APPLICATION NOTE

IT requirements Omnitrend Center

.

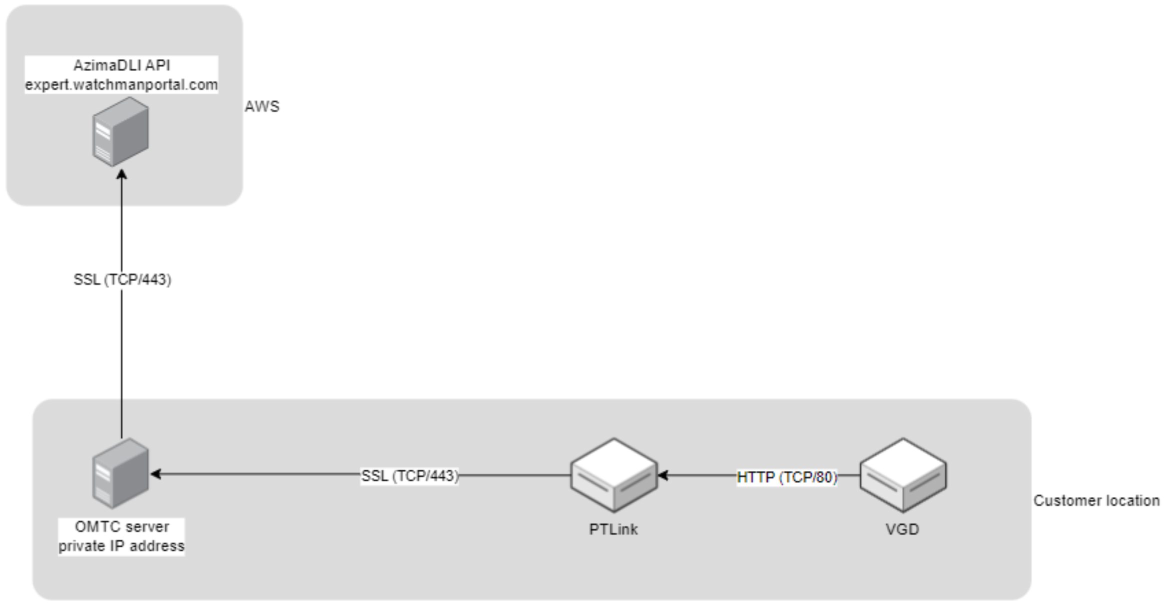

Fig. 1

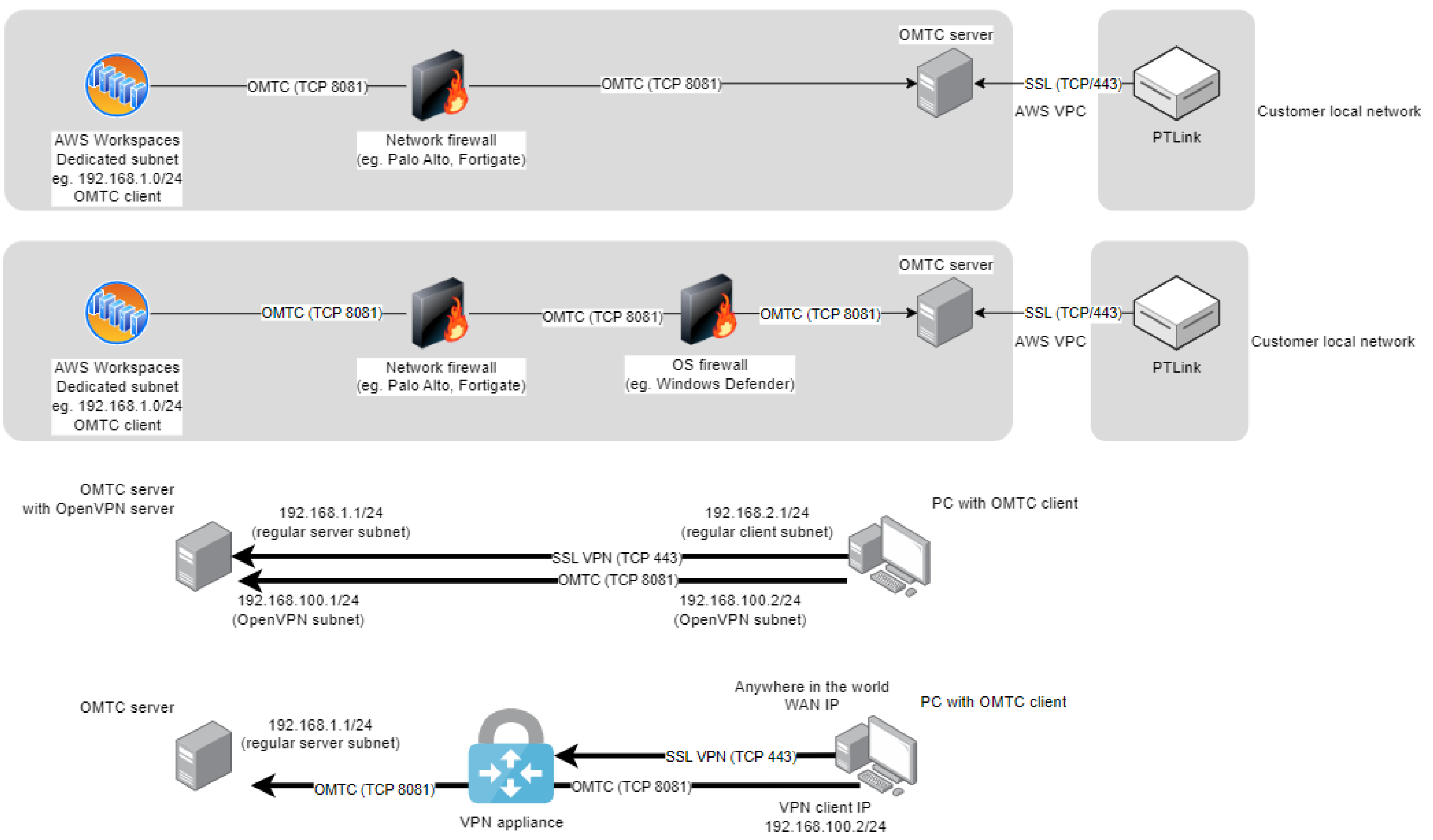
OMTC server
AWS Workspaces
Dedicated subnet
eg. 192.168.1.0/24
OMTC client
OMTC (TCP 8081)
Network firewall
(eg. Palo Alto, Fortigate)
OMTC (TCP 8081)
SSL (TCP/443)
AWS VPC
PTLink
Customer local network
OMTC server
AWS Workspaces
Dedicated subnet
eg. 192.168.1.0/24
OMTC client
OMTC (TCP 8081)
Network firewall
(eg. Palo Alto, Fortigate)
OMTC (TCP 8081)
OS firewall
(eg. Windows Defender)
OMTC (TCP 8081)
SSL (TCP/443)
AWS VPC
PTLink
Customer local network
OMTC server
with OpenVPN server
192.168.1.1/24
(regular server subnet)
192.168.2.1/24
(regular client subnet)
PC with OMTC client
SSL VPN (TCP 443)
OMTC (TCP 8081)
192.168.100.1/24
(OpenVPN subnet)
192.168.100.2/24
(OpenVPN subnet)
OMTC server
192.168.1.1/24
(regular server subnet)
Anywhere in the world
WAN IP
PC with OMTC client
SSL VPN (TCP 443)
OMTC (TCP 8081)
OMTC (TCP 8081)
VPN appliance
VPN client IP
192.168.100.2/24

Fig. 2

1. General considerations

OMTC is not meant to be deployed as a public internet-facing service. FRS recommends deploying OMTC within your corporate network's internal and secured network

OMTC uses client-server communication model. Application server should be installed on Windows Server OS family (recommended), however Windows 10 and 11 are also supported. For clients to be able to communicate with OMTC server you must whitelist TCP port 8081 on the machine where OMTC server is installed. You should avoid exposing port 8081 from OMTC server to the public internet. If you are running your server on the VPS or as cloud instance within any of the cloud providers (Azure, AWS, etc.) it is highly recommended not to assign public IP address to the machine where OMTC server is running. Instead, we advise keeping the machine in a secure private network and utilizing VPN connectivity or cloud-based managed desktops to allow your users OMTC client connections. Wherever applicable you should be using dual-layered firewall solution (e.g., Windows Firewall together with a hardware/virtual firewall appliance).

1.1. Providing access to OMTC server

1.1.1 VPN

VPN is the recommended way to access OMTC server by the employees out in the field and in locations different to where the server machine is hosted. You can leverage your existing VPN infrastructure making sure that your VPN client will be able to communicate with OMTC server on TCP port 8081.

1.1.2. Cloud-based managed desktops

If you run your server in AWS/Azure environment, you can utilize managed desktops solutions (AWS Workspaces / Azure VDI) available in their offer to maintain connectivity to OMTC server. You can provide your virtual desktops (with OMTC client installed there) in separated subnet and allow only this subnet to reach OMTC server by using any kind of firewall software (e.g., Windows Defender) running on the server machine or any kind of hardware firewall/network ACL as well to limit access on the networking device level. Such a solution allows for easy provisioning OMTC access to multiple employees by simply leveraging image template.

1.2. Connecting PT Link to OMTC

PT Link is a proxy solution which collects all the measurement data from online devices which don't support encrypted communication. Traffic from online device reaches PT Link via HTTP and then it gets encrypted and delivered to OMTC server via HTTPS. For PT Link to function properly you should open inbound TCP port 443 on the OMTC server and outbound TCP port 443 on machine where PT Link is running.

1.3. Connecting your OMTC server to Azima DLI EADS API

To allow your OMTC server to communicate with EADS API you need to allow outgoing traffic on TCP port 443 (TLS) to a specific IP address 35.80.234.155 (expert.watchmanportal.com). API is IIS based solution currently hosted in AWS (Oregon). Data is encrypted in transit using TLS 1.2. Legacy SSL/TLS protocols like SSL 3.0 or TLS 1.0 are not supported. At any time, you can verify security of the API by just visiting free SSL Labs analyzer by going to following URL

https://www.ssllabs.com/ssltest/analyze.html?d=expert.watchmanportal.com

2. Data transfer

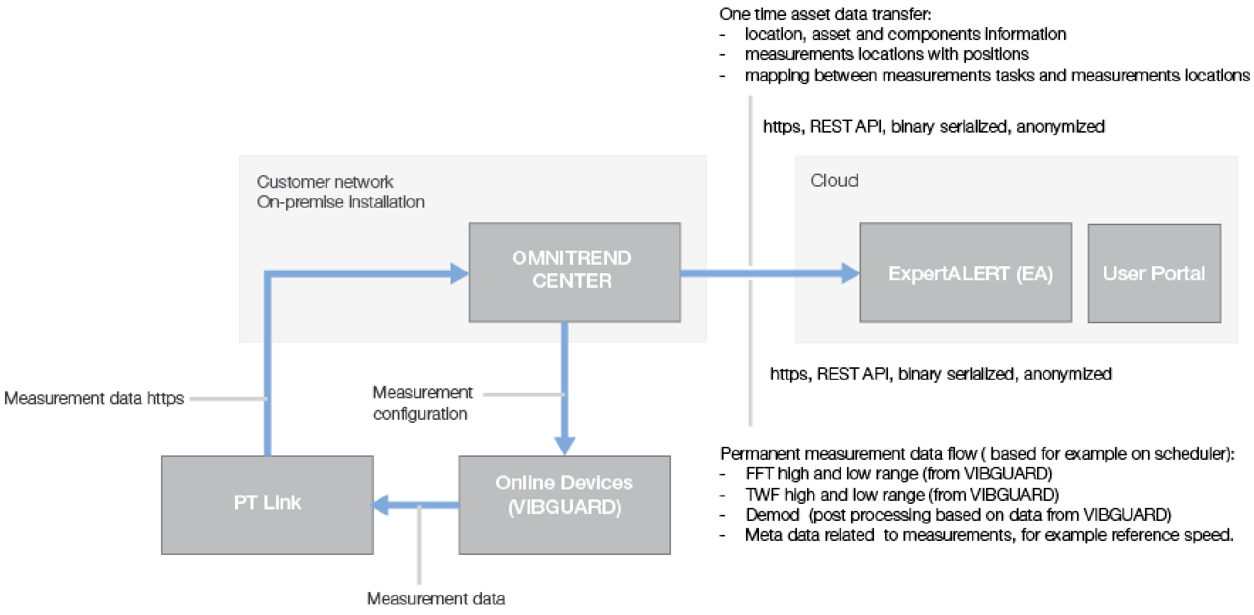
One time asset data transfer:
- location, asset and components information
- measurements locations with positions
- mapping between measurements tasks and measurements locations
https, REST API, binary serialized, anonymized
Customer network
On-premise Installation
OMNITREND CENTER
Cloud
ExpertALERT (EA)
User Portal
https, REST API, binary serialized, anonymized
Measurement data https
Measurement configuration
Permanent measurement data flow (based for example on scheduler):
- FFT high and low range (from VIBGUARD)
- TWF high and low range (from VIBGUARD)
- Demod (post processing based on data from VIBGUARD)
- Meta data related to measurements, for example reference speed.
PT Link
Online Devices (VIBGUARD)
Measurement data

Fig. 3

IT Acknowledgement (PRINT / Sign / Date):

____/____/__________________

Fluke Deutschland GmbH
Freisinger Str. 34
85737 Ismaning
Deutschland

Web access: www.pruftechnik.com