NWC OT Cybersecurity Secure File Transfer Detailed-Level Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-DLD-SFTP
Document Title:	NWC OT Cybersecurity Secure File Transfer Detailed-Level Design
Document Version:	0
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

1400 Broadfield Blvd Suite 200 Houston TX, 77084
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
Email: sales@acetsolutions.com |
URL: www.acetsolutions.com

NOTES AND COPYRIGHTS

NWC has contracted this project to [atm] under contract number 101200487. ACET Solutions is the technical consultant of [atm] responsible for planning and execution of this project. All references to ACET Solutions in this document should be construed as [atm]/ACET Solutions for contractual purpose. Acceptance of this deliverable by NWC shall meet the requirements of the respective deliverable under NWC contract number 101200487.

Questions or comment regarding this deliverable should be directed to the ACET Solutions Project Director.

ACET Solutions LLC
1400 Broadfield Blvd Suite 200
Houston TX, 77084
Email: sales@acetsolutions.com | URL: www.acetsolutions.com

APPROVALS

Name	Company	Signature	Date
Mubarik Mustafa (Project Director)	ACET Solutions		
Abdulhadi G. Alshammari (Project Manager)	NWC		
Ahmed I. Almutairi (Project Sponsor)	NWC		

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
0	24-Jan-2022	AR	NR/SK	MM	Issued for Approval

GLOSSARY

Acronyms	Meaning
AD	Active Directory
ADC	Additional Domain Controller
ATM	Advance System and Technology
BU	Business Unit
DLDD	Detailed-Level Design Document
DMZ	Demilitarized Zone
DNS	Domain Name System
FTP	File Transfer Protocol
GB	Giga Byte
HDD	Hard Disk Drive
HLD	High Level Design
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
IT	Information Technology
KSA	Kingdom of Saudi Arabia
MCBU	Makkah Central Business Unit
MDCBU	Madinah Central Business Unit
MGMT	Management
NCA	National Cybersecurity Authority
NERC	North American Electric Reliability Corporation
NIST	U.S. National Institute of Standards and Technology
NWC	National Water Company
OT	Operational Technology
PDC	Primary Domain Controller
PS	Pumping Station
RDP	Remote desktop services
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
VM	Virtual Machine
SFTP	Secure File Transfer Protocol
SSH	Secure Socket Shell
LDAP	Lightweight directory access protocol

REFERENCE DOCUMENTS

S/N	Document No.	Title
1	A01001045-HLD.00	NWC OT Cybersecurity High-Level Design
2	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
3	ISA–62443-1-1 (99.01.01)–2007	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models

Table of Contents

List of Figures

List of Tables

1. DOCUMENT PURPOSE

This document details the design of the Secure File Transfer solution in NWC OT and in between NWC IT & OT. The Secure file transfer solution is provided using CRUSHFTP. The document explains what is implemented or configured at each level. The document also explains the data flow and IT\OT integration.

2. SFTP DESIGN ARCHITECTURE

OT SFTP server is installed and configured in the OT-DMZ, and a dedicated IT SFTP Server is installed in the Enterprise Level to receive and send the OT files. The below figure shows the secure FTP design of NWC.

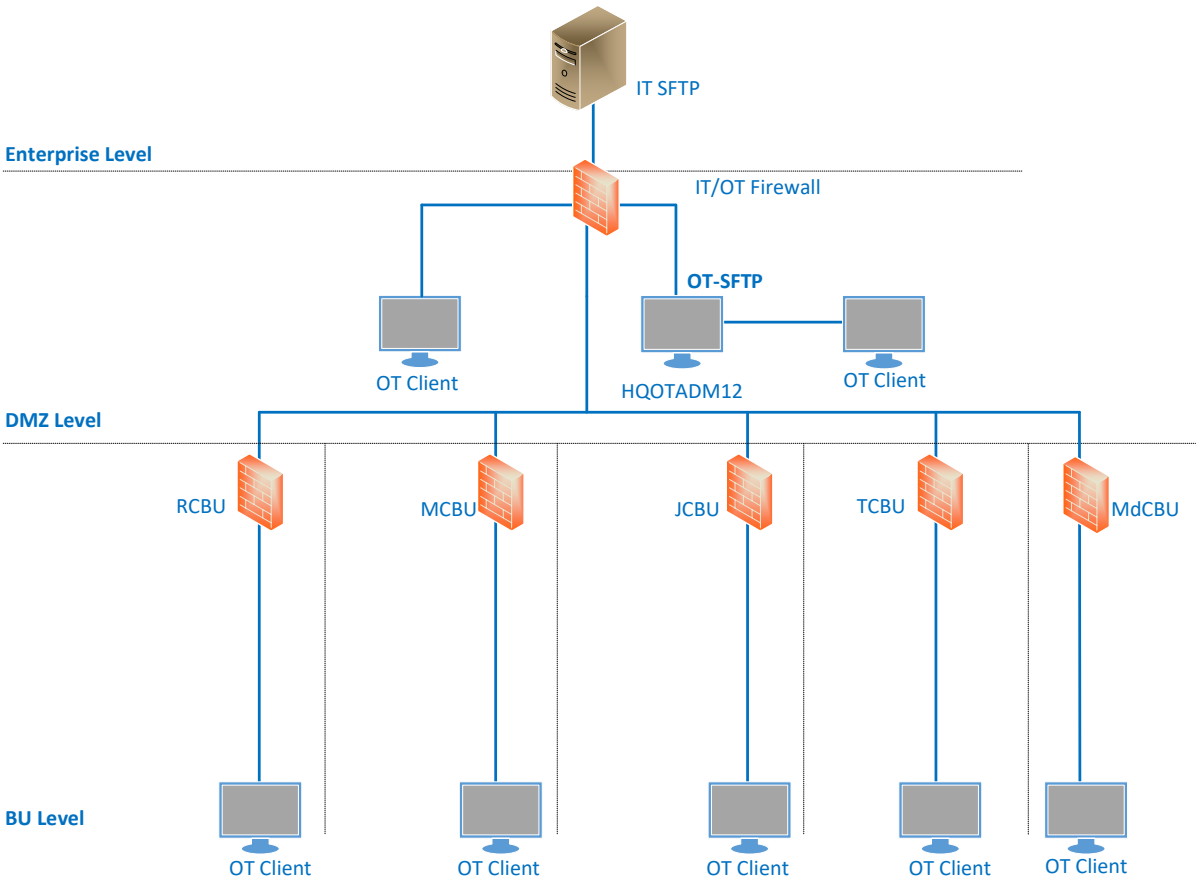

Figure 1: SFTP DLD Architecture

3. DETAILED DESIGN

The following section describes the detailed SFTP server configuration for NWC SCADA.

3.1 SFTP SERVER CONFIGURATION

3.1.1 IT SFTP

- A dedicated IT SFTP server is installed and configured at the enterprise level.
- IT SFTP server is integrated with the IT domain and only specified users are allowed to access the server.
- SFTP clients at the Enterprise Level are not allowed to connect to the SFTP Server in OT-DMZ.
- A secure and encrypted SSH connection is established from OT-SFTP to download files from IT-SFTP required in the OT manually.

Following are the VM configurations for the installation of IT SFTP server.

VM Component	Configurations
CPU Cores	6
O/S	Microsoft Windows Server 2016 Standard
C Drive (For VM O/S)	100 GB
Memory	12 GB
Software Installed	CRUSHFTP

Table 1: VM Configuration

3.1.2 OT SFTP

- A dedicated OT SFTP server is installed and configured in the HQOTADM12.
- The OT SFTP Server automatically uploads the files at real time to the IT SFTP server in the Enterprise.
- Only specified users are granted access to upload files from SCADA workstations and servers to OT SFTP Server.
- OT SFTP server is integrated with NWC-OT domain, and only specified users are allowed to access the server.
- The clients can access the OT SFTP server via web client over secure and encrypted HTTPS protocol.

3.1.3 IT/OT SFTP SERVER INTEGRATION

- A secure and encrypted SSH connection is established from HQOTADM12 to the IT SFTP server for file transfer.
- For integration, a user (with minimum credentials, non-interactive user) has to be created in IT AD, that user has access to IT SFTP directories.
- FTP Client in HQOTADM12 connect to IT SFTP using the IT user credentials and upload files automatically in real time to IT SFTP.
- FTP client in HQOTADM12 download files manually from IT SFTP.

- FTP synchronizer client is used for IT/OT integration. In HQOTADM12 ftp synchronizer connect to IT SFTP using IT user credentials, it uploads files from local OT directory to remote IT directory in real time.
- Users need to remotely login to HQOTADM12 using rdp and run the FTP synchronizer manually to download files from IT remote directory to local OT directory.
- A firewall is configured to only allowed connection from HQOTADM12 to IT SFTP and no connection is allowed from IT side to OT SFTP.

3.2 USERS CONFIGURATIONS

3.2.1 OT SFTP USERS GROUPS

The Following security groups are created in the active directory for OT SFTP.

Group	Name	Assigned Directories
1	FTP-OTUsers-Grp1	Home directory, Upload to IT and Received from IT
2	FTP-OTUsers-Grp2	Home directory, Upload to IT and Received from IT, Confidential Data

Table 2: OT SFTP User Groups

- When new users are added to their respective security groups, directories are created and assigned automatically according to their group scope.
- Whenever a user login to OT-SFTP server, home-directory with a username is created automatically where users can upload and download files. They can also access files within their home directory anywhere within the OT network.

#	Directory	Scope
1	Home	Private Home directory created for every OT SFT User
2	Upload to IT	Common Directory to Upload to IT
3	Received from IT	Common Directory to Received from IT
4	Confidential	Specific Directory to Upload to IT

Table 3: List of Directories

- By default, OT User will not get SFT (Secure File Transfer) User rights. Users approved for Secure File Transfer will be added to the above SFT User Groups.
- “Home”, “Upload to IT”, and “Received from IT” Directories are created automatically for all OT SFT Users.
- In “Upload to IT” directory, OT SFT Users have permission to upload files that are intended to send to the IT SFTP Server.
- “Received from IT” directory, OT SFT users have permission to download files received from the IT SFTP Server.
- OT SFTP server is integrated with the LDAPS Server for user authentication.
- Web browser is used to initiate secure https connection OT-SFTP Server using URL “https://HQOTADM12.NWC-OT.LOCAL or https://HQOTADM12/”.

- Communication between OT-SFTP Server and LDAPS server for OT SFT user authentication is end to end encrypted over a secure connection.
- Only LDAPS authenticated OT SFT Users are allowed to open OT SFTP webpage for upload and download files. Members of security groups 2 assigned directory i.e., “Confidential Data” to transfer confidential files.
- The communication between the client and the server is end-to-end encrypted over a secure HTTPS connection.
- Files in OT SFTP directories are automatically deleted after every week.

3.2.2 IT SFTP USER GROUP

The following security groups are created in Enterprise AD for IT/OT SFTP integration.

Group	Name	Assigned Directories
1	FTP-ITUser-Grp1	Upload to OT and Received from OT
2	FTP-ITUser-Grp2	Upload to OT and Received from OT, Confidential Data

Table 4: IT SFTP User Group

- “Received from OT” directory contains the files which are received from the OT side.
- Files that are intended for OT are to be placed in “Upload to OT”.
- Users in this group used for IT/OT integration is created with least privileges and they are only used for IT/OT SFTP integration.
- Communication between the web-browser and the IT SFTP Server is end-to-end encrypted over a secure HTTPS connection.
- FTP synchronizer in HQOTADM12 initiates connection to IT SFTP using the login credential of IT user for file transfer between IT/OT SFTP.
- This user group has full permission and control over directories assigned to him.
- Files in IT SFTP directories are automatically deleted after every week.

3.2.3 IT/OT SFTP DIRECTORY MAPPING

The below table describes the mapping of directories between IT/OT.

OT SFTP Directory	IT SFTP Directory
Upload to IT	Received from OT
Received from IT	Upload to OT
Confidential Data upload to IT	Confidential Data received from OT

Table 5 : IT/OT SFTP Directory Mapping

- Users on the OT side placed the OT files in the “Upload to IT” directory, FTP synchronizer detect the files and upload in real time without user intervention to the “Received from OT” directory on the IT side and in this way, users can access the OT files from IT SFTP.

- When files are required from the IT side, IT users placed the files in the “upload to OT” directory, then OT user remotely log in to HQOTADM12 and manually run the FTP synchronizer to downloads the required files in “Received from IT” directory in OT side.

3.3 PORTS CONFIGURATION

The following sections describe the details of port configurations.

Port	Default Value	Description
Server-server FTP communication port	22	IT/OT integration used FTP over secure SSH.
Server to client communication port	443	Client access SFTP server over Https
SFTP TO LDAP communication	389	For AD user authentication

Table 6: Server Communication Ports

ACET Solutions LLC
1400 Broadfield Blvd Suite 200 Houston TX, 77084.
United States of America.
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
sales@acetsolutions.com | www.acetsolutions.com