CLASSIC WALLIX BASTION ARCHITECTURE OT ENVIRONEMENT

Customer Success – Customer Support

TECHDOC360

Classification : Public

WALLIX
250 bis rue du Faubourg Saint-Honoré 75008 Paris
Tél : +331 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

FOLLOW-UP SHEET

Visa

	Name	Function	Date	Visa
Writer	Ihssen TRABELSI	Professional Services Manager	March 2023	ITR
Checker	Yoann DELOMIER	Business Strategy Leader for OT	March 2023	YDE
Approver	Grégory HAIK	Consulting director	April 2023	GHA

Review

Version	Nature	Author	Date
1.0	Creation	Ihssen TRABELSI	April 2023
1.1	Update	Ihssen TRABELSI	May 2023
1.2	Update	Ihssen TRABELSI	June 2023

TABLE OF CONTENTS

I. INTRODUCTION

I.1 OBJECT

The main objective of this document is to describe classic WALLIX Bastion Architectures in an OT environment.

I.2 COPYRIGHT NOTICE

II. MAIN ELEMENTS IN AN OT ARCHITECTURE

II.1 PAM4OT ACCESS MANAGER (AM)

The PAM4OT Access Manager is a blackbox HW/VM/Cloud appliance used primarily by external users to remove the need of VPN. It is also often used by internal users. It provides the following benefits:

- HTML5 graphical Interface with enhanced capabilities: folders, tags, drag& drop, session invite, …
- Centralized capabilities for: to access all targets, approvals, auditing, multi-criteria audit search, videos, logs, checking/checkouts...
- Security: no VPN, one single https port, out-of-the box hardening, protocol isolation…
- Inter-operabilities: MFA, AD, AAD…
- Multitenancy with dedicated or centralized organizations

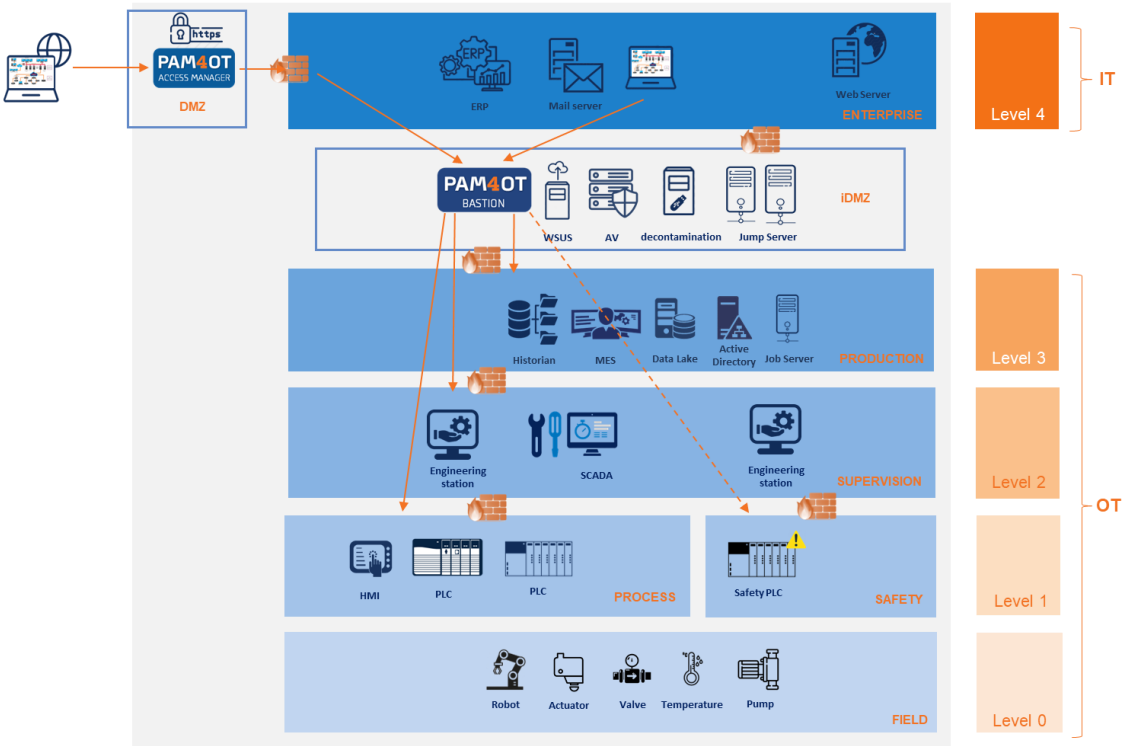
The AM is often located in a DMZ/datacenter and in some cases located within the plants in the iDMZ.

II.2 PAM4OT BASTION

The PAM4OT Bastion is a blackbox VM/Cloud appliance that provides capabilities such as:

- PAM features: RDP/OT/SSH/SFTP… access, Role Based Access Control, Least privileges, Local/vpn user&admin HTML GUI, unknown/unshared Passwords, local Audits, Recording, metadata, Application access only, check-in/checkout, Automatic password rotation, discovery.
- Security: Front-End hardening, No lateral movement, Approvals, Alerts, emails, Protocol breaks, Sub-protocol restriction, AV/DLP…
- Inter-operabilities: AD, AAD, MFA, AV/DLP with ICAP.

This appliance can be located centrally or distributed in plants at the Purdue level 3.5.



II.3 OTHER COMMUN ELEMENTS

Some other elements can also be seen in OT architectures such as:

- MFA (SAML/Radius...) to ensure the user identity: Azure, AWS, Trustelem, DUO, okta, RSA…
- Active directory, LDAP or AAD to centralize/simplify the user management
- AV/DLP to check the files during a file transfer
- SIEM or syslog server: to perform analysis, search or reports
- OT Discovery tools
- Others

III. MAIN OT ARCHITECTURE OPTIONS

Please find below a quick description of main options that can be implemented in an OT architecture.

III.1 APPROVAL WORKFLOW

WALLIX Bastion supports dynamic authorizations using workflows. This mechanism is based on defined timeouts for accessing targets or target credentials. Workflows allow administrators to further refine access to sensitive resources and/or allow access outside of defined time frames. When a user wants to initiate a connection to a target or access the target's credentials, a request is first sent to the approvers.

An approver is a user who has been designated by a WALLIX Bastion administrator with the right to manage approvals.

Approvers can choose to allow or deny connecting to a target or accessing the target's credentials. A request is approved when a quorum is reached. Quorum is the minimum number of favourable responses required for a particular authorization.

In the context of OT architectures, it is possible to activate the approval workflow on some (all) targets. the user's approval request and the approval of the approver's request can be done from the Access Manager or Bastion.

III.2 HIGH-AVAILABILITY REPLICATION MASTER/MASTER

Bastions as well as Access Managers can be clustered HA Replication Master/Master.

Master/Master mode allows replication in both directions. Any changes on one Stronghold will be replicated to the other.

In order to secure the communication between the MySQL databases, a SSH tunnel with

port forwarding is established between the Bastions. This tunnel is managed by the autossh service that keeps the tunnel permanently running. The port forwarding allows the databases to communicate without having to open a remote access to the MySQL database.

With this type of replication mode (Master / Master), the solution is limited to 2 Bastions max.

III.3 REMOTE STORAGE

In the architectures presented in the following chapter, the Bastions are connected to a remote storage (shared between the two Bastions).

Remote storage allows session video recordings to be exported to a remote file system by defining the connection to an SMB/CIFS, NFS, or Amazon EFS server.

It is then possible to externalize the automatic Backups which are generated by the Bastion every day on the remote storage (Example at 6:50 p.m.)

Note:

WALLIX Bastion moves automatically the recordings of recently terminated sessions from local storage to remote storage.

When remote storage is enabled but the file server is temporarily unavailable, the various features of WALLIX Bastion can still be accessed. The session recordings are nonetheless kept on local storage during server unavailability.

III.4 CONNECTIONS TO WEB CONSOLES AND/OR WINDOWS APPLICATIONS

As part of an IT/OT infrastructure, it is possible to connect to Web applications or heavy windows clients. To be able to run a session from the Bastion or the Access Manager on these applications, you must provide an RDS server (minimum required 2012 R2) with the RDS role installed on it and the published cmd. you also need to install a web browser (chrome).

III.5 PASSWORD ROTATION

WALLIX Bastion contains a module that allows to manage the rotation and complexity of passwords for secondary accounts (target accounts) and thus regain access governance.

The Password manager module applies to secondary accounts stored in the Bastion vault, the accounts can be AD accounts or local accounts of the target servers.

It is also possible to rotate SSH keys for Linux servers and many other types of targets.

In order to activate the password change module, you must define a password policy which must be greater than or equal to that defined on the target equipment (Target Servers or AD).

Password change can be set in two ways.

- ✓ With a frequency to be defined in the password change policy.
- ✓ When connecting or checking in a secondary account.

III.6 CONNECTIONS TO ICAP DLP/AV SERVERS

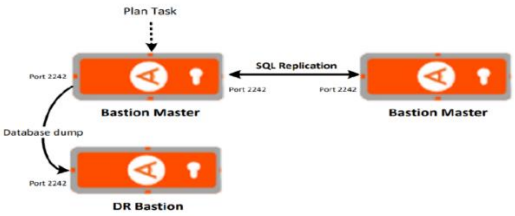
As part of an implementation of an OT architecture with the WALLIX Bastion and Access Manager solutions, it is possible to interface the Bastion with ICAP servers.

Connections to ICAP servers provided by anti-virus software or DLP (Data Loss Prevention) solutions can be configured to verify the validity of files transferred during RDP and SSH sessions.

Files that can be checked are those transferred via the SFTP and SCP subprotocols (SFTP_SESSION, SSH_SCP_UP and SSH_SCP_DOWN) during an SSH session and from the copy/paste function via the clipboard (RDP_CLIPBOARD_FILE) during an RDP session.

III.7 DISASTER RECOVERY (DR)

The principle of disaster recovery is to have a backup site if the main site goes down.
the diagram below shows the mechanism for updating the Bastion DR.



• Bastion in production: The production bastion is the one that is currently in use.

• Bastion DR: The DR bastion is the bastion that is not used. It is there to ensure the continuity of the service in case the production bastion would be unavailable.

The DR Bastion update is not in real time. Still, update frequency can be done once a day or more.

III.8 LOAD-BALANCER

A load balancer is positioned in front of the Access Managers. it then manages user connections from a single URL and load-balance the traffic between the two AMs.

Below the prerequisites of the LOAD BALANCER in front of the ACCESS MANAGER:

- The listening port of the virtual server or the VIP
- 443 assuming all users log into the web interface.
- Upgrade an HTTPS connection to a WebSocket.
- The type of persistence: By cookie if uses HTTPS.
- Redirect all HTTP traffic to HTTPS.
- Activate the X-Forwarded-For option to transmit the user's IP address to Access Manager.

III.9 ARCHITECTURES

The following chapters describe three OT architectures that are:

- Centralized Architecture: AM and Bastion in HA centralized.
- Hybrid architecture: AM centralized and Bastion distributed.
- Distributed Architecture: Both AM and Bastion are distributed.

Theses Architectures introduce generic situations, please do not hesitate to contact your WALLIX interface for a custom design.

IV. CENTRALIZED ARCHITECTURE

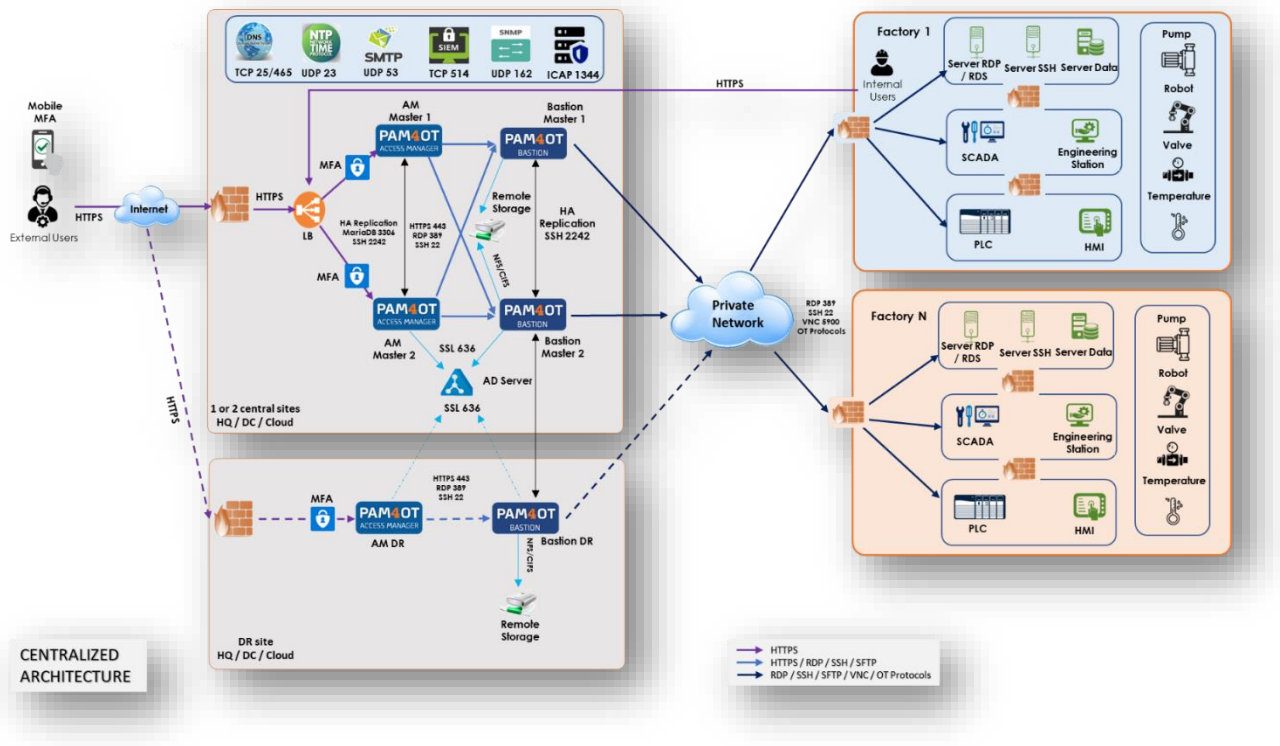
IV.1 WHEN DOES IT APPLY?

This architecture can be applied in both cloud and on-prem contexts. Access to the different sites is done in a centralized way, from a central site (on-prem or cloud) to the resources (servers, SCADA, PLC...), that are located in the factory.

An additional DR site can optionally be considered.

This is a simple setup for a small to medium perimeters.

IV.2 ARCHITECTURE



IV.3 FEATURES

The architecture presented above is centralized.

Users willing to connect to targets connect to the central Access Manager cluster with multi-factor authentication (MFA).

Target servers, PLC, SCADA are in remote factories. Connections between the centralized site and the factories can be made through a private network (WAN, SD-WAN, IPsec, VPN tunnel ...)

Two Access Managers are positioned in front of two Bastions: the Access Managers serve as load balancers between the Bastions.

The High Availability is activated both on the Access Managers and the Bastions.

HA replication for Bastions is configured in Master/Master mode, this means that the functional configuration (users and user groups, devices, device groups and authorizations...) is replicated among instances. This allows active/active mode (configuration and traffic).

Incoming RDP and SSH, RAW TCP connections are possible on the two Bastions nodes from the Access Manager.

Note that primary authentication on the Bastions or the Access Managers can be done via an AD or with accounts local to the Bastions.

In this architecture, the Bastions bring together all the resources of all the factories.

For disaster recovery (DR), a Bastion instance located in a third site can be added. This DR Bastion is in standby mode: no connection is established to the DR site while the production cluster is running. Replication to the DR site can be scheduled X times per day.

In the event of a complete failure of the production Bastion cluster, the user can connect directly to the DR Bastion or the DR Access Manager, depending on the network architecture and firewall rules.

An internal user located in a factory can connect to the Access Manager (or Bastion) located on the central site. He can then select the equipment he wants to connect to.

IV.4 PREREQUISITES

This architecture makes the assumption of a resilient network. If the IPsec VPN or SD-WAN link is cut between the central site and the factory, no user will be able to connect to the targets from the central site: it is necessary to connect via the DR site. If, in addition to this outage, the link is cut between the DR site and the factory, then it will not be possible for a user to connect to the factory targets.

In this architecture, all audit tasks must be done from one of the Access Managers through the "Global search" feature.

V. HYBRID ARCHITECTURE

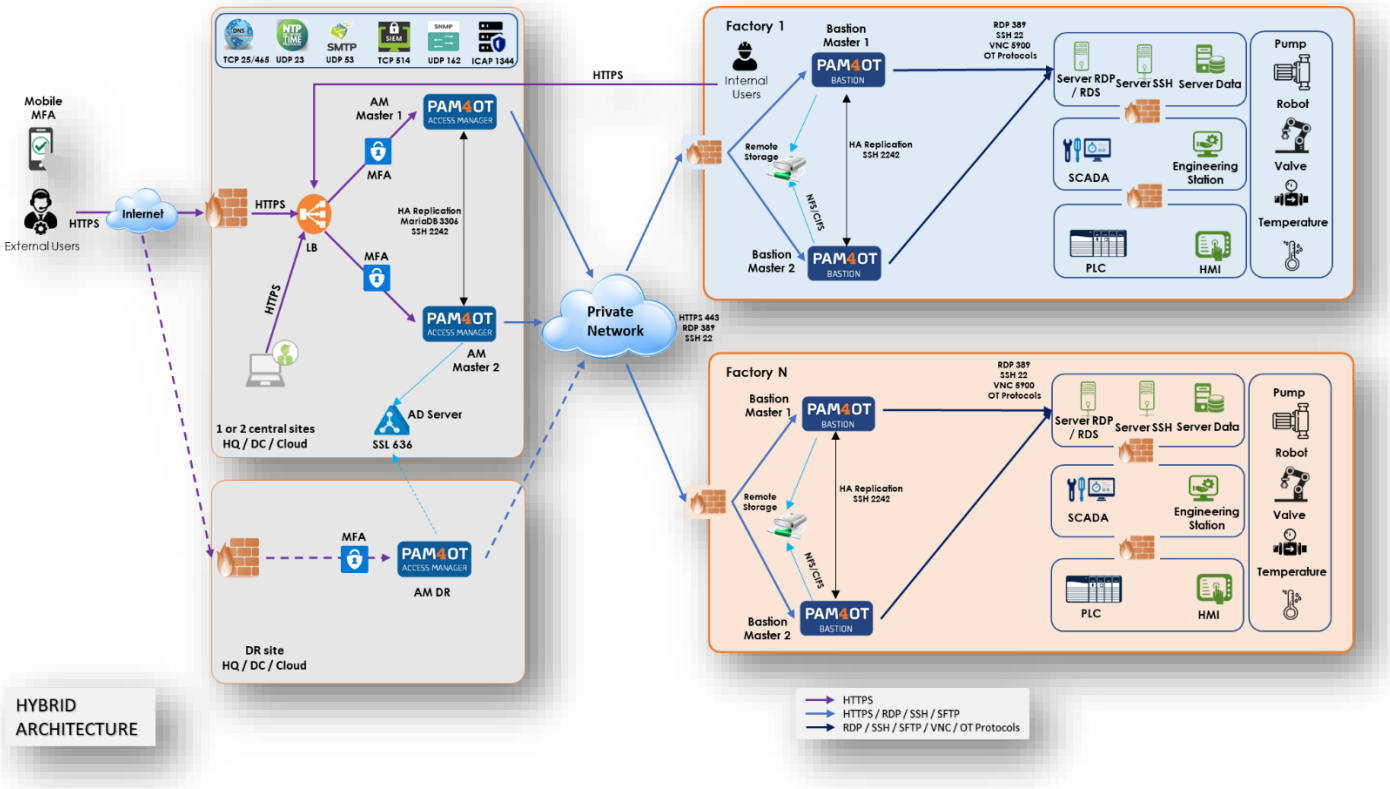
V.1 WHEN DOES IT APPLY?

This hybrid factory architecture applies to medium/large perimeters that require a distributed architecture. The access manager is then centralized in the DataCenter and the bastions are distributed in the plants. The Access Managers in the DataCenter are providing centralized features such as Access, Audit, Multicriteria search capability, Logs, … for all bastions.

An additional DR site may optionally be considered for the Access Manager.

The Bastions are located in the plants, to offer local management and resiliency (in case of private network failure).

V.2 ARCHITECTURE



V.3 ARCHITECTURE FEATURES

In this hybrid architecture, external third parties access the PAM solution through the centralized Access Managers, located in the central site.
The priority is that users go through the AMs. In the event of unavailability of AMs, users can go through the Bastions which are locally in the plants.

The Bastions are installed in each plant in HA replication Master/Master.
Functional configuration (user & user groups, target and target groups, authorizations) is managed locally, on a per-factory basis.

An internal user located in a plant who wants to connect to an equipment, can either connect to the Access Manager from the central site or in case of Private Network failure, he can then initiate the connection from Bastions located in the plant.

V.4 PREREQUISITES

In this architecture, all audit tasks must be done from one of the Access Managers through the "Global search" feature as audit data is not replicated among the Bastions.

The administration of the bastions is done on each of the bastion cluster, located in the plant. To reduce latency, Access Manager and Bastion might be deployed on the same continent.

VI. DISTRIBUTED ARCHITECTURE

VI.1 WHEN DOES IT APPLY?

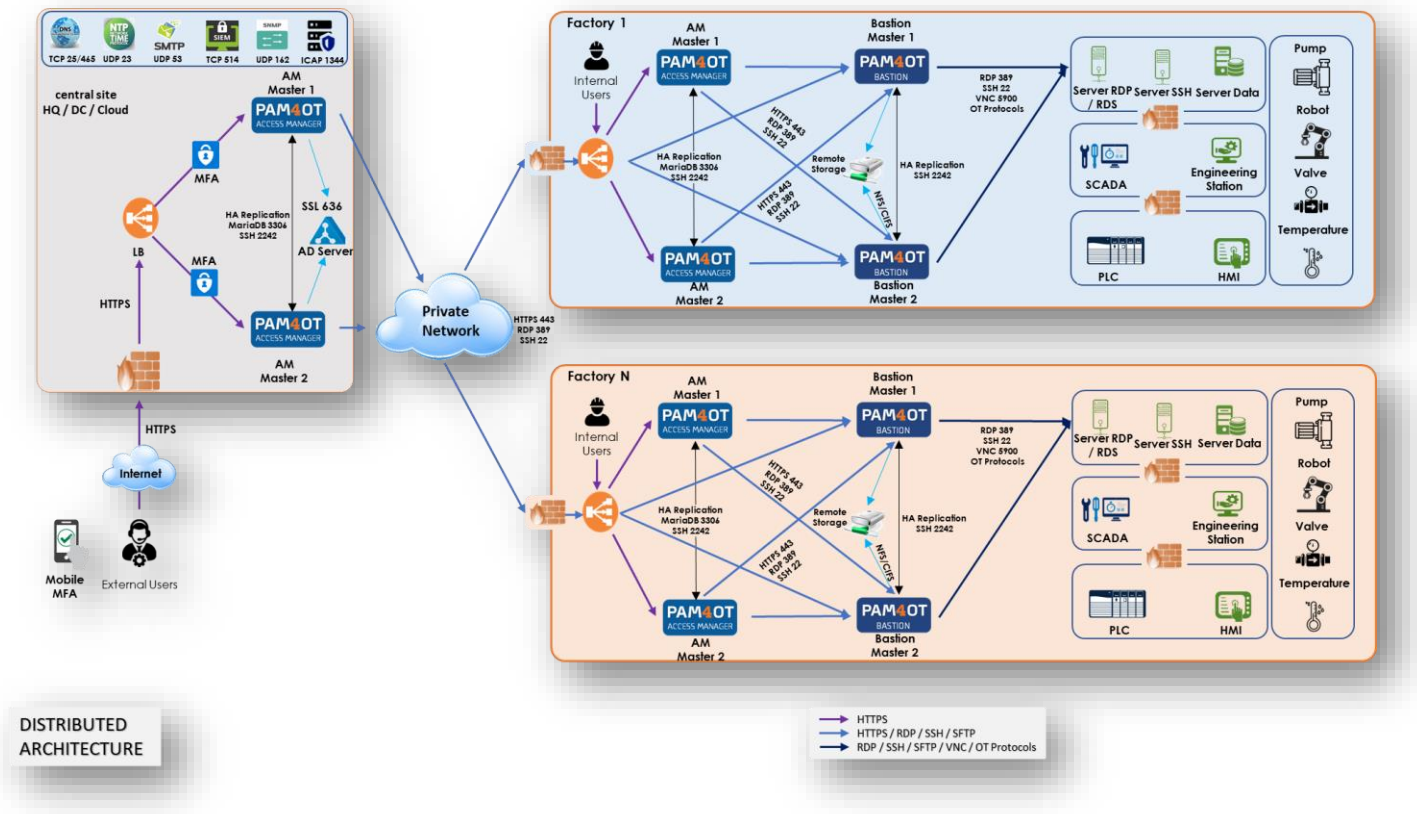
This architecture applies to large perimeters with a high level of criticality and resiliency. It provides a centralized access and management while allowing the production site isolation in case of cyberattack.

Each plant is completely independent of the others and answers to external and internal access autonomously.

The centralized Access Manager are used by 3rd party while the local Access Managers provide internal users access to targets.

The Access Managers in the DataCenter are providing centralized features such as 3rd party Access, Audit, Multicriteria search capability, Logs, … for all bastions.

VI.2 ARCHITECTURE



VI.3 ARCHITECTURE FEATURES

On the central site, there are two Access Managers that provide a centralized 3rd party access through all the bastions. An external user will be able to connect to a site's equipment from the Access Managers located on the central site.

In this architecture, each factory is equipped with a cluster of two Access Manager instances (HA Master/Master) and a cluster of two Bastion instances (HA Master/Master as well).
Each Bastion cluster meets the objectives of the plant in which it is deployed.

The benefit of this architecture is resilience to outage of inter-site network link (or sites isolation).
External user authentication is performed via the Access Manager with MFA.

An internal user located in a plant can reach a device through the Access Managers located in the plant. If the user wants to connect to an equipment located in another plant, then he can connect to the centralized Access Managers.

VI.4 PREREQUISITES

In this architecture, all audit tasks must be done from one of the centralized Access Managers through the "Global search" feature.
The administration of the bastions is done on each of the bastion cluster, located in the plant.
To reduce latency, centralized Access Managers and Bastions might be deployed on the same continent.