NWC OT Cybersecurity Network Devices Minimum Baseline Security Standard

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-MBSS-ND
Document Title:	NWC OT Cybersecurity Network Devices Minimum Baseline Security Standards
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
00	16 February 2022	AMS	SK	MM	

GLOSSARY

Acronyms	Meaning
ACL	Access Control Lists
AD	Active Directory
ADC	Additional Domain Controller
ATM	Advance System and Technology
ATP	Adaptive Threat Protection
BYOD	Bring Your Own Device
CAP	Client Authorization Policy
CAS	Central Administration Server
CIP	Critical Infrastructure Protection
CMC	Central Management Console (Nozomi)
CSMS	Cyber Security Management System
DCS	Distributed Control System
DLD	Detailed-Level Design
DMZ	Demilitarized Zone
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
ePO	ePolicy Orchestrator
EPP	End Point Protection
GPS	Global Positioning System
HCIS	High Commission for Industrial Security
HLD	High Level Design
HMI	Human Machine Interface
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
JCBU	Jeddah Central Business Unit
KSA	Kingdom of Saudi Arabia
MBSS	Minimum Baseline Security Standards
MCBU	Makkah Central Business Unit
MDCBU	Madinah Central Business Unit
MGMT	Management
NCA	National Cybersecurity Authority
NERC	North American Electric Reliability Corporation
NGFW	Next Generation Firewall
NIST	U.S. National Institute of Standards and Technology
NTP	Network Time Protocol
NWC	National Water Company

Acronyms	Meaning
OT	Operational Technology
PDC	Primary Domain Controller
PLC	Programmable Logic Controller
RAP	Resource Authorization Policy
RCBU	Riyadh Central Business Unit
RD	Remote Desktop
RDS	Remote Desktop Services
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident & Event Management Solution
SSL	Secure Socket Layer
TCBU	Taif Central Business Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

Table of Contents

1. DOCUMENT PURPOSE

The purpose of this document is to describe the minimum baseline security standard for NWC Network devices.

Devices in scope are listed as follows:

Sr.	Devices	Description
1	Switches	Connects network devices together.
2	Routers	Routes network packets, based on their addresses, to other networks or devices. Includes wireless routers.
3	Firewalls	Protects network by filtering traffic and blocking outsiders from gaining unauthorized access. Incudes NGFW and Industrial Firewalls.
4	Vulnerability Management Devices	Monitors networks, systems, and applications for security vulnerabilities and detects intrusions.

Table 1 Devices in Scope

2. MINIMUM SECURITY REQUIREMENTS

2.1 GENERAL

The following requirements are common between all the devices in the scope of this document.

1. Default username and passwords shall be changed.
2. Default administrator account must be disabled, where-ever possible.
3. Default IP Addresses shall be changed.
4. Every network user shall be provided a unique individual least privilege account.
5. Management port shall be on management LAN, separated from production LAN logically and physically if practically possible.
6. Communication on management LAN should be encrypted using.
7. NTP shall be configured for log time stamps.
8. Device logs shall be sent to a central syslog server.
9. All network devices must be kept up to date with the latest firmware, where-ever applicable.
10. Unused network ports on devices shall be protected physically by mechanical means (such as Port Lock) from unauthorized access.
11. Periodic backup of network device configuration hall be taken as per NWC backup policy.
12. Security configurations shall be tested periodically against security requirements.
13. Configuration files shall be protected with encryption while sending, storing and backing up.
14. Cabinets containing network devices should be kept under lock and key.
15. Tamper seals shall be installed on devices where-ever applicable, at the time of installation and checked periodically.
16. Periodic network assessment shall be performed.

2.2 SWITCHES

Following are additional minimum-security requirements for switches (for vendor specific details refer to “A01001045-MBSS-ND-APP.00 D0”)

1. Switch management shall be protected using NWC password policy.
2. User lockout feature if available in the device must be enabled
3. Service Password-Recovery shall be disabled.
4. Following unused service shall be disabled, wherever applicable.
    a. TCP and UDP small services shall be disabled. These services include:
        i. echo (port number 7)
        ii. discard (port number 9)
        iii. daytime (port number 13)
        iv. chargen (port number 19)
    b. Device shall be configured to logout sessions on vty or tty lines that are left idle.
5. Management Sessions shall be encrypted with SSH. SSHv2 must be configured, where-ever supported.
6. Console and AUX Ports must be protected in the same manner as privileged access

2.3 ROUTERS

Following are additional minimum-security requirements for routers:

2.3.1 STANDARD ROUTER

1. All security features implemented for switch security are also applicable for standard router.

2.3.2 GSM ROUTERS

1. Dedicated APN or WAN must be requested from a service provider.
2. GSM router shall be selected having appropriate access control features.
3. GSM router shall be configured with the dedicated NWC OT APN configuration.
4. GSM router shall never be configured with public APN configuration after/during commissioning/operation of L0-1 device.

2.4 FIREWALL

Following are additional minimum-security requirements for Firewalls (for vendor specific details refer to “A01001045-MBSS-ND-APP.00”):

2.4.1 STANDARD FIREWALL

1. Changes in Firewalls shall follow Change Management Procedure.
2. Firewall shall not be used with default configurations.
3. Security zones shall be configured and matched to network interfaces.
4. Access Control Lists (ACLs) shall be configured and shall be granular and specific.
5. Static routing shall be configured, wherever applicable.
6. Firewall changes shall be lab tested before deployment.
7. Source IP addresses allowed into management network shall only be limited to those of dedicated management devices.
8. Insecure services such as Telnet and HTTP shall not be allowed on management interface.
9. Ping services shall be allowed to test connectivity.

2.4.2 NEXTGEN FIREWALLS

Following are the additional features that are available in NextGen Firewalls with respect to standard firewalls.

1. Layer 2 to 7 (OSI model) granular policies shall be implemented.
2. Signature database shall be kept up to date for deep-packet inspection and Intrusion Protection.
3. Deep-packet inspection shall be enabled.
4. Intrusion Prevention shall be enabled.
5. Inbound and outbound traffic decryption shall be enabled, wherever applicable.
6. Firewall shall be integrated with threat intelligence services against advanced persistent threats (APT).
7. Network malware protection shall be enabled.

2.5 VULNERABILITY MANAGEMENT DEVICES

General security recommendations are as follows (for vendor specific details refer to “A01001045-MBSS-ND-APP.00”):

1. VMDs shall be configured to scan network passively, active probing shall not be allowed.
2. VMD shall be connected to node where maximum network traffic flows through.
3. VMD shall be connected to node capable of spanning or mirroring ports.
4. Vulnerability signature database shall be kept up to date.
5. VMD shall be configured to log all types of events and alerts.
6. VMD shall be tuned to know the normal network conditions.

7. VMD shall prioritize identified vulnerabilities based on Common Vulnerability Scoring System (CVSS).

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