Secure Remote ICS Access Using a VPN and Firewall

Summary

Most devices connected to an Industrial Control System (ICS) should not be connected to the Internet. Even so, technicians and others often need to be able to access these devices remotely via the Internet or using other shared networks. If proper precautions are not taken this will create a risk that can be exploited by hackers and cause expensive and/or dangerous security breaches. One way of reducing this risk is to encrypt all traffic to and from the ICS network by using a Virtual Private Network (VPN). Another way of reducing the risk posed by remote attackers is to implement a firewall.

Learning Outcomes

- Explain base firewall concepts.
- Explain basic Virtual Private Network (VPN) concepts.
- Compare different VPN technologies.
- Demonstrate how the use of a firewall can prevent many remote attacks.
- Demonstrate how the use of VPN secures network traffic.

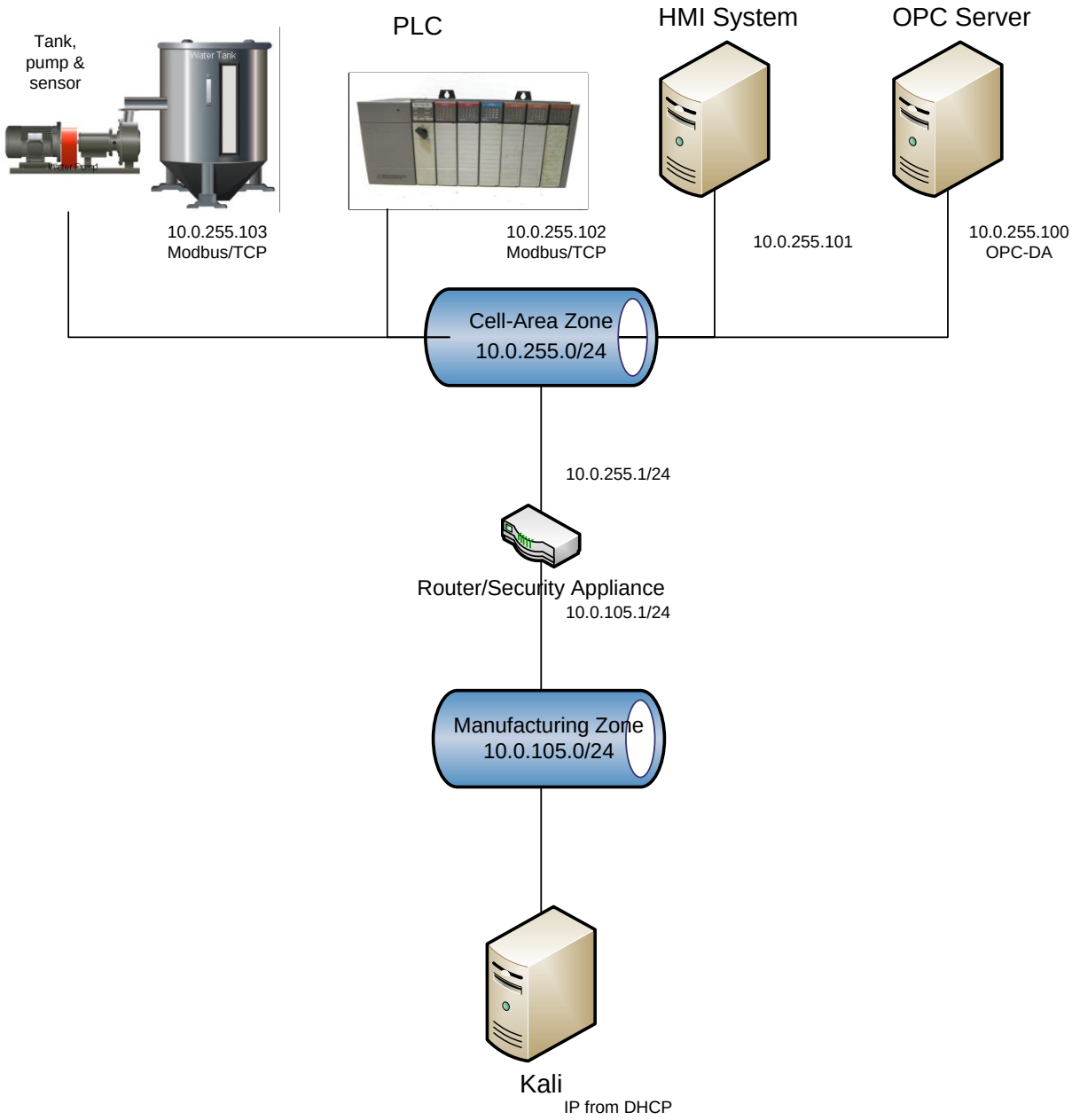
Systems

- Kali Linux – Hacker
    - Username: student; Password: Password01
- Industrial Control System
    - Windows XP – OPC Server
        - Username: student; Password: Password01
    - Windows XP – HMI
        - Username: student; Password: Password01
    - PLC/Pump/Sensors
        - Username: root; Password: Password01
- pfSense – Router/Firewall
    - Username: admin; Password: Password01

General Lab

In this lab students will configure an HMI system to provide remote access services. They will then use a Kali Linux system to perform a remote network scan on unprotected ICS systems. After the scan they will demonstrate how the lack of a firewall can allow a remote hacker to compromise passwords and file system security. The students will see that Wireshark can be used to capture and decode unencrypted remote communication sessions. Finally, the student will configure a firewall, VPN server and a VPN client and observe that this prevents the attacks carried out in the first part of the lab.

Setup and Deploy



For Further Information

National Institute of Standards and Technology (NIST) (May 2015). *Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

National Institute of Standards and Technology (NIST) (July 2016). *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST Special Publication 800-46 Revision 2*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.

National Institute of Standards and Technology (NIST) (July 2016). *User's Guide to Telework and Bring Your Own Device (BYOD) Security, NIST Special Publication 800-114 Revision 1*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf.