CI Fortify — Advice for isolating vital systems

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
NEW ZEALAND

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favour by the authoring agencies.

'Must' statements in this document represent cyber security best practices. Operators should consult their jurisdiction's relevant regulatory and legally binding obligations.

Table of contents

Purpose 4

Introduction 4

The critical path to isolation 5

1. Identify vital systems and networks 5

2. Identify critical customers 5

3. Identify common levels of criticality and trust for networks and hosts 5

4. Map connections to vital systems and identify potential isolation points 6

5. Build effective separation and isolation points 7

Understand and build dedicated OT capability 8

Implement physical separation and isolation 8

Isolation in distributed critical infrastructure 8

Layer 2 Services 9

Layer 3 Services 9

Further guidance on encryption 9

6. Create and test an isolation plan 10

Graduated plan for isolation 10

Test isolation plans 11

Post-isolation: Verify and monitor isolation effectiveness 11

Inspection of routing tables 11

Network flow monitoring and intrusion detection systems 11

Secure network management zones 12

The risks of isolated systems 12

Using data diodes and cross domain solutions 12

Additional information for implementing isolation when physical separation or isolation are not achievable 13

Administrative network controls 13

Virtual local area networks 13

IP access lists, route blocking, and routing black holes 15

Network orchestration and automation systems 15

Feedback 15

Recommended pre-requisite reading

If you have not read the introductory guidance from your jurisdiction's relevant agency, it is recommended to visit one of the following to learn more:

- The Australian Signals Directorate's (ASD's) CI Fortify. See *CI Fortify* at cyber.gov.au
- The United States' Cyber and Infrastructure Security Agency's (CISA's) *CI Fortify* [1]
- The United Kingdom's National Cyber Security Centre's (NCSC-UK) *How to prepare for and plan your organisation's response to severe cyber threat: a guide for CNI* [2]
- The Canadian Centre for Cyber Security (CCCS)'s *Critical infrastructure resilience and escalated threat navigation (CIREN) initiative* [3]

Purpose

This guide details steps to successfully isolate vital operational technology (OT) and enabling systems from all other networks. With this capability, OT owners, operators and cyber defenders can provide continuity of their critical services in instances of crisis or service disruption.

Introduction

State-sponsored cyber actors routinely target critical infrastructure (CI) to conduct espionage or to pre-position for disruptive and destructive effects in the event of crisis or conflict.[4]

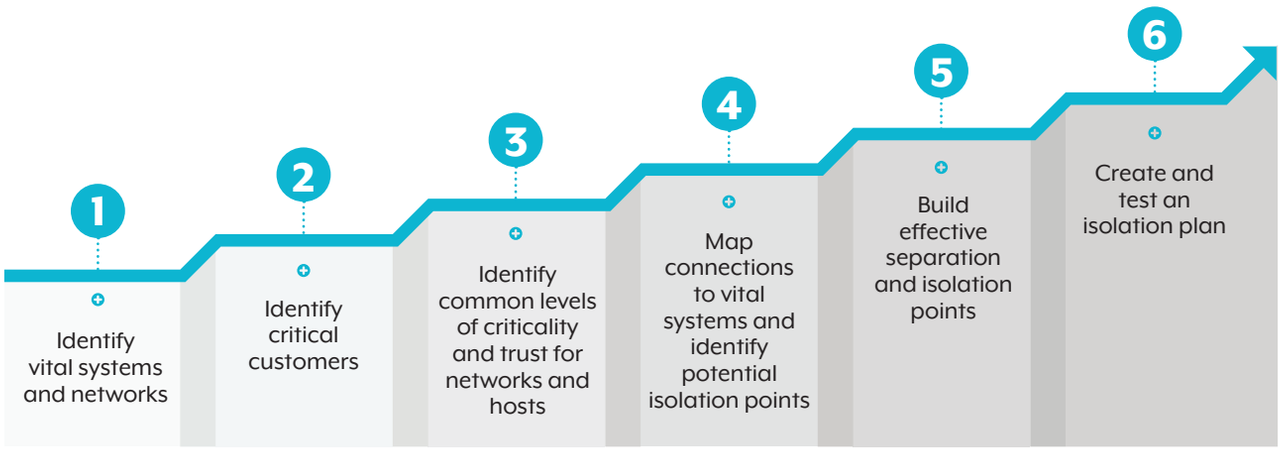
Cybercriminals continue to opportunistically target CI operators. The sensitivity of the data stored by these entities, and the importance of their services, makes them attractive for cybercriminals seeking to extort victims via data exfiltration or by conducting ransomware attacks for disruptive or destructive purposes.

In response to persistent threats, CI operators should have the capability to isolate vital OT and enabling systems from all other networks to ensure continuity of critical services. Isolating vital OT and enabling systems can disrupt the ability of malicious cyber actors to achieve their goal, contain active incidents, and allow for safe rebuilding of compromised systems.[5]

---

1 https://www.cisa.gov/topics/industrial-control-systems/ci-fortify
2 https://www.ncsc.gov.uk/collection/how-to-prepare-and-plan-your-organisations-response-to-severe-cyber-threat-a-guide-for-cni
3 https://www.cyber.gc.ca/en/cyber-security-readiness/critical-infrastructure-resilience-escalated-threat-navigation-initiative
4 https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
5 Refer back to the pre-requisite reading for jurisdiction specific considerations and guidance.

The critical path to isolation



1. Identify vital systems and networks

Begin by identifying the systems and networks that support the critical service. These are the minimum set of systems and networks required to deliver a critical service.

For additional guidance on OT asset identification, see the following at cyber.gov.au:

- *Foundations for OT cybersecurity: Asset inventory guidance for owners and operators*
- *Creating and maintaining a definitive view of your operational technology architecture*

2. Identify critical customers

Identify dependent critical infrastructure (critical customers), such as military infrastructure and lifeline services, and set a service delivery target based on their needs (e.g. Megawatts and quality of power, million gallons of water per day).

3. Identify common levels of criticality and trust for networks and hosts

Within OT environments, different degrees of criticality and threat exposure will apply. In a properly segmented network, hosts and systems are grouped into segments and zones with a common level of criticality, and similar threat exposure. Leverage risk management processes to identify the common levels of criticality and trust for networks and hosts to determine appropriate segments and zones. This will facilitate further segmentation within OT and the application of controls applicable to the assessed risk.

For more information, visit ASD and international partners' *Principle 3: Identify and categorise assets to support informed risk-based decisions of Creating and maintaining a definitive view of your OT architecture*.[6]

6 https://www.ncsc.gov.uk/collection/operational-technology/definitive-architecture-view/principle-3

4. Map connections to vital systems and identify potential isolation points

Once vital systems and networks have been identified and classified, identify and record all points of interconnection between critical networks and other systems. This information should be updated as part of routine operation and change management processes. This should include any connections to:

- non-critical corporate systems
- vendor remote access (both routine and emergency), including consultant, contractor and managed service provider workforces
- untrusted networks (e.g. internet access)
- cloud environments, including 'private cloud' offerings[7]
- peer critical networks, e.g. other utilities and scheduler or dispatch operators.

Identify where critical networks transit lower trust and vulnerable networks and their connection type, such as:

- carrier-provided networks
- radio point to point
- mobile
- satellite
- wireless access (Wi-Fi) networks.

Identify network transit connection type and any protection mechanisms in place, such as encryption.

Understand the business context for each identified connection. Record information, including:

- system owner for the vital system and connected system(s)
- third-party provider (if applicable)
- type of information flow enabled by the connection (e.g. protocol or application)
- criticality of information flow including availability and Recovery Point Objective (RPO) and Recovery Time Objective (RTO) targets.

For each identified connection, ensure that critical technical information is documented. This includes:

- architectural diagrams
- internet gateway documentation
- firewall, router and virtual private network (VPN) configuration information
- for connections to other entities, ensure routine and emergency contact details are captured.

This critical technical information will be necessary for building isolation controls.

It is important to note that isolating systems will trigger manual processes and interrupt system-to-system communication. This can impact connections to upstream dependencies and peers, such as other utilities and scheduler or dispatch operators. Organisations should identify and work through critical dependencies with impacted peers and partners as part of their isolation planning.

---

7 https://csrc.nist.gov/pubs/sp/800/145/final

For more information, visit ASD and international partners' *Principle 4: Identify and document connectivity within your OT system of Creating and maintaining a definitive view of your OT architecture*.[8]

5. Build effective separation and isolation points

Isolation points between critical and non-critical networks and services are highly effective at limiting the ability of malicious actors to pivot into vital systems.

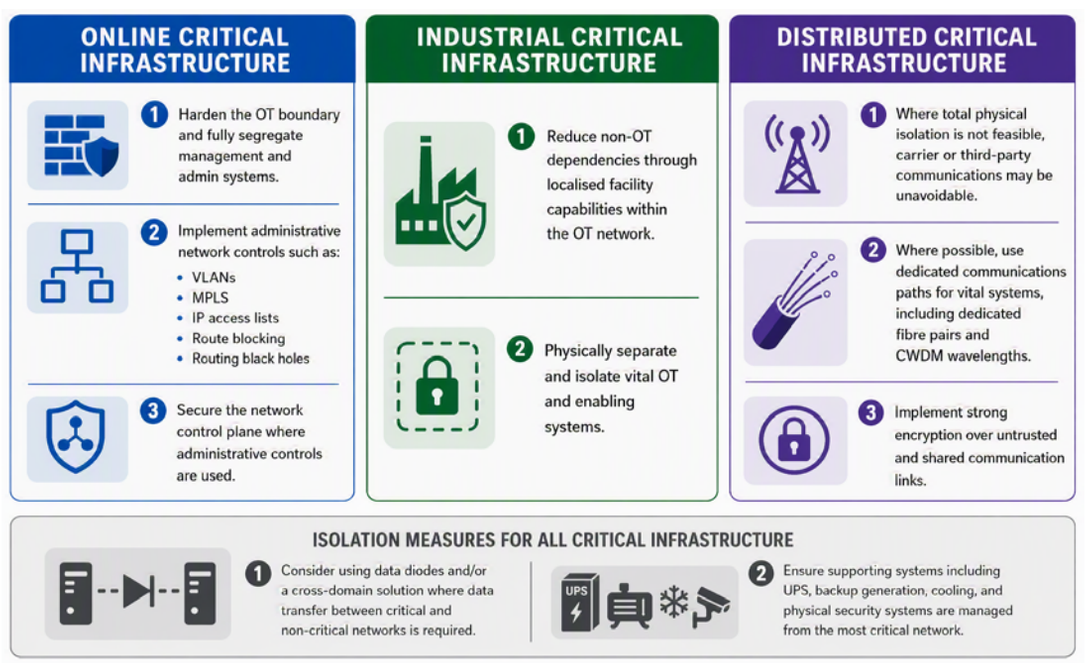
Isolation points within critical networks can:

- contain cyber-attacks
- limit the impact to operations
- reduce the time required to evict a malicious actor and restore full services.

Planned physical separation of vital systems from all other networks and systems is a pre-requisite for physical isolation. Organisations must build physical isolation points into their vital systems to enable the capability to operate in a state of isolation from all other networks and systems. Physical isolation requires that there is no connectivity or shared infrastructure between vital systems and non-vital systems. Physical isolation of vital OT and enabling systems is the most effective form of protection and is likely to trigger manual processes and interrupt system-to-system communication for its duration. Organisations must consider how they will operate in this state for an extended period.

For organisations whose core operations depend on internet-facing services or geographically dispersed sites, complete physical isolation at each site may not be operationally feasible. In these cases, a greater emphasis should be placed on strengthening and securing OT boundaries for the environments that must remain connected.

Achieving this capability will require time and resource investment. Every step in building separation and isolation points presents incremental improvements in aspects of attack surface reduction and can be considered an ongoing process of incremental gains. However, the end state must be to enable the continued operation of critical services in a state of isolation.



8 https://www.ncsc.gov.uk/collection/operational-technology/definitive-architecture-view/principle-4

Understand and build dedicated OT capability

Effective isolation of critical networks may be impacted by dependencies between OT and non-OT systems. CI operators must reduce and eliminate dependencies that will impede effective isolation of critical networks by **building localised, independent facility capabilities within the OT network**.

OT and non-OT systems often create dependencies in the following technology areas:

- unified routing and switching infrastructure, particularly in data centres
- native document management systems for configurations, firmware and binaries
- shared virtualisation infrastructure, including common hypervisors and physical hosts
- Shared Storage Area Networks (SANs) and Network Attached Storage targets
- backup and recovery services
- common identity, name, and address resolution services such as Active Directory (AD) Domain Name System (DNS), and Dynamic Host Control Protocol (DHCP)
- Public Key Infrastructure and Certificate Services
- Time synchronisation services, such as Network Time Protocol and Precision Time Protocol, provided by corporate and internet sources.

CI operators must assess and eliminate dependencies between their OT and non-vital OT systems to ensure physical isolation does not create any unforeseen performance issues resulting in the outage of the critical service and that performance issues, including degradation in quality of the critical service are kept to an acceptable level to support critical dependencies.

In a crisis there will be resource competition between operators for typical support resources such as vendors, integrators, consumable suppliers (fuel, chemicals), and incident responders. The human planning element of OT sovereignty includes elements such as:

- removing external dependencies for isolation or initial recovery
- verifying service level agreements for prioritized support
- pre-establishing emergency communication for normal staff, as well as any remaining third-party dependencies.

Implement physical separation and isolation

Physical separation and isolation are distinct concepts. Physical separation refers to infrastructure independence, while isolation refers to the ability to disconnect systems and continue operating independently when required.

To be physically separate, OT networks must not share any active infrastructure with non-OT networks. This includes switches, routers, repeaters, multiplexers, or compute elements. Supporting infrastructure such as uninterruptible power supplies and generators should not be controllable from non-critical networks.

Isolation in distributed critical infrastructure

CI operators often operate across a geographically distributed area with vital systems located at multiple, dispersed locations. For organisations that have communications assets spanning the entirety of their footprint, maintaining isolation between vital and non-vital systems can be achieved by having media dedicated for vital systems that is not shared with non-vital systems. For example, dedicated pairs in fibre optic cable or dedicated wavelengths in Coarse Wavelength Division Multiplexing (CWDM) systems.

Distributed critical networks may need to use carrier or third-party communications, making physical isolation not feasible. Here, effective isolation can be achieved through strong encryption over untrusted and shared communications links. CI operators must understand the impact of an outage on these links and consider developing an emergency plan to ensure continuity of connectivity for critical services.

CI operators must treat any carrier-provided service as untrusted and potentially hostile. Apply robust cyber security controls to protect the interface between the operator and the carrier, and to protect the integrity of data traversing the carrier network. Do not use encryption built into OT devices – always use a dedicated device to implement encryption over untrusted carrier links.

Layer 2 Services

Layer 2 carrier ethernet services such as E-Line and E-LAN, or Ethernet-over-MPLS (EoMPLS) and Virtual Private LAN Services (VPLS), can be protected with robust link ethernet encryption technologies such as Media Access Control security (MACsec). Dedicate the encryption device to the protected critical network, disable all unnecessary services, regularly assess and patch the critical network against known vulnerabilities, and prevent any remote access or configuration from the untrusted network.

Layer 3 Services

Carrier-provided Layer 3 services can be encrypted with IP-based encryption utilising Internet Protocol Security (IPSEC), or vendor proprietary technologies such as Group Encrypted Transport VPN (GETVPN) and Dynamic Multipoint VPN (DMVPN). Encryption must be implemented on the trusted network device that forms part of the critical network, the connection to the untrusted carrier network must be limited to only transmit and receive packets that are part of the encrypted tunnel, and all remote access to the network device must be from trusted management hosts (e.g. privileged access workstations) on the critical network. This should be enforced using conditional access.

Follow vendor, ASD and international advice on network device hardening and vulnerability management. This includes:

- *Securing edge devices* at cyber.gov.au
- *Principles for secure privileged access workstations* and *Using PAWs in OT environments* at ncsc.gov.uk.[9,10]

Further guidance on encryption

The advice on encryption provided here is not exhaustive. Implementing strong cryptographic controls for isolation of CI requires detailed consideration of protocols and algorithms, device selection and placement, key distribution and management, control plane isolation, and device hardening.

For further information on approved cryptographic protocols, algorithms, and implementation, search for *Guidelines for cryptography* and *Planning for post-quantum cryptography* at cyber.gov.au.

9 https://www.ncsc.gov.uk/collection/principles-for-secure-paws
10 https://www.ncsc.gov.uk/collection/operational-technology/using-paws-in-ot-environments

6. Create and test an isolation plan

Graduated plan for isolation

A graduated plan for isolation provides the ability to progressively isolate pathways to vital OT and enabling systems while balancing the need for continuity of business processes. Progressively removing access to OT systems as the cyber threat environment deteriorates may be effective in halting or hindering attacks on vital OT and enabling systems. However, CI operators must plan and build capability for the complete isolation of the most vital systems. The isolation plan must be aligned with the business mission and function requirements. A graduated approach must still have total isolation of vital OT and enabling systems as the target state.

Having a graduated plan for isolation considers the response to cyber threat against the impact to routine business operations. Early isolation of pathways into vital systems will reduce the attack surface presented to a malicious actor.

An example of a graduated plan for a fictitious electrical transmission company is below:

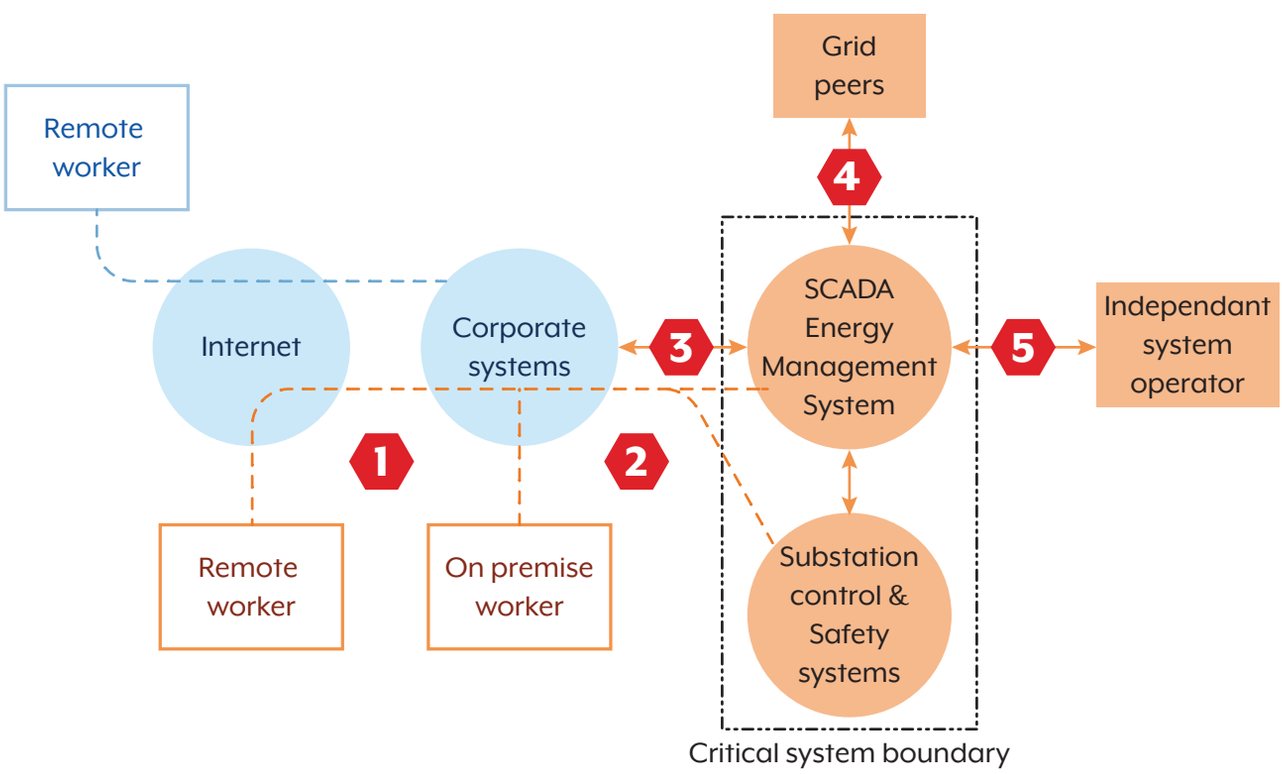


Figure 1. Graduated plan example (fictitious)

1. Disable the ability for remote workers to access OT environments (via jump hosts in intermediate non-OT systems).
2. Disable the ability for on-premises remote access to OT environments.
3. Isolate all connections between non-OT and OT environments.
4. Isolate lower priority connections between peer OT and OT environments.
5. Isolate OT environment and vital systems completely.

Trigger criteria for each isolation step should be defined in advanced and linked to the organisation's incident response plan.

Note: this is a simplified diagram and does not show existing boundary controls such as firewalls, demilitarized zones (DMZs), data diodes, or other gateway devices and architectures. This example focuses on isolation points for the vital systems in a fictional energy utility; additional isolation points into corporate and business systems would also be in place.

Test isolation plans

CI operators should review and test isolation plans regularly to ensure the process can be completed without unforeseen consequences. ASD recommends that CI operators test the isolation of all vital systems periodically. Testing the isolation of a single vital system or a subset of the vital systems may not identify all dependencies. CI operators should also store a secure offline (hard copy) version of the isolation plans.

For more information, see *Secure connectivity principles for Operational Technology (OT)* at cyber.gov.au.

Post-isolation: Verify and monitor isolation effectiveness

Upon initial isolation, and throughout the isolation period, CI operators must monitor the effectiveness of the isolation mechanisms and ensure unauthorised or unintentional interconnection between critical and non-critical networks does not occur.

Inspection of routing tables

Examine network routing tables on both vital and non-vital systems to determine if interconnection has occurred, or if static routing still exists that may facilitate inadvertent or malicious defeat of isolation measures. A well-defined, hierarchical IP addressing schema is essential in facilitating the categorisation and identification of route prefixes and summary routes of critical and non-critical networks. Inspect routing tables manually at key network convergence points or configure devices to automatically log routing table updates and adjacency changes to a logging server or on-premises Security Information and Event Management (SIEM) and set up queries to alert on route changes that indicate interconnection between OT and non-OT networks.

Network flow monitoring and intrusion detection systems

Monitor network traffic flows at key points in the critical network. Configure network monitoring tools to regularly perform reachability tests from and to both critical and non-critical networks. Alert staff if these tests indicate that the isolation controls are ineffective or have been removed.

Secure network management zones

CI operators must ensure that privileged access to network infrastructure is secured. Entities that rely on administrative controls for isolating critical networks (such as VLANs, MPLS, and IP Access Lists) must secure the network control plane to prevent a malicious actor from disabling or defeating isolation controls.

Physical segregation of the network management plane should be implemented wherever possible. Use dedicated physical management interfaces for firewalls and routers if available, otherwise assign a data port as the management interface and limit it to management zone traffic only. Connect management interfaces to dedicated out-of-band infrastructure and use privileged access workstations to administer network devices.

For geographically dispersed critical networks, it may be necessary to use carrier services for network management zones. These must be isolated with strong cryptographic controls dedicated for the management zone. Disable any ability to remotely access network management zones from networks of lower trust.

The risks of isolated systems

Adopting these islolated measures introduces a few operational and security risks. Organisations must account for these when operating in isolation or when reconnecting isolated vital systems. These may include:

- systems falling out of patch
- reduced external visibility
- increased risk of infected removable media affecting a system
  - CI operators will rely on removable media to transfer data across air gaps and machines used to 'sheep dip' (i.e. detect malicious code) removable media may not receive updates.

Using data diodes and cross domain solutions

Data diodes and cross domain solutions (CDS) provide a means of transferring data between critical and non-critical networks with a high assurance of protection, if appropriately designed, configured and maintained, which exceed standard network gateway architectures.

Data diodes and CDS may enable some data flows to remain during a period of extended isolation, however CI operators considering the use of data diodes and CDS must seek advice and guidance from organisations and bodies with expertise in the deployment and use of such solutions. Data diodes may be deployed incorrectly and therefore harm operational integrity, such as a data diode dropping handshakes.

For additional information, see *Introduction to Cross Domain Solutions* and *Fundamentals of Cross Domain Solutions* at cyber.gov.au.

Additional information for implementing isolation when physical separation or isolation are not achievable

Due to the requirements for internet-facing vital systems to support a critical service, or safety requirements, complete physical isolation of vital OT and enabling systems may not be possible. If this is the case, organisations should do the following:

- Implement and maintain the capability to rapidly rebuild vital OT and enabling systems completely to minimise disruptions to critical services.
- Harden the OT boundary by implementing best practice guidance. For more information see *Secure connectivity principles for Operational Technology (OT)* at cyber.gov.au.
- Consider implementing a Cross Domain Solution (CDS) for accessing or transferring information across security domains. For more information see *Cross Domain Solutions* at cyber.gov.au.

Administrative network controls

Administrative network controls provide **minimally effective** segregation between vital and non-vital systems networks. CI operators should consider the use of administrative controls, such as virtual local area networks (VLANs), as an interim segregation measure on the journey to implementing robust physical and/or cryptographic isolation. CI operators must not rely on these interim measures as a long-term solution for a fully segregated operations network.

Virtual local area networks

VLANs are universally supported in existing network infrastructure with robust interoperability between vendors. Only use VLANs to segregate systems, devices, and information flows when applying administrative controls in the same security domain.

However, VLANs should not be used to separate network traffic between networks belonging to different security domains as stated in ASD's *Information security manual* available at cyber.gov.au. In addition, CI organisations must fully consider the risks associated with this practice and implement more effective segregation and isolation controls.

Where VLANs are used to implement network segregation, the following measures should be considered:

- Do not automatically propagate VLAN configurations across the network – e.g. using Cisco's VLAN Trunk Protocol. Manually configure VLANs on devices only where that VLAN needs to be available.

- 802.1q trunks should explicitly allow only the VLANs necessary on that trunk – all other VLANs should be excluded. Do not allow trunk negotiation. Change the trunk native VLAN to an unused, shutdown VLAN ID.
- Network devices that implement VLANs for segregation must only be managed from the most trusted security zone, ideally from dedicated privileged access workstations within a dedicated management zone.
- Do not allow any internet-facing network zones, or DMZs, to share infrastructure with OT networks.
- Implement physical segregation of switching infrastructure wherever possible with dedicated switches for OT devices. Use dedicated uplinks and links for OT networks, to prevent IT and OT data being carried on common physical links.

Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) does not provide assurance of segregation and is not secure by default. CI operators using MPLS to segregate networks of different security domains – e.g. IT and OT – must use cryptographic isolation to protect critical OT systems. Encryption must be implemented on the router that forms the boundary of the OT network.

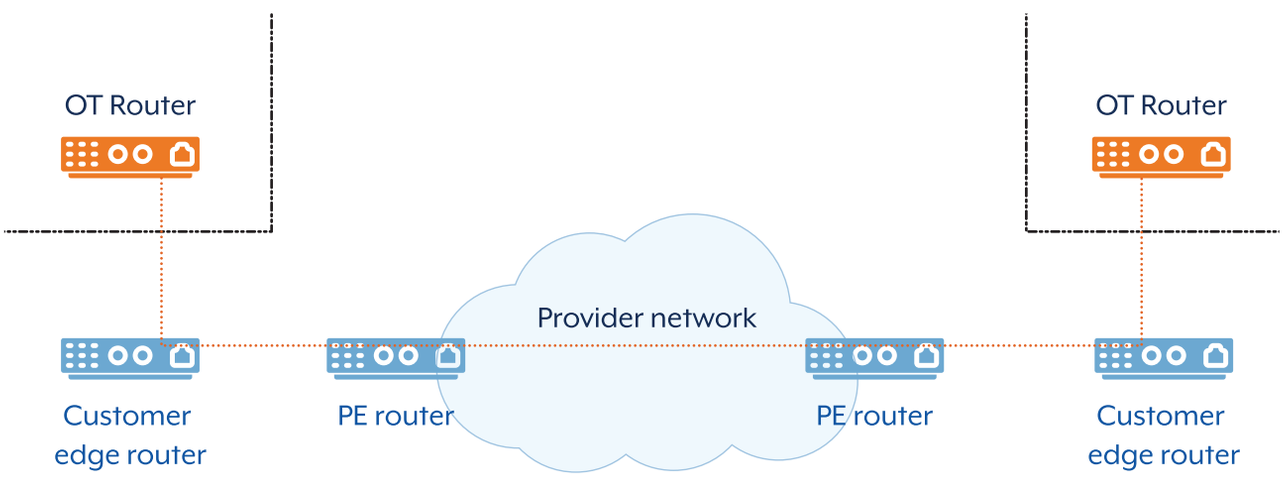


Figure 2. Provider network

In the diagram above, MPLS is used to carry OT and non-OT traffic across the provider network. The OT routers provide an encrypted tunnel over any non-OT devices including the untrusted provider network. The OT routers block all other traffic flows between the OT and non-OT networks. It is critical that the OT router in this example is only managed from the OT security domain and is hardened to the fullest extent possible.

Protection of Customer Edge devices from the untrusted provider network is crucial in preventing lateral movement from provider into operator environments. Access lists (IP and MAC) and filtering should be aimed at preventing anything but explicitly defined peers from communicating with operator equipment. Filtering of expected routes should be implemented in the operator-controlled equipment. Ensure provider-facing infrastructure is prioritised in the vulnerability management process.

IP access lists, route blocking, and routing black holes

Additional administrative controls can be applied to network infrastructure both in critical and non-critical networks beyond the isolation point. These additional controls should not be used solely in place of physical separation:

- Implement IP access lists used throughout the network to restrict flows and protocols.
- Use route maps to prevent propagation of critical network prefixes into non-critical networks, and vice versa.
- Use black hole routing to drop traffic at key network nodes.

Network orchestration and automation systems

Network orchestration and automation systems such as software-defined networking (Software-Defined Wide Area Network, Software-Defined Access, Security Service Edge/Secure Access Services Edge), Application Programming Interface (API) provisioning, and Network as Code may provide efficiencies in managing large networks. However, the layer of abstraction they provide between policy intent and device configuration may be exploited by an adversary. These systems provide logical separation and do not provide assurance that is equivalent to physical separation.

Any use of these platforms in CI networks must consider how the service platform is secured, and how its administration can be isolated from non-critical networks and integrations with corporate systems. Attention must be paid to instances where the network orchestration and automation system is used to enforce segregation and encryption across untrusted networks, including carrier networks and the internet.

Feedback

Australian organisations: ASD welcomes your comments and feedback. If you would like to provide feedback or have questions regarding ASD's *CI Fortify's Isolating critical services* guidance, please complete the *CI Fortify's Isolating critical services feedback form* at cyber.gov.au.

U.S. organisations: CISA value's your input. Please share your feedback so we can continue delivering actionable guidance that helps you reduce cyber risk.[11]

Canadian organisations: The Canadian Centre for Cyber Security (Cyber Centre), part of the Communications Security Establishment, encourages Canadian organizations to report cyber incidents and to strengthen the security of their networking devices. We also welcome feedback on our guidance and encourage Canadian organizations to contact us by:

- Emailing contact@cyber.gc.ca
- Reporting a cyber incident via our online reporting tool
- Calling 1-833-CYBER-88 (1-833-292-3788)

New Zealand organisations: The NCSC welcomes feedback and questions. If you would like to contact the NCSC about this publication, please email info@ncsc.co.nz.

11 https://cisasurvey.gov1.qualtrics.com/jfe/form/SV_9n4TtB8uttUPaM6

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.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre