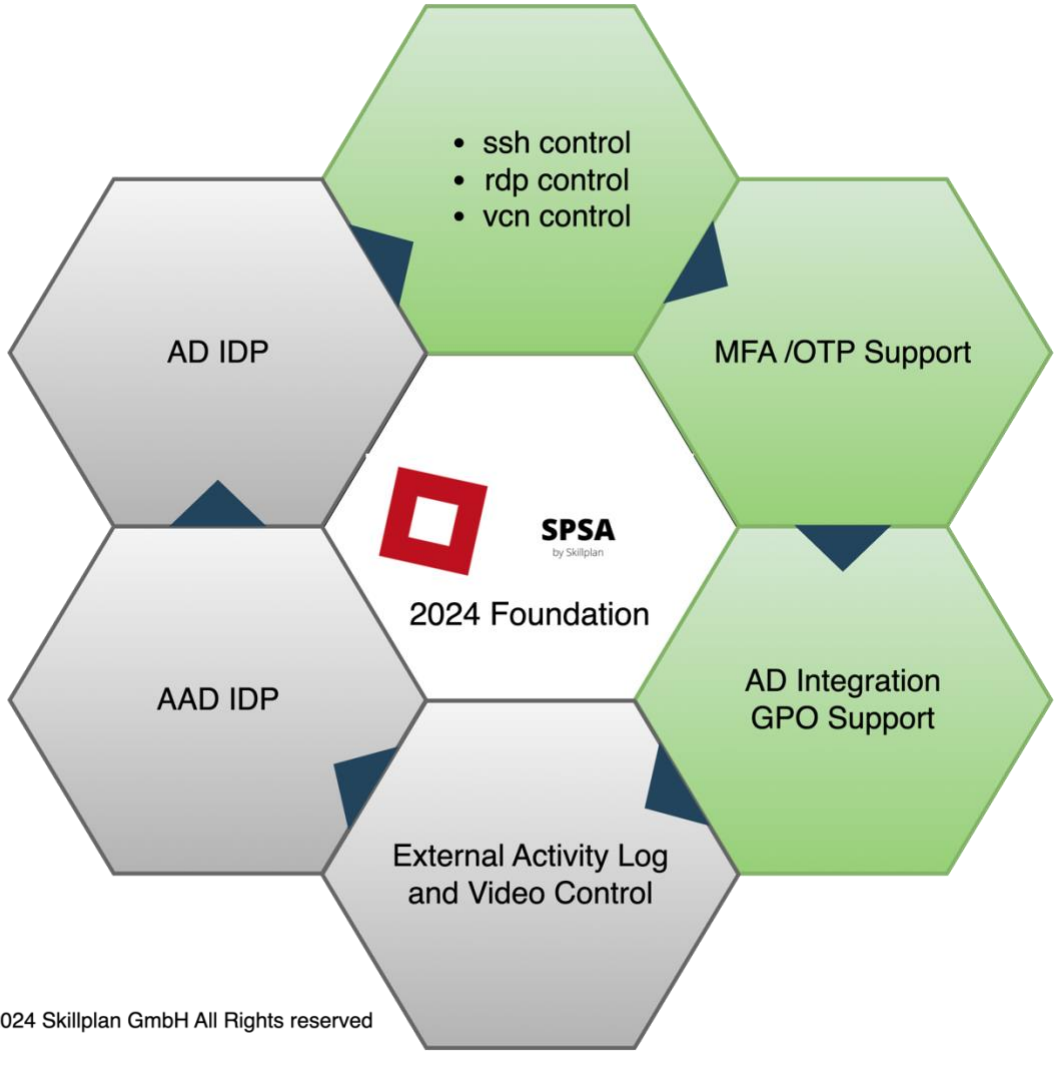
SPSA Foundation
Skillplan Secure Access

VERSION 02/2024

Overview

SPSA is the Zero Trust Access solution for RDP environments, SSH access and for isolating insecure legacy systems via RDP or VNC connections.



Fast implementation through **on-premises solutions "out of the box"**. SPSA can be installed quickly and cost-effectively as a **virtual appliance on VMware ESX-i** or as a **physical appliance** on a dedicated system. The Zero Trust solution is complemented by a **secure patch infrastructure** from Skillplan GmbH for **the appliance, operating system** and **SPSA**.

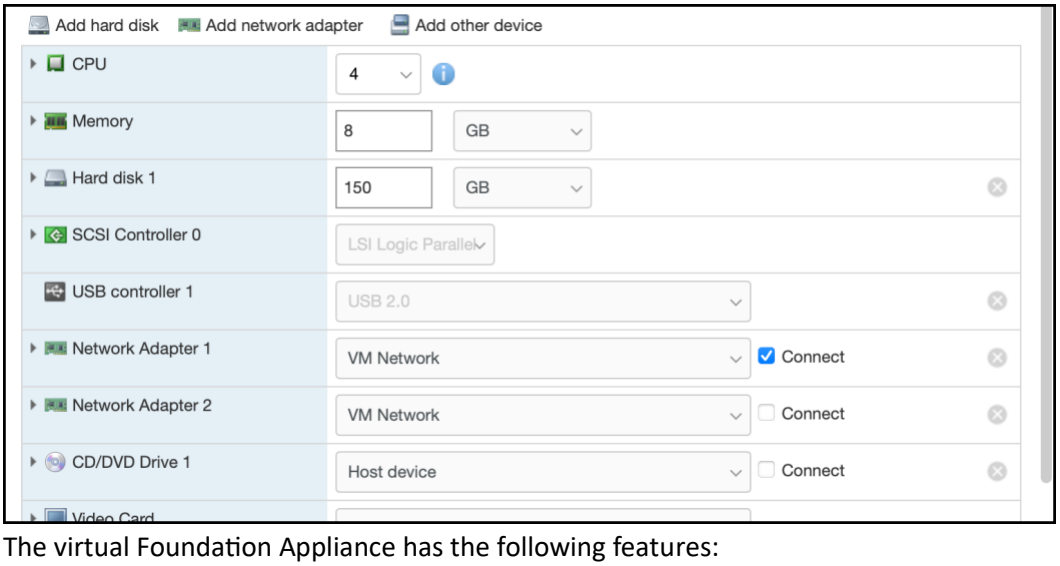
Physical appliance (currently available in Switzerland and the EU)

The Foundation Appliance has the following features:

- 4 Core CPU
- 32 GByte RAM
- 1 TB SSD
- 2 x NIC

The appliance supports up to 25 sessions simultaneously.

Virtual appliance for VMWARE from version 7.0



The virtual Foundation Appliance has the following features:

- 4 Core CPU
- 8 GByte RAM
- 150 GB storage
- 2 x NIC

The appliance supports up to 10 sessions simultaneously.

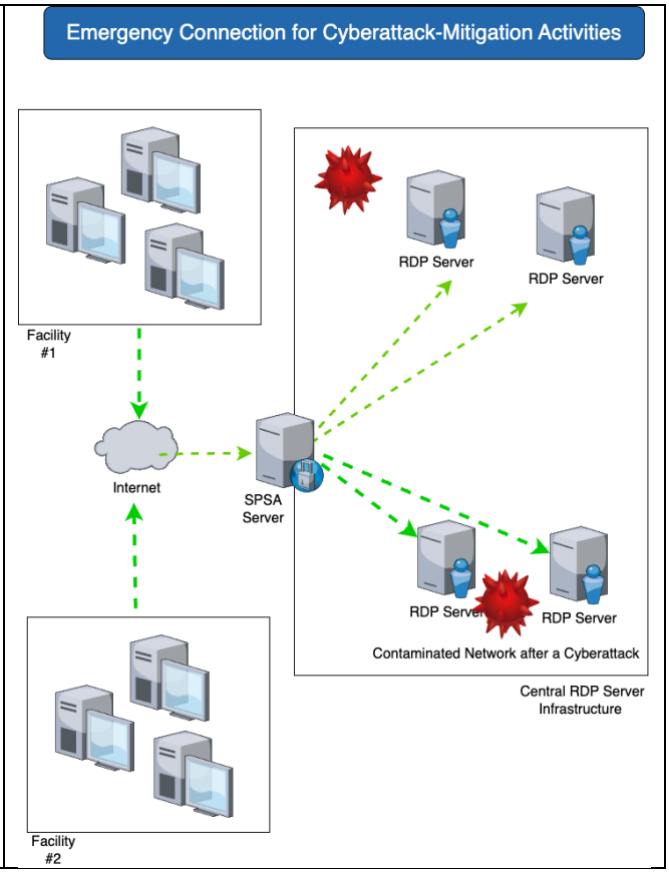
Abbreviation	Meaning
rdp	Remote Desktop Protocol for remote access to Windows systems
ssh	Secure shell for remote access to Linux/Unix systems, appliances and network components
SPSA Portal	User and administration portal of the SPSA environment
SPSA proxy	Proxy component for protocol conversion for SPSA

SPSA im Einsatz

Access to a compromised network after a cyberattack	
You need Secure access to compromised networks from a "secure" network. Access should be made possible so that production-relevant IT can be used again as soon as possible. Examples: production control or ERP systems.	

The solution with SPSA

SPSA enables access to production systems in contaminated networks without jeopardizing the ongoing rebuilding of the company's IT infrastructure.



Secure access to legacy systems

You need

The operation of isolated legacy systems, even with known zero-day gaps, without exposing these systems.

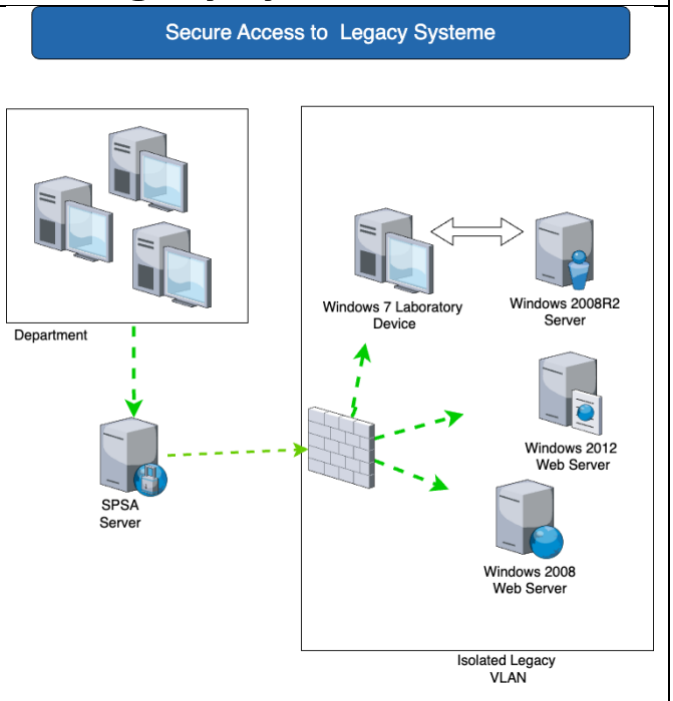
Risk minimization in the event of unrecoverable security gaps.

The solution with SPSA

Systems that can no longer be patched and systems with known security vulnerabilities can be isolated from the rest of the network and still be accessed without exposing the entire network.

Functions such as cut & paste or file transfer can be controlled granularly on a system and user basis, right down to pure display sharing without access to the system.

Examples are RDP connections to Windows Server 2008 applications or Windows 7 applications, which cannot yet be replaced.



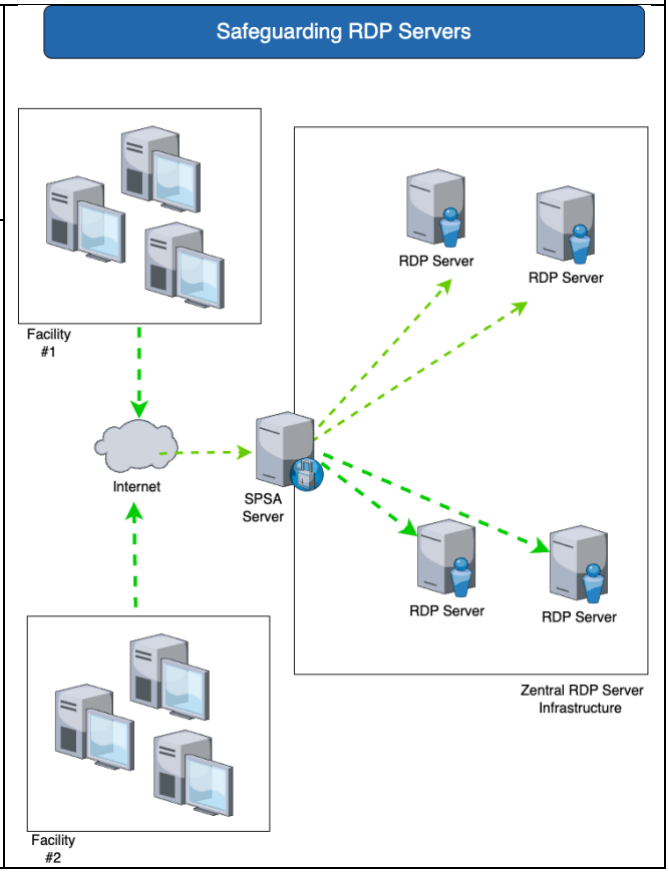
Securing RDP servers

You need

The existing RDP installations are to be secured in order to minimize the risk from the exploitation of RDP servers in the network.

The solution with SPSA

SPSA prevents lateral movement through a central access portal for server access via RDP. This enables SPSA to provide secure access to RDP servers for both internal and external access.



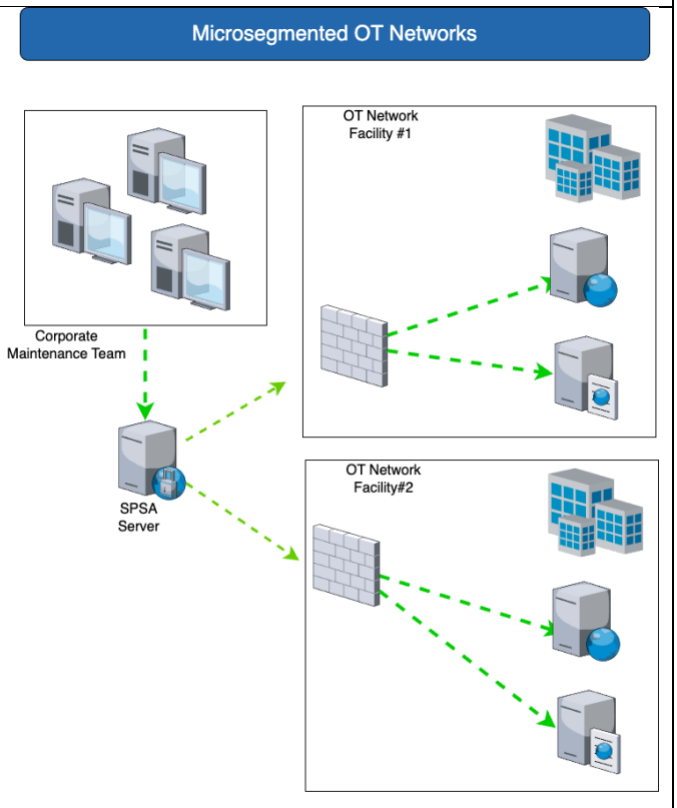
Access to segmented OT networks

You need

Secure access during segmentation of production networks, laboratory networks and OT networks should be made possible from office networks (without removing the segmentation).

The solution with SPSA

If OT and IT networks are to be operated separately (micro-segmentation), the use of SPA enables secure access from the IT network to systems in OT networks via a central access portal.



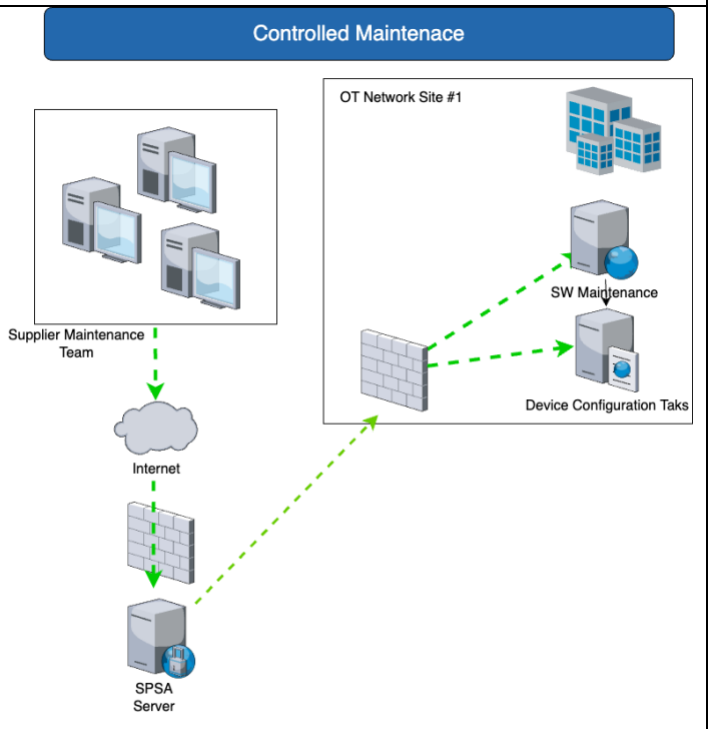
Controlled remote maintenance

You need

For maintenance purposes, support technicians must be able to access internal systems via the Internet. RDP, ssh or Telnet connections are used for this. Individual employees of acquired companies should be able to access selected systems quickly via the Internet in order to speed up the integration process

The solution with SPSA

Enables time-controlled access by suppliers to systems for maintenance purposes without installation of additional software at the suppliers for access via ssh, RDP and VNC. SPSA enables Managed Remote Maintenance Gateway for supplier access to server systems or for employees of companies that are not connected to the company network.



Central administration instance for the administration of MS servers

You need

As part of securing the Active Directory and business-critical applications based on MS Windows, the administration is to be centralized and secured.

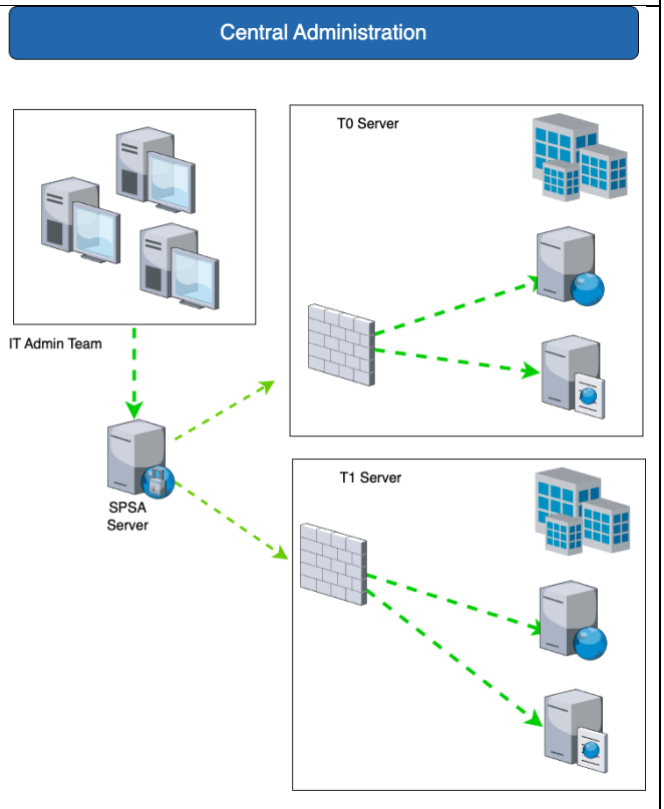
Furthermore, active directories, which are secured according to the MS Tiering model, are to be additionally secured by central administration portals.

The solution with SPSA

To secure administrative connections in the management of Tier 0, Tier 1 and Tier 2 systems when introducing the Microsoft tiering model (central provision of the PAW infrastructure).

SPSA enables the centralized management of administrative access to critical infrastructure components. This can be combined with the MS tiering model.

In addition, SPA enables centralized logging of privileged access to critical infrastructure servers via RDP or ssh.



SPSA features

Secure & proven software

based on Apache Guacamole™

- A secure system with Lowest Privileged Access
- A secure update and patching infrastructure that keeps your compliance up-to-date
- Simple admin interfaces for managing the appliance
- Integrated option to create and store backups of critical data
- Integrated performance monitoring with the option of uploading the monitoring data to Skillplan GmbH for evaluation
- Support for RDP, SSH, telnet and VNC connections
- Integrated user database with MFA support for standard authentication apps such as Microsoft or Google Authenticator
- The option to limit user logins in terms of time
- Active Directory Single Sign on (Pro Version)
- Azure Active Directory (SAML) Single Sign on
  with integration of Conditional Access (Pro version)
- Portal with up to 4 separate SPSA proxies at up to four locations (Pro version
- Recording and replay of RDP and SSH sessions via video recording (Pro version)

SPSA Next Steps

Would you like an SPSA demo?
Then please contact sales@skill-plan.com to arrange a demo appointment.

Would you like to try out SPSA during a 30-day trial?
Then please contact sales@skill-plan.com to register for a trial

Do you have further questions and need individual answers?

Describe your questions to sales@skill-plan.com so that we can find and arrange an appointment via Teams or Zoom.