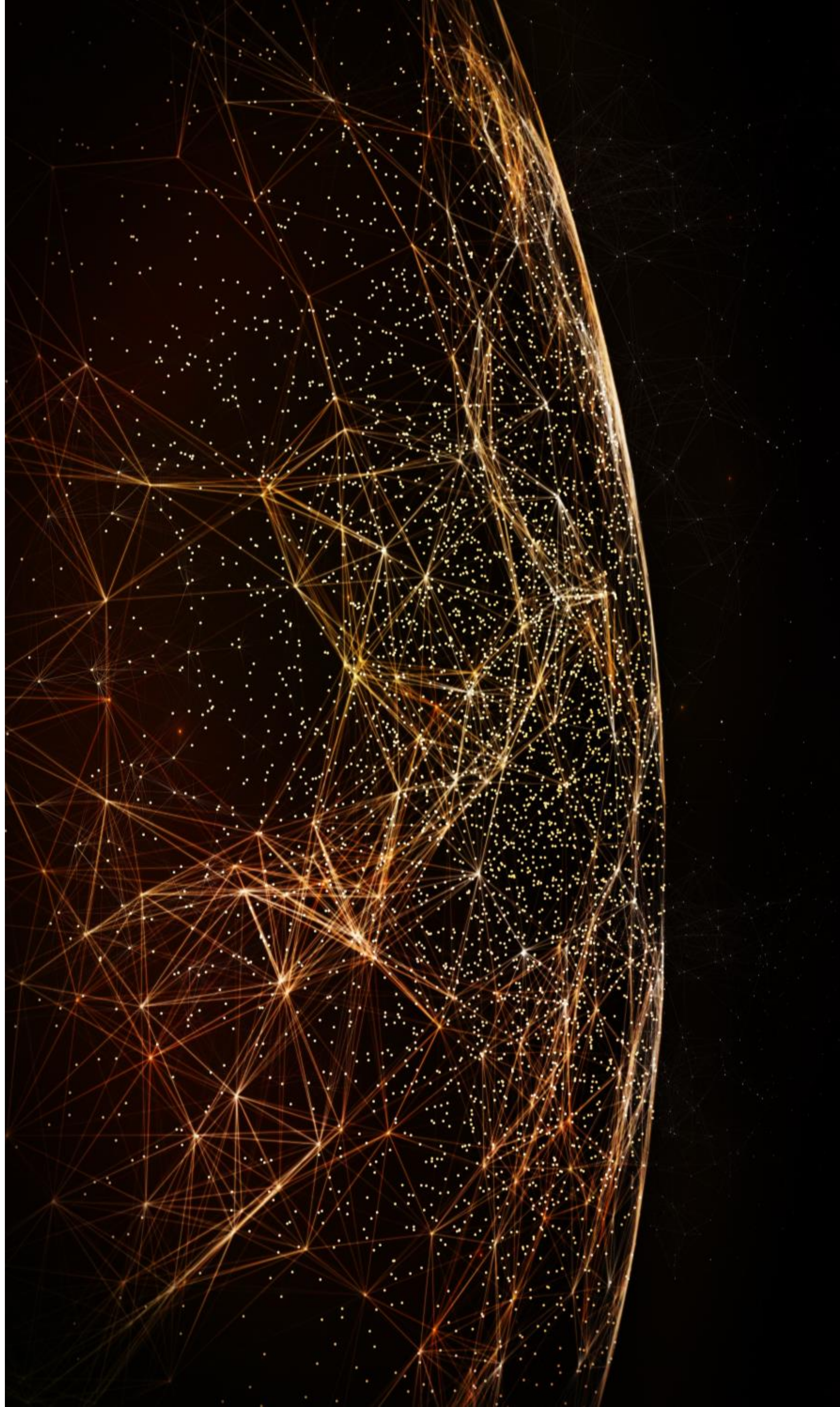
Securing SAP Web Dispatcher administation UI

Expose SAP Web Dispatcher administration UI only internally, never on the Internet

How to:

Profile parameter icm/HTTP/admin Subparameters:

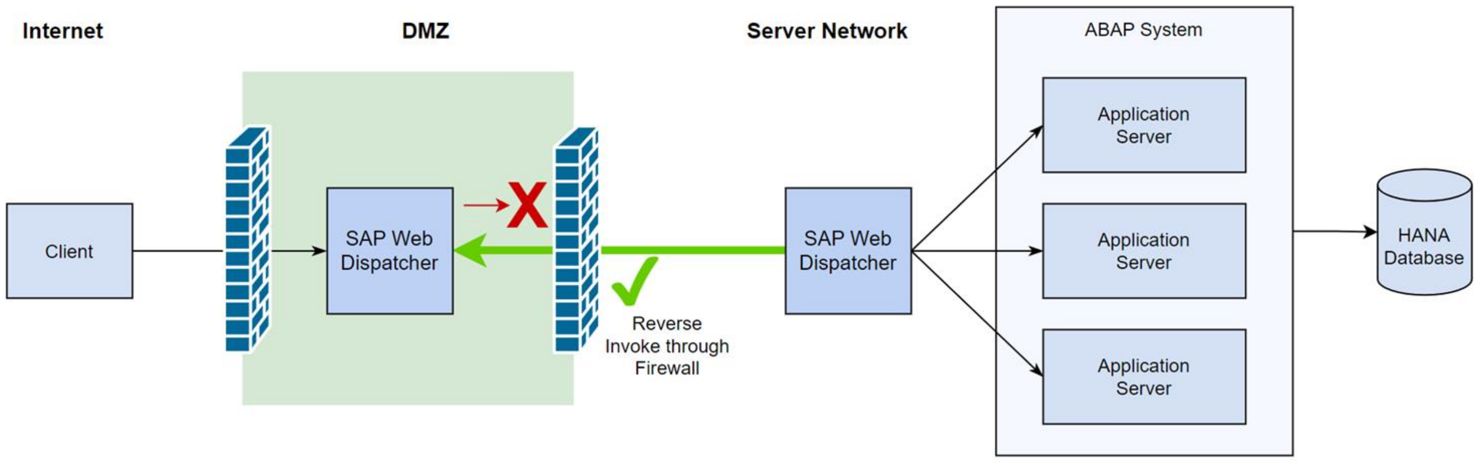
- PORT: Use a dedicated server port without access from the Internet
- STATEPORT: Default HTTPS port for health checks from the load balancer

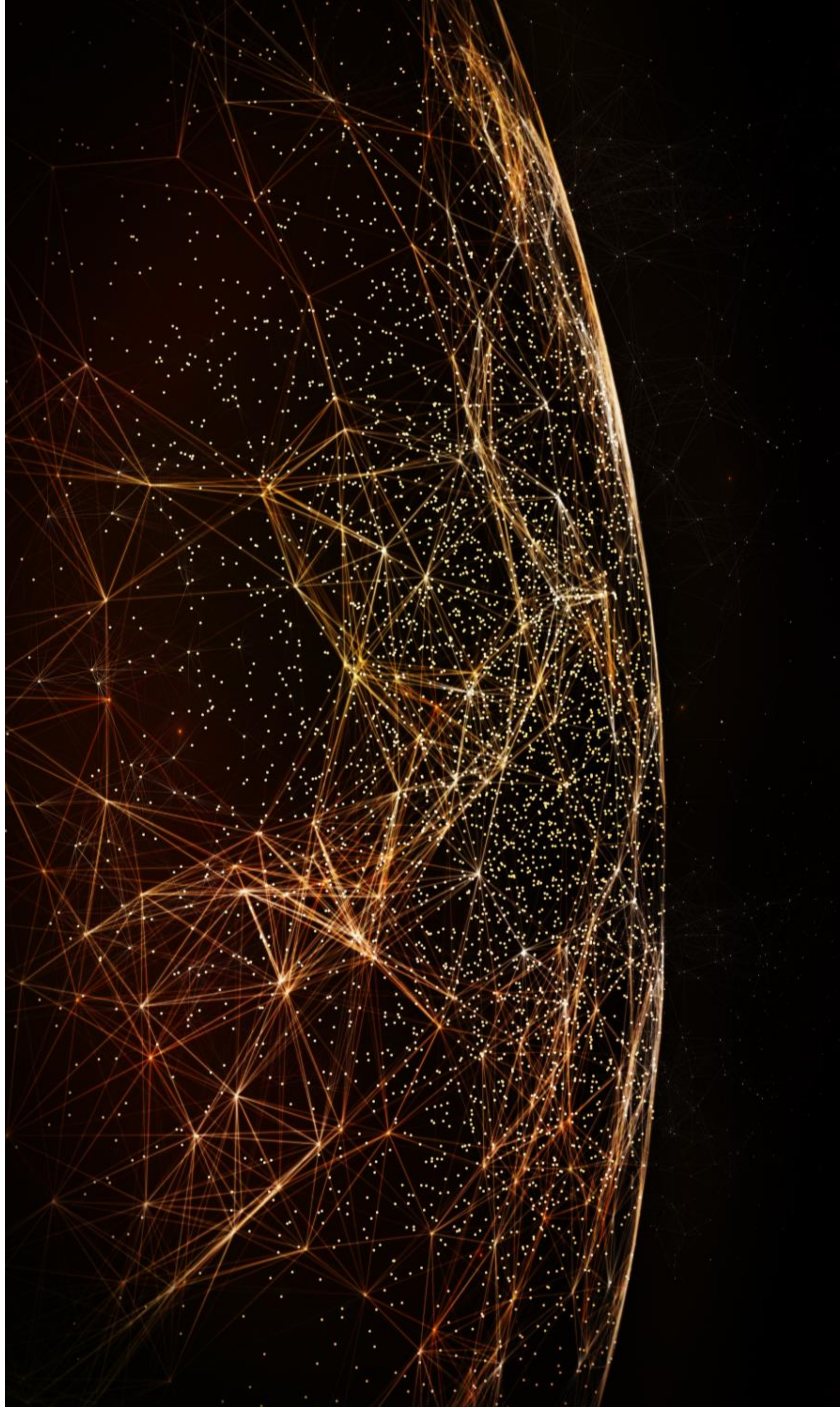


Prevent hacker attacks on your network

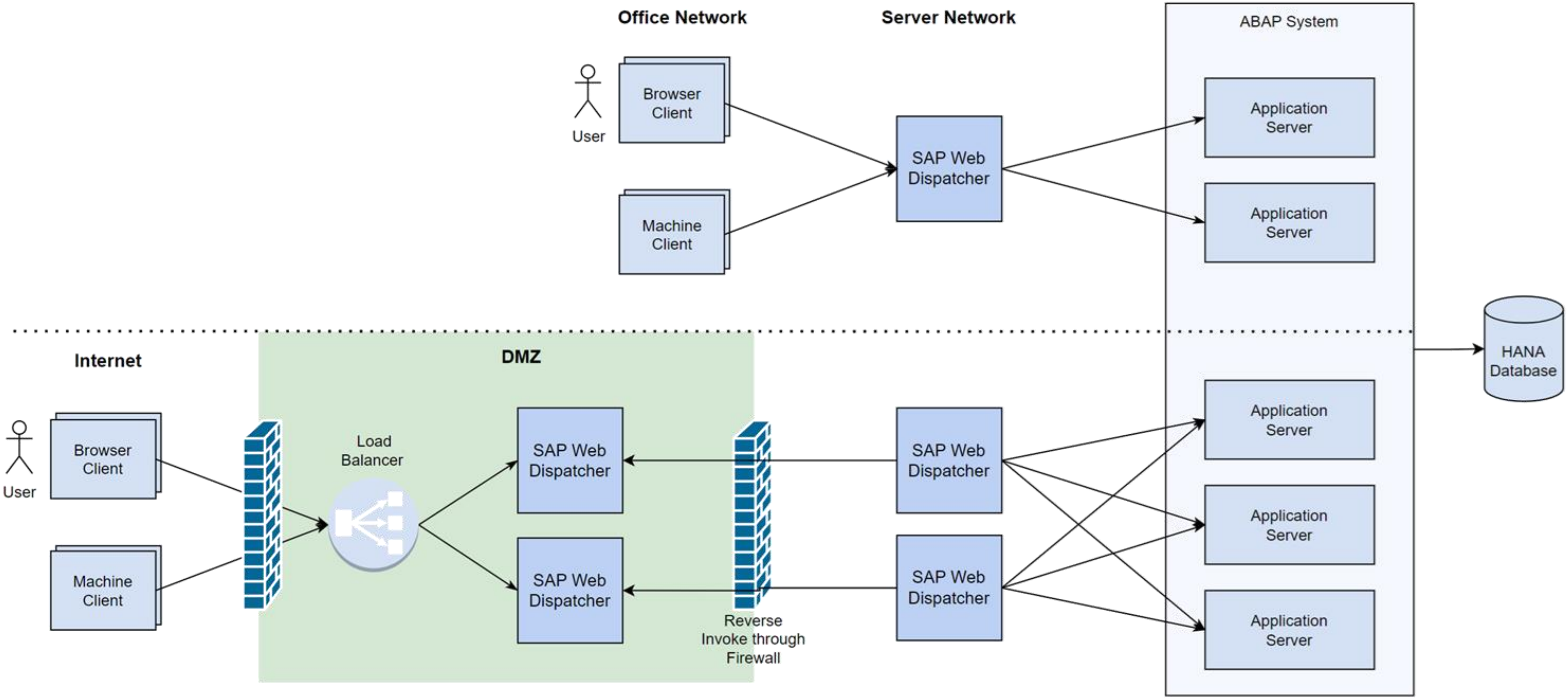
Potentially, SAP Web Dispatcher could be hacked and the attacker could gain access to the server network

Solution: Reverse invoke (*if you really need it*)





Full picture – With reverse invoke



Follow us

www.sap.com/contactsap

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

THE BEST RUN SAP