FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

In our first Technote – Bridging the Information Gap with Remote Access, the Technology Network brought up some challenges and solutions to gain remote access from the viewpoints of End Users, OEMs, Software Vendors, and Support service groups. Every group listed similar challenges, and multiple solutions were discussed as an overview – including:

- **DMZ Implementation managed by OT provider**
- **Industrial M2M communication**
- **Customer Managed VPN**

PART 2 – UTILIZING A DMZ – A deeper look into a remote access option:

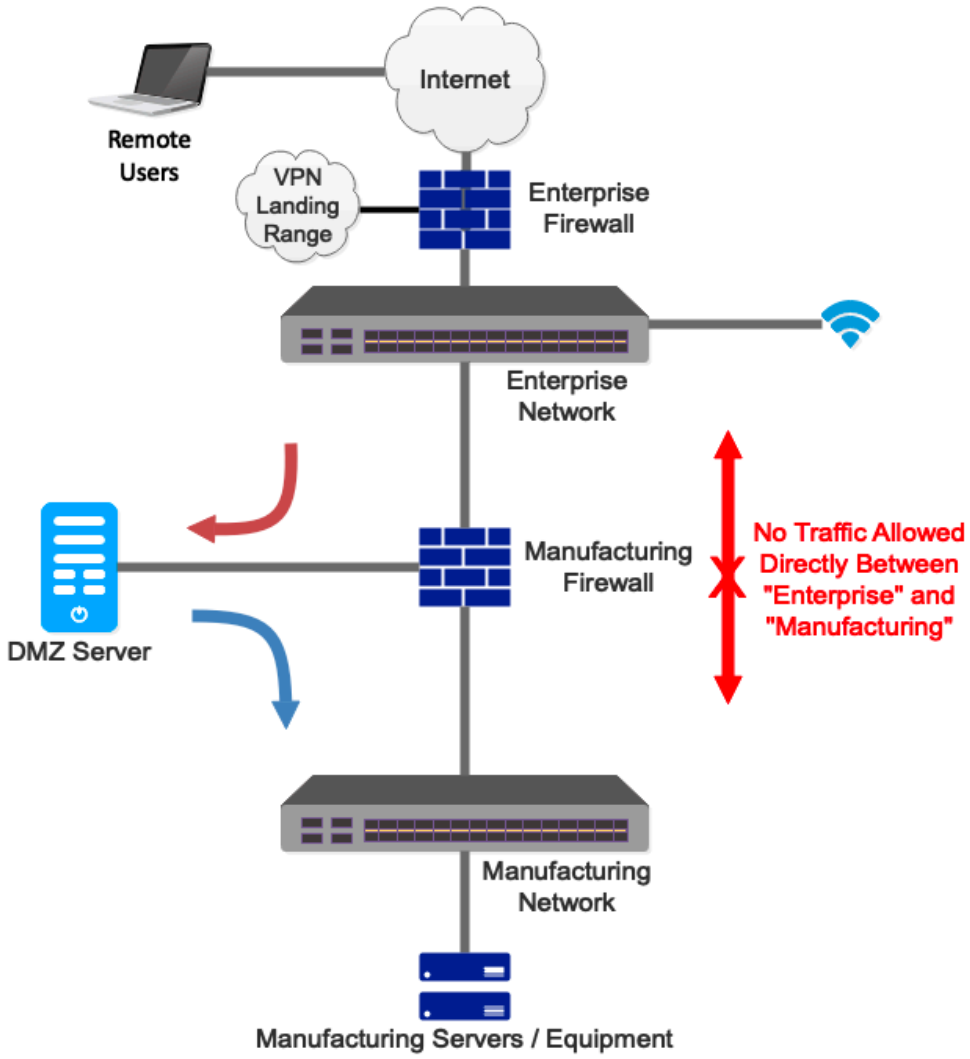
In this Technote, we will look at what a DMZ is, what benefits are gained by using it, and what efforts are needed to implement one.

1. WHAT IS A DMZ?

DMZs provide a robust boundary between enterprise (IT) and manufacturing (OT) environments and are recommended by security standards bodies such as IEC and NIST.

A standard DMZ offering incorporates common features essential to integrating manufacturing environments with enterprise networks. It is based on secure technologies with minimal ongoing subscription costs to enhance the security posture of our customers.

FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ



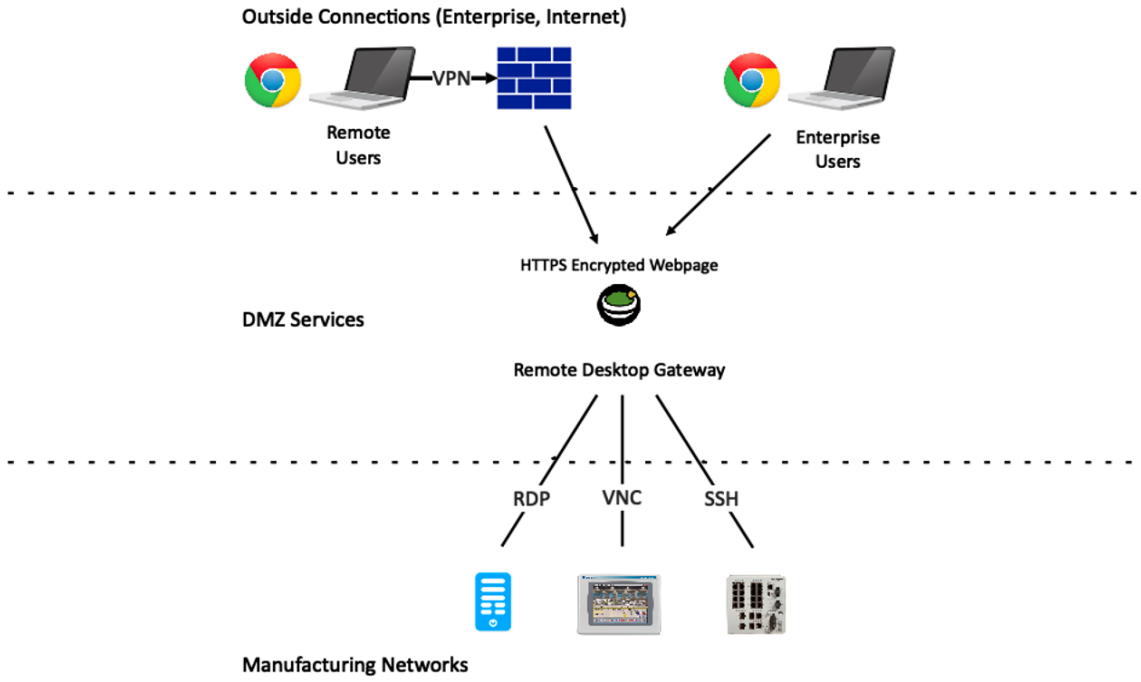
2. STANDARD DMZ FEATURES

- Remote Desktop Gateway
- Forward Proxy
- Reverse Proxy
- SMTP Relay
- Authentication Proxy

FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

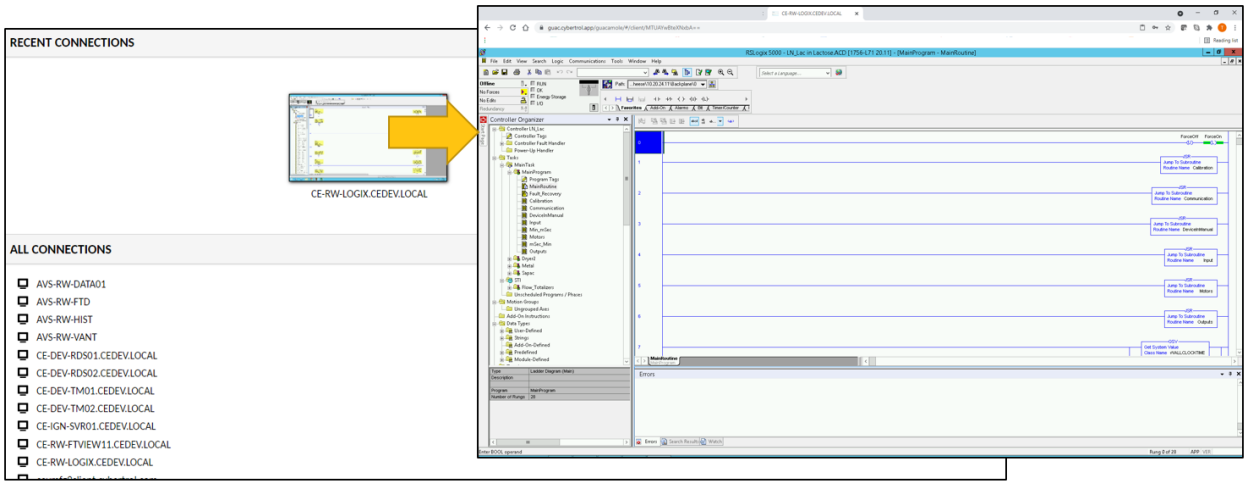
3. REMOTE DESKTOP GATEWAY

Remote Desktop Gateway allows for either internal users on the Enterprise network or remote users using a VPN into a configured webpage to access components on the factory floor.



FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

Using a web page to easily access the connections within the DMZ is simple to use, and is secured with multi-factor authentication for remote access support – click, open, and sign in.

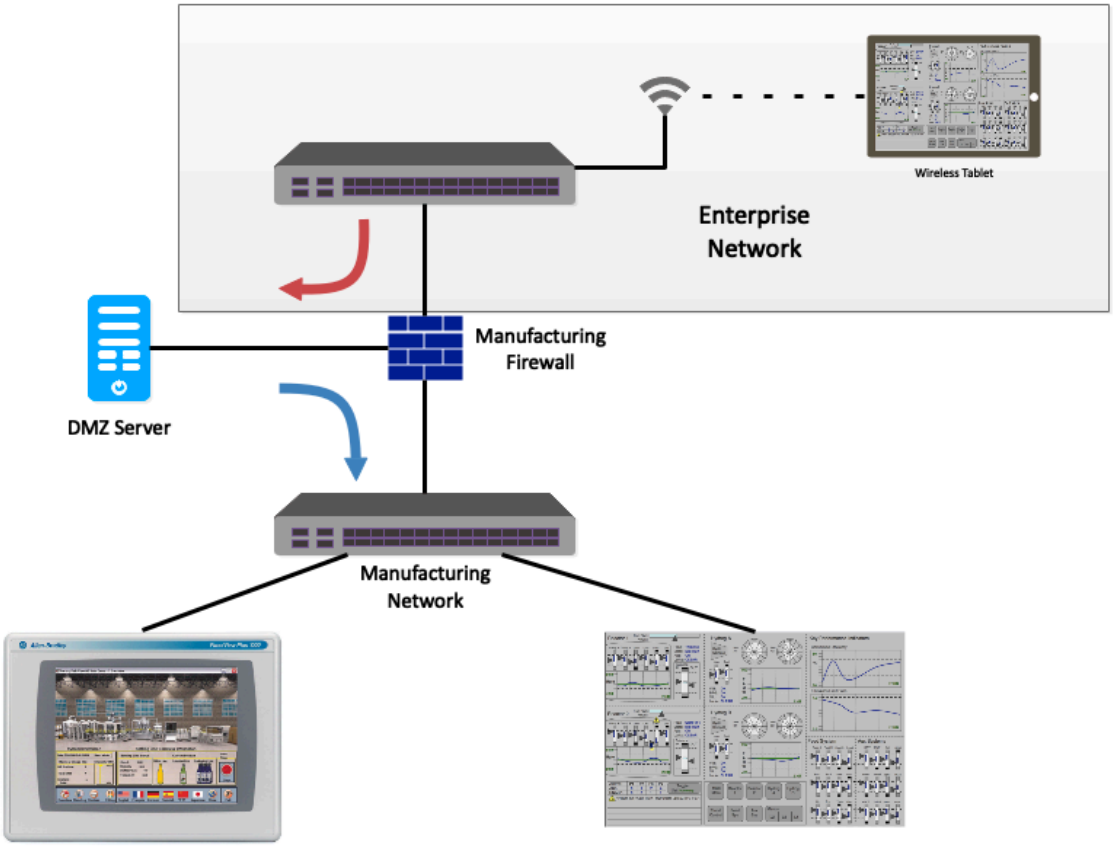


Suppose this methodology is not used, and people are given direct access to the OT network with an external laptop or other methods. In that case, the possibility of malware gaining access to the OT network increases with each 3rd party user. A local station accessed through the DMZ provides the needed layer of protection to keep the OT network secure.

FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

Remote Desktop Gateway Use Case: Wireless Tablet Access

A tablet on the Enterprise wireless network can connect to the manufacturing network to shadow clients, run an entire ViewSE session, or other plant floor operational needs.

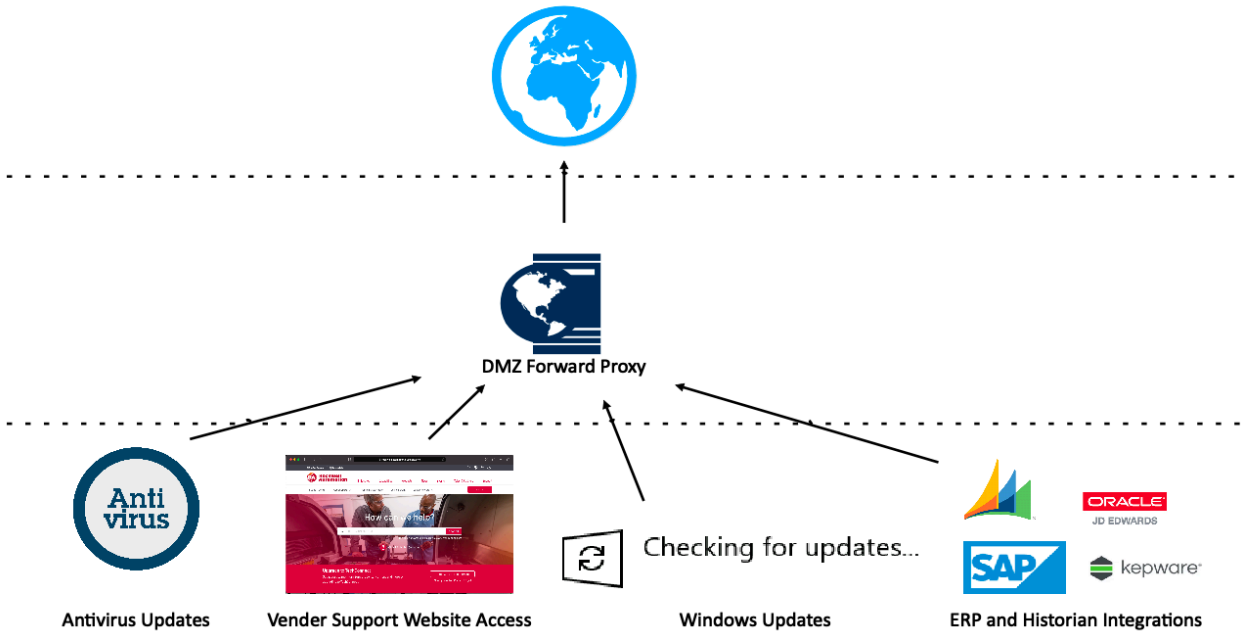


FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

4. FORWARD/REVERSE PROXY

A forward/reverse proxy allows specific devices to access enterprise or internet resources such as:

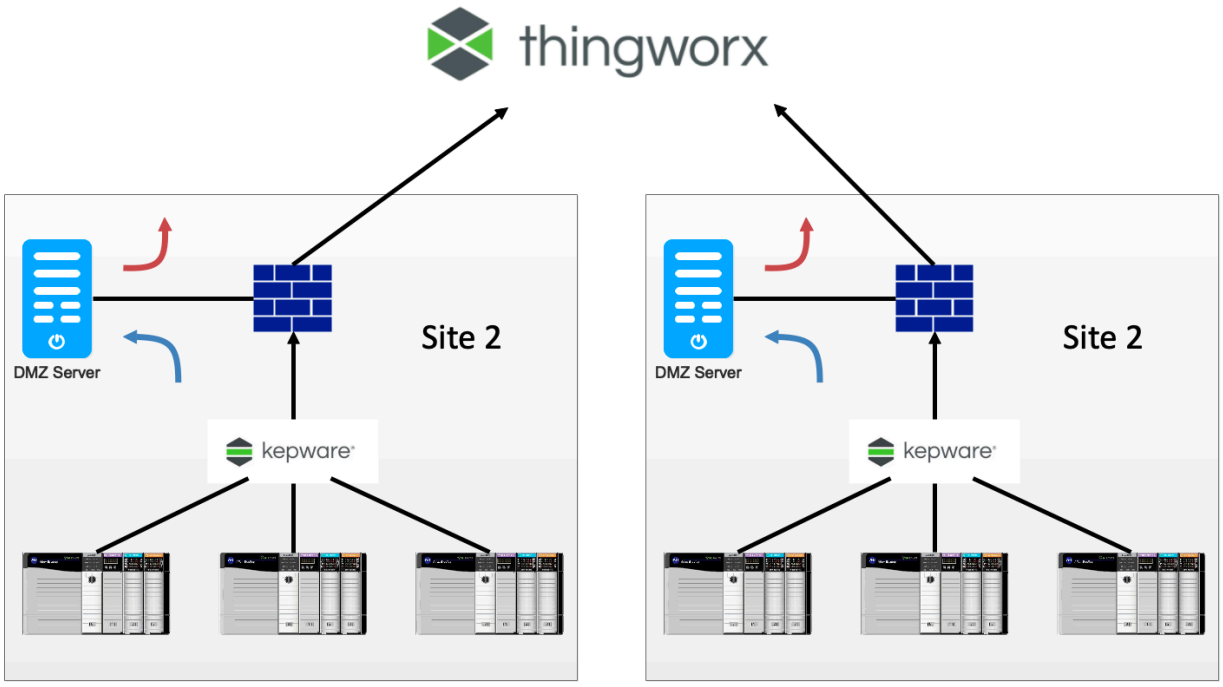
- Antivirus Updates
- Windows Updates
- ERP Integration
- Cloud Historians



FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

Forward Proxy Use Case: Multi-site deployments

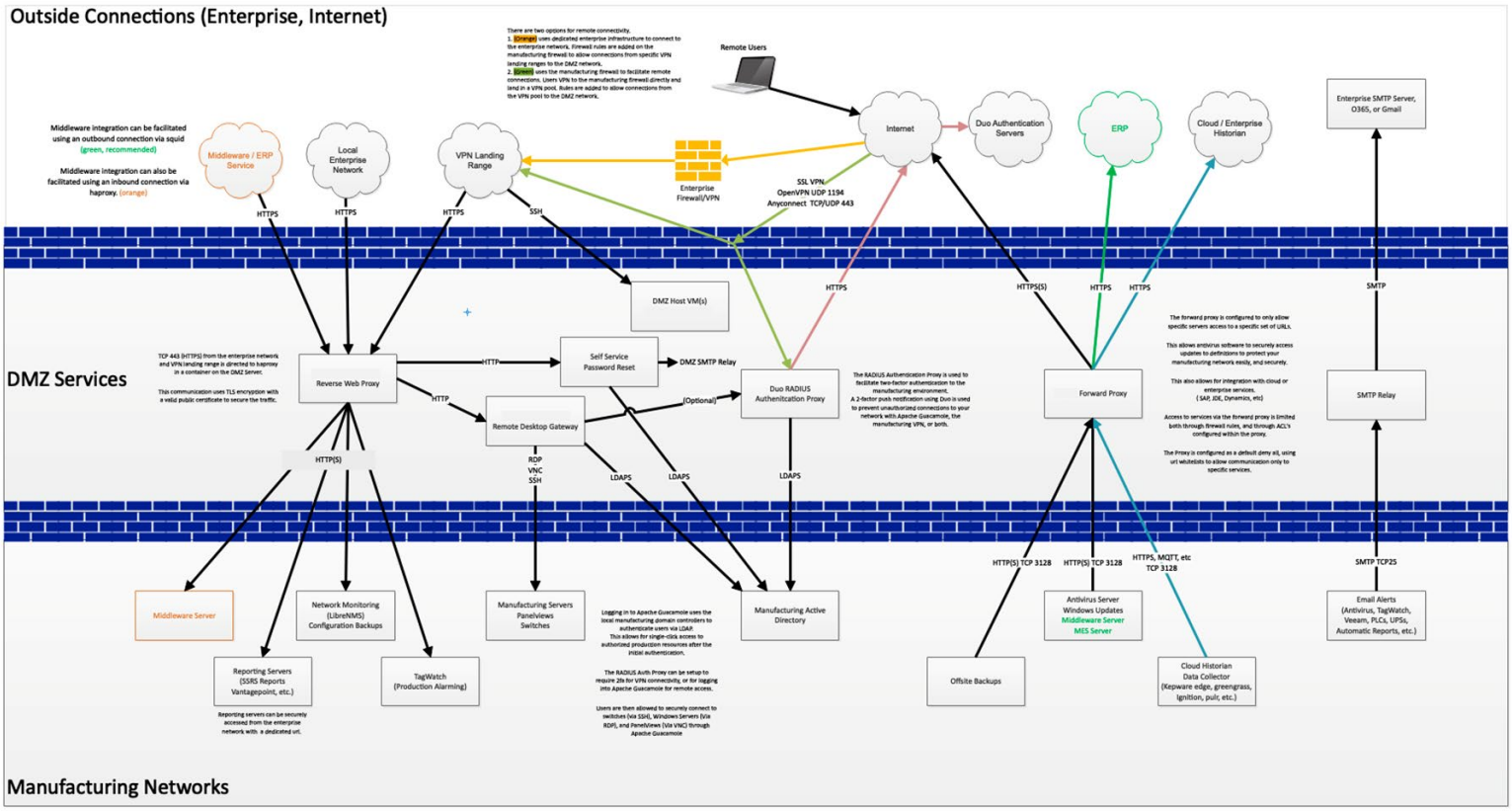
Pulling information into a data analysis system without poking holes into the firewalls adds greater visibility without security risks.



FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

5. SMTP RELAY

The SMTP Relay allows for email alerts from the production floor to the enterprise SMTP server, Office 365, or Gmail, as a few examples. Automatically triggered alarms or reports are items that are typically routed through the SMTP Relay:



FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

6. MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is a routine operation with every software platform available. It combines the following:

- A username and password you have granted the first step of access
- A verification step with a different tool (such as a cell phone)
- Access then granted

FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

7. PROS AND CONS

PROS

- Cybersecurity – the DMZ offers the most robust Cyber Security offering for access to the OT layer
- Access – access can be configured from one-to-many points based upon the configuration required to provide further flexibility in access both for internal and external resources
- Ease of Use – by using webpage front ends and standard dual authentication methods, access that is configured for users is easy to use

CONS

- Skill level required to implement and maintain – this is not a system that is dropped in and forgotten – it must be installed in coordination with the end-user IT department for proper access and maintained by an OT professional to ensure security stays up to date

FPSA – Technology Network
Technote – Bridging the Information Gap
Part 2 -Utilizing a DMZ

8. CONCLUSION/SUPPORT

DMZ combines access, security, and ease of use but is complex for an OT Cybersecurity provider to configure and maintain to ensure the security levels remain acceptable to the end-user.

A DMZ is something that can't just be implemented and left alone – it needs to be maintained for user access, updated for any security reasons, and generally checked for any system issues. This is why OT Providers offer this type of security as a DMZaaS.

By making this an operational cost – you keep your manufacturing network secure, while trusting the experts to maintain and support this access layer DMZ.