Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

005 – Network Management and Access Control v1.0

2021

Prepared by Department of the
Environment, Climate & Communications
gov.ie/decc

Table of Contents

1 Foreword

The Electronic Communications Security Measures (ECSMs) have been produced by the Electronic Communications Security Measures working group convened by the Irish National Cyber Security Centre (NCSC), which forms part of the Department of the Environment, Climate and Communications (DECC); and with the support of the Commission for Communications Regulation (ComReg). Industry participation in the WG has involved network operators, including the Mobile Network Operators (MNO) which have been awarded 5G licences, and selected fixed line operators.

This ECSM is part of a series of documents listed below:

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity
…	…

2 Introduction

Ireland's modern digitally connected society and economy is highly dependent on reliable and secure electronic communications networks and services (ECN and ECS respectively). They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisation security measures.

The ECSM Working Group Convened on the 02nd, 3rd and 04th of June to discuss matters concerning secure network design, deployment and operation. The group heard from experts in the field of telecommunications operations, security and incident response and held focussed discussions on the risks, challenges and best practices associated with network design and access control as it pertains to telecommunications networks. ECSM 005 –Network Management and Access Control has been developed by the NCSC informed by those meetings.

3 Scope

The ECSMs are applicable to all undertakings providing public Electronic Communications Networks and Electronic Communications Services.

The legislative basis for the ECSMs is set out in ECSM 001- General

4 References

Document	Title
ENISA	Supplement to the technical guideline on Security Measures under the EECC
ENISA	Technical Guideline on Security Measures under the EECC
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls
ITU Rec M.3016	Security for the Management Plane
NIST	Framework for Improving Critical Infrastructure Cybersecurity v1.1
NIST SP 800-100	Information Security Handbook: A Guide for Managers
NIST SP 800-53 R4	Security and Privacy Controls for Federal Information Systems and Organizations

5 Definitions, Symbols and Abbreviations

5.1 Definitions

Term	Meaning
Privileged Access Workstation	A dedicated computing environment for sensitive tasks that is protected from Internet attacks and other threat vectors.
Component	Part of a system that has operational and/or management significance
Control Plane	The control plane has a layered structure and performs the connection control functions; it deals with the signalling necessary to set up, supervise and release connections
EU 5G Security Toolbox	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures' document published jointly by member states on 31st of January 2020
EU Risk Assessment	EU coordinated risk assessment of the cybersecurity of 5G networks report published jointly by the EU Member States on 09th October 2019

Incident Response	Actions taken to mitigate or resolve a security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.
Interface	Common boundary between two associated systems.
Jump Server	A jump server is a hardened remote access server. It acts as a stepping point for administrators accessing critical systems with all administrative actions performed via a jump server.
Management Plane	Performs management functions for the User and Control Plane, and the system as a whole. It also provides coordination between all the planes. Performance, fault, configuration, accounting, and security management are performed in the Management Plane.
Multi Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Managed Service Provider (MSP)	A third-party that helps to run or administrate a network.
National Risk Assessment	Risk assessment carried out by the National Cyber Security Centre and forwarded to the European Commission on 15 July 2019.
Operator	An undertaking providing or authorised to provide a public electronic communications network or an associated facility
Privileged/Administrative Access	An access to network equipment where greater

	capabilities are granted than a regular user. Accounts granted privileged access can be used to perform elevated security relevant functions including modifying configurations, changing security controls, creating new accounts with equal or greater privilege or allowing full control of network equipment. .
Security Event	Any observable occurrence in a network or system that poses a risk to the security of networks and services.
Security Incident	An event having an actual adverse effect on the security of electronic communications networks or services.
Security of Networks And Services	The ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services
User Plane	Plane that has a layered structure and provides user information transfer, along with associated controls

34 ## 5.2 Symbols

35 Nil

36 ## 5.3 Abbreviations

Term	Meaning
AV	Anti-Virus
C2	Command and Control
ComReg	The Commission for Communications Regulation

CSIRT	Computer Security Incident Response Team
DECC	The Department of Environment, Climate and Communications
JML	Joiners, Movers, Leavers
MFA	Multi Factor Authentication
MNO	Mobile Network Operator
MSP	Managed Service Providers
NCSC	National Cyber Security Centre
PAW	Privileged Access Workstation
ECSM	Electronic Communications Security Measures

37

38

6 Overview of Risk

The Management Plane of a network is where administrative activity takes place. It is the most powerful part of the network infrastructure; whether that is the provision and configuration of new equipment, changes to existing infrastructure, or any other modification of running equipment or services. This also makes the management plane the primary target for any malicious attack intending to disrupt or otherwise compromise the operation of a network. Exploitation of the management plane could have a long-term impact on the availability and confidentiality of the operator's services, including critical services.

Most attacks originate directly or indirectly from internet sources and use the internet for exfiltration and command and control (C2). Securely separating the privileged access from the open internet is a key element to ensuring the management plane is not compromised. Given the number of users and devices with access to email and the internet, the corporate network is inherently insecure.

Administrative "Jump Server" architectures set up a small number of administrative console servers and restrict personnel to using them for administrative tasks. This is typically based on remote desktop services, a 3rd-party presentation virtualization solution, or a Virtual Desktop Infrastructure (VDI) technology.

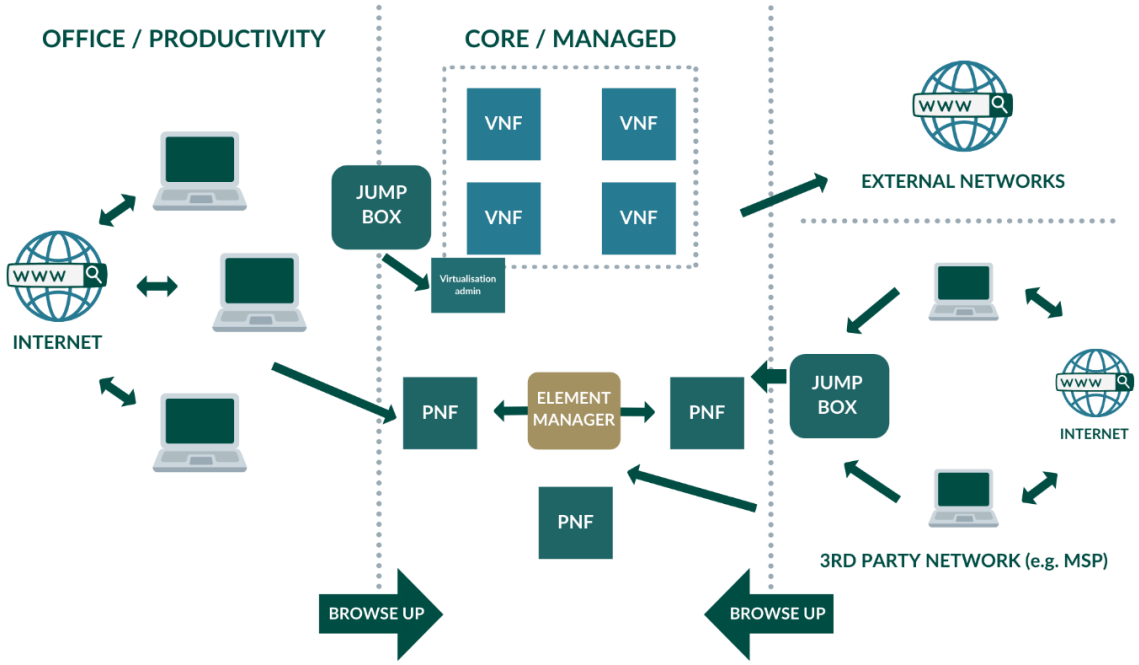

Figure 1 – Typical Administrative "Jump Server" Architecture

This approach is frequently proposed to mitigate risk to administration and does provide some security assurances. For example, it provides significant advantages over directly connecting to nodes as it allows more effective management, logging and monitoring of privileged access, as well as providing a platform to include additional security features such as multi-factor authentication (MFA), while providing cost saving over more secure architectures.

However, the jump server approach by itself is vulnerable to certain attacks because it violates the "clean source" principle[1]. The clean source principle requires all security dependencies to be as trustworthy as the object being secured. In the above architecture, a privileged user is using the same device to access the management plane of the operational network whilst also accessing less secure networks such as the operator's corporate network, and the wider internet, increasing the risk of an attacker compromising their device or privileged accounts. This could be achieved through a number of techniques such as phishing, drive-by compromise, and replication through removable media or moving laterally from other compromised hosts on the corporate network.

Figure 2 – Failure of the Clean Source Principle

Compromise of privileged user accounts (e.g. via phishing) could lead to:

- Credential loss (e.g. leading to unauthorised remote access or gathering of information for future exploitation).
- Remote code execution (enabling an attacker to gain a foothold on machines used for administrative use).
- Further exploitation of networks or users (the potential to move laterally to other resources through use of privileged user accounts).

By gaining access to the Management Plane of an operator's network, an attacker gains the highest possible levels of privilege, and in addition to accessing sensitive data, could cause

[1] Success criteria for privileged access strategy | Microsoft Docs

severe disruption or damage to the operational network, and have serious impacts on critical infrastructure and services which rely on the availability of electronic communications networks and services. As such, protection of the Management Plane should be of the highest possible priority for operators.

7 Security Measures

The operator should implement the Network Management and Access Control Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
NM.01	The operator shall securely separate their network based on purpose. Wherever feasible, network service planes that carry user, control and management traffic shall be separated either physically or logically.
NM.02	The Management Plane is the highest trust domain within the operator's networks. The Management Plane shall be securely separated from lower trust domains such as the operator's corporate network, other operator's networks and the internet.
NM.03	All components, equipment, and interfaces (both physical and virtual) comprising the Management Plane shall be clearly identified.
NM.04	The Management Plane shall remain under the oversight and ultimate control[2] of the operator.
NM.05	The operator shall explicitly grant authorisation and privileged access to the Management Plane.
NM.06	Access to the Management Plane shall be attributed to individual authenticated users, a purpose and a limited time period.
NM.07	Operators should enforce the principle of least privilege and separation of duties on their privileged users. Exceptions shall be documented, risk assessed and justified.
NM.08	Access to the Management Plane shall be through a dedicated jump server and require Multi Factor Authentication, wherever feasible. Exceptions shall be documented and follow a defined emergency access procedure.

[2] Ultimate control in this respect means that the operator retains the ability to undo actions by or remove access of third parties accessing the Management Plane of the network.

NM.09	All Access to and activity undertaken on the Management Plane shall be logged and monitored in line with ECSM 008.
NM.10	The Management Plane shall only be accessible from secure devices / PAWs, which are trusted and have been authenticated, and whose attack surface has been minimised.
NM.11	Managed equipment shall be locked-down. Only necessary management protocols shall be enabled. Where technically feasible, management traffic shall use secure encrypted protocols.
NM.12	Where third parties such as Managed Service Providers (MSPs) and equipment vendors require access to the management plane it should not reduce the overall security of the network and wherever feasible, shall use the same security measures as those employed by the operator themselves in line with ECSM 009.

96

97

8 Implementation Guidance

The following guidance sets out an illustrative security architecture for network management which is designed to meet the Security Measures set out in Section 7 and is intended to assist operators in defining their own solution to securing their Management Plane depending on their own specific operational and risk context. There is no single "silver bullet" technical solution that will entirely mitigate risks associated with privileged access to the Management Plane, operators are required to blend multiple technologies together into a holistic solution that protects against multiple attacker entry points.

The implementation guidance in the following subsections is applicable to the security measures in section 7 as shown in **Error! Reference source not found.** below.

Table 1 – Security Measures to Guidance Mapping

	NM.01	NM.02	NM.03	NM.04	NM.05	NM.06	NM.07	NM.08	NM.09	NM.10	NM.11	NM.12
8.1	✓	✓	✓	✓				✓		✓	✓	
8.2				✓	✓	✓	✓	✓	✓			✓
8.3		✓						✓	✓	✓	✓	✓
8.4	✓	✓	✓			✓			✓	✓		✓
8.5										✓	✓	
8.6		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

8.1 Network Architecture

Applicable Security Measures: NM.01, NM.02, NM.03, NM.04, NM.08, NM.10, NM.11

Building on the typical jump server architecture described in Section 6, the network architecture outlined below provides an enhanced level of security through increased network segmentation. The use of PAWs for administration of the Management Plane helps reduce the risks which emanate from less secure networks such as the internet.

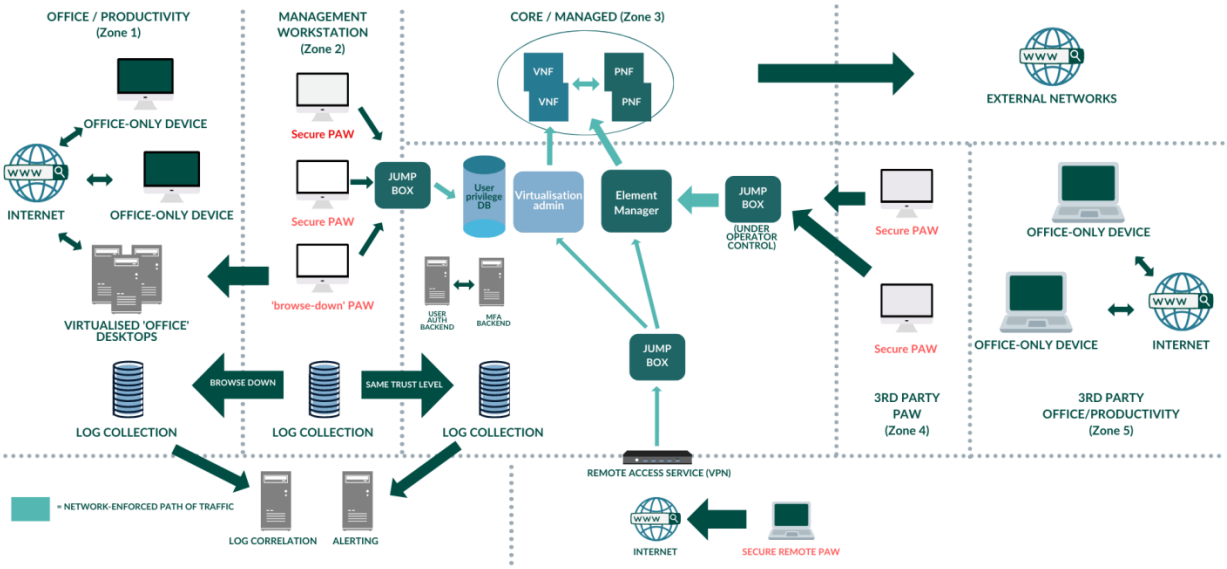

Figure 3 – Secure Network Architecture implementing PAWs

The architecture consists of a series of security zones:

- Zone 1 is the ‘productivity’ or ‘office’ zone used to perform business functions such as email and internet browsing.
- Zone 2 contains the workstations used by Administrators to manage the network
- Zone 3 contains the management infrastructure, used to support network management, and the managed network equipment itself.
- Zone 4 contains the workstations used by 3rd-party Administrators (3PAs) working in external organisations, such as Managed-Service Providers (MSPs) and vendors providing third-line support.
- Zone 5 is the ‘productivity’ or ‘office’ zone used by the 3PA.

8.2 Privileged Access

Applicable Security Measures: NM.02, NM.04, NM.05, NM.06, NM.07, NM 08, NM.09, NM12

Operators need to make securing privileged access to the management plane the top security priority due to the significant potential impact and high likelihood of attackers compromising this level of access. Securing privileged access to the management plane

effectively seals off unauthorized pathways and leaves a select few authorized access pathways that are protected and closely monitored.

8.2.1 Least Privilege & Separation of Duties

The principles of Least Privilege[3] and Separation of Duties[4] should be applied to privileged access to the management plane. To achieve this, privileged users should only be granted specific privileged accounts and associated permissions which are essential to their business role or function. Privileged user accounts should be generated from a least privilege role template and modified as required. Account privileges should not be copied from existing users.

Privileged access should be via accounts with unique user ID and authentication credentials for each user and these should not be shared. Privileged access should be temporary, time-bounded and based on a ticket associated with a specific purpose, including routine maintenance. Tickets should not have a duration of longer than 12 hours and access should be automatically revoked once the ticket is closed. As certain tasks, particularly when resolving incidents, may require periods of longer access, tickets may be reauthorised for further periods of 12 hours whilst the ticket is open. The process for re-authorisation should not be burdensome. Accounts with read-only access, such as those used for network monitoring purposes should not be considered as privileged access or require a ticket.

Administrators should not be able to grant themselves privileged access to the network. Privileged user access rights should be regularly reviewed and updated as part of business-as-usual management. This includes updating privileged user rights as part of the joiners, movers and leaver's (JML) process. Further details on JML process can be found in ECSM 004 – Training, Awareness and Personnel Security.

It is accepted that applying the principles of Least Privilege and Separation of Duties may be challenging, particularly for smaller operators with limited resources, where individuals may be responsible for managing large parts of the network. Therefore, given a business need, administrators can have multiple roles, each with its own account, provided the risk of doing so has been considered and accepted as part of the operator's risk management process.

8.2.2 Multi Factor Authentication

Privileged access should be via accounts secured with MFA. The second factor should be locally generated, and not be transmitted (i.e not SMS). The MFA mechanism should be

[3] Principle of Least Privilege - Glossary | CSRC (nist.gov)

[4] Separation of Duty (SOD) - Glossary | CSRC (nist.gov)

independent of the operator's network and secure device. Soft tokens (e.g. authenticator apps) can be used for this purpose.

It is important to ensure that the system implemented for MFA does not become a burden upon administrative users. For example, this could include multiple requests to authenticate within a session when connecting to multiple different hosts for example – implementations like this may promote negative behaviours such as blindly accepting any prompts or creating workarounds.

It is accepted that many nodes, particularly in legacy networks, do not supportt MFA. Therefore access should be through a jump server which supports MFA.. It is accepted that engineers may need to access nodes directly, particularly to resolve network issues; however this should not be the norm and should follow procedures as outlined in 8.2.3 Emergency Access Procedures.

8.2.3 Emergency Access Procedures

It is accepted that there is a requirement for emergency access procedures, particularly in response to incidents. Therefore break-glass credentials should exist to allow for network recovery, but existence of these credentials should not compromise the security of the network.

When an emergency occurs, security requirements may temporarily be suspended. Clean-up steps should be performed after the emergency is resolved to ensure the suspension of these requirements has not compromised the network. Where an ‘emergency’ event occurs, this should be recorded and reviewed, along with the reason and time period for which controls were suspended.

Emergency privileged user accounts should be present for emergency access outside of change windows, but security alerts should be raised when these are used, the circumstances investigated, and all activity logs reviewed post emergency.

All emergency privileged user accounts should have unique, strong credentials per network equipment. Emergency privileged user account credentials should be single use and changed after use.

8.3 Secure Devices / Privileged Access Workstations (PAWs)

Applicable Security Measures: NM.02, NM.08, NM.09, NM.10, NM.11, NM.12.

In simplest terms, a PAW is a hardened and locked down workstation designed to provide high security assurances for sensitive accounts and tasks. This is the highest security configuration designed for extremely sensitive roles that would have a significant or material impact on the organization if their account was compromised.

The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensitive tasks. This makes the PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: email and web browsing.

To provide productivity to these users, separate accounts and workstations should be provided for productivity applications and web browsing. While inconvenient, this is a necessary control to protect users whose accounts could inflict damage to most or all resources in the organization.

8.3.1 Deployment Options

There are two main options when considering implementing PAWs for Management Plane administration:

- **Dedicated Hardware**: A device solely used for administration of the management plane. In this scenario, a PAW is used for administration that is completely separate from the PC that is used for daily activities like email, document editing, and development work. All administrative tools and applications are installed on the PAW and all productivity applications are installed on the standard user workstation.
- **Simultaneous Use**: Use of OS virtualisation to separate privileged tasks from normal business user functions and the internet

There are advantages and disadvantaged of both approaches:

Scenario	Advantages	Diadvantages
Dedicated hardware	• Strong signal to users to the sensitivity of tasks being performed • Strongest form of security separation	• Additional desk space • Additional weight (for remote work) • Hardware Cost • Could encourage 'work-arounds' due to cumbersome nature

Simultaneous use	• Lower hardware cost • Single device experience	• Sharing single keyboard/mouse creates risk of inadvertent errors/risks

There are two potential options in implementing a simultaneous use for PAWs:

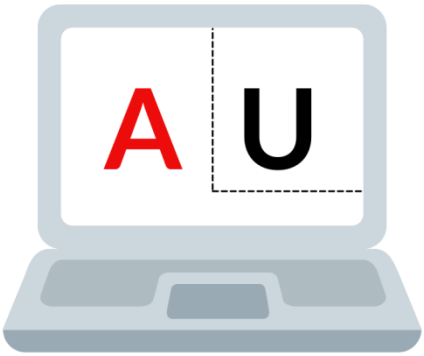

Figure 4 – Config 1

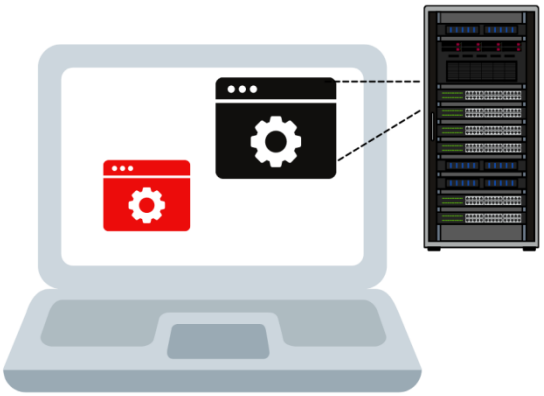

Figure 5 – Config 2

Config 1 illustrates the physical hardware running two operating systems locally. The physical host runs the secured Admin OS where all privileged administrative work is carried out whilst a hypervisor virtual machine runs a corporate image which is used for normal business functions.

Config 2 illustrates as similar setup except the corporate image is deployed and managed centrally on the cloud or in the operator's datacentre.

8.3.2 Hardening

When implementing a PAW-based solution, it is important to implement appropriate hardening to ensure their integrity for use as administrative workstations. Hardening should consider the following matters -

Hardening Guidelines for PAWs	
Secure OS	Use of a 'clean' known-good operating system image to build PAWs.
Applications	Ensure that only authorised applications are permitted to run, minimising the

	potential for malicious code to run
Encryption	Use of full-disk encryption to maintain security of data in the result of theft or loss..
Security updates	Security updates should be applied on a regular basis to ensure vulnerabilities are patched in a timely manner
Removable media	Removable media use should be blocked by default. In exceptional circumstances, whitelisted devices may be connected
Least privilege	Non-administrator accounts should be in use for routine tasks to minimise the ability for malicious code to run and to compromise the entirety of the PAW.
Local Admin	Local device administration rights should be removed
Endpoint Protection	PAWs should have up to date Anti-Virus (AV) protection installed
Web browsing	URLs should be restricted to an approved list with the default being to deny
Monitoring	PAWs devices should be monitored for the detection of malicious or unusual activity.

Web browsing and productivity applications are **not** allowed on PAWs in order to reduce the attack surface that an attacker can attempt to exploit. Web browsing here refers to general access to arbitrary websites which can be a high risk activity. Such browsing is distinctly different from using a web browser to access a small number of well-known administrative websites required to administer the network.

8.3.3 Remote Access for Secure Devices / PAWs

Whilst it is accessing networks are from dedicated PAWs directly on the network is generally more secure, changes in the working environment as a result of the COVID-19 pandemic mean that remote access will be required more often. This is particularly in response to incidents and/or outages. Remote access should be conducted in a way which does not reduce the overall security of the network.

Remote access can be securely configured using a VPN tunnel. Remote PAWs should not be able to make outbound connections (e.g. access the Internet) without first accessing this remote access endpoint. This would constitute an "always on" tunnel brought up at the point network connectivity becomes available, and all network traffic and administration activity being forced down this tunnel.

8.4 Information Flow Enforcement

Applicable Security Measures: NM.01, NM.02, NM.03, NM.06, NM.09, NM.10, NM.12

In order to prevent a compromised element from further compromising other elements of the core operators should ensure they have established adequate information flow enforcement rules. Restrictions should be put in place to ensure that valid management traffic is only permitted outbound from devices that are intended for this purpose (such as jump boxes and element managers). This is traditionally achieved through network segmentation tools such as firewall rules and Access Control Lists (ACLs), however next-generation networks concepts such as software defined networks (SDN) offer opportunities for this to be centrally and programmatically orchestrated.

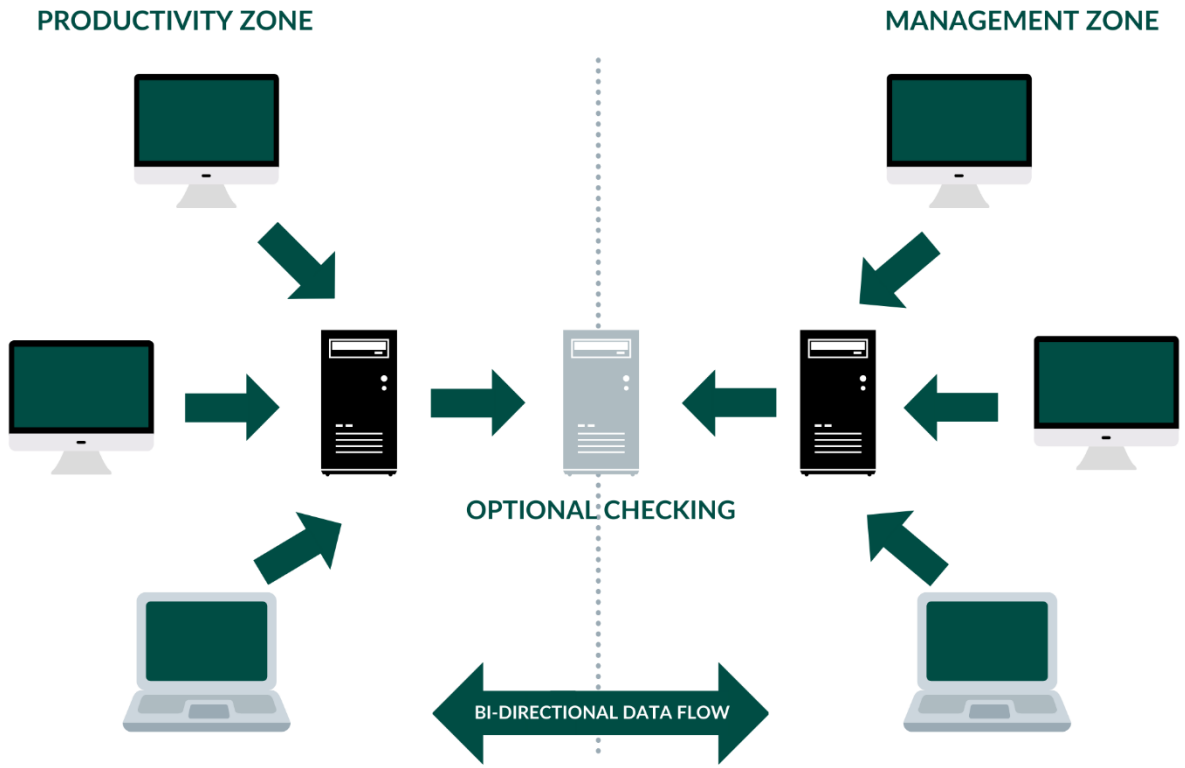

Figure 6 – Data flows between segmented networks

In order to facilitate data flows between segmented networks, dedicated endpoints should be placed in each segmented network which allows data to be pushed to or pulled from

respective security zones. The use of dedicated endpoints for this purpose allows the full chain of events to be understood such as: sending user, date & time, file details, metadata and receiving user etc. – this information can be used to investigate any unauthorised or malicious data flows. The endpoints can be configured to allow any additional file verification or filtering.

8.5 Secure Management Protocols

Applicable Security Measures: NM.10, NM.11

Certain network equipment may ship with legacy or insecure management protocols enabled. Even though an operator's Management Plane may be considered 'closed' from the purposes of observation of network traffic, due to the size and scale of some networks it may not be possible to guarantee that traffic is unobserved in all cases.

Given that management traffic typically involves sensitive information and/or credentials being passed via these channels, it is therefore essential that all management is performed over secure protocols. Manufacturer-supplied hardening guides typically exist for the vast majority of network infrastructure. These can be followed to ensure insecure protocols are disabled. Implementation should be followed up by scans against infrastructure to ensure that hardening has been properly implemented.

Management traffic should be secured as the norm using non-proprietary encryption protocols. Unencrypted network management is only permitted where no other option is technically feasible. Management protocols that are not required should be disabled on all network functions and equipment. Default and hardcoded accounts should be disabled and default passwords should be changed upon initialisation of the device or service.

For 5G networks, ENISA has published detailed guidance[5] on the security specifications and standards, including the key security controls that operators should implement and what the role of such controls are for achieving the overall security of 5G networks.

8.6 Third Party Access

Applicable Security Measures: NM.02, NM.03, NM.04, NM.05, NM.06, NM.07, NM.08, NM.09, NM.10, NM.11, NM.12

Providing third parties such as MSPs or 3PAs with privileged access to the Management Plane should not reduce the overall security or integrity of the network. Outsourcing responsibility for this task does not allow for the outsourcing of accountability.

[5] Security in 5G Specifications - Controls in 3GPP — ENISA (europa.eu)

Further guidance on the use of third parties is covered in detail in ECSM 009 – Supply Chain Risk Management however the following should be applied when providing privileged access to third parties:

- Access to the management plane should be via the same methods and associated security measures as those employed by the operator themselves
- PAWs which are separated from the third parties corporate system and the internet.
- Third party should be through a dedicated third party jump box which is under the operator's control.
- Third party access should be logged, monitored and audited.
- Contractual arrangements should be in place to enforce security measures.

It is expected that where an operator has an ongoing relationship with an MSP, whereby they manage large parts of the network on a day–to-day basis that the same level of security measures, including the use of PAWs would apply and be enforced through contractual arrangements.

It is accepted, however, that such a set up is not practical to implement for all third party access, such as where a vendor provides third line support on an irregular or infrequent basis. In such instances focus should be on the other security measures, such as access through a jump server under the operator's control, the use of a VPN restricted to specific IP ranges, access explicitly granted on a per ticket basis, for a purpose and a time limited period, and strict logging, monitoring and auditing of access.

8.7 Transitionary Arrangements

It is acknowledged that operators will have varying network architectures and security postures and transitioning to an architecture that meets the Security Measures set out in Section 7 is a complex task which may require significant investment both financially and in terms of subject matter expertise. It is also acknowledged that a significant amount of time may be required, particularly where an operator is starting from a lower base.

During the transition period operators should build their approach incrementally and focus on taking the most effective actions with the fastest time to value first. For example, ensuring that jump servers and workstations are hardened, access is strictly monitored and audited and multi-factor authentication is enabled.

A transition to a more secure architecture for administering the Management Plane, in particular the use of securely separated PAWs, may have a significant impact on current

workflows for the administrators of the operator’s network; however this implementation should be carefully planned and done thoughtfully to limit the usability impact and scope as much as possible. However, it may not be possible to completely eliminate all workflow disruption, as for users with privileged access the balance between productivity and security is weighted towards security due to the higher risks associated with compromise

9 Relevant References

The following standards, guidelines and reports offer further detail and will assist operators in designing policies, procedures and processes that meet the *Security Measures* outlined in Section 7 of this document.

9.1 MITRE ATT&CK Privileged Account Management

Privileged Account Management, Mitigation M1026 - Enterprise | MITRE ATT&CK®

MITRE ATT&CK guidance on privileged account management offers detailed advice on managing the creation, modification, use, and permissions associated to privileged accounts. It offers practical controls that organisations can implement to overcome real threat actor techniques.

9.2 UK National Cyber Security Centre Secure System Administration Guidance

Secure system administration - NCSC.GOV.UK

The UK NCSC has published detailed guidance on how an organisation can design principles for IT and OT systems and assist in developing and implementing a system management strategy to protect an organisation's most sensitive data.

9.3 Australian Cyber Security Centre Guidance

Secure Administration | Cyber.gov.au

The Australian Cyber Security Centre guidance on Secure Administration offers advice on protecting sensitive accounts and resources from an adversary who has gained a presence on a network. It details topics such as privileged access control, multi-factor authentication, PAWs, Logging and Auditing, Network Segmentation and Segregation and the use of Jump Boxes.

9.4 Microsoft Securing Privileged Access Guidance

Securing privileged access overview | Microsoft Docs

Microsoft has published detailed guidance on managing privileged access. Although this guidance is tailored to Microsoft products it contains principles and security measures that are technology agnostic. It contains advice on designing a privileged access strategy, measuring success, setting security levels, hardening privileged access devices and a rapid modernisation plan that allows organisations select the most impactful changes first.

9.5 Security in 5G Specifications – Controls in 3GPP

Security in 5G Specifications - Controls in 3GPP — ENISA (europa.eu)

The objective of this report is to help MS implementing the technical measure TM02 from the EU toolbox on 5G security. The report is also intended to help national competent and regulatory authorities get a better picture of the standardisation environment pertaining to 5G security and to improve understanding of 3GPP security specifications and its main elements and security controls. With this, competent authorities will be in a better position to understand what the key security controls that operators have to implement are and what the role of such controls is for achieving the overall security of 5G networks.