Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Network segmentation and segregation – Overview

Table of contents

Introduction

As organisations adopt cloud services, hybrid work models, and interconnected digital services, network environments have become more complex. Traditional security architectures that rely mainly on perimeter-based controls and internet gateways are no longer sufficient to address contemporary threats, necessitating a more holistic approach to network security. Once a malicious actor gains access to a network, lateral movement allows them to compromise additional services, increasing the impact, duration and cost of recovery.

Network segmentation and segregation is a foundational element of implementing ASD's modern defensible architecture (MDA) including a Zero Trust Architecture (ZTA). It is a recommended mitigation capability that helps prevent lateral movement, unauthorised resource access, and other malicious techniques. By establishing logical or physical boundaries within an enterprise network, organisations can create isolated environments with varying levels of trust, authentication and authorisation. This enables communication flow to be controlled according to business requirements and risk profiles while providing defenders with more granular options for network monitoring, traffic analysis and incident response.

Network segmentation and segregation enable organisations to position security controls closer to the assets they protect, improving visibility and policy enforcement. Investing in segmentation and segregation helps organisations meet government policy, regulatory obligations, and industry security requirements.

Network segmentation and segregation directly support a defence-in-depth strategy by reducing the potential consequences of a security compromise. By controlling how users, systems, applications and services communicate, organisations can better protect critical business functions, contain incidents, and maintain operational requirements while reducing overall cyber security risk.

Decision-makers need to prioritise segmentation and segregation activities according to business criticality, information sensitivity, regulatory obligations, and the potential consequences of a compromise.

Audience

This publication provides decision-makers with practical guidance to govern, fund and oversee network segmentation and segregation initiatives.

It is intended for executives, accountable authorities and senior decision-makers across small to large enterprises, including critical infrastructure organisations subject to regulatory compliance requirements, and government entities. It is also intended to help staff brief boards and other decision-makers on network segmentation and segregation risks and initiatives.

This publication is supported by ASD's MDA and ASD's *Information Security Manual* (ISM). It is designed to assist organisations in making informed, risk-based decisions that strengthen cyber

resilience while supporting business objectives. The publication outlines key business considerations, governance responsibilities, and strategic principles that enable effective implementation and ongoing management of network segmentation and segregation.

This document forms part of the network segmentation and segregation publication series:

- ***Network segmentation and segregation - Overview*****,** covering strategic, governance and assurance considerations.
- ***Network segmentation and segregation - Anti-patterns*****,** covering recurring operational failure conditions, threat-informed case-study analysis and continuing assurance.

Key terms and concepts

Network segmentation: the practice of partitioning a network into smaller logically or physically separated network segments or 'zones'. It architecturally divides one large network into distinct network zones or subnets.

Network segregation: developing and enforcing a ruleset for controlling communications between specific hosts and services. It is the policy enforcement and control capability.

Network isolation: the practice of physically and logically isolating a network or zone from all other networks or zones.

Lateral movement: (east-west movement) a technique used by a malicious actor to move from an initially compromised host to other systems on the same network.

Vertical movement: (north-south movement) permitted network traffic of a legitimate or malicious actor between zones of differing trust or sensitivity. For example, from user environment to a server environment or from the internet to a web server.

Microsegmentation: an extension of segmentation that enforces policy at a much finer granularity, down to the individual workload, application, device or service level within a network segment, to limit lateral movement within a segment and enforce least-privilege.

Macrosegmentation: coarse-grained division of a network into a small number of larger network zones, environments, or trust domains, to prevent a compromise in one broad area from spreading to another. For example, between corporate Information Technology (IT) network and Operational Technology (OT) network.

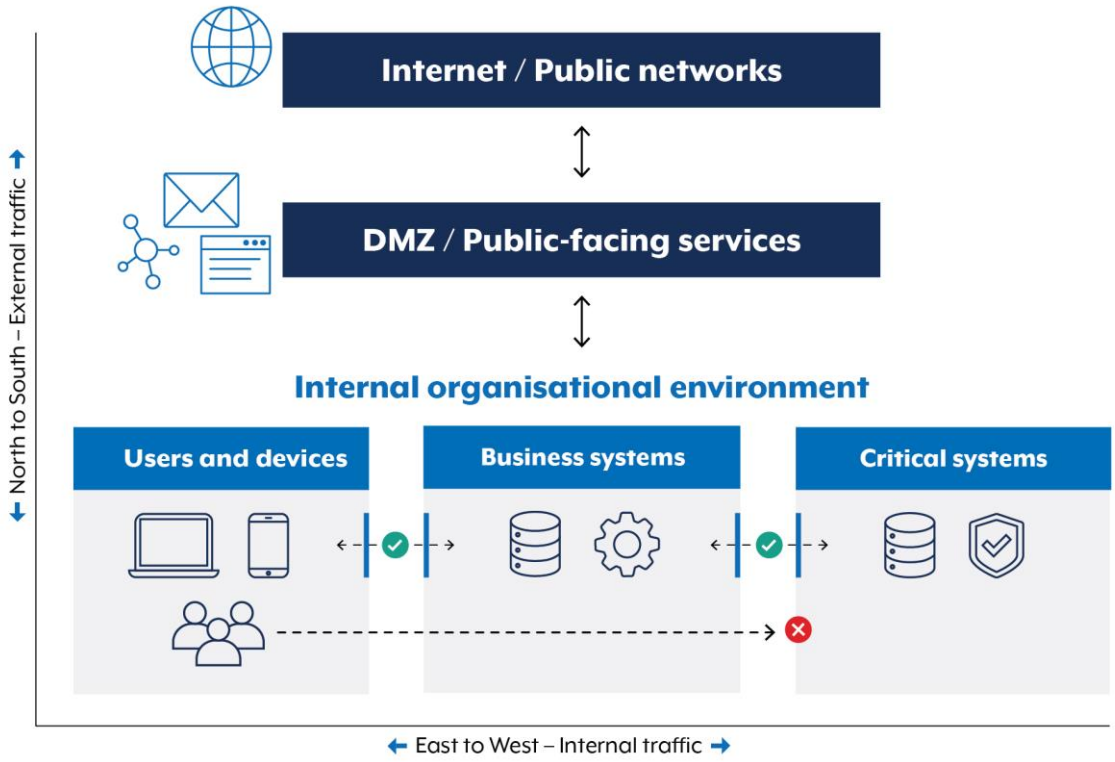

Figure 1: North/south and east/west traffic flows

Why network segmentation and segregation matters

MDA encourages organisations to take an 'assume breach' mentality to architecture and operations. Once a malicious actor gains an initial foothold, they often attempt to move laterally and/or vertically through the environment to discover accessible systems and resources, expand their access, evade security controls, and position themselves to achieve their objectives. Limiting these movements is a key objective of effective network segmentation and segregation.

Network segmentation, segregation and the proactive use of network telemetry enable organisations to detect, respond to, and contain malicious activity, reducing potential harm to their reputation, customers, critical services, and infrastructure. These capabilities can reduce the cost of incident response, reputational recovery and legal actions arising from a cyber security incident. Organisations need to consider all ten *foundations for modern defensible architecture* before developing their network segmentation and segregation strategy.

Network segmentation and segregation also support broader cyber resilience objectives. For organisations implementing ASD's *CI Fortify* guidance, macrosegmentation supports the rapid isolation of affected systems, services and network zones during a cyber security incident. Without defined and enforceable network boundaries, organisations may be unable to rapidly contain a compromise or perform the isolation activities required to protect critical operations and limit cascading impacts.

Enabling segmentation and segregation

Network segmentation and segregation strategies are most effective when treated as an organisational capability rather than a standalone technology initiative. While technical controls are necessary, they are rarely sufficient on their own. Effective outcomes depend on executive leadership establishing clear strategic direction, governance arrangements, risk appetite and investment priorities that align with business objectives and operational requirements.

Decisions made by boards, executives, and accountable authorities shape the scope, design, implementation and ongoing management of network segmentation and segregation. These decisions influence an organisation's ability to reduce cyber security risk, support operational resilience, adopt new technologies, and respond effectively to evolving business and threat environments. Without a clear strategic direction and sustained organisational commitment, technical controls alone are unlikely to deliver their intended security outcomes.

Australian regulatory and guidance context

Certain sectors may be subject to regulatory or compliance requirements. Within Australia, regulatory, policy and guidance sources approach network segmentation and segregation from different directions. Their scope and authority can differ, but they directly link the concepts of preventing lateral movement and concepts of asset criticality, operational resilience and continuing assurance. Decision-makers should seek to understand what regulatory or compliance requirements may apply to their organisation.

The Australian Government Protective Security Policy Framework (PSPF), Critical Infrastructure Risk Management Program (CIRMP) Rules 2026, and the Australian Prudential Regulation Authority's prudential framework outlines Australian regulatory requirements for network segmentation and applicable information security controls (APRA's Prudential Standard CPS 234). Organisations should determine which requirements apply to their circumstances.

ASD's ISM is a cyber security framework that an organisation can apply, using their risk management framework, to protect their information technology and operational technology systems from cyber threats.

ASD's MDA publication suite can assist organisations to adapt to the contemporary threat landscape by applying secure design and architecture in their cyber security strategy, resilience planning and implementation.

Key considerations for decision-makers

Decision-makers should focus on three outcomes: why segmentation matters to the organisation, what teams need to deliver it, and what evidence will show that risk and resilience are improving.

The following are key factors decision-makers need to consider before and during the implementation of network segmentation and segregation within their organisation:

Regulatory requirements: Some regulated industries have obligations to be resilient against cyber security incidents. Regulatory frameworks highlight the need to minimise the risks and impact associated with lateral movement through technical or procedural mechanisms.

Reduce the blast radius: Organisations implement network segmentation, segregation, and other isolation measures to reduce the severity of a security control failure. Network segmentation and segregation are established defence-in-depth practices that reduce the attack surface, and limit the blast radius in the event of a system compromise.

Improve observability and monitoring: Organisations that have implemented robust segregation policies limit a malicious actor's ability to move laterally without generating security signals that can be used to identify anomalies. Organisations may further enhance these incident detection capabilities through war-gaming exercises and threat modelling activities.

Changes in threat environment: AI models are increasingly capable of identifying new vulnerabilities, accelerating vulnerability research, and enhancing existing adversary tradecraft, including social engineering and phishing campaigns. A well-architected, segmented environment that implements defence-in-depth principles is better positioned to contain the impact of zero-day vulnerabilities and other security control failures. For more information, refer to ASD's *Five Eyes cyber security agencies statement*.

Re-architect for business resilience: Organisations face increasing pressure to rapidly identify, assess and remediate vulnerabilities while maintaining business uptime requirements. The expected increase in vulnerability discovery and security patching activity may accelerate the need to modernise and re-architect IT environments, including cloud migration initiatives. Changes to regulatory, policy, and risk management requirements may also drive business transformation and architectural changes.

Build for business benefit: Modern network architectures can improve organisational agility, reduce operational overhead, and support more efficient delivery of technology services through automation and orchestration. ASD recommends that organisations consider the long-term operational benefits of investing in technologies that support resilient, low-disruption maintenance, rapid security patching, and ongoing business continuity.

Protect the control plane: Organisations can combine ASD's *secure administration*, network segregation, and microsegmentation to protect the administrative interfaces of network infrastructure and other critical systems. Effective segmentation ensures that privileged administrative traffic is channelled through approved management pathways, such as privileged access management (PAM) solutions and jump hosts, rather than allowing direct access to

administrative interfaces. This strengthens control over privileged access and reduces opportunities for both internal and external threat actors to compromise the control plane.

Strategic investment: Network segmentation and segregation support MDA, including Zero Trust Architecture (ZTA), and align with ASD's *Secure by Design* advice. A strategic investment plan that incorporates network segmentation and segregation will help decision-makers with legislative or regulatory obligations to discharge their legal obligations.

Business-enablement: A well-architected and implemented network provides a foundation for innovation and organisational agility. Network segregation reduces risks associated with emerging technologies, software supply chain and third-party connectivity, while enabling organisations to adopt new operating models with greater confidence. This can accelerate business transformation initiatives such as mergers and acquisitions, cloud migration, remote working, and bring your own device (BYOD) programs.

Organisations with cyber insurance cover should understand which incidents their policy covers, and what they must do to keep the policy valid. For more information, refer to Center for Internet Security's Reasonable Cybersecurity.

Prioritisation: Organisations taking a strategic approach to implementing MDA need to consider the benefits of prioritising network security controls. Priority needs to be given to critical business functions, sensitive information, and systems that would have the greatest operational, financial, or regulatory impact if compromised. Continuity and disaster recovery plans, where applicable, should inform prioritisation decisions. Decision-makers need to ensure that investment delivers measurable business outcomes while protecting the organisation's most important systems and information. Early security improvements can often be achieved by segregating, isolating, or decommissioning high-risk systems, particularly where these systems are legacy, internet facing or no longer required for business operations. For more information, refer to *ASD's Managing the risks of legacy IT: Practitioner guidance and Security considerations for edge devices*.

The importance of architecture: Foundation 7 of the MDA (Resilient Networks) promotes the design of networks that can withstand failures, cyber attacks, and changing business requirements. By establishing and enforcing trust boundaries, organisations can restrict lateral (east-west) and vertical (north-south) movement to authorised communications, reducing the likelihood that a compromise in one part of the environment will affect critical systems or business operations.

Key questions decision-makers need to ask

- What regulatory, policy, contractual or industry obligations does our network architecture support, and where are the most significant compliance gaps?
- Who is accountable for the organisation's segmentation and segregation strategy, and how is it reviewed and updated as business requirements change?
- Which critical services, systems and information assets would have the greatest impact on the organisation if they were disrupted or compromised?
- How does the current network architecture support the organisation's risk appetite, security objectives and business continuity requirements?
- What resources, skills and ongoing investment are required to implement, operate and continuously improve this capability?
- Is the organisation's network segmentation and segregation roadmap appropriately prioritised and supported with clear funding, resources and governance?
- Does the organisation have sufficient visibility of its technology assets, systems and dependencies to make informed investment and risk decisions?
- Is there a plan to manage any short-term business impacts of implementation and ensure that business units are engaged with implementation in the long term?
- How will we measure success, and what evidence will demonstrate that the investment is delivering the intended security, resilience and business outcomes?
- What evidence shows that teams can isolate and protect critical systems during a cyber security incident without causing unacceptable disruption to the organisation?

Further reading

- ASD's *Network segmentation and segregation – Anti-patterns*
- ASD's *Information Security Manual*
- ASD's *Implementing network segmentation and segregation*
- ASD's *CI Fortify – Advice for isolating vital systems*
- NIST's *Special Publication 800-215 - Guide to a Secure Enterprise Network Landscape*

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license
https://creativecommons.org/licenses/by/4.0/

For the avoidance of doubt, this means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license https://creativecommons.org/licenses/by/4.0/legalcode.en

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website
https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre