NIST SPECIAL PUBLICATION 1800-45

Cybersecurity for the Water and Wastewater Sector: Build Architecture

Operational Technology Remote Access

CheeYee Tang
Jeffrey Marron
National Institute of Standards and Technology

Philip Fenimore*
Stephanie Saravia*
Bob Stea
Chalessa White
John Wiltberger
The MITRE Corporation

June 2026

FINAL

This publication is available free of charge from https://doi.org/10.6028/NIST.SP.1800-45

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-45

Cybersecurity for the Water and Wastewater Sector: Build Architecture
Operational Technology Remote Access

CheeYee Tang
Jeffrey Marron
Applied Cybersecurity Division
Information Technology Laboratory

Philip Fenimore*
Stephanie Saravia*
Bob Stea
Chalessa White
John Wiltberger
The MITRE Corporation

**Former MITRE employee; all work for this publication was done while at MITRE.*

FINAL

June 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-45, Natl. Inst. Stand. Technol. Spec. Publ. 1800-45, 43 pages, (DATE), CODEN: NSPUE2

NIST TECHNICAL SERIES POLICIES

AUTHOR ORCID IDS

CheeYee Tang: 0009-0000-2847-1443
Jeffrey Marron: 0000-0002-7871-683X
Stephanie Saravia: 0009-0006-5907-4380
Bob Stea: 0009-0000-0514-7085
John Wiltberger: 0000-0002-6412-8105

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

The Water and Wastewater Systems (WWS) sector plays an important role in our national critical infrastructure. It is important that these utilities are equipped with resources to help them address and reduce their cybersecurity risks. Through the *Cybersecurity for the Water and Wastewater Sector* project [1], the NIST National Cybersecurity Center of Excellence (NCCoE) has built and demonstrated secure remote access architectures for operational technology in the water and wastewater sector using commercially available technologies. Developed in collaboration with technology vendors, water utilities, and other experts, this project produced three representative examples for implementing secure remote access for water utilities of different capacities. Each example outlines the architecture and configuration details of the solution.

KEYWORDS

Remote access; secure communication; multi-factor authentication.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

- ABB Energy Industries: Patrik Boo
- Association of State Drinking Water Administrators (ASDWA): Anthony DeRosa
- Bedrock Systems: John Walsh
- Cisco: Colin Dupreay, Kori Rongey, Jason Salmons
- Cyber 2.0: Erez Kaplan, Guy Tessler
- Denver Water: Mark Thomas
- Dragos: Elan Alvey, Dawn Capelli, Joshua Carlson
- I&C Secure: Augustin Serino
- MITRE: Don Faatz*, Philip Fenimore*, Malaya Moon*, Andrew Passie*
- NIST: Juilie Anne Chua, Michael Pease, Cherilyn Pascoe, Keith Stouffer,
- Q-Net Security: Rick Arturo, Ray Indeck, John Pyrovolakis
- Radiflow: TJ Roe

- StrongDM: Ryan Edwards, Hermann Hesse, Shane Stephens*
- TDI Technologies: Ray Erlinger, Pam Johnson, Kyle Hussey, Clyde Poole
- Washington Suburban Sanitary Commission (WSSC): Nick Selock
- West Yost: Andrew Ohrt, Jeremy Smith

** Former employee; all work for this publication was done while at that organization*

Special thanks to all who reviewed and provided feedback on this document.

The Technology Collaborators who participated in this project submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Collaborators		
Association of State Drinking Water Administrators (ASDWA)	Dragos	West Yost & Associates
Bedrock Systems	I&C Secure	Washington Suburban Sanitary Commission (WSSC)
Cisco	Q-Net Security	
Cyber 2.0	StrongDM	
Denver Water	TDI Technologies	

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

PATENT DISCLOSURE NOTICE

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Contents

List of Figures

List of Tables

Executive Summary

The Water and Wastewater Systems (WWS) sector is one of the 16 designated U.S. Critical Infrastructure sectors and plays an important role in supplying clean water to our communities and removing harmful materials from wastewater. The WWS sector is undergoing a digital transformation, increasing its dependence on connectivity to systems that, for instance, monitor pumping stations, evaluate water quality, or analyze data to support more efficient operations and improve service. This increased reliance on an internet-connected ecosystem, however, increases the risk of introducing vulnerabilities into a water or wastewater utility's systems and networks that malicious actors can exploit. It is important that water utilities are equipped with resources to help them address and mitigate their cybersecurity risks.

The NCCoE project, "Cybersecurity for the Water and Wastewater Sector," is intended to collaborate with industry, utilities, and technology providers to demonstrate practical solutions for the water and wastewater utilities of all sizes to mitigate cybersecurity risks. This publication describes a high-level architecture and provides three reference designs that demonstrate secure remote access solutions using commercially available technologies. These implementations were built and integrated in the NCCoE lab environment to reduce adoption risk for organizations looking to deploy similar capabilities.

1 Introduction

As described in the preceding NIST NCCoE project description, "A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems" [1], the NCCoE has undertaken a project to identify common cybersecurity challenges among WWS sector participants, develop reference cybersecurity architectures, and propose the utilization of existing commercially available products to mitigate and manage risks. Through collaboration with stakeholders, the NCCoE identified several priority cybersecurity challenges, including remote access, network segmentation, asset management, and data integrity. This publication focuses specifically on secure remote access, which stakeholders identified as an immediate and high-priority need. Four technical areas were identified as priorities for the sector, as follows:

1. Remote Access – ensure security safeguards are configured to control access based on roles or responsibilities; collect, aggregate, and analyze log information.
2. Network Segmentation – demonstrate commercially available products for logical partitions of the operational network, such as firewalls, data diodes, unidirectional gateways, or software-defined networks (SDN).
3. Asset management – discover, identify, categorize, and manage all network-enabled devices: detect potential risks and validate patches and upgrades.
4. Data Integrity – protect the integrity of data by detecting a lack of protection, providing secure communications, sandboxing techniques, and methods to prevent software modifications.

This Special Publication addresses remote access scenarios and describes architectures and example solutions allowing authorized access to the Operational Technology (OT) assets of a WWS system. The reference cybersecurity architectures found in Figure 2-1 can be voluntarily adopted by WWS utilities as

a starting point for utilizing commercially available technologies, existing standards, and best practices to improve their remote access security. The other three priority areas listed above may be considered under subsequent NCCoE projects, which will generally address cybersecurity in OT environments.

1.1 Audience

The architectures introduced in this publication aim to offer solutions suitable for a broad range of WWS sizes, environments, complexities, resource constraints, and operational needs. This publication is intended for WWS sector operators; however, the concepts are generally relevant to any operator of operational technology.

1.2 Purpose and Scope

The purpose of this document is to provide guidelines for establishing secure remote access to WWS environments. Except for the Safety Considerations described in Section 3.1, it assumes that organizations already have a remote access implementation and intend to explore options to improve its security. Since the range of challenges and solutions related to securing remote access continues to expand, this material should be viewed as additional guidelines to secure organizations' networked environments.

The scope of the document includes (a) an overview of remote access, (b) a set of typical network topologies, and (c) three example implementations using commercially available solutions. The implementations provided should be seen as a starting point for understanding representative examples that may apply across a range of typical system configurations. Also, the implementations do not attempt to identify the entire range of challenges and solutions associated with remote access but instead describe possible solutions for common challenges. Your organization's infrastructure and security experts will identify solutions that best integrate with your existing OT assets within the WWS environment.

1.3 How to Use This Guide

This publication contains five sections and three appendices, as follows:

- Section 1 provides context for the project scenarios, identifies the publication's intended audience, and lists the project's purpose and scope.
- Section 2 provides background on the WWS sector and system characteristics for a range of utility sizes.
- Section 3 introduces the concept of remote access and presents product-agnostic remote access architectures.
- Section 4 describes proposed example solution implementations.
- Section 5 provides a summary.
- Appendix A provides a list of Acronyms.
- Appendix B provides a list of References.
- Appendix C provides a Glossary of Terms.

2 Background

The U.S. WWS sector is undergoing a digital transformation, and many sector organizations are leveraging data-enabled capabilities to improve utility management, operations, and service delivery [2]. The ongoing adoption of automation, sensors, data collection, network devices, and analytic software increases cybersecurity-related vulnerabilities and associated risks.

2.1 General Sector Characteristics

According to the Environmental Protection Agency (EPA), Public Water Systems (PWS) are characterized by the size of population and duration of service time over the course of a year [3]. Community Water Systems (CWS) are a subset of PWS that supply water to the same population year-round [4]. Table 1 categorizes CWS by population [5], ranging from fewer than 25 customers to those serving over 100,000 customers. While these systems perform similar functions and face similar cybersecurity challenges, the implementation of remote access technologies may differ across the range of system sizes due to factors such as scale, cost, or level of technical capabilities. This paper presents several architectures that offer practical remote access to address requirements for organizations of various sizes and capabilities.

Table 1. Size Categories of US Community Water Systems in 2024

System Size (Population Served)	Number of Systems	% of All Systems	Populations (millions)	% of Population
Very Small (25-500)	26,897	54.1%	4.6	1.4%
Small (501-3,300)	13,321	26.8%	19.2	6.1%
Medium (3,301-10,000)	5,010	10.1%	29.5	9.3%
Large (10,001-100,000))	4,005	8.1%	115.6	36.5%
Very Large (>100,000)	447	0.9%	147.6	46.7%
Totals	49,680	100%	316.4	100%

2.2 Individual System Characteristics

Generally, WWS characteristics tend to correlate with the size of the population served. Larger utilities are typically characterized by extensive watersheds and widely dispersed distribution networks, including possible interconnections to neighboring CWS. These systems require remote water sourcing, pumping, treatment, storage, and pressurized distribution systems. Technologies providing efficient monitoring and control (e.g., complex Supervisory Control and Data Acquisition [SCADA]) networks are required to support wide-area infrastructures. These systems are referred to as “higher-capacity systems" [6].

On the other hand, smaller WWS utilities, which comprise the majority of CWS in the U.S., may exhibit a few key differences impacting remote access utilization. Many smaller utilities do not have the spatial expanse of large systems with water sources closer to their treatment facilities. Their distribution networks may consist of elevated storage and gravity-fed networks to homes and businesses requiring less remote pumping. These types of systems are referred to as "lower-capacity systems" [6].

Table 2 summarizes these generalized system technology characteristics relative to system capacity and the size of the population served.

Table 2. WWS Size-Related Characteristics

Characteristics	Higher-Capacity WWS	Lower-Capacity WWS
SCADA	Utilize complex SCADA networks supporting many controls such as sensors, meters, actuators, including Programmable Logic Controller and Human Machine Interface capabilities for operators to manage remote operations.	May have simple SCADA capabilities with few sensors, data points, and alarms. Some systems may have no SCADA capabilities and operate entirely with manual controls.
Complexity	May have advanced treatment systems, sophisticated sensors, data collection, and alarms. These are supported by state-of-the-art capabilities such as real-time monitoring and predictive analytics.	May have lower complexity in all aspects of the WWS, OT, treatment, distribution technologies, and supporting network infrastructure.
OT Hardware	May have a wide array of OT infrastructure requiring support from multiple vendors and third-party management arrangements, utilizing remote access for maintenance, and updates of specialized SCADA components.	May have OT hardware that, while fully functional, lacks cybersecurity protection capabilities. Replacement may be necessary to add cybersecurity capabilities.
Staffing	May have staff dedicated to different aspects of the system including SCADA and IT specialists responsible for implementing cybersecurity safeguards.	May have limited personnel that are responsible for a wide range of duties.
Economic Constraints	May maintain budgets for IT and OT infrastructure. Elements of this infrastructure may be integrated into a larger municipal network. Additional requirements for cybersecurity safeguards may be challenging.	May have very limited financial resources to support upgrades.

The architectures in this publication, namely the Generalized System Model (Section 2.3) and the Remote Access Architectures (Section 3.3), have been developed to address the range of factors

previously mentioned. For Remote Access Architectures, the three examples listed in Section 4 require different levels of resources to configure and maintain. Lower-capacity utilities may prefer to leverage remote access infrastructure that is managed by third-party vendors (e.g., the Cloud), while larger-capacity systems may have the resources for in-house implementations. The proposed models and architectures shown in the following sections may include other design elements intended solely for illustration. The focus is on the equipment required for secure remote access.

2.3 Generalized System Model

This section proposes a simplified reference architecture as a model to develop the project scenarios. On a broad scale, a WWS utility can be typified by the generalized system model shown in Figure 2-1.

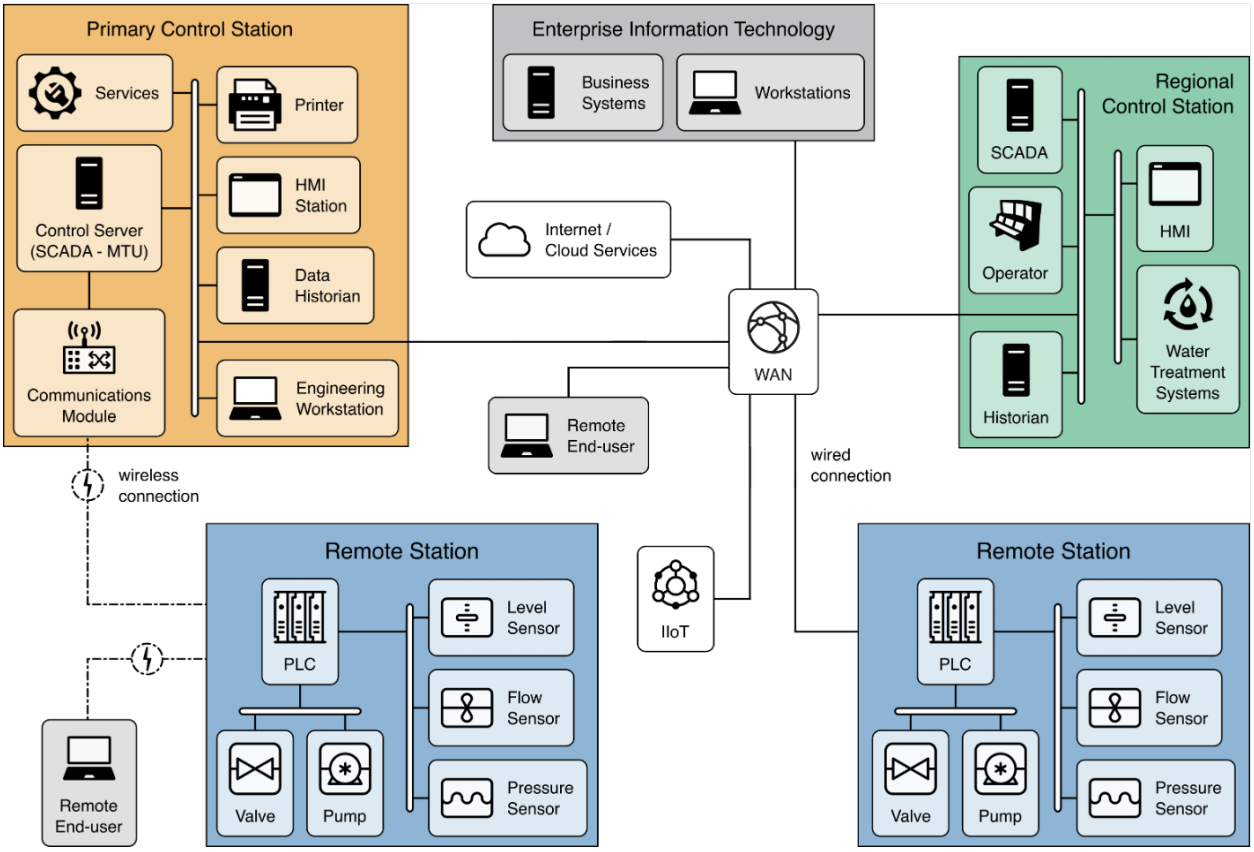

Figure 2-1 Generalized WWS System Architectural Model

As shown in Figure 2-1, a WWS utility generally consists of the following components:

- **Primary Control Station:** A centralized control station for operating water or wastewater treatment plant(s) with remote access to other control stations, remote stations, and business information systems.
- **Regional Control Station:** Larger utilities may have secondary control stations for monitoring and controlling multiple treatment plants. A secondary control station enables control over a service area. OT network infrastructure located in a service area or at localized treatment centers can include servers, SCADA systems, human-machine interfaces (HMIs), and programmable logic controllers (PLCs), with process control data and sensor readings.

- **Remote Stations:** Use wireless or wired telemetry to monitor remote infrastructure such as pump stations and water distribution networks that feed data back to SCADA servers and operators.
- **Various Locations/Stations:** Additionally, PLCs and controls are distributed among the network and pump stations, with sensors to enable logging of metrics such as pressure, temperature, and physical-chemical characteristics.

In this diagram, the WWS utility operates a treatment facility at a Regional Control Station, with several remote sub-facilities depending on the utility's geographic requirements. The SCADA control server in the Primary Control Station can connect to the Regional Control Station and Remote Stations via the externally managed communication networks using remote access capabilities. Secure communication and physical/logical separation among the clusters of connected devices is provided by a combination of security controls applied to remote access and network segmentation.

3 Remote Access

Remote access refers to the connection into an organizational system or asset by a user (or a process acting on behalf of a user) communicating through an external network [7]. In WWS utilities, remote access is the primary method for connecting to operational controls and SCADA systems from people and systems outside the organizationally managed infrastructure, as shown in Figure 3-1.

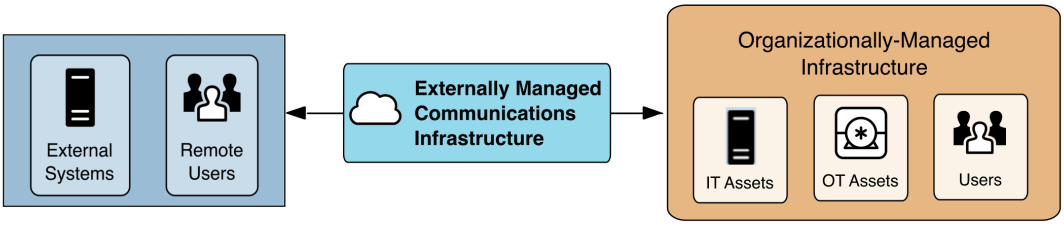

Figure 3-1 Remote Access Concept

There are two types of remote access demonstrations: interactive remote access and system-to-system remote access for process communication [8]. Interactive remote access is user-initiated access by a person outside of the organizationally managed infrastructure. That user could be an employee, vendor, contractor, or consultant authorized to access the organizationally managed infrastructure. System-to-system remote access is a cyber asset (or group of assets) communicating to another cyber asset (or group of assets) owned by the organization, passing through externally managed infrastructure to facilitate communication across long distances. One example of system-to-system remote access would be a PLC at one pumping station communicating with a PLC at another pumping station using telecom infrastructure.

3.1 Safety Considerations

Over the past several decades, some utilities have transitioned from on-site manual operations to on-site automated operations and now to remote operations. Each of these modes of operation comes with benefits and risks. For example, allowing remote access to independent safety systems increases the attack surface for malicious cyber actors to not only control the process but also create unsafe conditions. In safety applications, layers of protection analysis should consider the risk of remote access before implementing the technology.

There are several alternatives to remote access that utilities may consider. For example, remote alarming systems are a way to notify remote employees. If these remote-alarming systems are implemented using one-way communication, the attack surface is limited. Some facilities may choose to operate on-site only, requiring employees and contractors to come on-site to perform all operational tasks.

These are all risk-based decisions that each water utility must determine based on its own situation. This publication assumes that the utility has evaluated the risk and is proceeding with two-way remote access.

3.2 Primer - Remote Access Technologies in the WWS Sector

Remote access technologies provide a critical link in supporting infrastructure and operational requirements, including:

- A wide geographic distribution of components and subsystems
- High availability for ongoing operations and off-hour support requirements
- Remote diagnostics and rapid system maintenance
- Third-party vendor access for equipment troubleshooting
- Access to remote or unattended locations for service and incident response
- Convergence with existing IT networks, cloud storage, or Industrial Internet-of-Things environments

However, use of remote access may introduce several potential security challenges [9], such as:

- Increased exposure to cyber threats due to external connections
- Potential for unauthorized access to critical systems
- Risks of malware propagation and exploitation of vulnerabilities

Section 3.3 provides considerations and security outcomes to mitigate these remote access challenges. To further support the alignment of these outcomes with relevant risk guidance, Table 3 also includes a mapping to the NIST Cybersecurity Framework (CSF) 2.0. [10] This mapping provides an understanding of how these considerations fit into the broader security objectives.

3.3 WWS Remote Access Cybersecurity Considerations

Although system architecture and deployment will vary across systems of different sizes and capacities, there is a common list of capabilities needed to provide secure remote access [11]. Remote access necessitates security controls to reduce the risk of malicious cyber actors taking advantage of this access. Many of these security controls, when configured properly, are inherent to the remote access product, while others are procedural controls. If a remote access product does not provide this capability, technologies and processes may be combined to achieve the necessary security. Developed in conjunction with Technology Collaborators, Table 3 lists cybersecurity considerations for WWS systems when implementing remote access.

Table 3. Remote Access Considerations for WWS System

Consideration	Description	NIST CSF 2.0 Subcategory(ies)
Protect confidentiality and integrity of communications over externally managed infrastructure.	Encryption is commonly used for protection when traversing third party network infrastructure, such as internet service providers. If the remote access solution does not offer encryption, another encryption solution such as a Virtual Private Network should be incorporated into the architecture to prevent data from traversing third party infrastructure in clear text.	PR.DS-02: Data-in-transit is protected (confidentiality, integrity, availability) PR.IR-01: Networks and environments are protected from unauthorized logical access and usage

Consideration	Description	NIST CSF 2.0 Subcategory(ies)
Restrict remote access to authorized users or systems only.	Access to operations should only be provided to individuals or systems with predetermined roles and responsibilities required for secure functioning of the process or technology. A process such as identity and access management should be established to ensure only authorized users have access to specific resources via remote access [12].	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization PR.AA-05: Access permissions are defined, managed, enforced, and reviewed, incorporating least privilege
Authenticate all remote users and systems.	The system should establish and manage remote access to include the use of authentication methods to verify the identity of users and systems [7].	PR.AA-03: Users, services, and hardware are authenticated PR.AA-02: Identities are proofed and bound to credentials based on context
Use multi-factor authentication (MFA) for remote access services.	MFA is an accepted best practice for securing remote access to OT applications [7]. The service should be capable of implementing unique usernames and complex passwords with no default credentials. Usernames and passwords should be just one of the multiple factors used for authentication. (Note: Remote access to the OT environment should use MFA, while local access to OT may only require a user ID and password due to other mitigating factors, such as physical access controls before gaining physical access to the area where the user ID and password may be used.)	PR.AA-03: Users, services, and hardware are authenticated (MFA is the key implementation vehicle) PR.AA-01: Identities and credentials are managed (covers credential hygiene: unique IDs, no defaults)
Maintain logs of remote access user and system actions.	Logging should be enabled (where possible). Logging enables an organization to capture and analyze events that occur within its systems and networks [9].	PR.PS-04: Log records are generated and made available for continuous monitoring DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events
Update remote access services regularly.	The remote access solution should contain the latest versions of firmware and software. The utility should regularly monitor for security advisories on the remote access solution. Up-to-date firmware/software should extend to the devices exposed by the remote access solution.	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk
Employ least privileges for remote access.	Users should only be allowed access to the specific assets required for the user's role and scope of work [13].	PR.AA-05: Access permissions incorporate principles of least privilege and separation of duties
Ensure remote access services are terminated at a protected network segment.	Utilizing protected network architectures minimize risks by providing additional restrictions and security measures such as controlling traffic flows, packet inspection, or segmentation using demilitarized zones (DMZ) to ensure remote sessions are safely and securely managed [7].	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.AA-05: Access permissions are enforced at access control points
Implement inventory management.	Clear inventory and labeling of remotely accessible systems should be implemented for quick disconnection in the case of unauthorized use. Demarcation information should be included in an incident response plan.	ID.AM-01: Inventories of hardware managed by the organization are maintained

Consideration	Description	NIST CSF 2.0 Subcategory(ies)
		ID.AM-02: Inventories of software, services, and systems are maintained
Restrict access based on temporal requirements.	Remove remote access when no longer required. Consider implementing automatic timers for removing access or managing change processes to manually confirm the removal of access.	PR.AA-05: Access permissions are managed, enforced, and reviewed (time-bound access and revocation) PR.AA-01: Identities and credentials are managed, including timely revocation
Provide endpoint security for remote access.	End-user devices should provide security capabilities that protect against malware infection, such as antivirus software.	DE.CM-04: Malicious code is detected PR.PS-01: Configuration management practices are established and applied (endpoint hardening/least functionality)
Develop security requirements for third-party remote access in advance.	All conditions for remote access should be addressed in contracts and agreements between utility and remote user employees, vendors, contractors, and consultants.	GV.SC-05: Cybersecurity requirements in supply chains are established and integrated into contracts and agreements with suppliers and third parties GV.SC-07: Risks posed by suppliers and third parties are understood, recorded, assessed, and monitored over the course of the relationship
Utilize change and configuration management.	All devices, equipment, and software associated with remote access should be maintained through strict change control and vulnerability/patch management.	PR.PS-01: Configuration management practices are established and applied PR.PS-02: Software is maintained, replaced, and removed commensurate with risk (vulnerability/patch management)
Coordinate scheduled maintenance and activity.	Ensure that operations personnel are aware of planned or unscheduled remote activity in the OT environment to prevent authorized remote changes from being perceived as adversarial actions.	PR.PS-04: Log records are generated and available (scheduling/coordination artifacts) DE.CM-03: Personnel activity and technology usage are monitored to detect adverse events (distinguishing authorized from adversarial activity)
Restrict access based on operational requirements.	Networks should be configured to restrict inbound and outbound traffic to only what is necessary for operations. This includes disabling unused ports and protocols.	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.PS-01: Configuration management practices are applied (least functionality – disabling unused ports/protocols)

4 Product Agnostic Architectures

This section presents three product-agnostic architectures for securing remote access to an OT environment.

4.1 Secure Remote Access

Figure 4-1 shows a secure remote access architecture that provides the cybersecurity capabilities described in Section 3.3. This "traditional" approach to remote access using firewalls and a remote access server is a commonly used and recommended architecture [12]. The remote access session is terminated in the DMZ, and a separate connection is initiated from the DMZ into the OT environment.

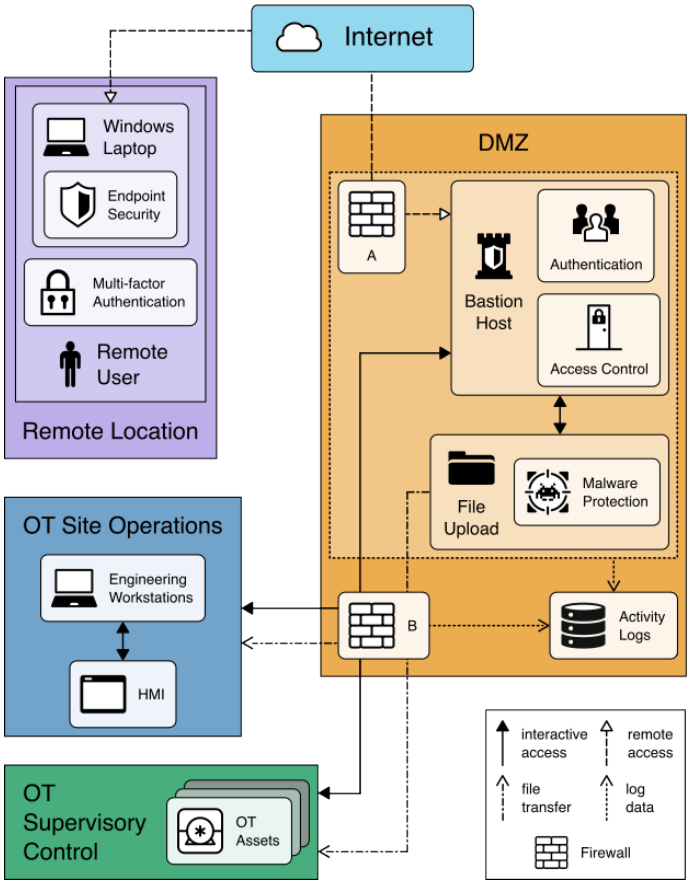

Figure 4-1 Secure Remote Access Architecture

- In this architecture, an MFA capability provides the remote user credentials to authenticate to the remote access server in the DMZ. The end-user device has an endpoint protection capability to prevent infection with malicious software.
- The end-user device connects to a DMZ over an externally managed communications infrastructure such as the Internet. The communications security capability provides confidentiality and integrity protection for data in transit between the end-user device and the DMZ.

- At the DMZ, a pair of firewalls (A and B) control the networks, ports, and protocols which are allowed to enter and exit the DMZ. Within the DMZ the remote access server capability authenticates the remote user and controls the user's access to services and systems in the OT environment. For interactive access, the remote access server can permit connections to engineering workstations, HMIs, and other OT assets such as programmable logic controllers (PLCs).
- A secure file upload capability could exist to receive the files from the remote user, scan the files for malicious content and authorized origin, and make them available for transfer to other assets in the OT environment.
- Each security capability and service in the DMZ records remote user activity to a log which records security relevant information for use in reviewing remote access usage. DMZ System events are also recorded.

4.2 Cloud Based Remote Access

While the approach discussed in 4.1 for remote access is to build and operate remote access-capabilities on site, several vendors offer cloud-based remote access services. These services offload much of the infrastructure management to the service provider in an Infrastructure as a Service (IaaS) model. Cloud-based remote access services may be attractive to a wide range of utilities, and particularly the lower-capacity systems. The utility should verify that the contract or Service Level Agreement with the cloud service provider includes appropriate cybersecurity measures.

A typical cloud architecture can be broken down into three sections: the edge, the network, and the applications. The edge section is where there are any sensors and equipment to collect, pre-process, and communicate data from the field. The network section is where communications are utilized to move data from the edge into a central cloud-based platform that stores, organizes, and manages the collected data. Finally, the application section is where the data can be visualized, analyzed, and processed by end users. This may include any applications that facilitate monitoring, control, and configuration of edge systems and their associated alarming.

Figure 4-2 illustrates the components of a cloud-based remote access architecture for WWS.

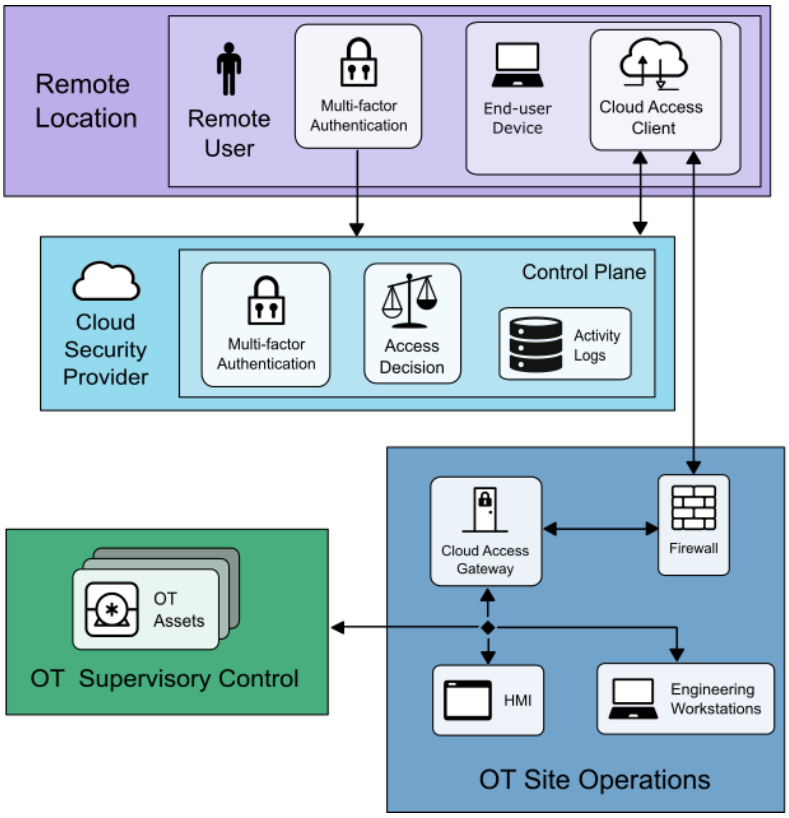

Figure 4-2 Cloud-based Remote Access Architecture

- In this case, the architectural considerations will include a cloud security provider that handles authentication and authorization in the cloud environment, with security gateways and relays within the operational networks.
- A remote user will initiate an authentication request to the cloud security provider using an MFA solution (which may include an Identity Provider) to obtain an access token for their cloud-based user access client.
- This client will then authenticate to the cloud access gateway within the operational network via a secure communications channel.
- This token will assign an access profile to the authenticated user, and the gateway will handle privileges assigned to that role.
- Logging and routing controls are then submitted back to the cloud security provider for storage and analysis.

For a cloud-based remote access architecture, one should recognize the potential security implications of the design. Public clouds may be cost-effective and scalable; however, there may be security concerns with an open cloud system. It is important to consider additional security measures in the contract or SLA, including end-to-end encryption, access control, intrusion detection systems, and vulnerability management.

4.3 System-to-System Remote Access for Process Communication

System-to-system remote access is the automated data exchange of process information between two OT systems through an externally managed infrastructure without direct user interaction. It is used to communicate control or monitoring information between devices such as control systems, sensors, and actuators that are geographically distant, warranting communication through externally managed infrastructure.

Control information may need to be communicated across long distances between SCADA systems such as the central controller and remote terminal units (RTUs). This information should be protected against unauthorized disclosure or modification using security controls such as authentication and encryption.

The implementation of a DMZ, firewalls, and physical security barriers should be determined by requirements or risk assessment. The asset owner should perform a risk assessment to understand the risks in their systems before making any changes. This architecture, as shown in Figure 4-3, is mitigating the risk of unauthorized viewing or manipulation of data between system-to-system communications by using an encryption appliance (EA) as a security control.

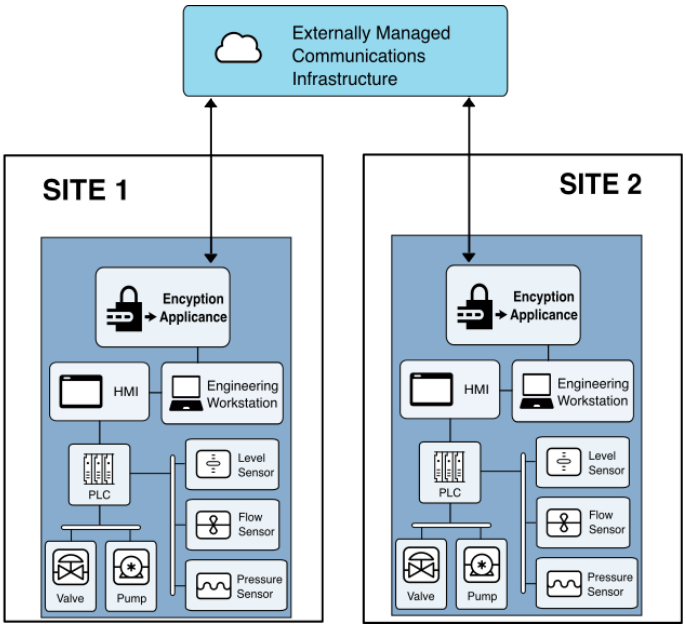

Figure 4-3 System-to-System Remote Access Architecture

- In this architecture, process data (e.g., pump status or pressure indication) from the PLC at Site 1 triggers an input signal to the PLC at Site 2.
- PLCs at Sites 1 and 2 are programmed to send and receive process information using an industrial protocol. This requires configuring tags at both locations with appropriate read/write settings to enable communication.
- Encryption appliances that have previously authenticated with each other are placed at the edge of the process network at each site, ensuring that all process data traveling between Site 1 and Site 2 is encrypted and preventing unauthorized viewing or manipulation of data.
- The EA at Site 1 encrypts the process information before passing it through the appropriate network infrastructure to route the information to Site 2.

- The EA at Site 2 decrypts the process information before passing it to the correct PLC in Site 2.

5 Demonstration Architectures

While the NCCoE used commercial products provided by collaborators to build this example solution, NIST and the NCCoE do not endorse these products. Utilities can select products that offer similar capabilities to build a secure remote access solution. It should be noted that these example implementations only highlight technical steps for demonstration purposes. In addition to the technical solutions, adequate resources (staffing and funding) will be required to ensure proper configuration of the remote access applications. The CRADA collaborators offer a suite of products with many features. The following subsections highlight the features and configurations selected for demonstrations in this project.

5.1 Remote Access using TDI ConsoleWorks

Figure 5-1 illustrates how the NCCoE is using TDI ConsoleWorks to build an example secure remote access solution for WWS based on the architecture shown in Figure 2-1.

TDI ConsoleWorks was used as our remote access management tool, utilizing Role-Based Access Control for ingress to OT resources. In this specific architectural build shown in Figure 5-1, TDI ConsoleWorks offers multiple capabilities that align with the recommended secure remote access considerations found in Section 3.3. Among these, the features highlighted in this build include (but are not limited to):

- MFA
- Logging
- Least privilege through access management

A subset of their features is highlighted below with screenshots taken from the NCCoE lab environment.

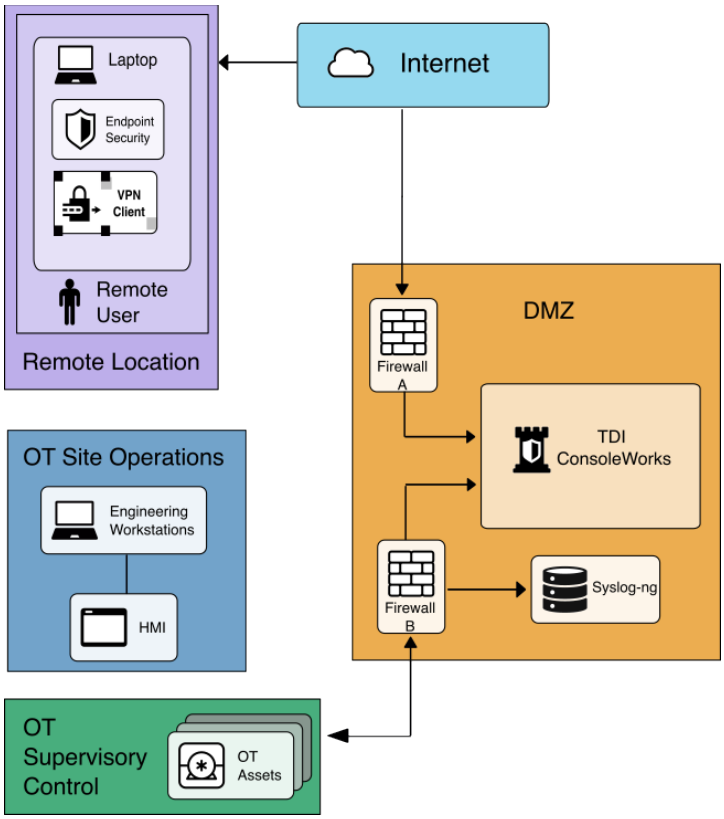

Figure 5-1 TDI ConsoleWorks Example Solution

In this example solution:

- A currently supported and patched laptop initiates the connection to the remote access server. Updated malware protection is included as part of the endpoint security capability.
- TDI Technologies' ConsoleWorks application acts as the remote access server. ConsoleWorks authenticates the remote user, then uses configured roles and permissions to control remote user access to resources in the OT environment.
- Firewall A protects the DMZ by controlling the networks, ports, and protocols that can enter and exit the DMZ. The syslog-ng open-source log manager implements the activity log security capability. If the organization has Security Information and Event Management capabilities, it could be used as a security log collection and analysis capability.
- Figure 5-2 illustrates the ConsoleWorks Administrative Dashboard. Restricted access can be set based on timeframes, roles, or other limitations.

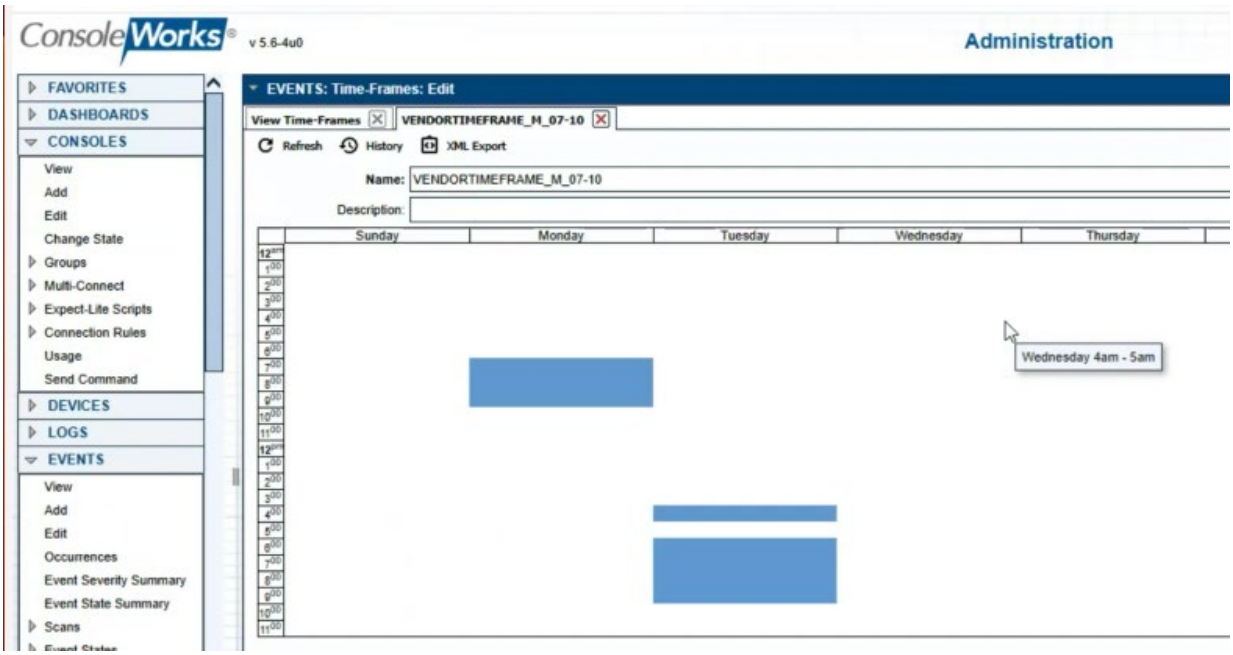

Figure 5-2 Time-Based Access Control with ConsoleWorks

In a typical remote access session:

- Using a Web browser, the remote user connects to TDI ConsoleWorks and authenticates using MFA credentials. Firewall A only allows Hypertext Transfer Protocol Secure (HTTPS) traffic to reach ConsoleWorks.
- Based on defined roles, ConsoleWorks allows remote users to access authorized resources via multiple connection types, as shown in Figure 5-3.

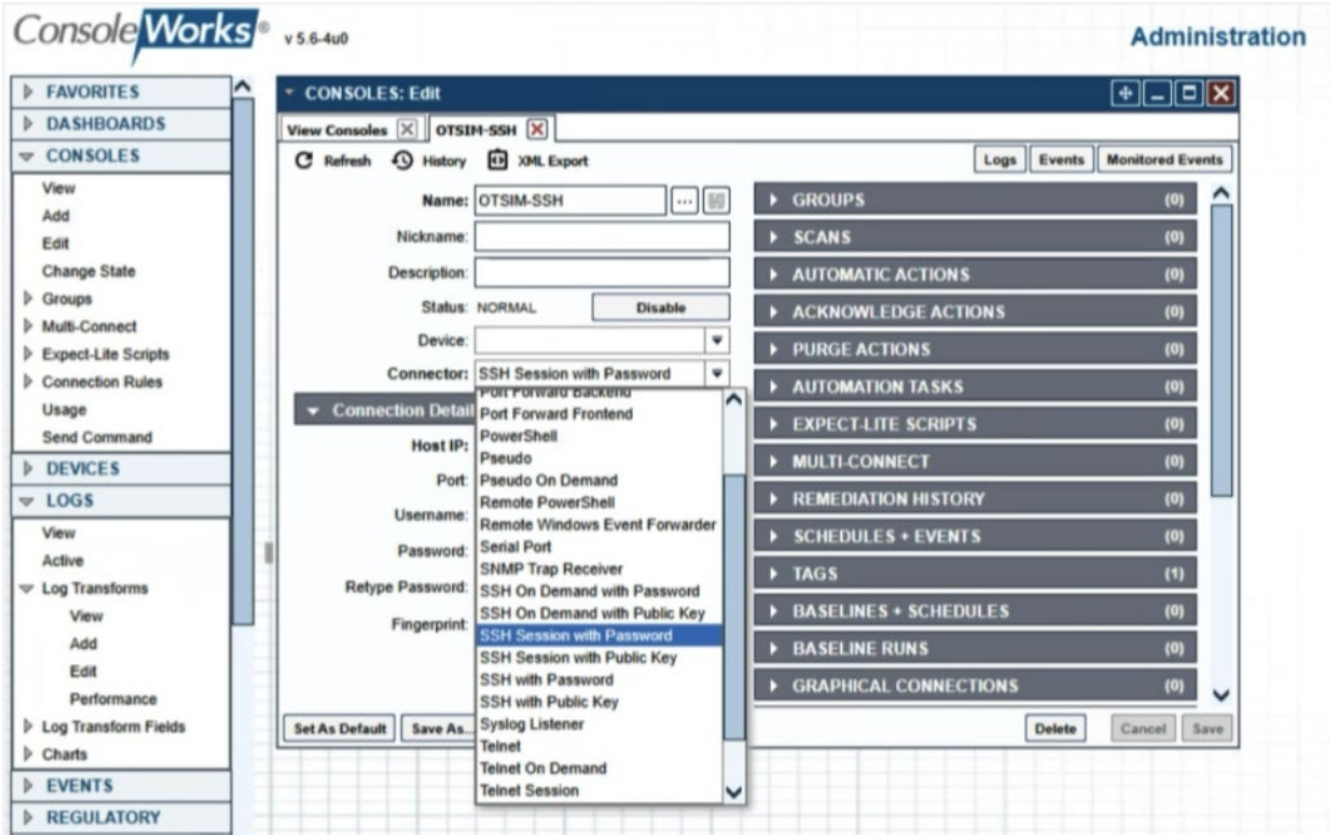

Figure 5-3 Multiple Connection Capabilities for ConsoleWorks

- ConsoleWorks brokers interactive sessions between the remote user and resources in the OT environment. All remote user interactions with ConsoleWorks are via the HTTPS protocol. ConsoleWorks establishes connections to OT resources using appropriate protocols and credentials that ConsoleWorks manages. There are many options for connection type, including Remote Desktop Protocol (RDP) and Secure Shell (SSH).
- Firewall B controls the network traffic between ConsoleWorks and the rest of the OT environment. In this example, the firewall allows an SSH connection to be brokered between ConsoleWorks and a client console.
- Figure 5-4 shows the SSH session being established via the ConsoleWorks interface.

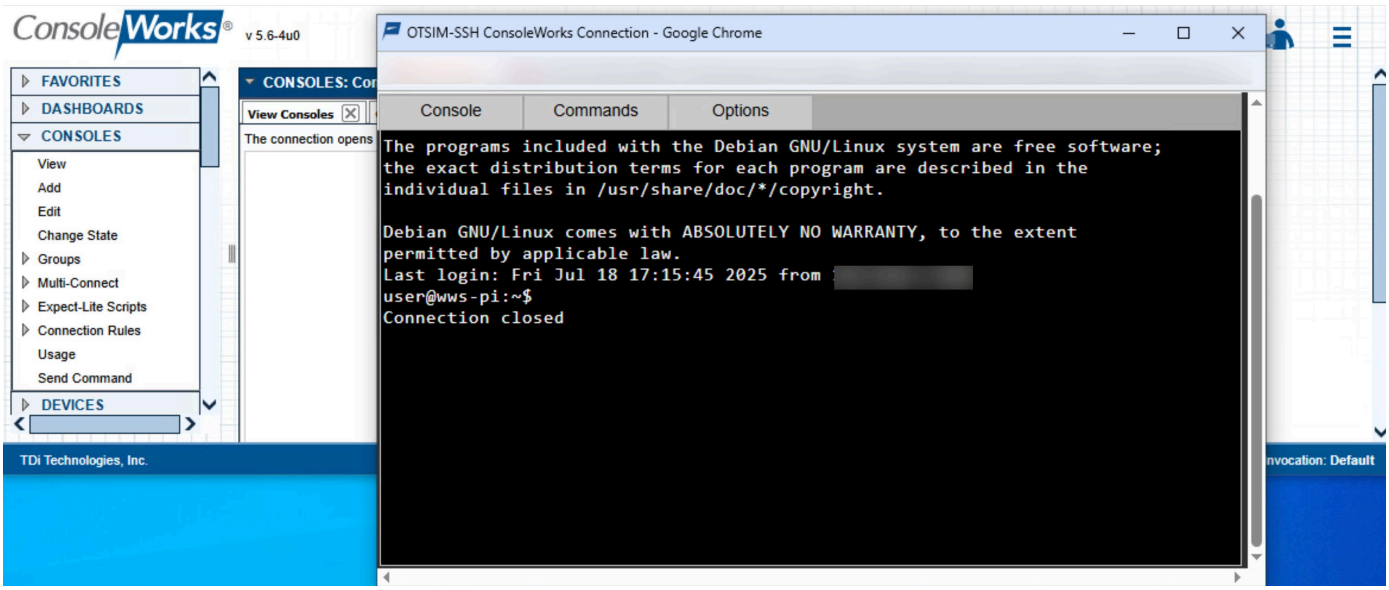

Figure 5-4 SSH Session Using ConsoleWorks Interface

- ConsoleWorks records all remote user actions in local logs, as shown in Figure 5-5. These logs can be exported and reviewed.

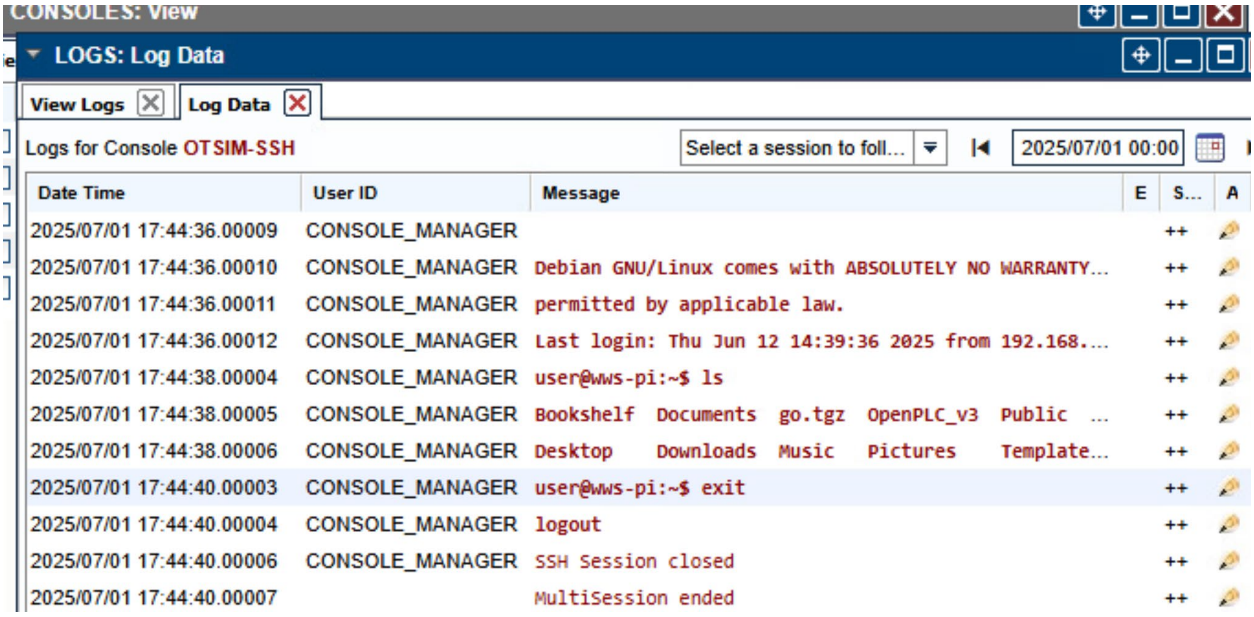

Figure 5-5 Example Log from ConsoleWorks

- Depending on the network access controls and capabilities extended to the remote user, the user can monitor and access the resources in the OT environment with the same level of access as if they were physically located in the SCADA control room.

5.2 Cloud-Based Remote Access Using StrongDM and Cisco Duo

The NCCoE used StrongDM technology as an example demonstration of a cloud-based remote access solution integrated with Cisco's Duo multi-factor solution. The NCCoE has implemented StrongDM's cloud-based remote access solution, as illustrated in Figure 5-6.

StrongDM was used as a cloud-based access management and observability platform. Cisco Duo was the multi-factor authenticator used in this build for identity management and authentication, providing the capability of implementing a combination of unique usernames and password-less authentication to verify users, with adaptive and customizable access policies.

In this specific architectural build shown in Figure 5-6, the combination of StrongDM and Cisco Duo offers multiple capabilities aligning with the secure remote access recommendations described above in Section 3.3, including (but not limited to):

- Identity and access management
- Built-in support for MFA
- Logging and auditing capabilities
- Least privilege restrictions via authorization

A subset of their features is highlighted below with screenshots taken from the NCCoE lab environment.

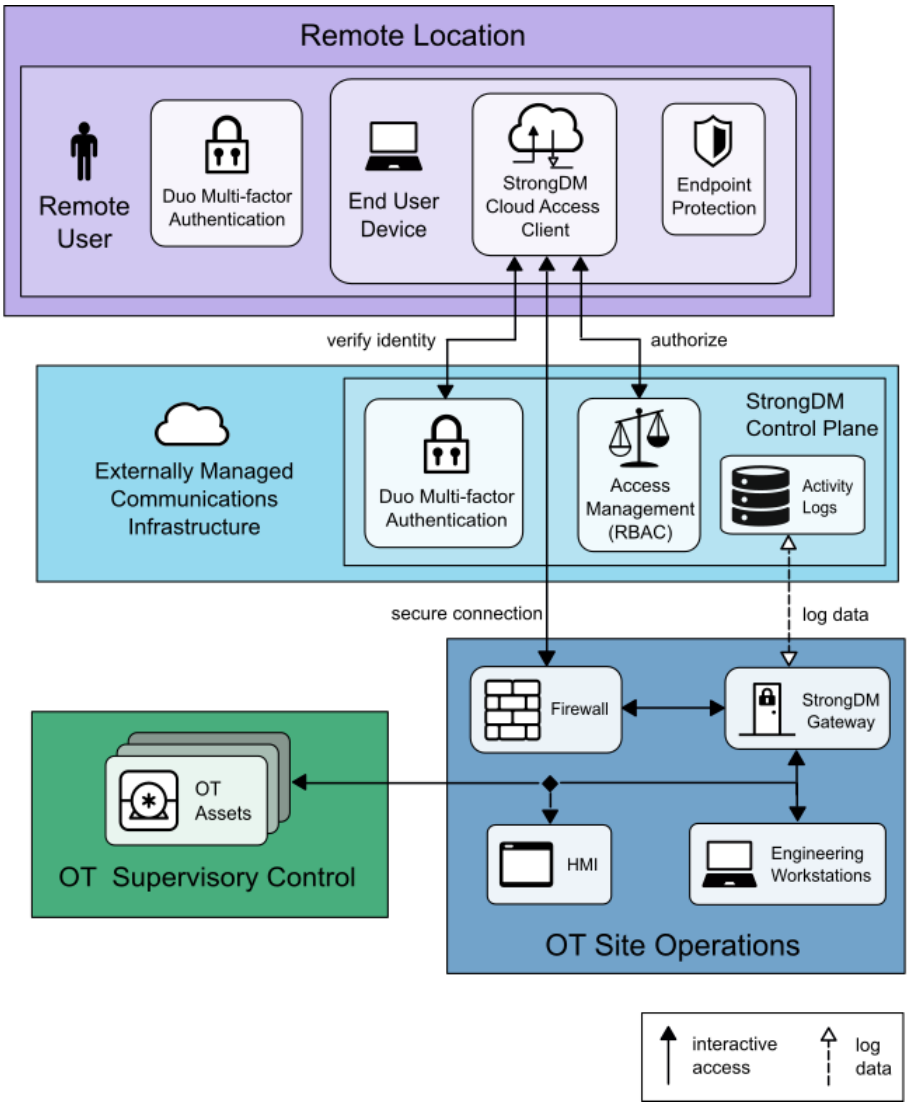

Figure 5-6 StrongDM Example Solution

In this example solution:

- A laptop implements the end-user device with endpoint security capability.
- StrongDM provides communications security through the StrongDM Cloud Access Client, the StrongDM Control Plane, and the StrongDM Gateway. The StrongDM Control Plane provides MFA and access decision-making. The StrongDM Gateway enforces access decisions made by the Control Plane. The StrongDM Control Plane also stores activity log information about all remote user activity.
- StrongDM can be configured to use a variety of MFA solutions. As shown in Figure 5-7, Cisco Duo was used for MFA in this example implementation.

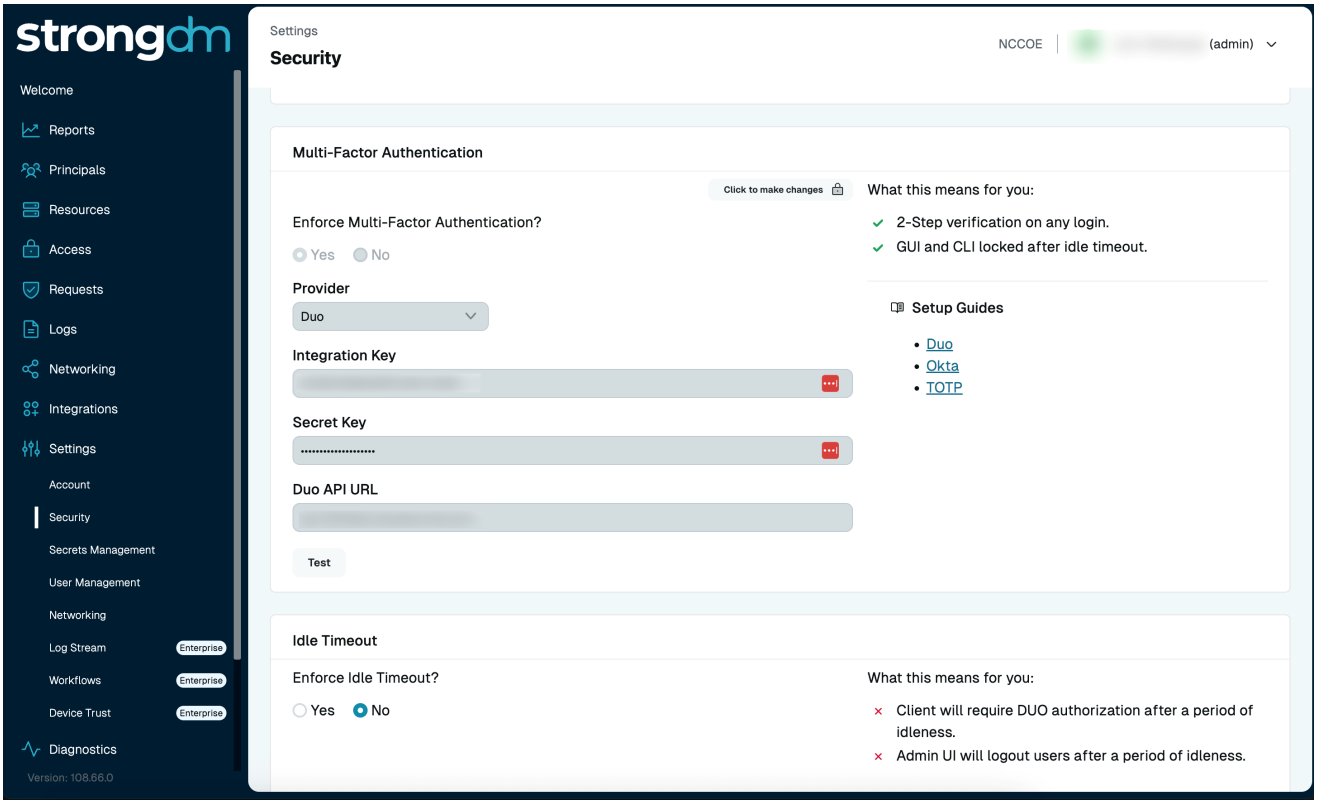

Figure 5-7 Duo Configuration in StrongDM

- The StrongDM Gateway brokers secure, authorized remote connections to internal resources through the client endpoint application.
- The firewall controls the ports and protocols that can access the StrongDM Gateway.
- In a typical remote access session:
    - Using the StrongDM Cloud Access Client, the remote user connects to the cloud-based StrongDM Control Plane and is presented with the login screen displayed in Figure 5-8.

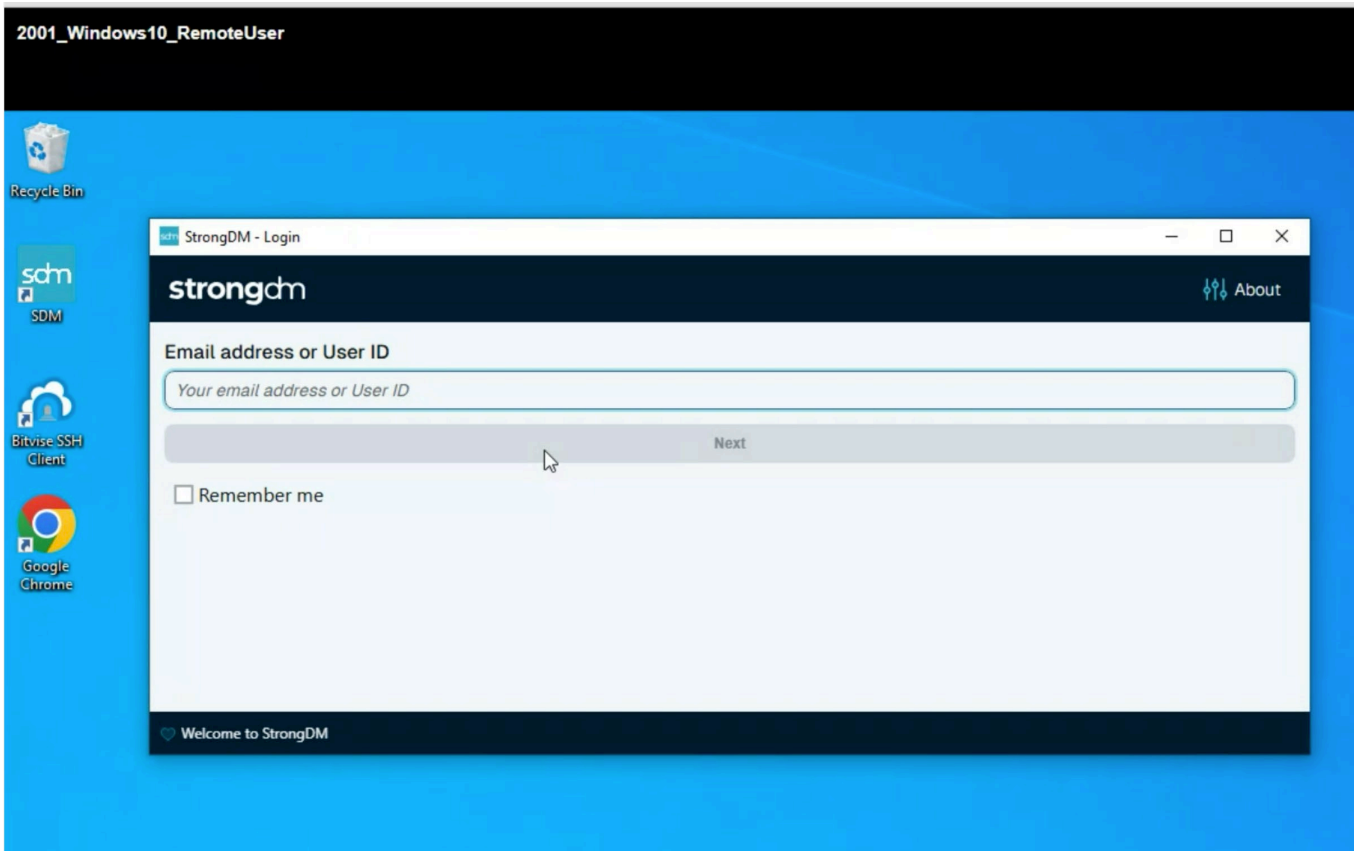

Figure 5-8 Login Screen for StrongDM

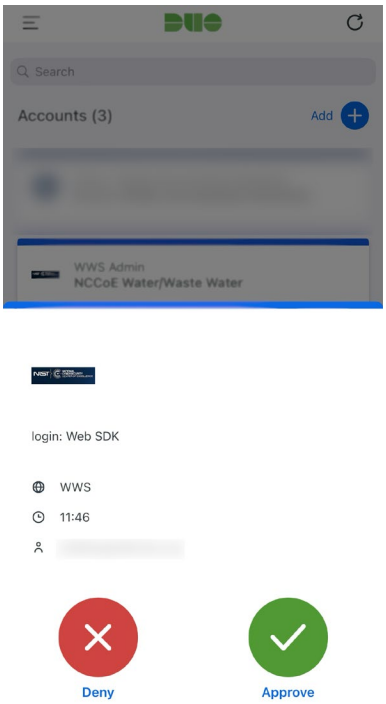

Figure 5-9 Duo Factor of Authentication

- StrongDM integrates with Cisco Duo to offer MFA. This allows for a common platform to be used across the organization for a second factor of authentication, as shown in Figure 5-9.
- The StrongDM Control Plane logs all authentication attempts, successful and unsuccessful.
- In addition, Cisco Duo logs all second-factor activity, shown in Figure 5-10, only after a successful authentication through StrongDM, providing end-to-end visibility of the approved access.

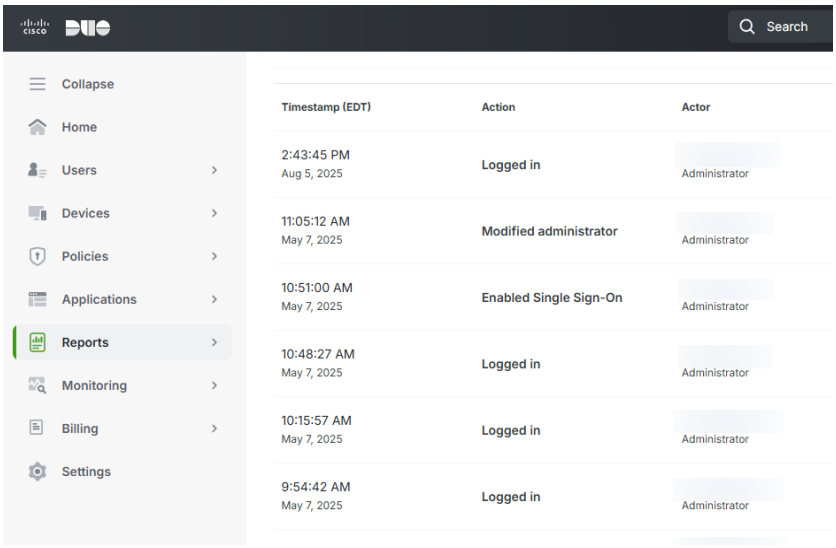

Figure 5-10 Cisco Duo Logs

- Figure 5-11 illustrates the remote user accessing an OT resource by connecting through the StrongDM Gateway and providing the access token received from the Control Plane. The Gateway allows or denies access based on the information in the access token.

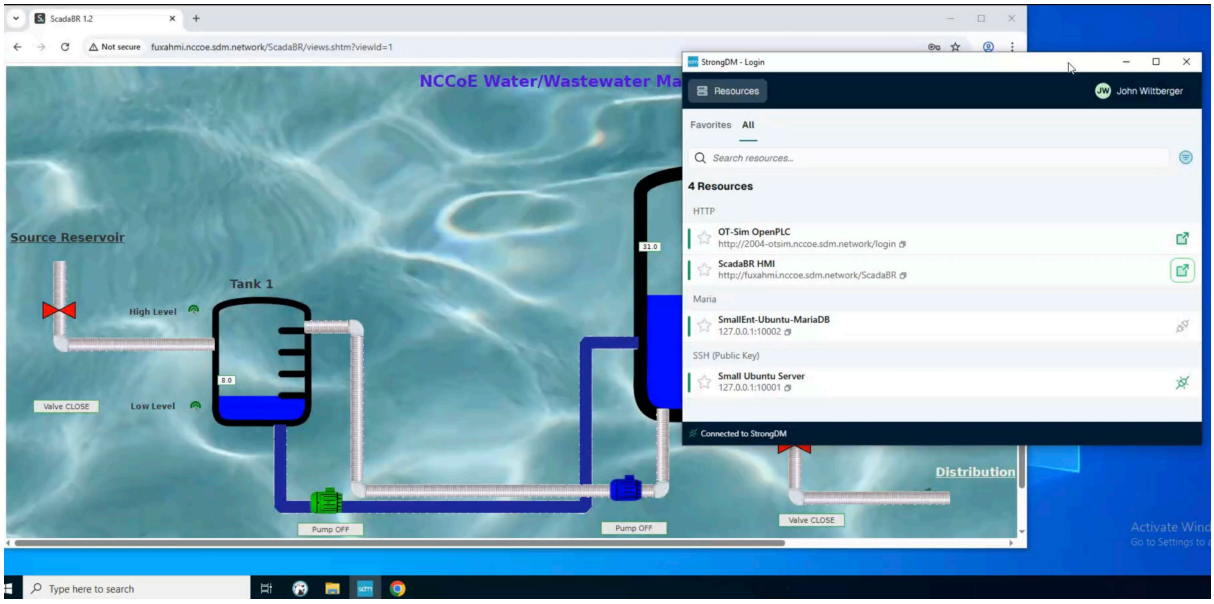

Figure 5-11 StrongDM Used to Access HMI

- Figure 5-12 shows the StrongDM Gateway recording all access attempts, successful and unsuccessful, in an activity log stored in the Control Plane.

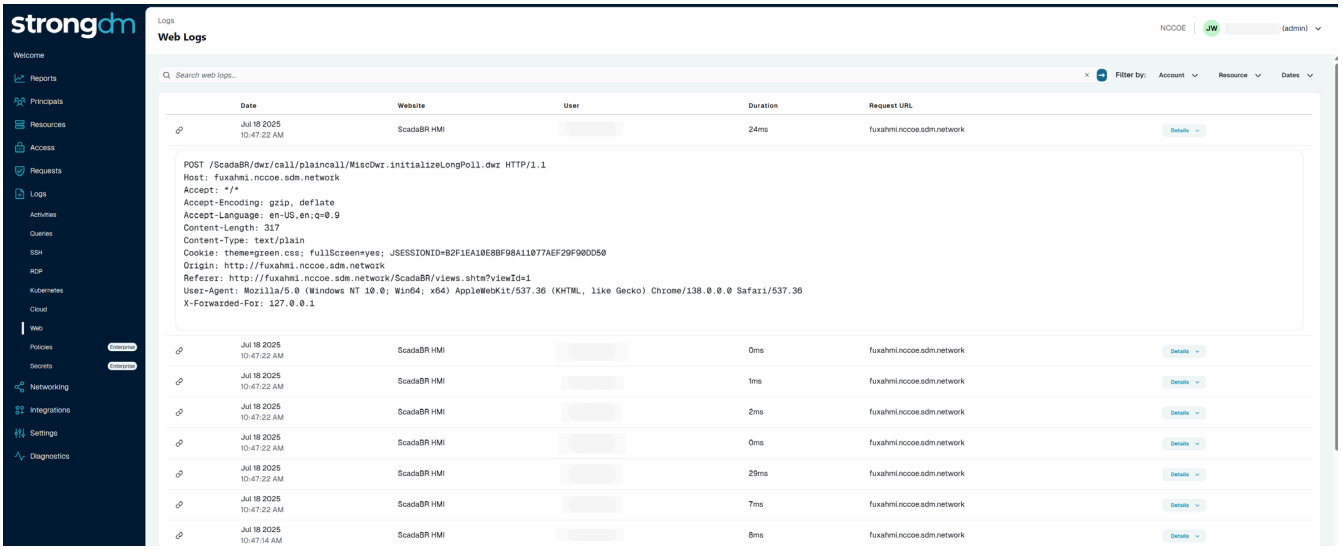

Figure 5-12 StrongDM Logging Capabilities

- Depending on the network access controls and capabilities, the remote user can monitor and access the OT systems as if they were physically located in the SCADA control room.

5.3 System-to-System Remote Access Using Q-Net

Figure 5-13 illustrates how the NCCoE used Q-Net Security products to build an example secure remote access solution for a machine-to-machine configuration within the architecture.

Q-Net was used to demonstrate the protection of data in transit by employing encryption and decryption algorithms between two designated endpoints through their Q-Box devices. The encryption is managed by the organization, independently of the externally managed communications infrastructure. The Q-Box is a hardware device that can be installed to encrypt network traffic using Federal Information Processing Standards (FIPS)-compliant algorithms (based on the Advanced Encryption Standard) that run directly on the hardware. (FIPS information can be found in the reference section [14].) An endpoint, such as an engineering workstation (as shown in Figure 5-13), utilizing a Q-Box will only be able to connect to another endpoint that is also connected to a Q-Box. This arrangement provides confidential communications and restricts network ingress and egress traffic by limiting communications to only the preconfigured and preauthorized Q-Boxes. Before deploying the Q-Boxes to their locations in the architecture, Q-Net defines the allowed communications and the authentication between the Q-Boxes with a Q-Net Policy Manger (QPM) system. This system is used to manage any policies between the systems.

In this specific architectural build, Q-Net was used to implement multiple capabilities that align with the recommended secure remote access guidance found in Section 3.3. Among these, the features highlighted in this build include (but are not limited to):

- Confidentiality and integrity protections via encrypted communications,
- Restricted access to authorized users or systems only,
- Remote access services should route traffic through authorized, managed network access control points.

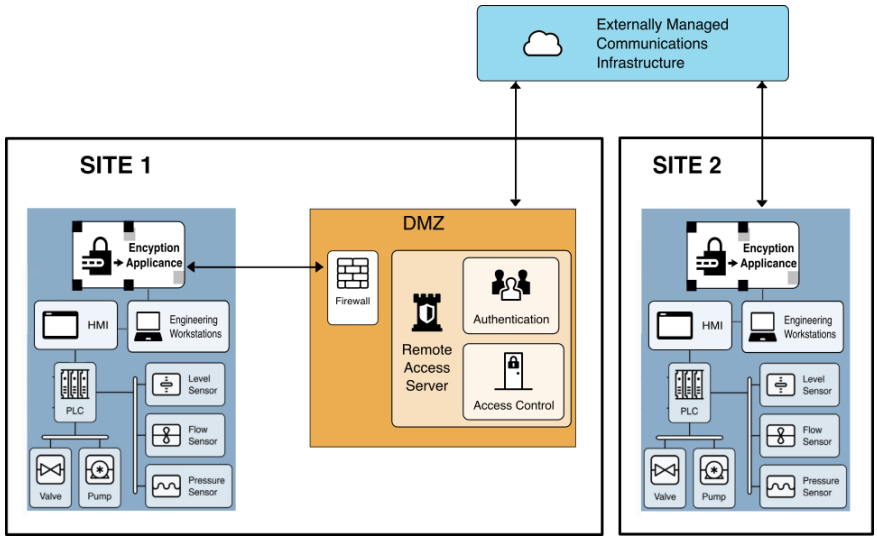

Figure 5-13 Q-Net Example Solution

In this example solution:

Two endpoint PLCs and HMIs located at physically separated sites are connected via two Q-Net Q-boxes. The Q-boxes are communicating via a cryptographic overlay network implemented in hardware.

- Q-Net's cryptographic overlay network, implemented by the Q-Box hardware devices, provides the communications security capability. The Q-Box at Site 1 communicates with the Q-Box at Site 2, establishing an authenticated, encrypted connection.
- Q-Net protects data in transit without the use of external software or hardware.
- A firewall controls access to the QPM ports and protocols.

In a typical remote access session:

- A PLC communicates through the Q-Net cryptographic network using the Q-Box as an encryption appliance.
- The firewall in Site 1 enables only the ports and protocols required by the QPM.
- Once the connection is established, only network traffic coming from the Site 1 Q-Box is authorized to pass through the Site 2 Q-Box to the Site 2 OT network.
- Communication between the two Q-Boxes is encrypted.
- Figure 5-14 illustrates unencrypted Modbus traffic before the Q-Boxes are added to the network. Figure 5-15 demonstrates the benefits of using a Q-Box to encrypt traffic, as seen in the difference in the packet dissection. In Figure 5-14, the top packet shows the Modbus command and data sent across the network. In Figure 5-15, that same traffic is now encrypted, and the data from that packet is indecipherable.

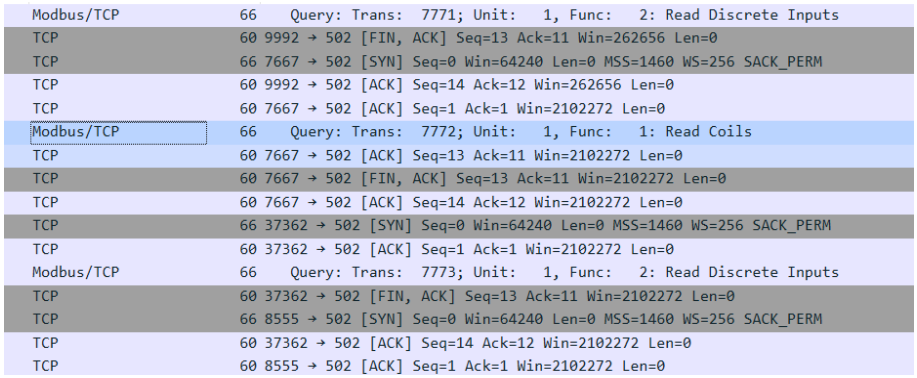

Figure 5-14 Plaintext, Unencrypted Modbus Prior to Installing Q-Boxes

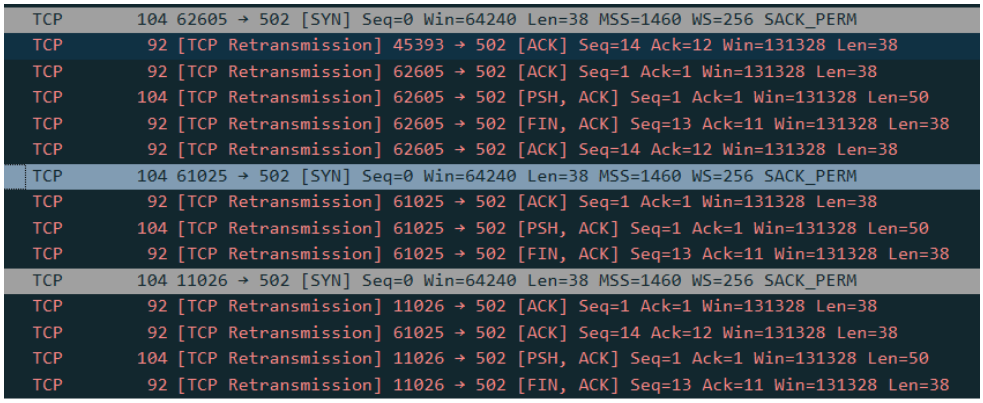

Figure 5-15 Encrypted Modbus after Installing Q-Boxes

Q-Net's capabilities are not limited to machine-to-machine. If a Q-Box is located in a SCADA control room instead of Site 1, then, depending on the network access controls and capabilities extended to the remote user, the user can monitor and access the OT systems from the SCADA control room.

6 Summary

The ability to provide secure remote access to the water systems is crucial to the efficient operation of today's WWS. Through hands-on collaboration with technology companies and utilities, the NCCoE demonstrated how secure remote access to OT environments can be implemented using commercially available technologies. This publication demonstrates three example solution architectures to improve the cybersecurity posture of remote access using commercially available technologies. These example implementations serve as a practical reference for organizations implementing the WWS. Each utility should tailor their cybersecurity practices to address the unique needs of its own organization. The goal is to assist the WWS utilities in ensuring the security and availability of remote access capability so that operations can continue uninterrupted, despite current and evolving threats.

Appendix A List of Acronyms

CRADA	Cooperative Research and Development Agreement
CSF	Cybersecurity Framework
CWS	Community Water System
DMZ	Demilitarized Zone
EA	Encryption Appliance
FIPS	Federal Information Processing Standards
HMI	Human Machine Interface
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
MFA	Multi-factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OT	Operational Technology
PLC	Programmable Logic Controller
PWS	Public Water System
QPM	Q-Net Policy Manager
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication
TLS	Transport Layer Security
WWS	Water and Wastewater Systems

Appendix B References

[1] NIST NCCoE (2023), “Cybersecurity for the Water and Wastewater Sector” https://www.nccoe.nist.gov/sites/default/files/2023-06/securing-water-and-wastewater-utilities-project-description-final.pdf

[2] AWWA (2024), “State of The Water Industry 2024”, https://www.awwa.org/wp-content/uploads/2024-SOTWI-Full-Report.pdf

[3] USEPA Public Water Supply Categories. https://echo.epa.gov/help/drinking-water-qlik-dashboard-help

[4] USEPA, Information about Public Water Systems, https://www.epa.gov/dwreginfo/information-about-public-water-systems

[5] University of Michigan (2024), “U.S. Water Supply Factsheet”https://css.umich.edu/publications/factsheets/water/us-water-supply-and-distribution-factsheet

[6] EPA (2025), "Securing the Future of Water", https://www.epa.gov/system/files/documents/2025-08/water-cybersecurity-recommendations_water-sector-cybersecurity-task-force_apr25-072525.pdf

[7] NIST SP 800-53r5, "Security and Privacy Controls for Information Systems and Organizations", https://doi.org/10.6028/NIST.SP.800-53r5

[8] NERC (2022), "Reliability Standards CIP-005-7", https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-7.pdf

[9] NIST SP 800-82r3, Stouffer KA, Pease M, Tang CY, Zimmerman T, Pillitteri VY, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M (2023) Guide to Operational Technology (OT) Security. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.SP.800-82r3

[10] NIST (2024) “The NIST Cybersecurity Framework (CSF) 2.0”. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[11] CISA, NSA, DoJ, MS-ISAC (2023), “Guide to Securing Remote Access Software” https://www.cisa.gov/sites/default/files/2023-06/Guide%20to%20Securing%20Remote%20Access%20Software_clean%20Final_508c.pdf

[12] Mathezer, Stephen, “Introduction to ICS Security Part 3: Remote Access Best Practices,” The SANS Institute, October 1, 2021, Introduction to ICS Security Part 3 | SANS Institute

[13] CISA (2024), "Modern Approaches to Network Access Security", https://www.cisa.gov/resources-tools/resources/modern-approaches-network-access-security

[14] NIST (2019), " Security Requirements for Cryptographic Modules" https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

Appendix C Glossary

authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS200]

authorization

The right or a permission that is granted to a system entity to access a system resource. [RFC4949]

configuration (of a system or device)

Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections.

data diode

A network appliance or device that allows data to travel only in one direction. Also referred to as a unidirectional gateway, deterministic one-way boundary device, or unidirectional network.

demilitarized zone (DMZ)

An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Network traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.

encryption appliance

A hardware device with the primary function of applying encryption to network traffic.

firewall

An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). [RFC4949]

human-machine interface

The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software. [NISTIR 6859]

industrial control system

General term that encompasses several types of control systems, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as programmable logic controllers. An industrial control system consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). [NIST SP 800-82r3]

industrial internet-of-thing devices

The sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications. May include devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. [NIST SP 800-172]

logs

A record of the events occurring within an organization's systems and networks. [NIST SP 800-92]

malware

Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. [NIST SP 800-53r5]

multi-factor authentication

An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-factor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.

operational technology

A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. [NIST SP 800-82r3]

overlay network

A software-defined networking component included in most orchestrators that can be used to isolate communication between applications that share the same physical network. Additionally, a *cryptographic* overlay network is an overlay network implemented using cryptography.

programmable logic controller

A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode control, communication, arithmetic, and data and file processing. [ISADICT]

protocol

A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [RFC4949]

remote access server

Devices, such as virtual private network gateways and modem servers, that facilitate connections between networks. [NIST SP 800-86]

risk

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. [FIPS200] (adapted)

role-based access control

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

supervisory control and data acquisition

A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. These systems are designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. They are usually shared rather than dedicated.

threat

Any circumstance or event with the potential to adversely impact agency operations (including safety, mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [FIPS200]

virtual private network

A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. [RFC4949]