

No. 19

SAP NETWORK

# SAP Network and Web Security

Protecting SAP S/4HANA connections, protocols and web access, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 19

# SAP Network and Web Security

Protecting SAP S/4HANA connections, protocols and web access, explained for beginners

**oJAYo**
Published by oJAYo.com

FREE SAMPLE · ojayo.com

**SAP Network and Web Security**

Protecting SAP S/4HANA connections, protocols and web access, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. SAP, SAP S/4HANA, SAP Fiori, SAP Gateway, SAP BTP, SAP Build Work Zone and other SAP products mentioned are trademarks or registered trademarks of SAP SE in Germany and other countries. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by SAP SE or any other vendor named in this book.

The information in this book is provided for education. Product features change between releases; always confirm details in the official documentation for your release before changing a production system. Screens marked “Illustration” are simplified drawings, not captures of real SAP software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

# CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why network and web security matters for SAP 5

2 Components, ports and zones 8

PART II · PROTOCOLS

3 TLS and certificates 13

4 SNC for SAP GUI and RFC 17

5 RFC gateway and message server 21

PART III · WEB ACCESS

6 ICM and ICF services 26

7 Web Dispatcher and reverse proxies 30

8 Browser-side protections for Fiori 34

PART IV · EDGES AND OPERATIONS

9 SAProuter and remote support 39

10 Cloud connectivity 41

11 Host, management and database ports 44

12 Monitoring and continuous checks 46

13 Checklists and cases 49

Glossary 53

Further reading 55

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

# How to use this book

What this book covers, who it is for, and how to use it.

Roles and authorizations decide what a logged-on user may do. But before anyone logs on, data must travel across networks: from SAP GUI to the application server, from browsers to Fiori, from one SAP system to another, from the cloud into the data center. If those paths are open or unencrypted, attackers do not need a user at all.

This book explains, for beginners, **how to secure the network and web side of SAP S/4HANA**: ports and zones, encryption with TLS and SNC, the RFC gateway and message server, web access through ICM and Web Dispatcher, browser-side protections for Fiori, remote support, and cloud connectivity.

## Which SAP versions this book covers

The book is written for current releases:

- **SAP S/4HANA 2023 and 2025** on the current **ABAP platform** and kernel, on-premise and in **SAP S/4HANA Cloud Private Edition**;
- **SAP HANA 2.0** as the database;
- **SAP Business Technology Platform (BTP)** connectivity through the **SAP Cloud Connector**.

Some settings discussed here have existed for many years (gateway ACLs, message server ACLs); others reflect newer recommendations such as TLS 1.3 support and cloud-based certificate services for SAP GUI. Where a practice is outdated (for example unencrypted SAP GUI connections or TLS 1.0/1.1), the book says so.

FREE SAMPLE · ojayo.com

In **RISE with SAP** and Private Edition, SAP operates much of the infrastructure. The split of responsibilities is defined in your contract; customers usually remain responsible for application-level settings, connections to their own networks and users. Ask your SAP and hosting contacts which settings you can change.

## Who this book is for

- **Basis administrators** who maintain SAP systems.
- **Network and security engineers** who need to understand SAP protocols.
- **SAP security analysts** who want to go beyond roles.
- **Auditors** reviewing SAP technical security.

## How the book is organized

- **Part I — Foundations** (Chapters 1–2): why network security matters for SAP, and the SAP components, ports and zones.
- **Part II — Protocols** (Chapters 3–5): TLS and certificates, SNC for SAP GUI and RFC, and the RFC gateway and message server.
- **Part III — Web access** (Chapters 6–8): ICM and ICF services, Web Dispatcher and reverse proxies, and browser-side protections for Fiori.
- **Part IV — Edges and operations** (Chapters 9–13): SAProuter and remote support, cloud connectivity, host-level protection, monitoring, and checklists with cases.

## Conventions

**TIP**

Practical advice you can apply straight away.

**IN SAP**

Product-specific details, such as profile parameters and transactions.

FREE SAMPLE · ojayo.com

**WATCH OUT**

Common mistakes and risks.

**KEY IDEA**

The one thing to remember from a section.

## A note on screens and examples

Screens are **simplified illustrations**, not copies of SAP screens. Host names, ports and values are examples. Parameter values in this book illustrate concepts; always take exact recommended values from the current SAP Notes and security guides for your release, and test changes before production.

FREE SAMPLE · ojayo.com

PART I

# Foundations

Network security for SAP starts with knowing what talks to what. These chapters explain the risks and map the components, ports and zones.

FREE SAMPLE · ojayo.com

CHAPTER 1

# Why network and web security matters for SAP

Many serious SAP security incidents never touched a user's role. They came through the network.

## Attacks that bypass roles

Some of the most serious SAP vulnerabilities and attack techniques of the past decade share a feature: they work **before** or **without** a normal user logon. Examples of the patterns involved:

- **misconfigured RFC gateways** that let unknown programs register or start, allowing commands on the server;
- **open message server ports** that let an attacker pretend to be an application server;
- **unprotected management services** (such as the SAP start service) that reveal information or allow control actions;
- **web services exposed to the internet** without need, including test or administrative services;
- **unencrypted SAP GUI and RFC traffic** from which passwords and business data can be read on the network.

Public discussions of such issues (for example around SAP's gateway and message server security notes) led SAP to tighten defaults and to publish clear recommendations. Many older systems still run with the old settings.

FREE SAMPLE · ojayo.com

**KEY IDEA**

Authorization concepts assume that the network around them is controlled. If attackers can reach SAP's internal services directly, roles alone will not protect the system.

## What this book protects

- **Confidentiality**: business data and passwords on the wire.
- **Integrity**: data cannot be changed in transit; only trusted programs can connect.
- **Availability**: exposed services cannot be abused to stop systems.
- **Accountability**: connections can be traced to systems and users.

## Shared responsibility

Network security for SAP involves several teams:

| Team | Typical responsibility |
|---|---|
| Network | Firewalls, zones, VPNs, load balancers, WAF |
| Basis | Profile parameters, ICM, gateway, message server, certificates |
| Security | Standards, reviews, monitoring |
| Application | ICF services, OData services, RFC destinations |
| SAP / hosting provider | Infrastructure in RISE and Private Edition, per contract |

A common failure is that each team assumes another one has handled a topic. A shared checklist (Chapter 13) helps.

## Principles used in this book

1. **Know your interfaces**: list every port, protocol and connection your SAP systems use.

FREE SAMPLE · ojayo.com

2. **Encrypt everything** that crosses a network: TLS for HTTP, SNC for SAP GUI and RFC, TLS for database connections.
3. **Allow only what is needed**: firewall rules, gateway ACLs, message server ACLs, ICF services, Cloud Connector resources.
4. **Put an edge in front**: users and partners from outside reach SAP only through a reverse proxy or router in a controlled zone.
5. **Keep software current**: kernel, CommonCryptoLib, Web Dispatcher and SAProuter versions all carry security fixes.
6. **Monitor**: logs from ICM, gateway, Web Dispatcher and the security audit log show attacks and misconfigurations.

These principles match the **Zero Trust** ideas covered in another book of this series: never assume a connection is safe because it comes from "inside".

## Summary

- Many SAP attacks target network services, not roles.
- Network security protects confidentiality, integrity, availability and accountability.
- Several teams share responsibility; make it explicit.
- Know interfaces, encrypt, allow only what is needed, use an edge, patch, monitor.

FREE SAMPLE · ojayo.com

CHAPTER 2

# Components, ports and zones

An SAP S/4HANA system is not one program but a set of services, each listening on its own port. Knowing them is the first step to protecting them.

## The main components

An S/4HANA system on the ABAP platform consists of:

- **application server instances**, each with a **dispatcher** and work processes;
- the **ABAP central services (ASCS)** instance with the **message server** (which knows all application servers) and the **enqueue server** (locks);
- the **RFC gateway**, which handles remote function calls and external programs;
- the **Internet Communication Manager (ICM)**, which handles HTTP(S) traffic;
- the **SAP start service (sapstartsrv)** on each instance, used to start, stop and monitor;
- the **SAP HANA** database with its own ports;
- optional **Web Dispatcher** instances as reverse proxies, and **SAProuter** for remote connections.

FREE SAMPLE · ojayo.com

# The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

## SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
**SAP Network and Web Security (you are readin…**
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

## CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

# The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

## AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

## CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

## BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

# SAP Network and Web Security

Enjoyed it? The full book has 60 pages and 13 chapters.
Instant PDF download, $49.

**Get the full book**

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.