CRIS
Cybersécurité Réseaux Infrastructure Système

wallix

WALLIX PAM: PROOF OF CONCEPT PREREQUISITE GUIDE

Release date: March 2025

WALLIX Bastion 12.0.9

WALLIX Access Manager 5.1.2

WALLIX
250 bis rue du Faubourg Saint-Honoré 75008 Paris
Tel : +33 1 53 42 12 90 / Fax : +33 1 43 87 66 38
SARL au capital de 50 000 Euros – RCS PARIS B 450 401 153 – FR67 450 401 153

Contents

1. Copyright & Licenses 3
2. Scope of Work 3
   2.1. Objective 3
   2.2. Deliverables 3
   2.3. Technical requirements guideline 4
      2.3.1. System guideline 4
      2.3.2. Network flows guideline 5
3. WALLIX PAM Suite deployment 7
   3.1. WALLIX Bastion 7
      3.1.1. Material 7
      3.1.2. Requirements 7
   3.2. WALLIX Access Manager 7
      3.2.1. Material 7
      3.2.2. Requirements 8
   3.3. Jump Server, Windows RDS 8
      3.3.1. Material 8
      3.3.2. Requirement 8
      3.3.3. Further information on RDS configuration: 8

1. Copyright & Licenses

This guide does not supersede or replace any of the legal documentation covering WALLIX products including the WALLIX Bastion, the WALLIX Access Manager, the WALLIX Bastion Discovery or the WALLIX Bastion AAPM use rights. Specific product license terms are defined in the End User License Agreement (EULA). This POC guide is not a legal use rights document.

The information is subject to change without notice. The information in this publication is provided as is. WALLIX makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any WALLIX software described in this publication requires an applicable software license.

As part of an effort to improve its product line, WALLIX periodically releases revisions of its software. Therefore, some features described in this document might not be supported by all versions of the software currently in use. The product release notes provide the most up-to-date information on product features. Contact your WALLIX technical support if a product does not function properly or does not function as described in this document.

2. Scope of Work

2.1. Objective

The Proof of Concept will let you have a hands-on experience with WALLIX PAM solution: WALLIX Bastion and WALLIX Access Manager. The PoC will demonstrate how the WALLIX solutions can integrate smoothly within your existing infrastructure and shows added benefits of privileged access management to secure your environment.

Before starting the PoC workshop, several prerequisites must be validated to have an environment PoC ready and for the PoC team to be able to demonstrate efficiently how the WALLIX suite addresses your key concerns.

This document details those pre-requisites and guides you through the necessary procedures to have an environment “PoC ready”.

2.2. Deliverables

The following elements must be set up and validated 72 hours before the POC workshop to ensure its smooth execution:

- **Install and configure a WALLIX Bastion virtual appliance** (VMware, Hyper-V, etc.).
- **If necessary, install and configure a WALLIX Access Manager virtual appliance** (VMware, Hyper-V, ...). The Access Manager must be reachable through the appropriate

URL. **Ensure WebSocket communications are enabled to the WALLIX Access Manager.**

- **Compile a list of local WALLIX Bastion users** (primary users) along with their passwords. Users can alternatively be sourced from a source of identity (AD/LDAP/SAML) if relevant.
- If user accounts are provisioned from a source of identity, **ensure that both the WALLIX Bastion and the WALLIX Access Manager can connect to the source of identity.** Prepare any required information for integrating with AD/LDAP/SAML if needed for the POC.
- **Create a list of target accounts** (secondary users) and their passwords. Confirm that these users can access the relevant targets.
- **Define roles and permissions**, specifying the correlation between primary and secondary users to determine access levels.

- If applicable, **deploy up to 2 applications** to be used as RemoteApp on the Microsoft RDS server.
- **Configure network flows** according to the "Network Flows Guideline" provided below.

2.3. Technical requirements guideline

2.3.1. System guideline

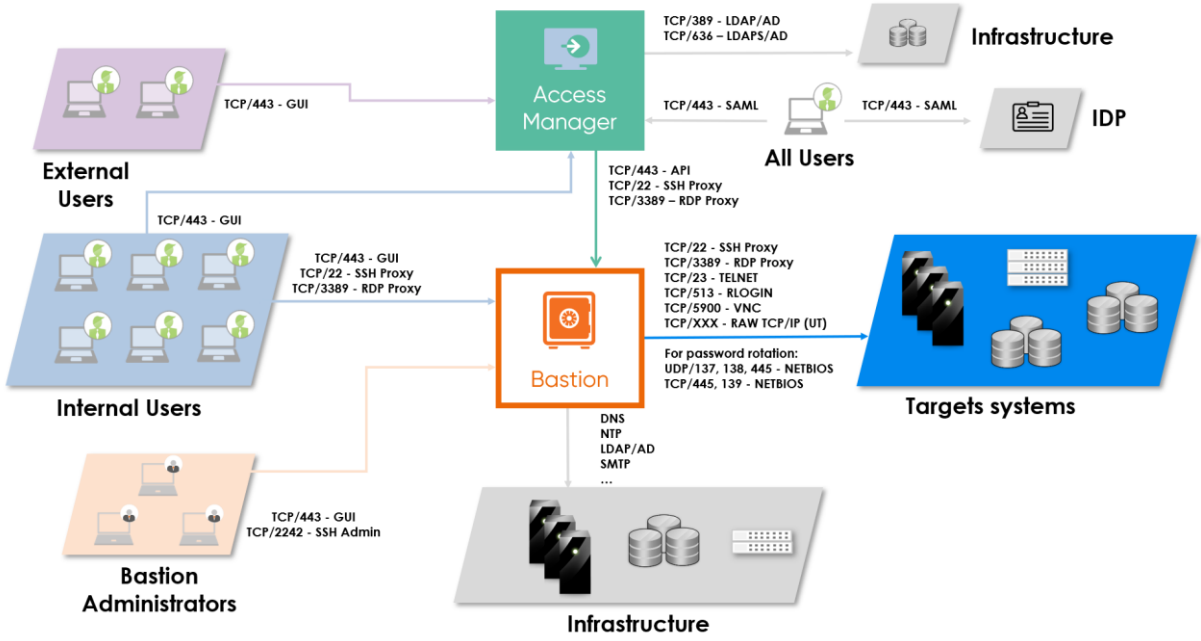
A typical PoC environment includes:

- WALLIX PAM solution related resources:
  - **A WALLIX Bastion virtual machine** (mandatory)
  - **An WALLIX Access Manager virtual machine** (necessary only for secure remote access and/or full access to privileged resources through a web browser).
  - **An RDS Windows server** (required solely for privileged access to standalone applications).
- The resources to be tested, e.g.:
  - A Windows system with RDP enabled,
  - A Unix, Network, or other system with SSH enabled,
  - Applications (e.g., MMC console, SQL clients, web application)
  - OT/IoT targets
  - ...

Section 3 provides the necessary links to deploy and set up the Bastion appliance.

2.3.2. Network flows guideline

The following network flows should be authorized for the POC:



2.3.2.1. Users access

The following ports are necessary for the users to reach the Bastion and Access Manager:

- Internal Users access to the WALLIX Bastion:

Service	Port	Use
SSH	22	SSH Proxy to the targets
RDP	3389	RDP Proxy to the targets
HTTPS	443	WEB Interface (GUI)

- Admin access to the WALLIX Bastion:

Service	Port	Use
HTTPS	443	WEB Interface (GUI)
SSH	2242	For admin access through SSH

- Admin access to the WALLIX Access Manager:

Service	Port	Use
HTTPS	443	WEB Interface (GUI)
SSH	2242	For admin access through SSH

- External Users access to the WALLIX Access Manager:

Service	Port	Use

HTTPS	443	WEB Interface (GUI) with WebSocket

2.3.2.2. Access from the WALLIX Bastion to critical assets*:

Service	Port	Use
SSH / SFTP / TELNET / RLOGIN	22	Access from the Bastion proxy to the target
TELNET	23	Access from the Bastion proxy to the target
RLOGIN	513	Access from the Bastion proxy to the target
RDP	3389	Access from the Bastion proxy to the target
VNC	5900	Access from the Bastion proxy to the target
RAW TCP/IP (UT)	502, 102, 3306, ...	Access from the Bastion proxy to the target
SMB NETBIOS	137, 138, 139, 445	For password rotation

* Port listed in the tabs depends on the actual implementation.

2.3.2.3. From the WALLIX Bastion to the infrastructure:

Service	Port	Use
SMTP / SMTPS / SMTP + STARTTLS	25 / 465 587	Email (notifications/alerts)
NTP	123	Time synchronization
DNS	53	Name resolution
KERBEROS	88	Authentication
LDAP / LDAPS	389 / 636	Authentication
RADIUS / TACACS+	1812 / 49	Authentication
NFS / CIFS	2049 / 445	Remote storage
SYSLOG	514	For SYSLOG communication (SIEM)
SNMP	182	SNMP polling

2.3.2.4. From the WALLIX Access Manager to the WALLIX Bastion:

Service	Port	Use
SSH	22	To connect to the Bastion's SSH proxy
RDP	3389	To connect to the Bastion's RDP proxy
HTTPS	443	Bastion API connection

2.3.2.5. From the WALLIX Access Manager to the infrastructure:

Service	Port	Use
LDAP(S) / AD	389 / 636	Authentication
DNS	53	Name resolution
NTP	123	Time synchronization

3. WALLIX PAM Suite deployment

This section provides links and references to install and set up the POC environment.

3.1. WALLIX Bastion

The WALLIX Bastion provides secure access to critical resources. The deployment of the Bastion is straightforward and can be completed in a short time frame.

3.1.1. Material

Images and documentation to deploy and set up the Bastion can be found at

Bastion repository

A video showing the deployment's first configuration is available at

Bastion setup first steps video

3.1.2. Requirements

A minimum of 4 vCPU / 8GB RAM / 70 GB HDD is recommended for a POC environment (production environment recommendations may vary).

3.2. WALLIX Access Manager

The WALLIX Access Manager provides remote VPN-less and/or internal secure access to privileged users through a simple HTLM5 web interface, requiring only a web browser on the privileged users' workstation.

3.2.1. Material

Images and documentation to deploy and set up the Bastion can be found at

WALLIX Access Manager repository

A video showing the deployment's first configuration is available at

WALLIX Access Manager setup first steps video

3.2.2. Requirements

A minimum of 2 vCPU / 4GB RAM / 50 GB HDD is recommended for a POC environment (production environment recommendations may vary)

3.3. Jump Server, Windows RDS

An RDS server is required to provide secure access to standalone applications. Applications such as fat clients (MMC consoles, SQL clients) and web applications are to be deployed on the RDS server to be used as a Microsoft "RemoteApp" through the WALLIX PAM solution.

3.3.1. Material

To get more information on the deployment of Jump Servers and RDS farms, please consult the following link:

https://www.veeam.com/blog/deploy-remote-desktop-services-2019.html

https://rdr-it.com/en/deploy-rds-farm-windows-2012r2-2016-2019/

3.3.2. Requirement

The RDS server must be integrated in the AD domain. Access rights with a Domain admin account must be available and NLA activated. The Jump Server requires a dedicated Windows VM (2019) with 4vCPU, 8GB RAM, 70 GB HDD as a minimum recommended for a POC testing.

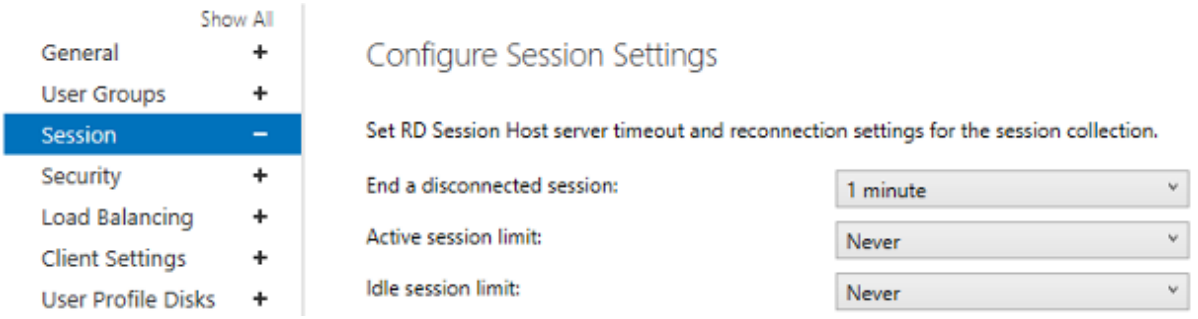
3.3.3. Further information on RDS configuration:

3.3.3.1. Several sessions with same account

Local / Group Policy Editor > Computer > Administrative Templates > Windows components > Remote Desktop Session Host > Restrict Remote Desktop Services users to a single Remote Desktop Services session: Disabled

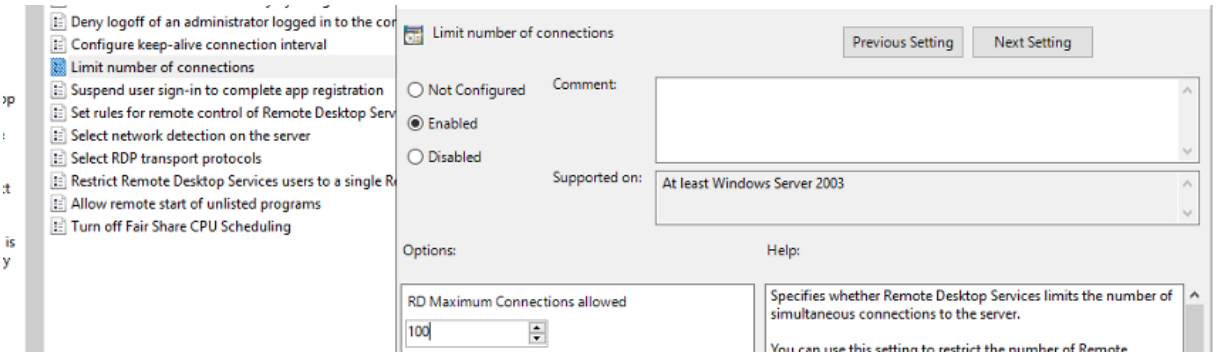
3.3.3.2. Session auto-Kill after 1min if not closed properly

Server Manager > Remote Desktop Services > Collections QuickSessionCollection > Properties / TASKS / Edit Properties > Session > End a disconnected session: 1 minute



3.3.3.3. Increase maximum connections allowed

Local / Group Policy Editor > Computer > Administrative Templates > Windows components > Remote Desktop Session Host > Limit number of connections: Enabled



Highly recommended :

For each Bastion project, it's highly recommended to use Multi-Factor Authentication.

Wallix recommends to use their IDaaS Solution .

Ask for a free trial (30 days) here

CRIS

Cybersécurité Réseaux Infrastructure Système

about WALLIX

WALLIX protects identities and access to IT infrastructure, applications, and data. Specializing in Privileged Access Management, WALLIX solutions ensure compliance with the latest IT security standards and protect against cyber-attacks, theft and data leaks linked to stolen credentials and elevated privileges.

www.wallix.com

wallix