Eskom	Guideline	Technology

Title: **CYBER SECURITY CONFIGURATION GUIDELINES OF NETWORKING EQUIPMENT FOR OPERATIONAL TECHNOLOGY**

Unique Identifier:	**240-91479924**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Guideline**
Revision:	**2**
Total Pages:	**20**
Next Review Date:	**August 2026**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Kgomotso Manyapetsa	Rishi Hariram	Naresh Hari
Senior Engineer – Control and Automation	Manager – Control and Automation	General Manager - Engineering Transmission
Date: 03/08/2021	Date: 03/08/2021	Date: 2021-08-16

Supported by SCOT/SC

Nelson Luthuli
Acting PTM&C TC Chairperson
Date: 16 August 2021

PCM Reference: **Manage Item Configuration**
SCOT Study Committee Number/Name: **<Number or name>**

Content

Page

Executive summary 3

1. Introduction 4

2. Supporting clauses 4
   - 2.1 Scope 4
     - 2.1.1 Purpose 4
     - 2.1.2 Applicability 4
   - 2.2 Normative/Informative references 5
     - 2.2.1 Normative 5
     - 2.2.2 Informative 5
   - 2.3 Definitions 6
     - 2.3.1 General 6
     - 2.3.2 Disclosure Classification 9
   - 2.4 Abbreviations 9
   - 2.5 Roles and Responsibilities 10
   - 2.6 Process for monitoring 10
   - 2.7 Related/supporting documents 10

3. Cyber security configuration guidelines of networking equipment for Operational Technology 11
   - 3.1 Prerequisite information 11
   - 3.2 Prerequisite laptop/computer and/or ICS Based Clients 11
   - 3.3 Initial upgrades 11
   - 3.4 Management configuration 12
   - 3.5 Configuration of Networking Devices 12
   - 3.6 Firewall 17
   - 3.7 Intrusion Prevention System (IPS) 17
   - 3.8 Logging of Devices 18

4. Authorisation 19

5. Revisions 20

6. Development team 20

7. Acknowledgements 20

Executive summary

Many forms of security threats have emerged due to the rapid growth of industrial networks and communication systems in general. Viruses, malicious hackers and employees of an organization are potential security hazards to Operational Technology networks. These threats have the potential to steal and destroy sensitive data, tie up valuable resources and inflict major damage due to network downtime. This situation may lead to a cost crisis and cripple the organization financially.

Common threats to network device security and mitigation strategies can be summarized as follows:

- Remote access threats: unauthorized remote access is a threat when security is weak in remote access configuration. Mitigation techniques for this type of threat include configuring strong authentication and encryption for remote access policy and rules, configuration of login banners, use of ACLs and VPN access.
- Local access and physical threats: these threats include physical damage to network device hardware, password recovery that is allowed by weak physical security policies and device theft. Mitigation techniques for this type of threat include locking the wiring closed and/or cabinet and allowing access only to authorized personnel. It also includes blocking physical access through a dropped, raised floor, window, ductwork or other possible point of entry, use electronic access control, log all entry attempts, and monitor facilities with security cameras where possible.

This document describes the minimum requirements of cyber security functionality for the configuration of the following networking devices in the Operational Technology (OT) environment:

- Layer 2 switches
- Layer 3 switches and routers
- Physical hardware firewalls

These networking components provide the core services through the various network highways, in getting data from the field to the end-user for a variety of reasons including but not limited operations, maintenance (reactive and preventative), general analysis, condition monitoring etc. Attackers often target these networking devices as they know that if they succeed, they can gain control of the entire network system and expand the attack horizon to cause a significant amount of damage in terms of data loss.

1. Introduction

This guideline describes how to implement cyber security functionality on networking equipment. This guideline should be used in conjunction with the product specific manuals containing the actual commands.

Products are evolving and strictly defined functionality based on the Network OSI Model are becoming merged and overlapped, therefore this document is applicable to all types of devices. Where functionality is specific for a type, it is indicated as such.

This document includes recommendations from various government and utility regulatory security departments.

2. Supporting clauses

2.1 Scope

The scope of this guideline is based on a system that has a full complement of networking devices, such as a firewall, IPS, Layer 7 device, RADIUS / Authentication server and a separate Management Network. It might only be possible to implement a small portion of what the guideline recommends, specifically for smaller installations. This document does not apply to the Eskom Telecommunications (ET) Wide Area Network (WAN).

The document does not cater for all types of equipment in existence; it is intended for use in multiple environments and is not specific for any OS. Each manufacturer has multiple product versions and each has unique functionality, products with new functionality are released daily, but existing functionality is seldom removed.

The following device configurations are excluded from this document:

1) Description of the overall network layout, network connectivity between equipment or high level designs as this information is unique to each application.
2) The actual commands or configuration settings because they are unique for each manufacturer
3) Functionality that does not pertain to cyber security settings
4) Cyber security at a software application layer for software residing on servers
5) Cyber security on equipment connected to the network equipment
6) Cyber security on high level protocols and high level routing protocols
7) RADIUS / Lightweight Directory Access Protocol (LDAP) / Authentication server environment
8) Deep Packet Inspection Systems (DPIS)
9) Operating systems, except for OS's on networking equipment

2.1.1 Purpose

The purpose of this document is to provide guidance to system administrators, network engineers and technicians during the configuration of networking equipment in the Operational Technology (OT) environment.

2.1.2 Applicability

This document shall apply to the Operational Technology environments throughout Eskom Holdings Limited. This guideline is specifically targeted at system administrators, network/system engineers and technicians working directly with networking equipment.

This document does not apply to Eskom Telecommunications (ET) Wide Area Network (WAN)

2.2 Normative/Informative references

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] ISO 9001 Quality Management Systems.

[2] 240-55410927: Cyber Security Standard for Operational Technology.

[3] 240-79669677: Demilitarised Zone (DMZ) Designs for Operational Technology

[4] 32-373: IT OT Remote Access Standard

[5] 240-79669677: DMZ Designs for OT

[6] 240-55863502: Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities.

[7] NERC CIP-005-3 Cyber security – electronic security perimeter(s)

[8] NERC CIP-006-3c Cyber security – physical security of critical cyber assets

[9] NERC CIP-006-3d Cyber security – physical security of critical cyber assets

[10] NERC CIP-006-4c Cyber security – physical security of critical cyber assets

[11] NERC CIP-006-4d Cyber security – physical security of critical cyber assets

[12] NERC CIP-007-3 Cyber security – systems security management

[13] NERC CIP-007-4 Cyber security – systems security management

[14] NERC CIP-007-5 Cyber security – systems security management

[15] NERC CIP-007-6 Cyber security – systems security management

[16] 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security

2.2.2 Informative

[17] 240-55863502: Definition of Operational Technology (OT) and OT/IT collaboration accountabilities

[18] 32-373: Information Security- IT/OT Remote Access Standard

[19] 240-153804009: Firewall Application Philosophy Guide

[20] 32-368: Incident Management

[21] 240-83684419: PTM&C Technology Development

[22] 32-85: Information security Policy

[23] Minimum Information Security Standard (MISS) – South African National document

[24] IEC 62443 - Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.

2.3 Definitions

2.3.1 General

Definition	Description
Access Control list	Access Control list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack related attacks. ACLs are used to filter traffic based on the set of rules defined for the inbound or outbound of the network interfaces. Some advantages of the ACLs: • Improve network performance. • Provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network. • Provides control over the traffic as it can permit or deny according to the needs of a network.
Cyber Security	Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: • Availability, • Integrity, which may include authenticity and non-repudiation • Confidentiality.
DHCP	DHCP serves the purpose of issuing IP addresses and other network-related configuration values to clients to allow them to operate on the network. DHCP uses UDP ports 68 & 67.
End device	An end device refers to a piece of equipment that is either the source or the destination of a message on a network. Sometimes referred to as a host.
Firewall	Any combination of hardware device and/or software application designed to protect network devices from outside network users and/or malicious applications and files.
HTTP	Hypertext Transfer Protocol (HTTP) is the protocol used for communication (in clear text) between a web server and a web browser (also Application server and Client models). It uses TCP/UDP port 80.
HTTPs	Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS), or HTTP Secure, is a protocol used to make a secure web connection. It uses TCP/UDP port 443.
IDS/IPS	Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are network security appliances that monitor networks and packets for malicious activity. An IDS monitors and records and informs about problems, whereas an IPS can work in real time to stop threats as they occur. The main difference between them is that an IPS works inline to actively prevent and block intrusions that are detected based on the rules set up. IPSs can send an alarm, create correlation rules and remediation, drop malicious packets, provide malware protection, and reset the connection of offending source hosts.

Definition	Description
LDAP	Lightweight Directory Access Protocol (LDAP) is a protocol that provides a mechanism to access and query directory services systems. These directory services systems are typically Microsoft's Active Directory. LDAP uses TCP/UDP ports 389 and 3268.
NTP	Network Time Protocol (NTP) is used to keep all of the devices in the network synced to the same time source. This helps keep the timestamps of all network events that may be sent to a central server synchronized so that the events can be placed in the order in which they occurred. It operates on UDP port 123.
Operational Technology (OT)	OT is the technology that is used to operate, monitor and control the power system. For a more specific definition refer to the OT Practice Note [4]
OSI	The OSI reference model is a layered, abstract representation created as a guideline for network protocol design and instruction. The OSI model divides the networking process into seven logical layers, each of which has unique functionality and to which are assigned specific services and protocols. This reference model is often used to interpret the TCP/IP protocol suite
OT Systems	Are all systems (including electronic, telecommunications, computer systems and components) which process, store or communicate operational data or information [2]
RADIUS	RADIUS is an open standard that combines authentication and authorization services as a single service. It is a network protocol that provides security to networks against unauthorized access. RADIUS secures a network by enabling centralized authentication of dial-in users and authorizing their access to use a network service. It manages remote user authentication, authorization and accounting (AAA).
Router	A router is a network device used to connect many, sometimes disparate, network segments together, combining them into an internetwork. A router can make intelligent decisions about the best way to get network data to its destination.
Routing Protocol	Is set of processes, algorithms and messages) by which routers dynamically share their routing information. Routing protocols are either distance-vector or link-state based examples of routing protocols are: OSPF,EIGRP,RIPv2, IS-IS and BGP
Routing Table	Contains a list of all networks that are known to a particular router and information about how to reach those networks. A routing table typically includes the following types of entries: Directly connected networks, static routes, default routes and dynamic routes.
SNMP	Simple Network Management Protocol (SNMP) is a protocol that facilitates network management functionality. It operates over UDP port 161.
SSH	Secure Shell is a remote administration tool that can serve as a secure alternative to using Telnet to remotely access and configure a device like a router or switch. It provides an encrypted command-line session for managing Devices remotely. It uses port TCP 22.
SSL/ TLS	SSL/TLS are protocols for establishing authenticated and encrypted links between networked end devices. HTTPs leverages both SSL/TLS to provide secure web browsing between a webserver and a web client. TLS is a successor of SSL. Both protocols use either TCP/UDP port 443.

Definition	Description
Switch	Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network. A switch has many ports, to which end devices are connected in. When a data frame arrives at any port of a network switch, it examines the destination MAC address, performs necessary checks and sends the frame to the corresponding end device(s).It supports unicast, multicast as well as broadcast communications.
Syslog	System logging (Syslog) is protocol that allows a device/s to send event notifications across networks to event message collectors. The messages include time stamps, event messages, severity, host IP addresses, diagnostics and more. It uses port UDP 514
System Owner	The System Owner is the authorised Eskom representative that has overall accountability for the OT system.
TCP/ UDP	These are two transport layer protocols in the TCP/IP stack. TCP provides guaranteed, connection-oriented delivery whereas UDP provides nonguaranteed, connectionless delivery. Each protocol or service uses one of the two transport protocols (and in some cases both). Both protocols use port numbers to listen for and respond to requests for communications. RFC 1060 defines common ports for a number of services routinely found in use.
Telnet	Telnet is a remote administration tool, it has a security vulnerability in that Telnet sends data including passwords in plain-text format. Telnet runs on TCP port 23
Time to Live (TTL)	A field in the IP header that prevents a packet from indefinitely looping around an IP internetwork. Routers decrement the TTL field each time they forward a packet, and if they decrement the TTL to 0, the router discards the packet, which prevents it from looping forever.
VLAN	Virtual Local Area Network (VLAN) is a network of end devices that behave as if they are connected to the same network segment, even though they might be physically located on different segments of a LAN. VLANs are configured through software on the switch and router. Its main feature is to reduce broadcast domains. Some important notes on VLANS is that: • VLAN is equivalent to a broadcast domain • VLAN is equivalent to a logical network/subnet
VPN	A virtual local area network (VLAN) is a logical group of end devices, and other network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of end devices and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.
Operational Technology (OT)	OT is the technology that is used to operate, monitor and control the power system. For a more specific definition refer to the OT Practice Note [4]
OT Systems	Are all systems (including electronic, telecommunications, computer systems and components) which process, store or communicate operational data or information [2]
System Owner	The System Owner is the authorised Eskom representative that has overall accountability for the OT system.

2.3.2 Disclosure Classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.4 Abbreviations

Abbreviation	Description
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ASCII	American Standard Code for Information Interchange
BPDU	Bridge Protocol Data Unit
CLI	Command Line Interface
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DNS	Domain Name System
DOS	Denial of Service
DPI	Deep Packet Inspection
ESP	Electronic Security Perimeter
ET	Eskom Telecommunications
FTP	File Transfer Protocol
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
ID	Identification
IED	Intelligent Electronic Device
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MD5	Message Digest Algorithm
MIB	Management Information Base
NAT	Network Address Translation
NGF	Next Generation Firewall
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System

Abbreviation	Description
OSI	Open Systems Interconnection
OSI	Open System Interconnect
OSPF	Open Shortest Path First
OT	Operational Technology
QOS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comment
RTU	Remote Terminal Unit
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Secure Network Time Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
SYN	Synchronise
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protocol
UTM	Unified Threat Management
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network

2.5 Roles and Responsibilities

Eskom OT System owners are accountable for the implementation of this guideline. The Eskom OT System owners may delegate the responsibility of the implementation, management and support of the devices defined in this guideline.

2.6 Process for monitoring

Not applicable.

2.7 Related/supporting documents

Not applicable.

3. Cyber security configuration guidelines of networking equipment for Operational Technology

3.1 Prerequisite information

This information is required prior to configuring the network equipment security settings, and should reside within the electronic security perimeter (ESP) being protected:

1) High level network designs
2) Physical network layout diagram
3) Diagram indicating network connectivity between networking equipment
4) Hardware parameters and authentication types per interface
5) Internet Protocol (IP) Address allocation
6) Virtual LAN (VLAN) table
7) Virtual network and Quality of Service (QOS) allocation
8) Firewall Rules
9) AAA policy
10) WAN parameters to establish connectivity to telecommunications/IT equipment
11) Intrusion Prevention System (IPS) Configuration and rules
12) Authentication server details
13) Syslog logging server and list of requirements to be logged
14) Specific security parameters
15) Virtual Private Network (VPN) parameters

3.2 Prerequisite laptop/computer and/or ICS Based Clients

For most Industrial Control Systems (i.e. DCS, SCADA or PLC based systems) there are existing user interfaces configured which allows for direct access to the switches, routers and firewalls for management purposes, these across the Eskom fleet. However, there are instances were smaller ICS systems do not have an inbuilt management interface for networking devices, in such cases a vendor recommended mobile devices such as laptops could be used to carry out management activities on the devices. Where there is, no vendor recommended devices specified then an Eskom IT user laptop can be used through following the right processes to gain the necessary access rights and install the required applications to enable the management of the network devices.

3.3 Initial upgrades

The following configuration settings are listed in sequence of execution to ensure security:

1) Initially the device must have no network cables plugged in and must be totally standalone. Certain devices are shipped with the capability to perform some basic network functionality; it is dangerous to use a device in this mode as no security settings are configured and this could compromise the environment.
2) Certain devices will automatically attempt to “find home” on power up, this should not be allowed.
3) When configuring encryption, certain devices will initially send out unencrypted messages; this should be monitored externally and negated.
4) If a device has previously been connected to a network and its security status is unknown, then it is recommended to restore the device to factory default settings.

5) The same applies to new equipment that arrives from the factory even if it is in a sealed box or plastic that is designed to be broken. Refer to the specific equipment manual on how to restore factory settings. On some equipment, the resetting to a factory default is achieved at a hardware level by either pressing external switches in a certain sequence; holding down switches on power up; or with the internal PC Board switches.

6) To perform a software upgrade the following applies:

   a) Perform firmware/EPROM/bios upgrade.

   b) Upgrade Memory monitoring software bootstrap program

   c) Perform OS upgrade

   d) Perform software application upgrade which includes the management and monitoring and HTTPS environment.

   e) Perform security upgrade, latest signatures and protocols.

It is recommended to perform these software upgrades even if the version numbers indicate that you are at the latest version. The reason for this is to ensure that you are able to build a system from scratch which may be required if the system security has been compromised. It also guarantees that the device is clean in the event of the device been tampered with on its journey from the factory.

3.4 Management configuration

The following management configuration directives apply:

1) Access to the equipment's management and configuration software must be achieved securely.

2) If the device comes with a local management port, then it shall be mandatory to perform the initial configuration using this port.

3) If the device does not come with a local management port, then a physically or virtually isolated network consisting of the source computer and the device must be created. This should be done through a dedicated VLAN, which needs to be created.

4) The computer used to manage this equipment should reside in an equal or higher security level than the device that it is configuring.

5) Users accessing the network management computer should be from an equal or higher security level than this computer.

3.5 Configuration of Networking Devices

Users should consider the following, as applicable, when configuring their devices:

1) When powering up a device the auto-configuration utility should be disabled as it may skip certain parameters and use factory defaults for authentication. Users should only use this function if the manufacturer explicitly guarantees that the auto-configuration includes all such parameters. Auto or quick configuration utilities usually only configure minimum settings to get the device operational. It might also only configure settings that are applicable to the IT environment, and leave out settings that are used in the OT environment.

2) The local physical management port shall have full privileges throughout the different OS functionality / security layers, but each layer shall have a different username and password.

3) The local physical management port shall have different username and passwords to that of virtual users accessing the device from the network.

4) The device username and password shall be configured in accordance with the Cyber Security Standard for OT [2] for each OS functionality / security layer.

5) The compact flash memory cards to be fully erased prior to commencement.

6) Low level memory management and monitoring to be enabled, including the following settings:

   a) Allocation of reserve memory for critical applications.

   b) If abnormal memory usage is detected, this event shall be logged by the device automatically. High level usage should be logged, as once reached it is an indication of not healthy

   c) Allocation of reserve memory to enable management console access to ensure that if the device is going through a DOS attack the network manager will always be able to get into the device.

   d) Memory leak detection and logging.

   e) Allocate a portion of memory for system crashes that is to be manually accessed and cleared via the management port to ensure that the next crash is saved.

   f) Buffer overflows detection and logging.

   g) Detection and logging of access to memory portions that are factory programmed, should not be accessed by anyone else.

7) The device shall be configured to disable any network boot capabilities.

8) The device shall be configured to disable any scripting environments found on actual devices.

9) Configure backups to reside on both internal and external flash memory before having to back-up to an external device. It is also critical for the user to know how to restore a device from new as backups can contain the incorrect version of configuration.

10) The device shall be configured with at least the following memory allocations; there should be a section of un-writeable memory, a section for user definable parameters, a section for logging, and a section for backups.

11) The device shall have its download parameters configured to enable the OS to be downloaded from a server; e.g. IP address, subnet, default gateway, server name, file, verbose mode, retry count, timeout and checksum parameters.

12) Configure any boot default parameters. For example, if the device is new, it may boot each time from the factory default settings and this will have to be changed for it to boot using your own settings.

13) Ensure that your physical layout and connectivity allows for the physical reduction of your network down to a minimum. This should be achieved by powering off or remotely shutting down the devices. Ensure that network points are available to allow disconnection from the outside world to allow total isolation.

14) Configure host name and IP address.

15) Configure local and virtual terminal characteristics.

16) Limit virtual terminal access to 2 concurrent users.

17) Configure that all passwords cannot be recovered, even from low level memory dump; this means that if passwords are forgotten there is no way of recovery. You then have to attempt passwords until the attempts reach a maximum count of ten and then you have to do a factory reset. If the configuration is not backed up then the configuration will be lost. You might have to manually transfer the configuration onto the device line by line, as a full backup might be locked behind the forgotten password.

18) Each interface is to have a unique name, as this helps when processing log information.

19) Each interface to be configured with the correct hardware interface parameters, such as speed, duplex, auto detections, flow control, media type. Although these parameters have no direct impact on security, if they are incorrectly configured, an error threshold limit might be invoked which could bring the interface down. If an interface continually changes state between up and down it should be treated as a security threat.

20) The device should be configured with the STP Port-fast enabled. The purpose for this is to speed up the interface advertisements on the network and if disabled can negatively affect higher level applications that are time critical in issuing security checks and features to the server that is connected on that interface.

21) The device should be configured with the STP BPDU-guard enabled if the interface is not a member of STP. Some device can assume the root bridge function and affect the active STP topology. To assume the root bridge function, the device would be attached to the port and would run STP with a lower bridge priority than that of the current root bridge. If another device assumes the root bridge function in this way, it renders the network suboptimal. This is a simple form of a Denial of Service (DoS) attack on the network. The temporary introduction and subsequent removal of STP devices with low (0) bridge priority cause a permanent STP recalculation. BPDU guard is set in end node/user interfaces, and its purpose is to prevent an external device become part of the STP algorithm. Never put BPDU guard on trunk ports that are used for inter-switch connectivity as it will bring down the network. Dynamic trunking should also be disabled.

22) Network virtual user access to devices shall be authenticated to an authentication server before being allowed to proceed to the device. The authentication rules on this server for these users are not included in this document but the security access to the networking devices will largely depend on how these rules are configured. Functionality of this authentication server should be to disable the interface of the source upon failed attempts. The reason is to prevent DoS attacks and data floods on your network, which ensures that attackers are stopped on the perimeter of your system.

23) Configure ACLs to filter IP fragments, IP options and TTL. These options should be available on layer 3 devices. Extensive ACLs are used on hardware firewall type devices.

24) Network devices to be configured to allow virtual interfaces to be connected from a specific server that is known to be secure and resides at the correct security level.

25) Network virtual user access to management interfaces to be restricted to HTTPS and SSH access via a separated management VLAN, from a computer located in a higher or equal security zone than the device being accessed. The source of these sessions to be restricted to local users on that network segment, and these HMI computers to be isolated from any remote access capability. MD5 hashing of username and passwords must be selected, and this cannot be used with a plain text type protocol.

26) Disable Telnet, FTP, and HTTP services.

27) Disable unused protocols such as specific manufacturer implemented management protocols. If this is not possible then use them cautiously.

28) DHCP and DNS should not be used on OT systems and therefore be disabled.

29) Auto-discovery type protocols should not be used in an OT environment and therefore should be disabled.

30) Disable any dedicated internet connected interfaces.

31) Configure a virtual user's initial login with username and passwords to not exceed 5 unsuccessful attempts. If this is exceeded then disable all virtual access for 24 hours. If the failed attempts exceed a count of 20 then disable all virtual access permanently. Re-enabling shall only be achieved from the local management port.

32) If a virtual terminal user's username and password fails in excess of 5 times when proceeding through the different functionality levels, then terminate that user's session.

33) Implement user role based functionality, e.g. certain users should only be given view-only and logging type privileges or authorisation.

34) ICMP packet filtering, ping and trace-route can be enabled when its use is required, but should not be allowed from outside the ESP into the trusted network. Its source should come only from a trusted, identified maintenance server, and it should be disabled from all other sources. This prevents HMI users initiating these commands from the end computers, but as a network manager you can use these commands in an outward direction to the HMIs. ICMP contains various functions and it should be tuned according to applicability.

35) Where possible, use of SFTP and SNMPv3 and other management protocols, destination of such data to be located in a higher or equal security level zone to the level of the device/network sending out the data.

36) Select SNMP Management Information Base (MIBs) that will achieve the required logging and remove unused MIBs. SNMP community strings should be unique, default strings such as public or private should be removed.

37) Configure SNTP and ensure that this is the time source that is used for log entries. Configure the device with a SNTP source server within the ACL (Access Control Lists) to guarantee that the source is a valid NTP server.

38) Log everything. All logs must be retained for a predefined amount of time.

39) Backup and restoration to use SFTP and stored in an encrypted format.

40) Any interactive session to have a 15 minute timeout.

41) User Group based restraint to be fully implemented, through all security / management levels.

42) Limit the number of simultaneous human interactive users per group user level.

43) Non-human users connected to device interfaces are to have different authentication credentials to human users. HMI PCs need to have 802.1x authentication, using a username and password. Switch interfaces and servers to have different authentication, such as IP address, MAC address and software based authentication. The rules for the 802.1x should include the shutdown of the interface after 5 failed attempts for 24 hours, if the failed attempts counter reaches 20 then the interface should be shutdown permanently and only re-enabled manually by a network manager.

44) Limit number of simultaneous non-human users to 2 for each switch interface. This is for server type connections and changes will require physical access. This rule will allow a single swop of a MAC address. It should be limited to 2, as a hacker might want to change the profile and apps of this server remotely which might require the change of the MAC address.

45) Local management port to have full privileges but have a different authentication user profile (username and password) to users accessing the device on the other virtual interfaces.

46) Limit access from source via VLAN, for example, once a user has authenticated to work on one device, force the user to re-authenticate centrally before access to another device.

47) Implement a privilege level hierarchy for switch management and monitoring using account based login privileges.

48) Transmission of logs via dedicated VLAN to secure syslog server, that resides at an equivalent or higher security level to the device been logged.

49) Local log buffer to be sized at maximum.

50) Unused interfaces to be administratively shutdown.

51) MAC addresses assignment per interface.

52) For HMI the maximum MAC address per interface is set to one (1).

53) Within restricted secure computer centres, spare interfaces can be left in a non-shutdown and ready to connect state, with its maximum MAC address set to one (1). The reason for this is to assist with breakdown testing. Note that should a spare interface be used, you might be require d to first configure the VLAN number.

54) If the error threshold is exceeded in an interface, shutdown to be automatically activated. Error threshold parameters are dependent on use; the threshold should be configured at levels as to prevent interference with applications.

55) Configure Access Control Lists for routers and layer three (3) switches with IP addresses, ports and unique application signatures (e.g. a protocol) to traverse between two (2) sites or network segment zones.

56) Every switch interface should be allocated a VLAN number and all VLANs should be routed via a firewall. This is to prevent man-in-the-middle attacks as well as to guarantee that users and applications have access to where they are allowed. This VLAN allocation is extremely important when multiple servers reside on a single DMZ network segment. For each server and application holes have to be made in the firewall. If VLANs are not implemented, you are effectively making that hole for all the servers on that segment.

57) QOS should be implemented based on VLANs. At no time should it be possible to bring down the entire network due to data floods. For example, an internal database administrator copies entire database sets for backup. This is extremely important on WAN links with limited bandwidth.

58) Time of use should be implemented, specifically on firewall rules that only require opening for short periods and only a few times a month. Time of use functionality on switches for HMI users is seldom included in the switch; this is done through a RADIUS / authentication server.

59) If a security violation (e.g. unauthorised access) is reached, it is recommended to shut down that interface. If the user selects protect or restrict modes, the port security rate limiter to protect the CPU against excessive load should be configured. When protect or restrict violation modes are configured, the port continues to process traffic after a violation occurs, which might cause excessive CPU load. It might cause the effect of slowness on the network or flip between a working and non-working state.

60) Do not select MAC-address aging timers, as most OT systems are stagnant and any change to network should be planned and done manually.

61) Be careful in selecting MAC-address sticky or the functionality to learn the MAC-address, as these parameters usually come with an aging parameter, allowing the interface to learn a new MAC address.

62) TCP and UDP-small-servers must be disabled, as they could be exploited to indirectly gain information about the target system or directly as is the case with the fraggle attack which uses UDP echo. The services name and port numbers are the following, echo – 7, discard – 9, daytime-13, chargen -19.

63) Incoming packets sourced with invalid addresses (that is not in accordance with the Eskom standard) should be discarded.

64) All username and passwords characteristics, such as strengths and expiry times, shall adhere to the Cyber Security Standard for OT [2].

65) Layer 4 and above type devices host their own certificate authentication for management. It is recommended to use and configure this mechanism even if you had already authenticated at another server.

66) WAN routers are to be configured to their full filtering capability. For example, regarding the controllability of equipment in a substation, if it is IP based and traversing a WAN, the following filter settings should allow only this data through and stop all other data. This should be applied to the router:

a) The Tele-control protocol type number.

b) The Tele-control protocol source and destination port ID number.

c) A specific term in the first payload packet.

d) Multiple filters of specific ASCII characters in the x number byte in the x number packet of the flow.

e) If encryption is used through this router, then this functionality should be provided by a layer 3 physical device or virtualised by an OS or VM host firewall.

3.6 Firewall

1) Before physical network connectivity, validate if default hardware interface prioritisation (level of security) is implemented. If not implemented, any interface may be used for any segment. If implemented, choose the priority from the highest to the lowest security zone.

2) Initially, only physically connect to the management interface of the firewall. The device configuration might be unknown and there might be factory default rules that need to be removed, for example: the device might automatically attempt to get back to vendors servers, which is undesirable.

3) Management should gain access from the highest security zone as this is what is being protected and should also apply to the physical location of the device doing the configuration. The reason for this is that entire desktop sessions can be hijacked and a remote user can gain access to the HMI device and have full control of the user interface. Even if a remote user has to authenticate and is using an encrypted session, if that user interface is compromised, all security measures are rendered ineffective.

4) After completing any upgrades to the firewall, attempt to remove default rules. For example; there might be a rule allowing all traffic from a high security zone to a low security zone. This is undesirable, seeing as once the session is established, unwanted code could come from the lower zone into the higher secure zone.

5) As soon as possible, establish a syslog server in the highest security zone possible and configure the firewall to send all types of messages and include all types of parameters in the firewall syslog. Establish a SNTP server in the highest secure zone; ensure that this time is the single time that is going to be used in all the different types of functionality of the firewall. For example, often the syslog might use a different time to the CLI or HTTPS session.

6) As physical interfaces are established, it is important to perform some threat detection on each zone. The reason for this is to establish how clean the environment is. This should be done before establishing rules that will allow anything to be transferred between two zones. Threat detection is a network scan and listens to all traffic, profiling potential threats. Examples of threats include: incomplete session detection (TCP SYN), no data UDP session, ICMP packets, DOS, connection limit exceeded and bad packet format, other nodes performing network scans. The firewall can handle this in various ways. Firstly it must log any findings and secondly it should “shun” the IP address that is deemed insecure. Once an IP is shunned, the firewall will ignore all traffic relating to this IP. Once you have removed the problem then you have to un-shun the IP. It’s important to keep threat detection enabled, however the CPU performance on operational data would be impacted.

7) Configure IP address to English names of servers and then create logical groups based on same or similar functionality. Grouping of IPs have to reside physically in the same zone.

8) Configure static NAT. Dynamic NAT is not used in OT, it is a static environment.

3.7 Intrusion Prevention System (IPS)

1) **IP Audit** - This feature looks at the composition of the IP packet, if it matches a predefined signature, it can be acted upon based on user preferences. Signatures are pre-classified based on the severity or likelihood of the packet format and the content containing vulnerabilities. Each manufacturer has a different classification rating, but they usually range from “informational” to “attack”. The actual signatures themselves are vendor specific, and descriptions can be found on Internet. Signature definitions require upgrades as hackers evolve their methods of attack.

   It is important to have knowledge of the software applications traversing the firewall as some apps might match a signature and the action might be to discard this packet.

2) **Fragmentation** - The fragmentation method of IP packets is used by hackers to insert vulnerabilities. The IPS can be configured with multiple parameters to define how it will handle fragmentation - there are threshold points that once exceeded will block the packet.

   If you have an application that routinely fragments packets and it's unavoidable to upgrade or change the app then you will have to configure the IPS to allow these packets through. For this reason it's better to run the IPS in a listening mode first in order for the human to learn the network, otherwise interruption of production data might occur.

3) **Anti-Spoofing** – Unicast Reverse Path Forwarding (URFP) guards against IP Spoofing by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table of the firewall. IP Spoofing is when a packet deliberately uses an incorrect source IP address to obscure its true source. A standard router usually looks at the destination address that is used to determine where that packet must be routed to; through this mechanism the routing table includes fields containing the route back to the source address.

4) **TCP Options –** Functionality that could be implemented at a TCP level includes: Inbound and Outbound Resets and timer settings, maximum and minimum segment size, counter settings for Time-Wait state.

5) **High level application protocols –**This document covers generic protocol and low level functionality at an IP and TCP level. IPS functionality for higher level protocols requires a separate unique document for each protocol and is out of this scope.

3.8 Logging of Devices

It is recommended to, at a minimum, log the following events for equipment, and send such logs to a syslog server or network management environment.

1) Power off and on off switch.
2) CPU utilisation (sampled per second with minimum, maximum and average logged per minute).
3) Failure for interface to connect after an auto discovery.
4) Authentication success and failure.
5) Log detection of malicious code.
6) Network topology change and the change of switches role.
7) Activation of a level that allows for switch configuration changes.
8) Environmental parameters:
   a) Temperature (update once per second)
   b) Fan failure
   c) Failures that identify replacement modules
   d) Power supply monitoring parameters.
9) Interface operation state changes:
   a) Shutdown due to physical disconnection or power off of connected device.
   b) Shutdown due to maximum MAC address parameter been exceeded.
   c) Shutdown due to error threshold state exceeded.
   d) Shutdown by administrator.
10) VLAN:
   a) Creation
   b) Joining or inclusions into trunks
   c) Deletion

d) Membership changes

11) Protocol specific parameters:

a) Changes

b) Health

c) Monitoring of performance

12) Performance monitoring:

a) Bandwidth utilisation per interface (update once per second)

b) CPU utilisation (update once per second)

c) Memory errors and utilization

d) Memory buffer pool

e) Memory pool

f) Memory buffer peak

4. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Prudence Madiba	Senior Manager - Control and Instrumentation
Rishi Hariram	Middle Manager – Control and Automation Technology and Support
Amelia Mtshali	Middle Manager – Metering, DC and Security Technology and Support
Rosalette Botha	Corporate Specialist – System Operator
Marius van Rensburg	Transmission Grid Representative
Johan Botha	Senior Consultant – System Operator
Geoffrey Ive	Chief Technologist – System Operator
Reshin Moodley	Chief Engineer – OT Cyber Security Care Group Convenor
Craig Boesack	Chief Engineer - Control and Instrumentation
Zameka Qabaka	Senior Technologist – Koeberg Power Station
Ian Naicker	Chief Engineer - Control and Automation Technology
Tertius Hyman	Senior Engineer - Western Cape Operating Unit

5. Revisions

Date	Rev	Compiler	Remarks
Aug 2021	2	K. Manyapetsa	Expanded the Executive Summary page Reduced the list of excluded items on section 2.1 Scope, to be more in line with the objectives of the guideline. Elaborated on the intended audience on section 2.1.1 and 2.1.2 Expanded the normative and informative on section 2.2 Added more definitions and abbreviations on section 2.3 and 2.4 Generalized section 3.2 Removed section 3.9 as it was mainly addressing WAN and layer 3 dynamic routing protocols which are not prevalent on the OT domain.
May 2015	1	G. Ive	First Issue

6. Development team

The following people were involved in the development of this document:

Cyber Security Care group Members.

7. Acknowledgements

- Johan Botha
- Geoffrey Ive