NIST Technical Note
NIST TN 2283 ipd

Cybersecurity for the Water and Wastewater Sector: Build Architecture

Operational Technology Remote Access

Initial Public Draft

CheeYee Tang
Don Faatz
Bob Stea
John Wiltberger
Chalessa White

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2283.ipd

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Technical Note
NIST TN 2283 ipd

Cybersecurity for the Water and Wastewater Sector: Build Architecture

Operational Technology Remote Access

Initial Public Draft

CheeYee Tang
Smart Connected Systems
Communications Technology Laboratory

Don Faatz
Bob Stea
John Wiltberger
Chalessa White
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2283.ipd

June 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

How to Cite this NIST Technical Series Publication
Tang C, Faatz D, Stea B, Wiltberger J, White C (2024) Cybersecurity for the Water and Wastewater Sector: Build Architecture Operational Technology Remote Access. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) 2283 ipd. https://doi.org/10.6028/NIST.TN.2283.ipd

Author ORCID iDs
CheeYee Tang: 0009-0000-2847-1443

Public Comment Period
June 12, 2024 – July 15, 2024

Submit Comments
water_nccoe@nist.gov

Abstract

This Technical Note describes the product-agnostic remote access security architectures and the example solutions the NIST National Cybersecurity Center of Excellence (NCCoE) plans to demonstrate as part of the Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems project. These security architectures were developed in collaboration with technology vendors, water utilities, and other experts. The NCCoE continues to work with these collaborators to develop example solutions that demonstrate how these security architectures can be leveraged to address cybersecurity risks associated with remote access to water and wastewater operational technology systems.

This Technical Note presents a traditional on-premises remote access architecture and two example solutions, one for medium to large water and wastewater systems (WWS) and one for very small to small water and wastewater systems. A cloud-based remote access architecture and example solution are also described.

Keywords

Multi-factor authentication; remote access; secure communication.

Table of Contents

List of Tables

List of Figures

1. Introduction

As described in the preceding NIST NCCoE publication "Cybersecurity for the Water and Wastewater Sector: 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 Water and Wastewater Systems (WWS) sector participants, develop reference cybersecurity architectures, and propose the utilization of existing commercially available products to mitigate and manage risks. The reference cybersecurity architectures outlined in this report can be voluntarily leveraged by water and wastewater utilities to use commercially available technologies and existing standards and best practices to address their cybersecurity risks. Specifically, our work focuses on four areas identified by the United States Cybersecurity and Infrastructure Security Agency (CISA) [2][3] as priority:

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 open-source products for logical partitions of the operational network, such as firewalls, data diodes, or SDN (software defined networks)
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 lack of protections, provide secure communications, sandboxing techniques, and methods to prevent software modifications.

This first guide addresses the remote access scenario and describes architectures and example solutions allowing authorized access to a water or wastewater utility's Operational Technology (OT) assets. Subsequent publications will address the other identified risk scenarios and solutions.

1.1. Audience

The publication is designed for use by those in the water and wastewater systems sector. The architectures presented in this report for water and wastewater utilities are categorized by system size; specifically, from very small to small (25-3,300 customers) and the medium to large (3,301 – 100,000 customer) size ranges. This categorization allows the use of appropriate technologies based on assumptions of system complexity, budgetary constraint, and operational requirements. This proposed guidance does not offer prescriptive solutions but rather showcases example approaches appropriate within each range of system sizes.

1.2. Collaborators

The NCCoE has assembled a team of collaborators who provide products and expertise in formulating remote access architectures and building example solutions. Table 1 lists the

cybersecurity product vendors, water and wastewater utilities, professional associations, and industry consultants who have volunteered to collaborate on this project.

Table 1. Project Collaborators

Cybersecurity Product Vendors	Water and Wastewater Utilities and Professional Associations	Consultants
StrongDM	Association of State Drinking Water Administrators (ASDWA)	Bedrock Systems
Cisco	Denver Water	I&C Secure
Cyber 2.0	ReWa	West Yost & Associates
Q-net Security	Washington Suburban Sanitary Commission (WSSC)	
TDI Technologies		

The NCCoE is using commercial products provided by our collaborators to build secure remote access example solutions. NIST, the NCCoE, and this guide do not endorse these specific products. Your organization should identify and select products that will best integrate with your existing infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices.

1.2.1. Report Organization

This report contains six sections and two appendices. A brief description of each follows:

- Section 1, this section, provides context for the project scenarios, identifies the report's intended audience, and lists the project's collaborator.
- Section 2 introduces the concept of remote access and provides background on water and wastewater systems for a range of utility sizes.
- Section 3 presents a traditional product-agnostic remote access architecture and describes two proposed example solution implementations of this architecture, one for medium to large WWS and one for very small to small WWS.
- Section 4 presents a product-agnostic cloud-based Software as a Service (SaaS) architecture for remote access and describes an example solution that is scalable from very small to large WWS.
- Section 5 summarizes this technical note.
- Appendix A is a selected bibliography.
- Appendix B provides a glossary of terms.

Your organization can adopt the remote access solutions presented in this technical note or ones that adhere to the guidelines presented here. Your organization may use this guide as a starting point for tailoring and implementing parts of the reference architecture to provide a remote access solution that best meets your needs.

2. Remote Access Background

A remote access solution connects people or systems over an external communications infrastructure to an organizationally-managed communications infrastructure for accessing organization information and operations assets. In WWS utilities, remote access is used as a primary method for connectivity into the operational controls and SCADA system from people and systems outside the WWS operations network.

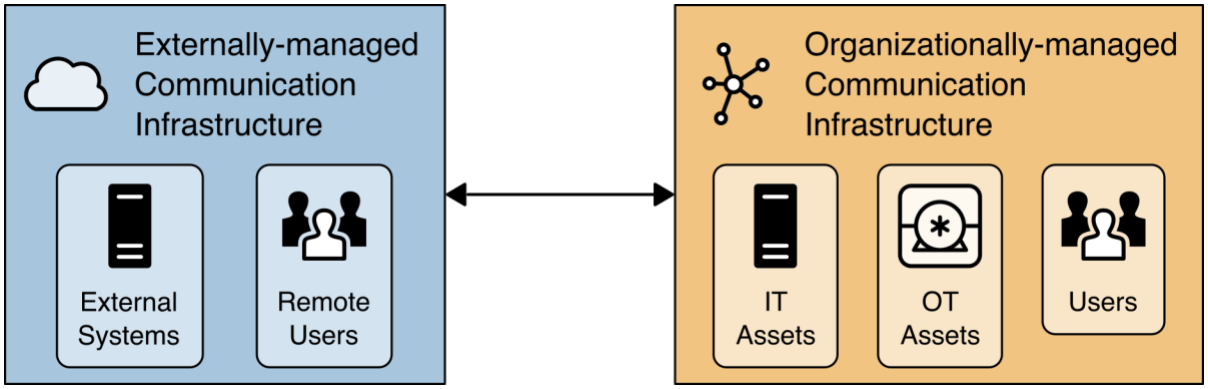


Figure 1. Remote Access Concept

2.1. Remote Access Technologies in the WWS Sector

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

- A widely 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 unmanned locations for service and incident response
- Convergence with existing IT networks, cloud storage, or IIoT environments

However, use of remote access also introduces several potential security problems. NIST SP.800-46r2, “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,” [4], identifies several concerns, including:

- Lack of physical security controls of client-side devices
- Unsecured networks of externally managed communications infrastructure
- Potential for infected devices transferring malware into the utility’s network

The implementation of solutions for secure remote access may also correlate to system size. According to the Environmental Protection Agency, public water systems are characterized by the size of population and duration of service time over the course of a year [5]. According to this categorization, Community Water Systems (CWS) are a subset of public water systems that

supply water to the same population year-round [6]. Table 2 shows a categorization of all CWS by population [7], with sizes varying from less than 25 customers to those serving over 100,000 customers. While these systems perform similar functions and have similar cybersecurity challenges, a solution for remote access in medium or large systems would not be practical for very small and small systems due to scale and cost. This report proposes multiple architectures and solutions to provide practical remote access solutions for systems from very small to large. For simplicity, medium and large systems will be discussed together as one group, and very small and small systems will be discussed as a second group.

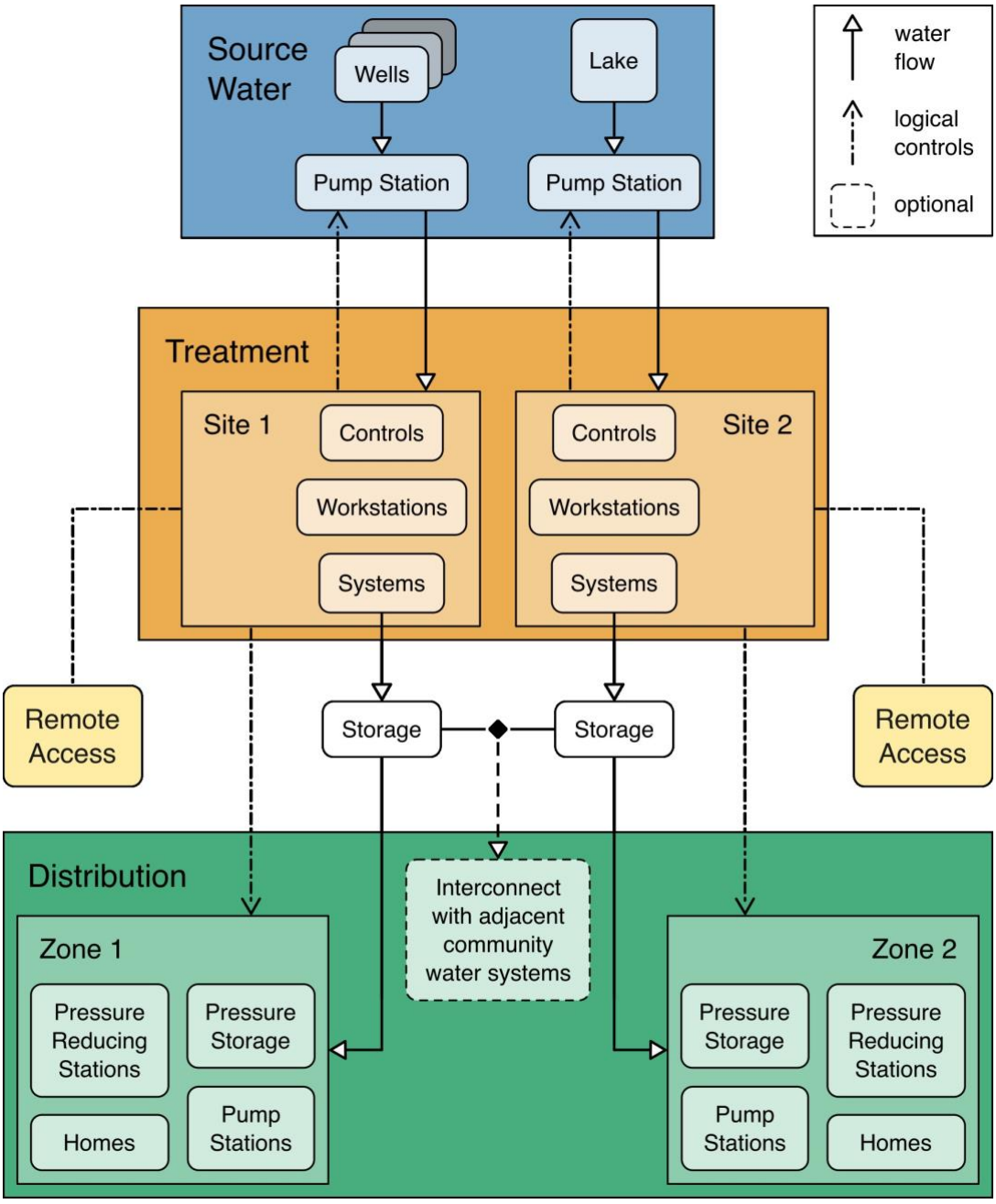
Table 2. Size Categories of US Community Water Systems [8]

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

2.2. Medium to Large WWS

As explained in the previous paragraph, medium to large utilities serve populations of 3,301 to 100,000 people. Figure 2 illustrates basic elements found in many medium to large water systems. These utilities are typically characterized by larger watersheds and widely dispersed distribution networks, including possible interconnection to neighboring community water systems. These systems require remote water sourcing, pumping, treatment, storage, and pressurized distribution systems. Technologies providing efficient monitoring and control are required to support this wide-area infrastructure. Other potential characteristics may include:

- High-capacity systems with complex SCADA networks
- Advanced treatment, sophisticated sensors, data collection, and alarms
- State-of-the-art capabilities, such as real-time monitoring and predictive analytics
- Dedicated staffing for different aspects of the system
- High maintenance costs and dedicated resources
- Multiple vendors and third-party management arrangements, requiring remote access for maintenance and updates of specialized SCADA components
- Integration with municipal IT networks to store and process data
- Vendor provided subsystems, or "skid systems", which are a modularized set of components to provide a specific function (such as a membrane filtration skid or a UV disinfection skid)



171 **Figure 2. Components of a medium to large water system**

172 **2.3. Very Small to Small WWS**

173 Very small to small water and wastewater utilities serve populations of 25 to 3,300 people. Very
174 small to small water systems comprise around 80% of community water systems in the U.S.
175 Figure 3 illustrates the typical components of a very small to small water system.

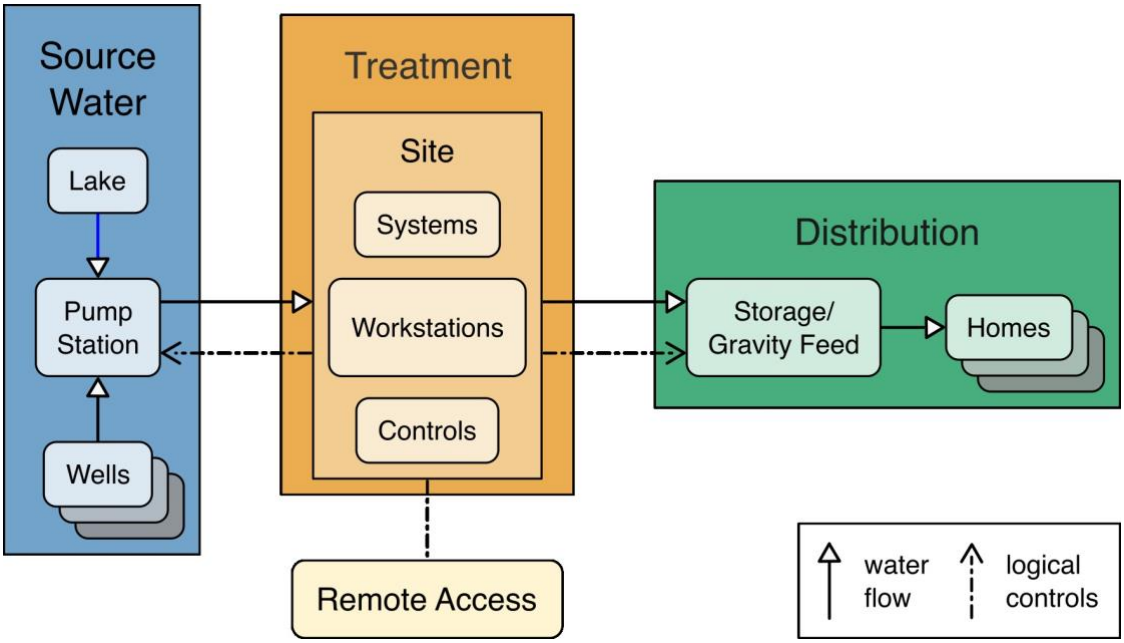


Figure 3. Components of a very small to small water system.

While systems in this category share many similarities to larger ones, a few key differences impact remote access utilization. Most smaller utilities do not have the spatial expanse of large systems. They often have source points in closer proximity to their treatment facilities, water distribution with elevated storage and gravity-fed networks to homes and businesses, and less remote pumping requirements. Other characteristics are:

- Simpler (or even no) SCADA with fewer sensors, data points, and alarms, or completely manual controls
- Lower complexity in technology, both in infrastructure (treatment and distribution) and supporting network architecture
- Existing OT hardware that may lack compatibility with required cybersecurity protections or security upgrades, the costs of which may be difficult to justify
- Staffing challenges, where personnel may be responsible for a wide range of duties
- General economic constraints with proportionately less to spend on upgrades

2.4. WWS Characteristics Comparison

To determine the appropriate types of technical solutions relative to system categories, the NCCoE consulted with its team of collaborators to develop a comparative list of characteristics among water and wastewater utilities of different sizes. This comparison has also been informed by site visits to determine context and capabilities of small and large utilities. Table 3 is a summary of these findings, organized by either very small to small systems versus medium to large systems.

Table 3. WWS Characteristics

Characteristics	Medium-Large WWS	Very Small-Small WWS
SCADA	May have high-capacity systems with 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, or skid system vendor provided control panels	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, or skid system vendor provided control panels. These are supported by state-of-art capabilities, such as real-time monitoring and predictive analytics.	May have lower complexity in all aspects of the WWS, OT, treatment, and 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.

2.5. WWS Remote Access Cybersecurity Considerations

Although system architecture and deployment of different sized systems vary, there is a common list of capabilities needed to provide secure remote access [9]. All remote access architectures should at least provide, but are not limited to, the capabilities that address these security needs:

- End-user devices should provide security capabilities that protect against malware infection
- Communications over externally managed communications infrastructure should have confidentiality and integrity protection
- Remote access to WWS should only be available to authorized users
- Remote access services should authenticate all users connecting to the service

- Remote access services should maintain a log of user actions.
- Remote access services should prevent the introduction of malicious content into the OT environment.
- Remote access should employ the concepts of least privilege and be configured to only allow access to the specific assets required for the user's role and scope of work.
- Recognizing that systems or vendors may install their own (or other third-party) remote access solutions, the utility should ensure that all the aforementioned characteristics are met and properly integrated to meet all required security standards. This will also include considerations for ongoing support, maintenance, updates, and upgrades to address ongoing cybersecurity concerns.

3. Traditional Remote Access Architecture

This section presents a product-agnostic traditional architecture for secure remote access to an OT environment. Two example solutions that implement this architecture are described, one each for medium to large and very small to small WWS.

3.1. Product-Agnostic Remote Access Architecture

Figure 4 shows a traditional on-premises remote access architecture that provides the cybersecurity capabilities described in Section 2.5, WWS Remote Access Cybersecurity Considerations. This architecture uses a "traditional" approach to remote access using firewalls and a bastion host in an OT Demilitarized Zone (DMZ) that is recommended [10][11] and used extensively.

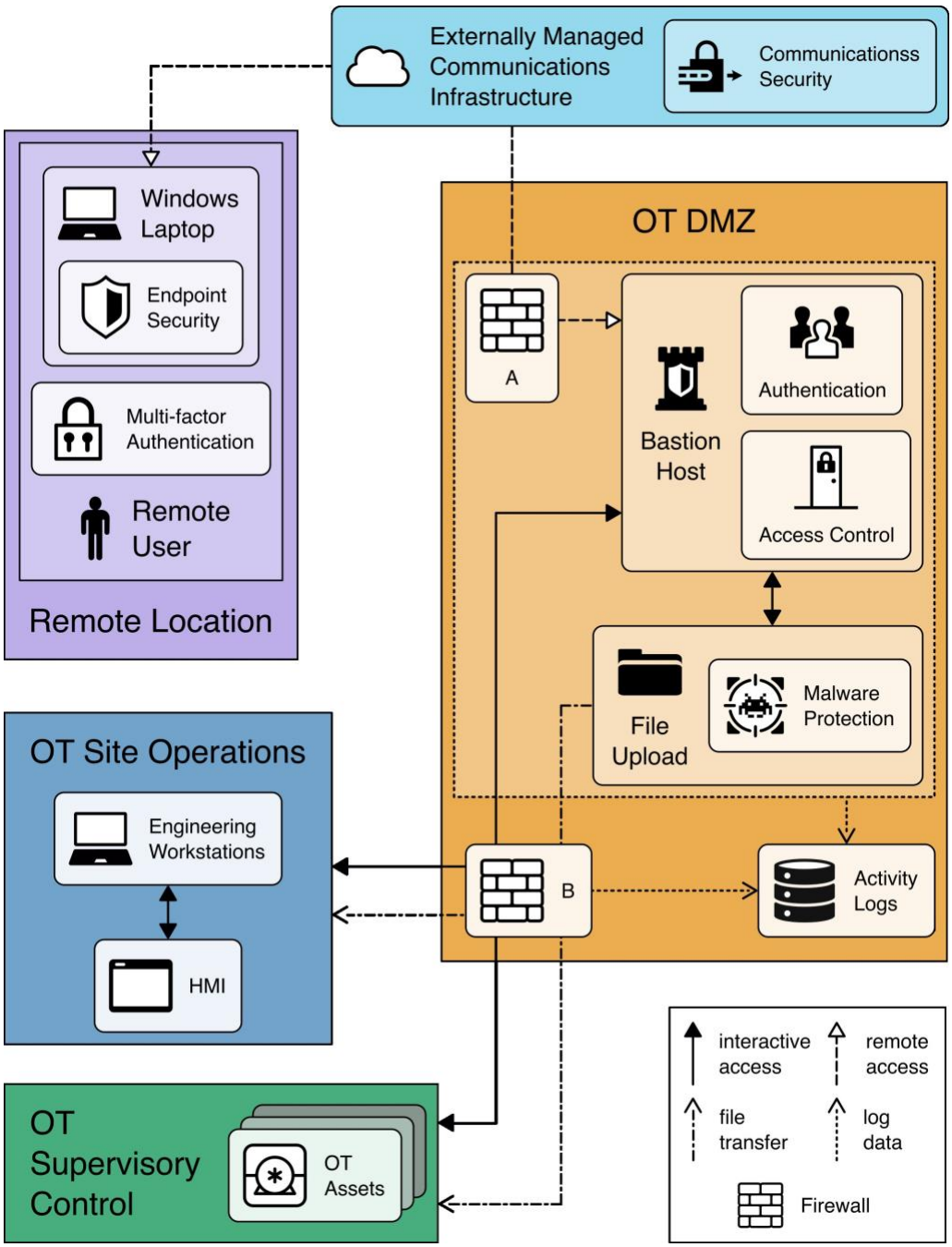


Figure 4. Traditional Remote Access Architecture

- In this architecture, a multi-factor authentication capability provides the remote user credentials to authenticate to the bastion host in the OT DMZ. The end-user device has an endpoint protection capability to prevent infection with malicious software.
- The end-user device connects to an OT 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 OT DMZ.

- At the OT DMZ, a pair of firewalls controls the ports and protocols which are allowed to enter and exit the DMZ.
- Within the OT DMZ the bastion host capability authenticates the remote user and controls the user's access to services and systems in the OT environment. For interactive access, the bastion host can permit connections to engineering workstations, human-machine interfaces (HMIs) and other OT assets such as programmable logic controllers (PLCs). The bastion host can also permit a remote user to access the file upload service to transfer files into the OT environment.
- The file upload capability receives the files from the remote user, scans the files for malicious content, and makes them available for transfer to other assets in the OT environment.
- Each security capability and service in the DMZ records remote user activity to the activity logs capability which records security relevant information for use in reviewing remote access usage.
- This basic architecture is the basis for example solutions for both medium to large WWS and very small to small WWS by using scale-appropriate solutions to provide the cybersecurity capabilities in the architecture.

3.2. Medium to Large WWS Remote Access Example Solution

Figure 5 illustrates how NCCoE plans to use products from project collaborators[1] to build an example secure remote access solution for medium to large WWS based on the architecture shown in Figure 4.

[1] While NCCoE uses commercial products provided by our collaborators to build this example solution, NIST and the NCCoE do not endorse these products. Your organization can select other products that offer similar capabilities to build a solution.

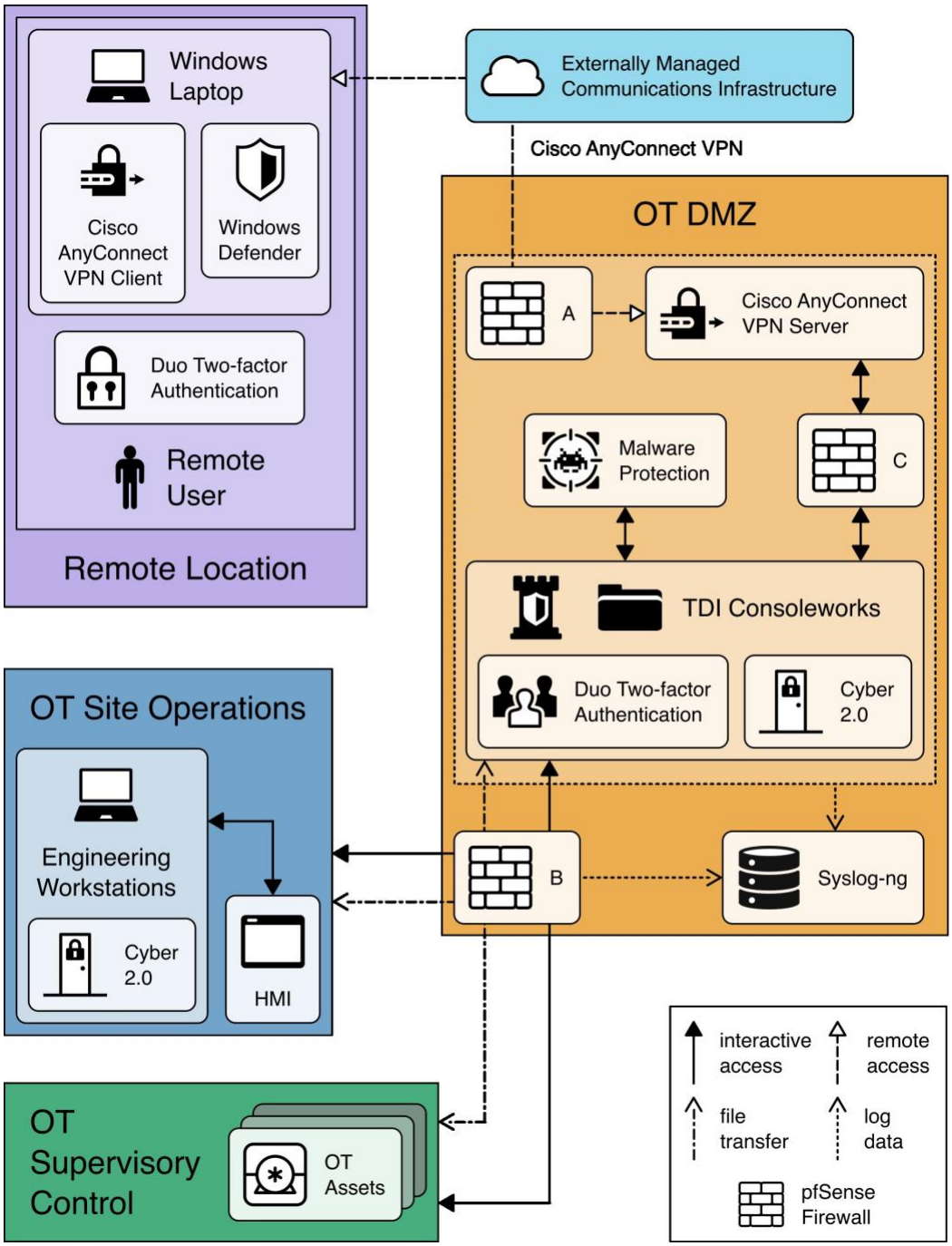


Figure 5. Remote Access for Medium to Large WWS example solution

In this example solution:

- A currently supported and patched Microsoft Windows laptop implements the end-user device. Windows Defender provides the endpoint security capability.
- Cisco's Secure Client application, including the AnyConnect VPN/ZTNA system, provides the communications security capability. An AnyConnect client is installed on the Windows laptop and makes a secure connection to the AnyConnect VPN server in the

OT DMZ. AnyConnect also authenticates the end-user device and the remote user. The user is authenticated using Cisco DUO multi-factor authentication. Connections are only created for authorized devices and users. The Cisco Secure Client ecosystem handles automatic connection/reconnection/disconnection, endpoint compliance, monitoring, and threat protection from the user.

- TDi Technologies' ConsoleWorks application implements both the bastion host and file upload security capabilities. ConsoleWorks authenticates the remote user using Cisco DUO multifactor authentication and then uses configured roles to control remote user access to resources in the OT environment. The file upload capability provides a call-out capability to malware protection. The example solution does not include a product for malware protection. This capability is implemented by a script which randomly chooses between "safe" and "not safe" for uploaded files.
- Cyber 2.0 is installed as an agent on the ConsoleWorks host and other systems that a remote user can access. Cyber 2.0 provides monitoring and additional control of network traffic and access to these systems.
- The pfSense® open-source firewall implements the firewalls that protect the OT DMZ by controlling the network ports and protocols that can enter and exit the OT DMZ. This example solution incorporates a third firewall, pfSense® C, between the Cisco AnyConnect VPN server and ConsoleWorks to control network restrict the ports and protocols accessible on the ConsoleWorks host. This third firewall is needed as the pfSense® (A) firewall cannot control traffic carried within the VPN.
- The syslog-ng open-source log manager implements the activity log security capability. Syslog data from all the security capabilities in the OT DMZ is collected and stored in syslog-ng. If the organization has security information and event management (SIEM) capabilities, it could be used as a security log capability.

In a typical remote access session:

- Using the Cisco AnyConnect client on their windows laptop, a remote user logs into Cisco AnyConnect VPN server using their Cisco DUO multi-factor authentication credentials. The pfSense® (A) firewall ensures that only the ports and protocols required by Cisco AnyConnect can reach the server.
- The AnyConnect server records all VPN connection attempts, successful and unsuccessful, in syslog-ng.
- Once the VPN connection is established, using a Web browser the remote user connects to TDI ConsoleWorks and authenticates using the Cisco DUO multi-factor authentication credentials. The pfSense®(C) firewall only allows https traffic from the VPN to reach ConsoleWorks.
- Based on defined roles, ConsoleWorks allows the remote user access to authorized resources.

- 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 creates connections to OT resources using appropriate protocols and credentials which ConsoleWorks manages. pfSense® (B) controls the network traffic between ConsoleWorks and the rest of the OT environment. Cyber 2.0 controls ConsoleWorks' access to resources in the OT environment.
- ConsoleWorks provides a file upload service that allows authorized users to bring files into the OT environment.
- ConsoleWorks records all remote user actions in syslog-ng.
- Cyber 2.0 records all connection attempts, successful and unsuccessful, from ConsoleWorks to resources in the OT environment.
- Depending on the network access controls and capabilities extended to the remote user, they can monitor and manipulate OT systems as if they are physically located in the SCADA control room.

3.3. Very Small to Small Remote Access Example Solution

Figure 6 illustrates how NCCoE plans to use products from project collaborators to build an example secure remote access solution for very small to small WWS based on the architecture shown in Figure 4. It should be noted that in addition to the technical solution, adequate resources (staffing and funding) will be required to ensure proper operation of remote access applications.

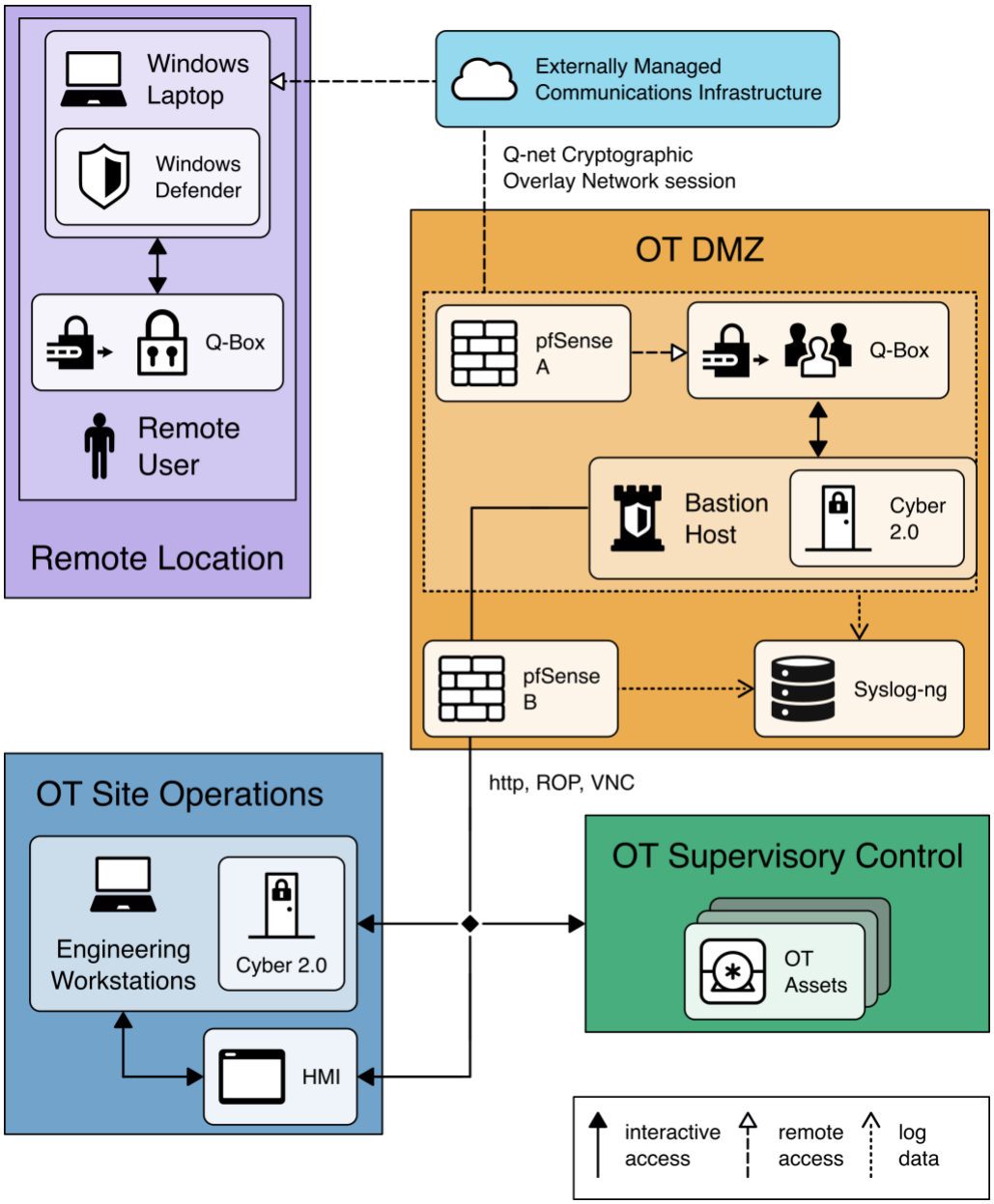


Figure 6. Remote Access for Very Small to Small WWS example solution

In this example solution:

- A Microsoft Windows laptop implements the end-user device. Windows Defender provides the endpoint security capability.
- Q-net's cryptographic overlay network, implemented by the Q-Box hardware devices, provides the communications security capability. The remote user connects a Q-Box to the windows laptop. This Q-Box communicates with the Q-Box attached to the bastion host providing an authenticated and encrypted connection.
- A hardened Linux platform provides the bastion host. The Linux platform authenticates the remote user with a username and password. An MFA capability is not used here as

the combination of a Q-Box, something the remote user has, with a password uses multiple factors to control access. MFA for the remote user could be added to this example solution if stronger identity assurance is desirable. The bastion host provides remote desktop (RDP, VNC) and Web (https) access to resources in the OT environment. The engineering workstation will be for access to resources that use industrial control protocols (e.g., Modbus). Remote users will first need to establish a remote desktop connection to the engineering workstation.

- Cyber 2.0 is installed as an agent on the bastion host and other systems that a remote user can access. Cyber 2.0 provides monitoring and additional control of network traffic and access to these systems.
- The pfSense® open-source firewall implements the firewalls that protect the OT DMZ by controlling the network ports and protocols that can enter and exit the OT DMZ.
- The syslog-ng open-source log manager implements the activity log security capability. Syslog data from all the security capabilities in the OT DMZ is collected and stored in syslog-ng.
- The very small to small WWS example solution does not include a remote file upload capability.

In a typical remote access session:

- Using the Q-Net Q-Box attached to their windows laptop, a remote user connects to the Q-Net cryptographic overlay network. The pfSense® (A) firewall ensures that only the ports and protocols required by Q-Net can reach the Q-Box on the bastion host.
- Once the cryptographic overlay network connection is established, the remote user connects to the bastion host and authenticates with a username and password.
- Based on defined roles, the bastion host allows the remote user access to authorized resources.
- The bastion host records all remote user actions in syslog-ng.
- Cyber 2.0 records all connection attempts, successful and unsuccessful, from bastion host to resources in the OT environment.

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

4. Cloud-Based Remote Access

While the traditional approach to remote access is to build and operate remote access capabilities on site, several vendors offer cloud-based remote access services. These services generally have broad scalability to address small to large utilities and offload much of the infrastructure management to the service provider. Cloud-based remote access services may be attractive to a wide range of utilities and can broadly 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, preprocess, 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 application programming interfaces (APIs) to pull the data into local tools, a cloud-based analytics dashboard, a remote client interface for monitoring, control, and configuration of edge systems, an alerting platform for notifying stakeholders of alerts and critical events, or more.

In this case, the architectural considerations will include a cloud security provider that handles authentication and authorization uses in the cloud environment, with security gateways and relays within the operational networks. A remote user will initiate an authentication to the cloud security provider utilizing an MFA solution to gain an access token for their cloud-based user access client. This client will then authenticate to the cloud access gateway inside of the operational network using a secured communications connection. This token will assign an RBAC 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.

4.1. Product-Agnostic Architecture for Cloud-Based Remote Access

Figure 7 illustrates the components of a cloud-based remote access architecture for WWS.

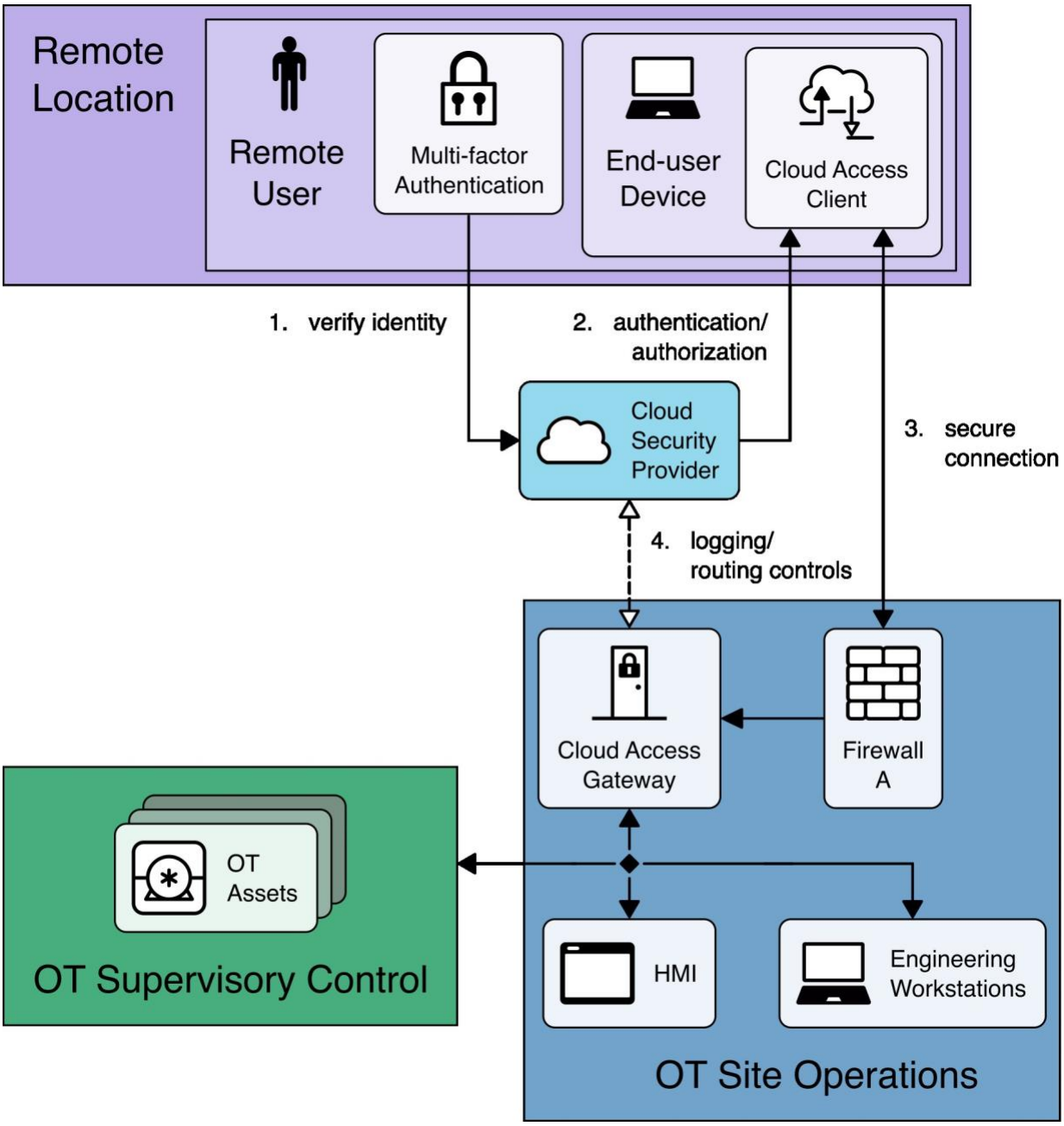


Figure 7. Cloud-based remote access

An architecture to utilize cloud-based remote access solutions will require the solutions in multiple sections of the design.

4.1.1. Edge

For edge devices and processes, there is a need for three different types of devices: data acquisition, gateways, and communication. For data acquisition, devices such as sensors and meters measuring water flow, pressure, quality, and more that support the water and wastewater process will fall into the edge section. For gateways, this is any system that will

process and collect the raw data from the data acquisition devices and hand it off to the communications systems, and they may include initial filtering and security of data. Communications will then transmit the data to the cloud provider, utilizing either IP-based communications, cellular, satellite, or other communication methods.

Remote access solutions in these areas will include devices such as edge gateways with remote access capabilities. This could include VPN connections, SSH connections, or other dedicated and secure remote management protocols. These systems will most likely be connected to or through an application in the cloud-based application section, providing required information and access including but not limited to remote management, monitoring, and data acquisition.

4.1.2. Network

Network devices are devices that include systems that connect the data collected at the edge to the cloud service and the cloud systems themselves. This includes the gateways utilized at the cloud to securely connect to the edge gateways, managing authentication and authorization as well as handling data routing. Another aspect of this is the cloud platform, which provides the infrastructure used for data storage, processing, and analysis. This can include multiple forms of clouds, public, private, and hybrid (mix of public and private cloud).

Concerning remote access solutions in the network layer, this may include the conduits to support VPNs, remote access shells, or other dedicated and secure remote access solutions. This may also include the capabilities of transporting network protocols specific to the water/wastewater utility, depending on the amount of remote management that is desired and the architecture in place to support that management.

4.1.3. Application

The final section is the application, and this includes multiple capabilities. One is remote monitoring and control software, which can be web-based dashboards including real-time data analysis and visualization. There are also data management and analytic tools, used for data storage, retrieval, analysis, and reporting. There may be algorithms used for predictive maintenance, anomaly detection, optimization, and other support systems. Finally, the application section may include integration technologies, such as SCADA interfaces, content management systems, and other enterprise applications.

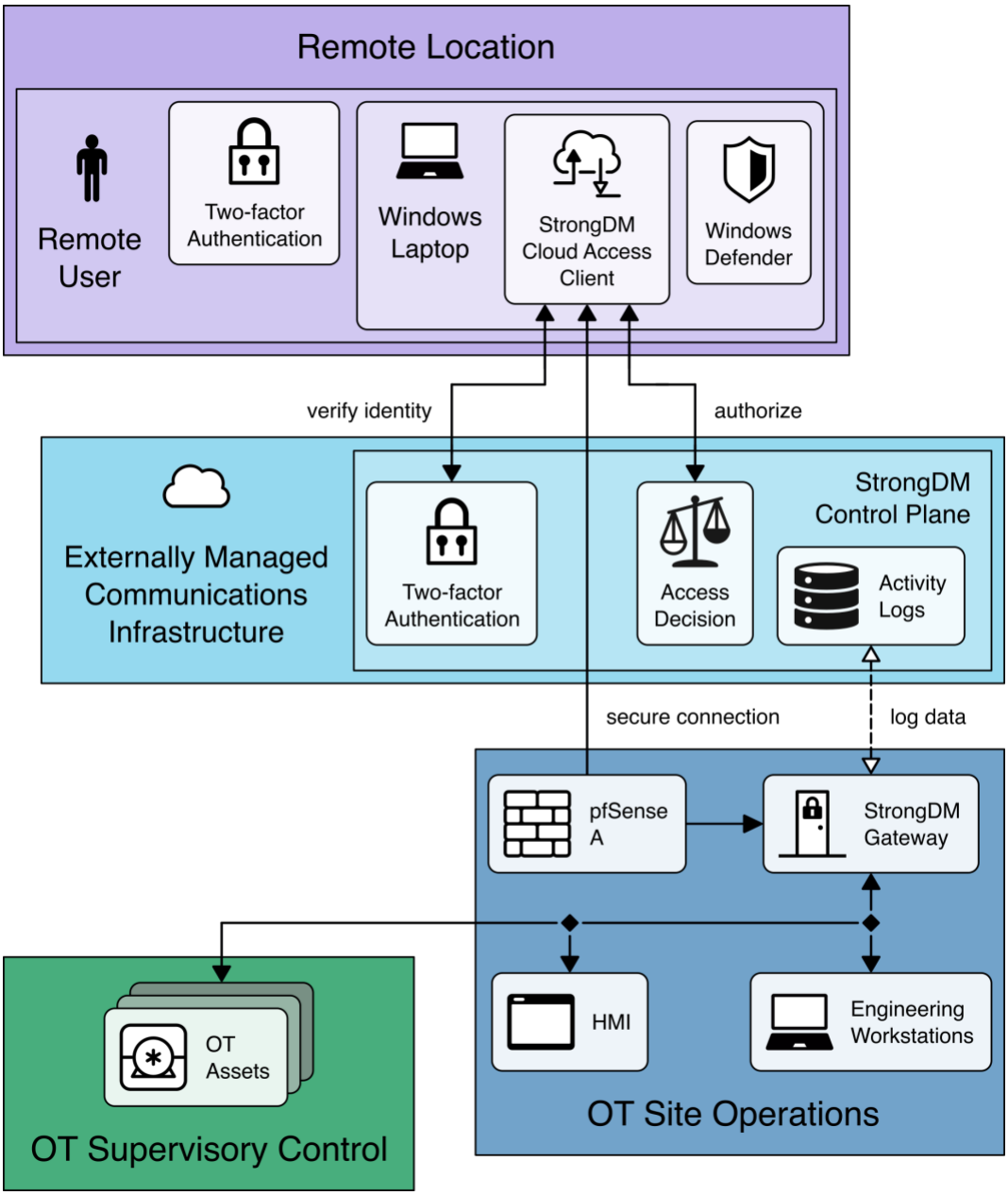
Remote access applications within the application layer may include portions of the web-based dashboard that allows direct interaction with the system and will be the focal point for individual user authentication and authorization. Considering the main remote connection to the water/wastewater utility will be brokered by the cloud infrastructure, all forms of identification, authentication, authorization, and accountability will be handled by the cloud application.

4.1.4. Security Considerations

For a cloud-based remote access architecture, it's important to recognize the potential security implications of the design. Public clouds may be more cost effective and scalable; however, there may be more security concerns on an open cloud system. Application capabilities may also present security concerns, specifically with remote access and control, as well as data integrity and confidentiality. It is important to consider multi-layered security solutions, including end-to-end encryption, access control, intrusion detection systems, and vulnerability management.

4.2. Cloud-Based Remote Access Example Solution

The NCCoE selected StrongDM technology as an example demonstration of a cloud-based remote access solution. The NCCoE plans to implement StrongDM' s cloud-based remote access solution, as illustrated in Figure 8.



445 **Figure 8 Cloud-based remote access example solution**

446 In this example solution:

447 • A Microsoft Windows laptop implements the end-user device. Windows Defender
448 provides the endpoint security capability.

449 • StrongDM provides communications security through the StrongDM cloud access client,
450 the StrongDM control plane the StrongDM gateway. The StrongDM control plane
451 provides multi-factor authentication and access decision making. The StrongDM
452 gateway enforces access decisions made by the control plane. The StrongDM control
453 plane also stores activity log information about all remote user activity.

- The pfSense® (A) firewall controls the ports and protocols the 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. The remote user authenticates to the StrongDM control plane using multi-factor authentication. The StrongDM control plane verifies the remote user's identity and returns an access token to the cloud access client.
- The StrongDM control plane logs all authentication attempts, successful and unsuccessful.
- The remote user accesses 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. The gateway records all access attempts, successful and unsuccessful, in an activity log stored in the control plane.
- Depending on the network access controls and capabilities extended to the remote user, they can monitor and manipulate OT systems as if they are physically located in the SCADA control room.

5. Summary and Next Steps

Secure remote access to industrial control systems was identified as a primary challenge in a 2021 water and wastewater sector survey [2], this project will demonstrate example solutions to improve the cybersecurity posture of remote access to water/wastewater operations. Although water/wastewater utilities vary widely in size and level of complexity, cybersecurity practices for remote access can still be tailored and applied to fit the unique and individual needs of an organization.

Water and wastewater utilities face potential challenges that may result from unauthorized access, such as the use of default or shared authentication credentials, broad access to OT and related networked systems, and lack of MFA requirements. The expected outcomes of demonstrating solutions to these challenges include ensuring security safeguards are configured on all devices and systems on the network, providing role-based access control mechanisms, and detecting an intrusion/anomalous behavior. This, in turn, offers solutions that can protect water/wastewater utilities from potential cyber-attacks while enabling and maintaining secure, available remote access systems so utility operations can continue undisrupted.

The NCCoE is currently building lab prototypes of the example solutions described here. The architectures, example solutions, and lab prototypes may be modified in response to feedback received on this initial public draft. This publication will be updated to describe any modifications and document the results of lab prototyping efforts.

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] CISA, (2021) "Ongoing Cyber Threats to U.S. Water and Wastewater Systems", https://media.defense.gov/2021/Oct/14/2002873650/-1/-1/0/CSA_ONGOING_CYBER_THREATS_TO_U.S._WATER_AND_WASTEWATER_SYSTEMS_20211014.PDF

[3] CISA, Improving Cybersecurity in Small and Medium-Sized US Water Utilities, https://www.cisa.gov/sites/default/files/publications/nipp-challenge-awwa-cybersecurity-508.pdf

[4] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2

[5] Drinking Water Dashboard Help, United States Environmental Protection Agency, Drinking Water Dashboard Help | ECHO | US EPA

[6] Information about Public Water Systems, United States Environmental Protection Agency, Information about Public Water Systems | US EPA

[7] U.S. Water Supply and Distribution Factsheet | Center for Sustainable Systems (umich.edu)

[8] Dragos, Inc. (n.d.) "5 Critical Controls for World-Class OT Cybersecurity" 5 Critical Controls for World-Class OT Cybersecurity | Dragos

[9] 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

[10] Dragos, Inc. (2023) "Getting Started Secure Remote Access – Part 1" https://hub.dragos.com/hubfs/OT-CERT/Dragos%20OT-CERT%20Secure%20Remote%20Access%20Getting%20Started%20Guide.pdf?_gl=1*u74qov_ga*MTc1MjA1MDc3NC4xNjg3Mjc4ODEz*_ga_8Z0JSJN44D*MTY4NzI4MTM4Ny4yLjEuTY4NzI4MTQ1My42MC4wLjA

[11] Mather, 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

Appendix A. Glossary

Bastion Host
A special purpose computer on a network where the computer is specifically designed and configured to withstand attacks. [Bastion Host - Glossary | CSRC (nist.gov)]

Note: Wikipedia notes that securing remote access in the main use case for bastion hosts – which suggests a Jump Server is a Bastion Host [Bastion host - Wikipedia]

Cryptographic Overlay Network
A cryptographic overlay network is an overlay network implemented using cryptography.

Jump Server
"… a system on a network used to access and manage devices in a separate security zone. A jump server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them." [Jump server - Wikipedia]

Overlay Network
An overlay network is a virtual or logical network that is created on top of an existing physical network. [What is an overlay network? (techtarget.com)]