PNWS AWWA
Conference 2022
April 28, 2022

Advanced SCADA Cybersecurity for Water Utility Personnel

Presented by L. Lee Tumbleson, P.E.

SCADA/Control Senior Engineer

RH2 Engineering

& Control Systems Northwest

Introduction

- Speaker – Lee Tumbleson, P.E.
  - Senior Control System Engineer
  - RH2 Engineering/Control Systems Northwest
- BS Mechanical Engineering
- 5 Years water/wastewater design
- 32 Years of networking experience
  - 20+ Years RH2 IT Manager
  - 27 Years of industrial networking experience
- 27 Years of water/wastewater SCADA/Control experience
- 32 Years of computer experience/software development

Session Overview

- For non-Information Technology (IT) water/wastewater professionals
- Review common cybersecurity technology/terminology
- Improve communications with IT Staff/Consultants regarding cybersecurity topics
- AWWA/Homeland Security cybersecurity areas of concern

Disclaimer – Every network is different, and the information contained in this presentation may or may not be relevant to your system. RH2 and CSNW recommend using qualified IT staff or IT consultants that have cybersecurity experience.

Top Vulnerabilities in 2022

- Phishing for usernames/passwords is #1 method of unauthorized access; phishing has moved to an almost industrial scale worldwide
- Exploiting Remote Access security holes has climbed to #2 due to Covid
- Hacking is typically done for…
  - Spying (industrial/political, military) – typically covert
  - Money – Ransomware Attacks or Blackmail
  - Political Message – Russia/Ukraine, Russia/US. Ransomware or worse
- Bitcoin is typical money transfer method for Ransomware password to unencrypt data – this is difficult, but not impossible, to trace
- Phishing can also be used for impersonating someone with the power to move money around, this is rare but very profitable

Very Short History of Cyber Attacks

Early hacking attempts via governments

1980's

1990's

Mid-2000's – General purpose computer viruses used to gather data, money, and destroy computer systems. 9/11 terrorist fears of SCADA attacks.

Stuxnet released by Israel/US Against Iranian Uranium Enrichment Plant. First acknowledged Nation State engineered hacking system

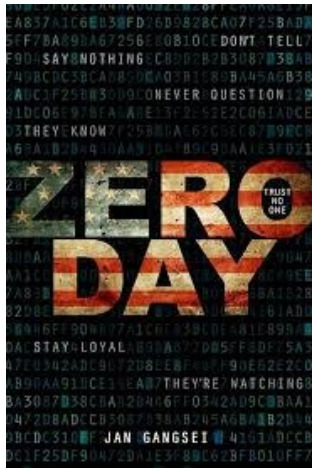
Late 2000's

2010's

Mid-2010's – Edward Snowden exposes US Cyber Monitoring and Attack programs. Governments deploying cyber attacks on businesses and government agencies. Russia attacking Ukrainian infrastructure.

Hacking up 400% since Covid. Russian SolarWinds Hack. Russia hacking U.S. infrastructure.

Today



Opportunistic vs. Intentional Attack

- **Opportunistic** attackers only **attack** when given the right opportunity or reason – most common
  - Clicking on the wrong website/email link
  - Downloading free infected software
  - Using an infected USB drive
  - Being infected on a network by another computer with security rights
  - Router/firewall weakness exploited
  - Remote access exploited – Florida Treatment Plant
  - Forgot to lock the door or logout (operation security/physical security)
  - Disgruntled Insider has access
  - Opportunistic attacks can turn into intentional attacks once hacker identifies specific targets

Opportunistic vs. Intentional Attack

- **Seven Stages of Intentional Attacks**
  - **Reconnaissance –** Harvesting information on target *(phishing/social media)*
  - **Weaponization –** Creating deliverable payload
  - **Delivery –** Delivering payload to target
  - **Exploitation –** Exploiting OS vulnerability *(Most expensive part of attack)*
  - **Installation –** Installing malware
  - **Command and Control –** Remote manipulation of victim
  - **Action on Objectives –** Bitcoin ransom, information gathering, other motivations

SCADA System Designs

- **Old School – 1980's through early 2000's**
  - Air gapped systems – no internet
  - Only uses analog phone lines and serial communications
  - Little to no TCP/IP networking. Serial, RS-232, RS-485, Proprietary
  - Remote access over dial-up phone lines
- **Modern – Last 20 years**
  - TCP/IP industrial Ethernet
  - Systems commonly integrated with utility business IT
  - Used by operations, engineering, planning, management, etc.
  - Remote access vulnerabilities

Common SCADA Cybersecurity Risks

- Physical and Remote access to SCADA system components
- Sharing SCADA network resources with business network
- Running office applications on SCADA computers
- Allowing SCADA network full access to internet
- Cloud-based control and/or data storage
- No onsite or offsite backup of SCADA computer systems
- Poor operational security (OPSEC)
- Exposed remote facility SCADA Ethernet ports
- Lack of third-party security testing/review

Common Cybersecurity Risks

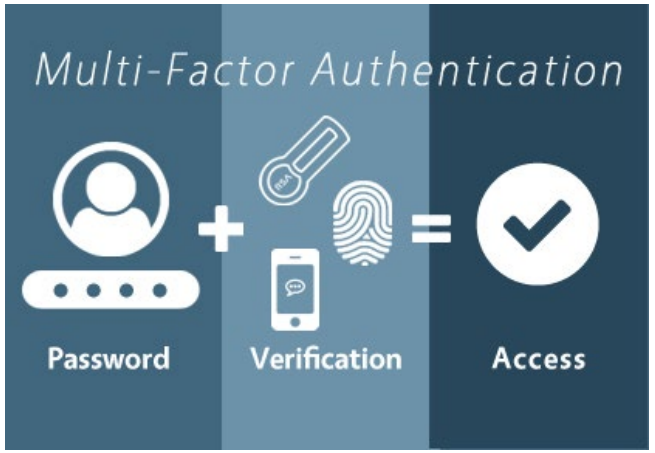
Physical/Cyber Access to SCADA System Components

- **Facility Intrusion Alarms –** Physical barriers, door/hatch switches, motion detection, IR beams, camera systems with human motion alarms
- **Facility Staff Access –** Dual factor authentication for computer systems, passwords, and eventually RFID for facility access

Dual Factor Authentication = Something you KNOW & something you HAVE/ARE

Examples:

1. Password/Biometric
2. Password/RFID Card
3. No Cloud Authentication (Phone)



Common Cybersecurity Risks

Sharing SCADA Network with Business Network

- **Majority of malware infections come from business networks**
- This is due to the following reasons (mostly opportunistic):
  - Infected email
  - Hosting email or web server on-premise
  - Social engineering/Phishing – “Use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.”
  - Installing infected software
  - Infected websites

Common Cybersecurity Risks

Running Office Applications on SCADA Computers

- Exposes SCADA network to business side infections
- SCADA computer should be single purpose machines for stability and security purposes
- Possible SCADA infection via USB drives/email/etc.

Allowing SCADA Network Full Access to Internet

- Full access is a very bad idea for reasons explained above
- Limited access is sometimes necessary for alarming and remote access:
  - Data should be encrypted from end to end when using remote access
  - Alarm email and text messages should go through an email relay so that alarm software is not directly exposed to Internet.

Common Cybersecurity Risks

Cloud-based control and/or data storage

- Exposes SCADA network to the internet
- Internet outage impacts control

Common Cybersecurity Risks

No Backup of SCADA Computer Systems (Disaster Recovery)

- In the chance of an infection, the typical response is to rebuild computers from backup media
- Many organizations backup their server data to “on-line” backup servers
  - This exposes the backup to malware while it’s on-line
- Modern malware and particularly ransomware will encrypt all storage media it can find on a network

Operational Security

- Not using dual factor authentication
- Not changing passwords or having no passwords for access and/or control
- Poor malware protection
- Remote access by staff not monitored

Common Cybersecurity Risks

3rd Party Remote Access Services

- TeamViewer, RemotePC, LogMeIn, GoToMyPC
- Centralized target for hackers

Lack of Third-Party Security Testing/Review

- QA/QC of cybersecurity design can be critical to identifying holes in the system
- Review should be handled by a knowledgeable third-party not involved in SCADA network design
- Outside security review can be expensive depending on scope of review
  - Review of existing design and then testing for security limitation
  - Secret physical/cyber breach based on no or limited information from client

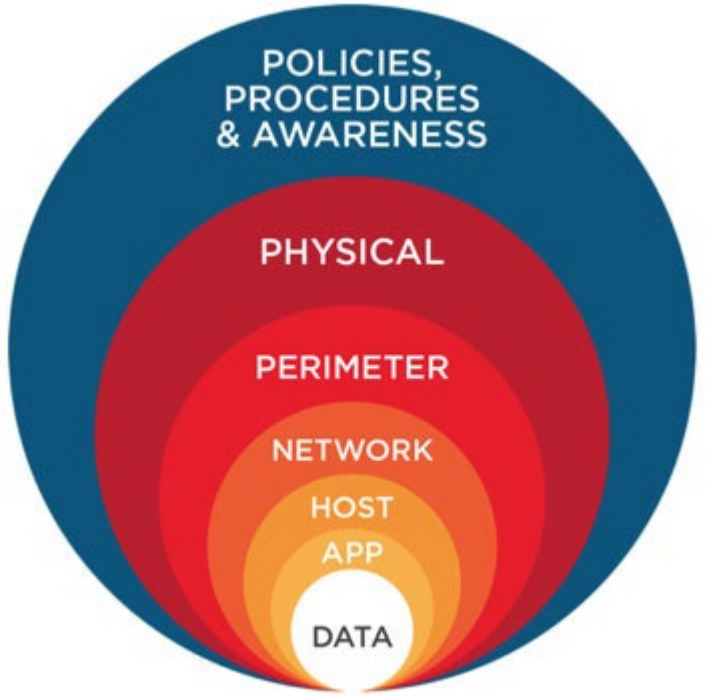
Cybersecurity Architecture

- A framework that specifies the organizational structure, standards, policies and functional behavior of a computer network, including both security and network features.
- A security architect (or IT staff trained in security design) is an individual who anticipates threats and is quick to design systems to preempt them.
- Secure network designs are dependent on the systems they are protecting. SCADA networks are fundamentally different than business enterprise networks and require different security.

Examples of Cybersecurity Architecture

Layered Defense - Using layers of network security tools and procedures.

- Each layer adds additional % of security.
- Each layer approaches a different area of security.
- If one layer is compromised, additional layers provide additional protection.
- Security access that bypasses layers of protection will not see advantages of layered defense.



Examples of Cybersecurity Architecture

Security Through Obscurity

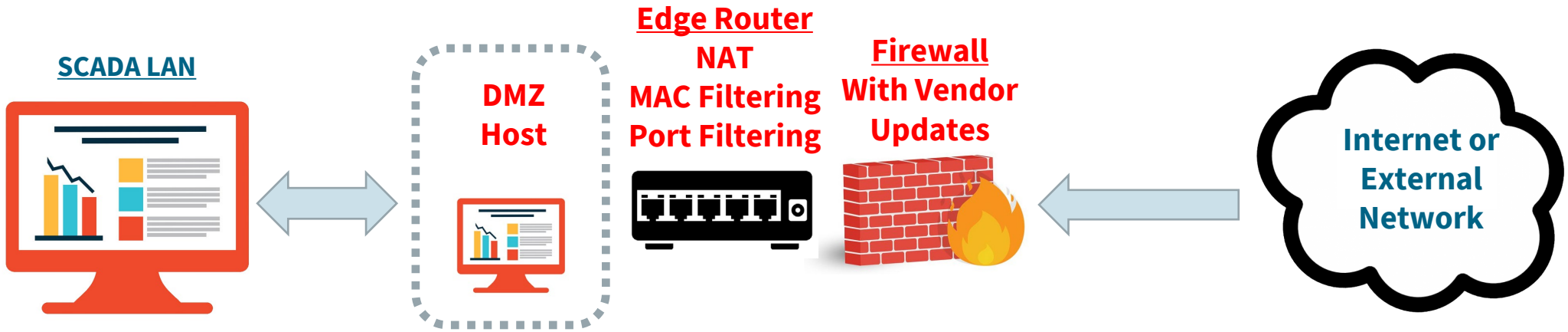
- A process of implementing security by enforcing secrecy and confidentiality of the system's internal design architecture.
- Security through obscurity aims to secure a system by deliberately hiding or concealing any security flaws or weaknesses.

Combined Security

Using layers of network security tools for “layered defense”

Example:

Firewall, NAT, MAC Filtering, Port Filtering, DMZ Host



Common Network Security Terms

Common Network Terms to be Understood before Meeting with IT Staff/Consultants

- TCP/IP Protocol
- Industrial Protocols
- LAN/WAN Borders/Edges
- TCP/IP Port Filtering
- MAC Address and MAC Filtering
- VPN
- VLAN
- NAT
- Firewalls
- DMZ

TCP/IP Protocol Stack

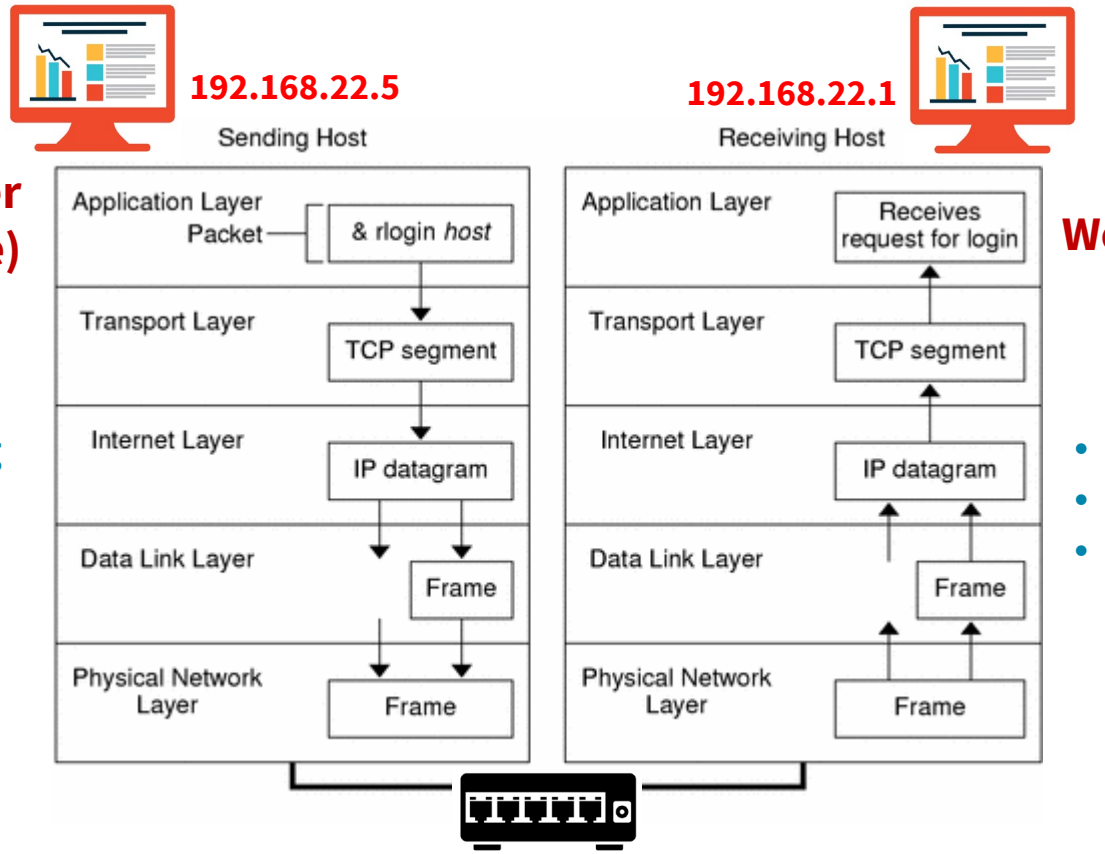
How to Transmit Data from Point A → Point B and Guarantee Delivery

Data broken into separate packets with delivery confirmed at Point B (or an error)

Web Browser (log into website)

<u>**Bottom 4 Layers**</u>

- Data Packaging/unpackaging
- Confirmation of delivery
- Interface with network hardware



Web Server

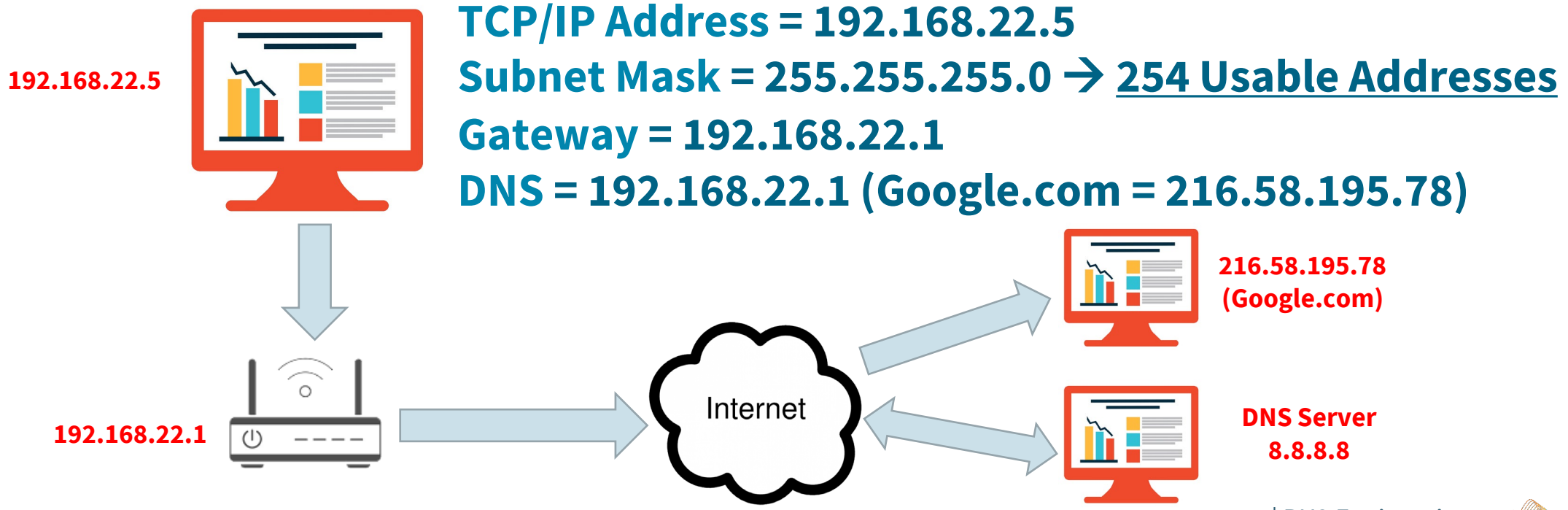
<u>**Bottom 4 Layers**</u>

- Data packaging/unpackaging
- Confirmation of delivery
- Interface with network hardware

TCP/IP Protocol Stack-Device Addressing

Home Network Example:

TCP/IP Address - Address of current device
Subnet Mask - Total addresses allowed on local subnet
Gateway - Address of device that leaves local subnet (*internet router/WiFi router*)
DNS - Address of device that translates readable addresses to actual TCP/IP address (*Google.com*)



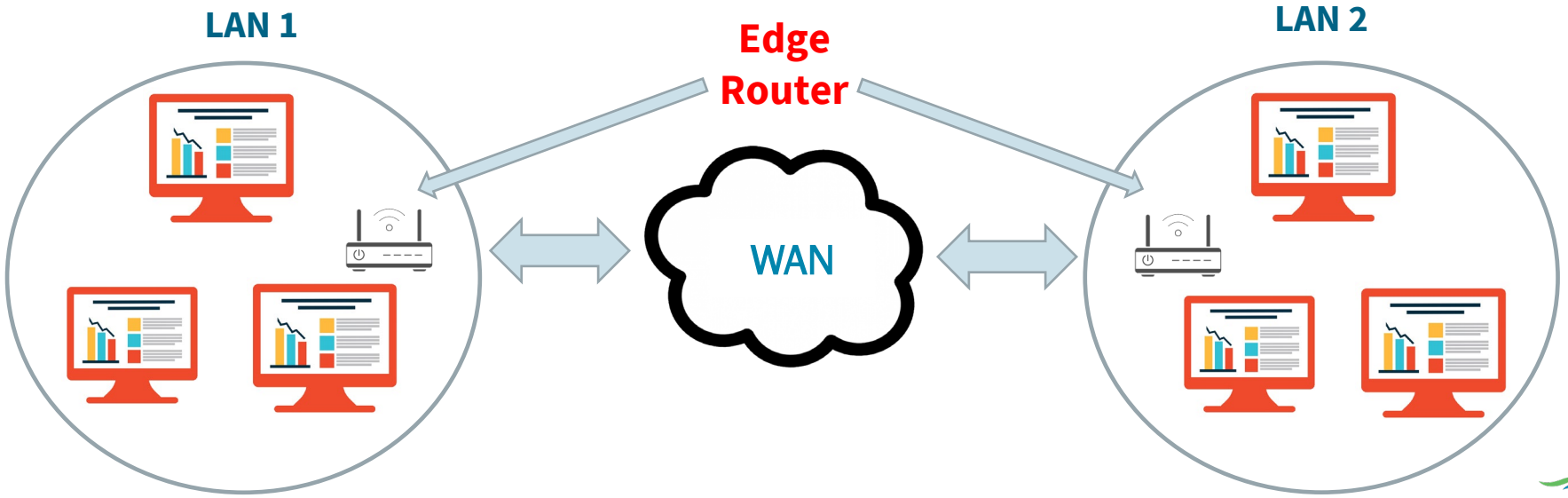
TCP/IP Protocol Stack

- All computers and devices that are on a network contain the TCP/IP protocol stack in software.
- Microsoft, Apple and Linux computers all have robust TCP/IP stacks that have been exposed and tested with Internet for decades.
- PLC’S and other IoT devices typically use Nichestack, an open-source TCP/IP software stack that vendors can slip into their systems.
- Several Nichestack security holes have been identified over the last decade with many of these issues never resolved in deployed systems.
- IoT devices are typically not able to protect themselves at the network level.
- Industrial networks must be protected at network borders/edge points.

LAN/WAN Borders/Edge Security Tools

LAN - Local Area Network: "Typically" a private network that interconnects computer devices within a limited area
Examples: Home, office, water facility, wastewater facility

WAN - Wide Area Network: "Typically" a public or private network used to connect Local Area Networks
Examples: Internet, cellular network, Radio Network-Typically a private network for SCADA systems



Port Address and Port Filtering

Port - A port is a number that identifies a specific application or a type of network service. Port numbers extend from 0 to 65535

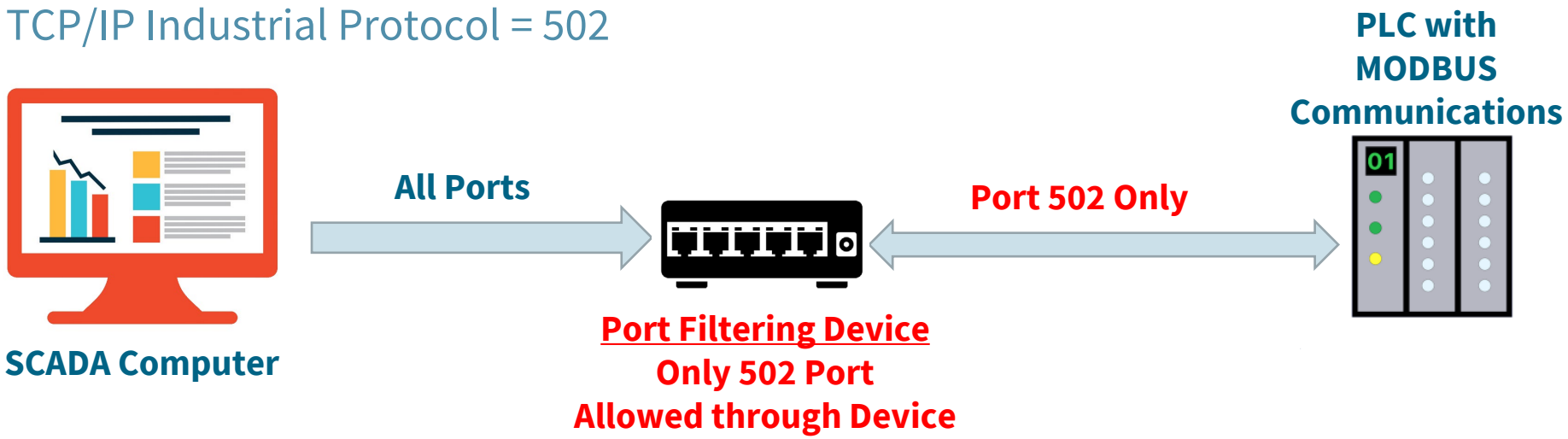
Port Filtering - Ability to only allow certain ports to communicate between networks. Used as a filter tool for network security

Examples:

HTTP = 80

Allen Bradley Industrial Protocol = 2222 and 44818

MODBUS TCP/IP Industrial Protocol = 502



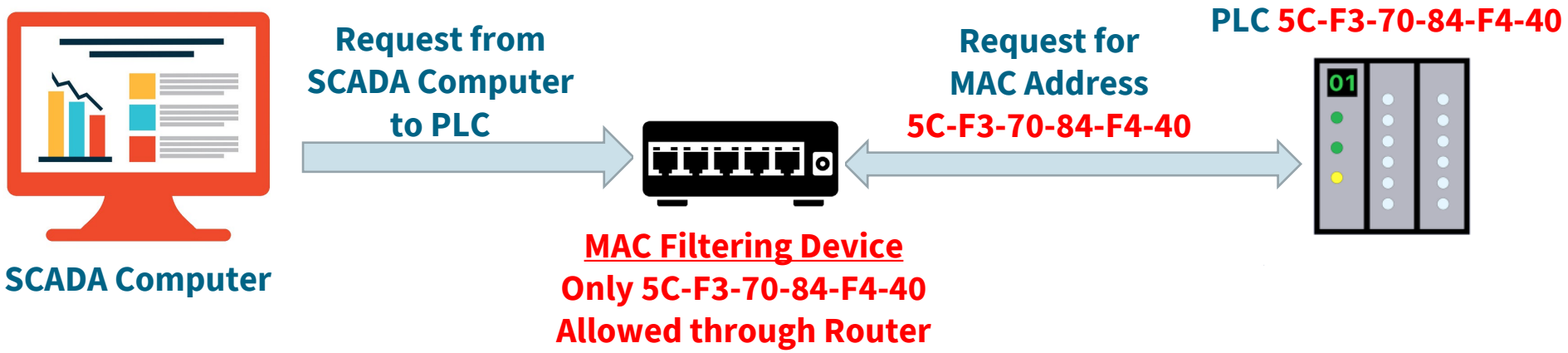
MAC Address and MAC Filtering

MAC Address - A Media Access Control address (MAC address) is a unique identifier assigned to a Network Interface Controller (NIC). Should be unique to every Ethernet device

MAC Filtering - Ability to only allow certain MAC address devices to communicate between networks. Also used as a tool for network security

Example:

5C-F3-70-84-F4-40 (281 trillion different addresses)



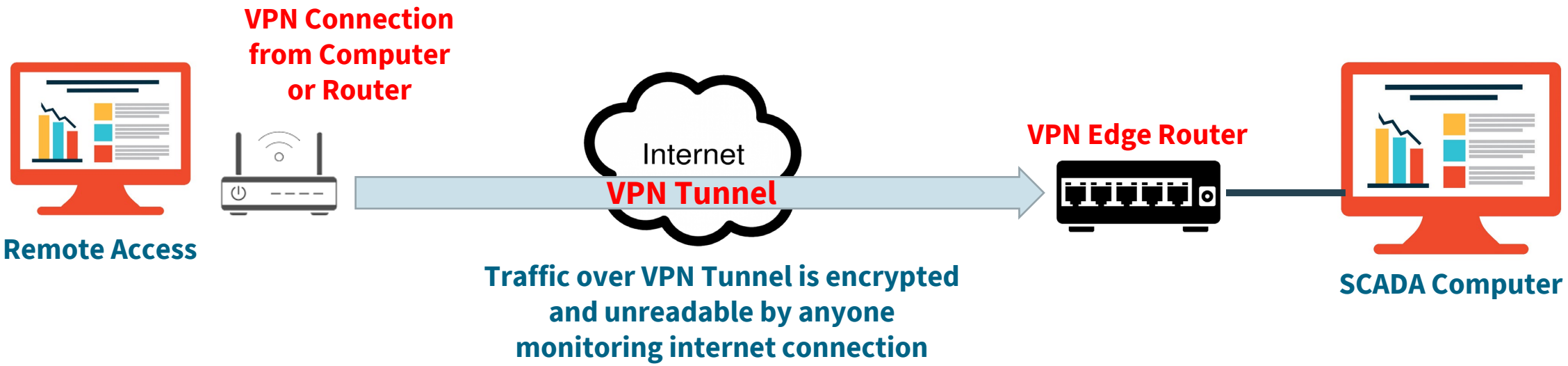
VPN-Virtual Private Network

VPN - Extends a private network over a public network through the process of encrypting all communications data packets. Typically used as a way of securely connecting to remote devices. Illegal in many countries like China/Russia, Iran. IPSec is currently most popular standard version.

Examples:

Home Office Computer → Work Network

Smartphone/Tablet/Laptop → SCADA Computer Network



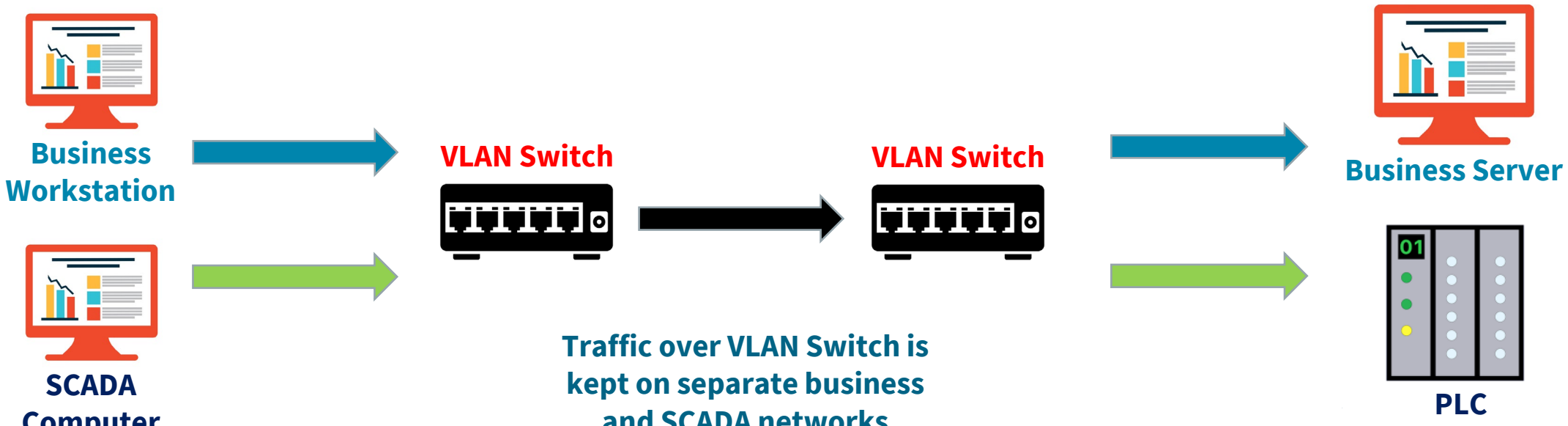
VLAN-Virtual Local Area Network

VLAN - Method of isolating Local Area Networks on shared network equipment

Examples:

VLAN 1 → Business Network

VLAN 2 → SCADA Network



NAT-Network Address Translation

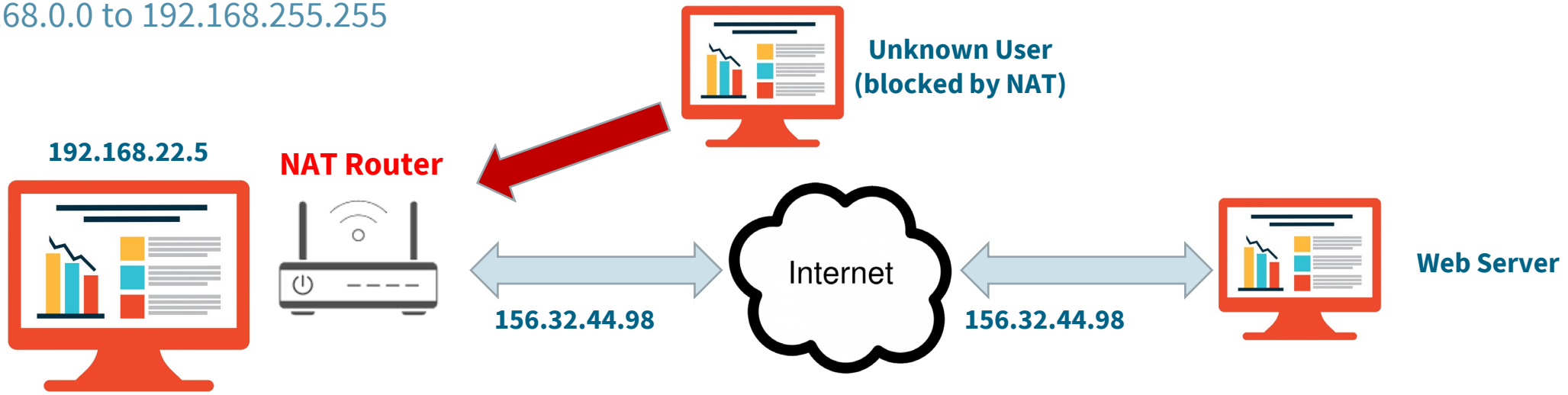
NAT - Remapping LAN IP addresses into public IP addresses by modifying network address information as data passes through edge router. Prevents internet traffic from directly accessing LAN devices unless request started on LAN device.

Private IP Address Examples:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

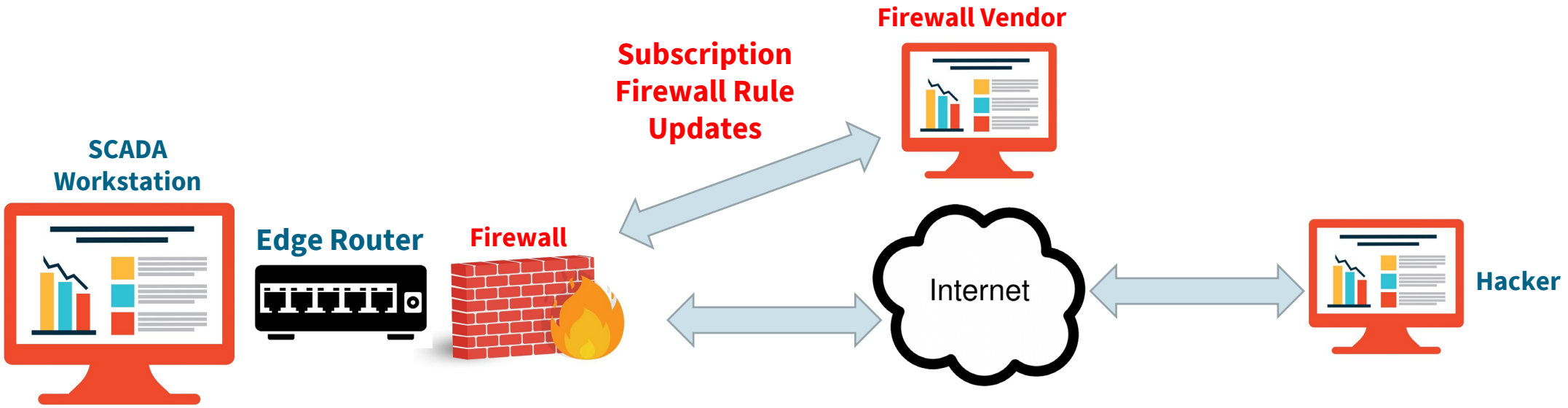


Firewalls

Firewall - A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Establishes a barrier between a trusted internal network and untrusted external network

Vendor Examples:

SonicWALL / Cisco / Fortinet / Barracuda

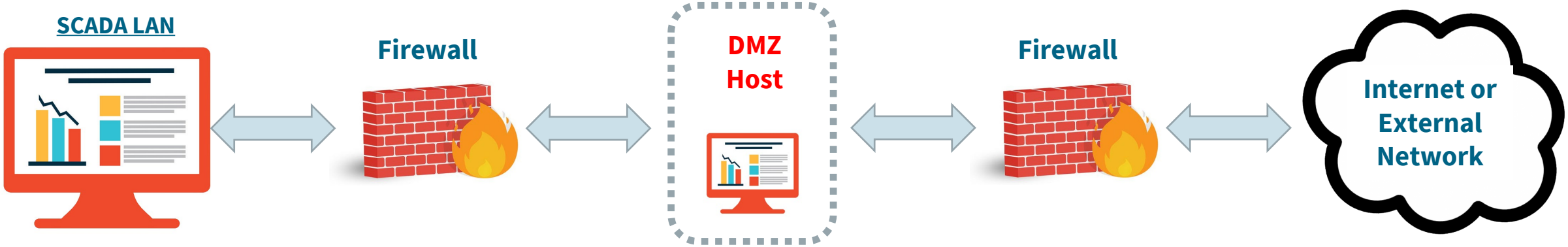


DMZ-Network Demilitarized Zone

DMZ - A location on a network that is open to another network (or internet) while securing a Local Area Network (LAN) behind a firewall. Exposes an organization's external-facing applications to an untrusted network while protecting LAN.

Examples:

- Alarm notification software that uses email/SMS
- Remote Access



SCADA Computer Recovery Plan

- If we assume that infection of malware is inevitable, then mitigating the infection becomes our highest priority.
- In all infection scenarios, restoring the SCADA computer system as fast as possible while maintaining safety/security is first step even if the infection vector has not been identified.
- Identify steps necessary to isolate network and recover SCADA computers even if infection has been on system for a long time.
- Identify the proper backups necessary for a complete backup/recovery of operating system and applications along with their restoration process.
- Do not backup up SCADA computers to online storage as the storage can be compromised. Backups should be kept in an offline media location that can not be compromised from the network.

What is the Future of SCADA Cybersecurity?

Zero Trust Network Access (ZTNA) – Security framework more than new technology. Organizations should not trust any entity inside or outside of their perimeter at any time. Network constantly verifying all devices, configurations, users, and network traffic.

AI Cybersecurity – AI Tools are being implemented in cybersecurity platforms to detect very complex intrusion attempts. This type of technology works with the ZTNA framework identified above to try and block regular and AI created hacking tools.

Secure USB Drives – USB drives that cannot be infected when transferring files should be used whenever possible if moving data or programs to/from SCADA computers.

SCADA Recovery Master Plan – Identify steps to restore systems in case of malware attack.

Splinternet – The internet is splintering and dividing due to various factors, such as technology, commerce, politics, nationalism, religion, and special interests. Currently, your internet router/firewall is exposed to 3.4 billion people.

AWWA Cybersecurity Guidelines

Risk and Resilience Assessment and Emergency Response Plan

https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960

- Governance and Risk Management
- Business Continuity and Disaster Recovery
- Server and Workstation Hardening
- Access Control – Edge Protection
- Application Security
- Encryption
- Data Security
- Telecommunications/Network Security & Architecture
- Physical Security
- Service Level Agreements
- Operations Security (OPSEC)
- Education
- Personal Security
- Cyber-Informed Engineering

Additional Resources

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Homeland Security - Industrial Control Systems Website

- https://us-cert.cisa.gov/ics
- Website includes alerts, advisories and reports.
- Cyber Security Evaluation Tool (CSET) – Provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. This is not a network scanner; this is Q&A software that grades an industrial networks security.

Google 7 Hour Cyber Security Full Course for Beginners:

https://www.youtube.com/watch?v=6MYF6Zo6i6A

Questions?