Mitigations for network defence

First published: October 2025

Executive summary

Malicious actors continue to target internet-facing network devices as entry points into organisational networks and subsequently leverage internal network devices to facilitate lateral movement or data exfiltration. In doing so, malicious actors maintain persistence by compromising network devices, such as routers, switches, firewalls and virtual private networks (VPN). Protecting network infrastructure is important, as it often represents the first line of defence against external threats.

By implementing effective network defence mitigations—such as secure configurations, segmentation, and continuous monitoring—organisations can protect themselves against compromises that could lead to significant monetary loss, regulatory consequences, reputational damage and business disruptions.

Designed for both executives and technical staff, this guidance supports a defence-in-depth approach that enhances resilience across the entire network environment – not just at the edge. It complements the Australian Signals Directorate's (ASD) existing guidance for *securing edge devices* by extending mitigations across the wider network environment, including core routing, switching and intermediary network components.

Organisations that maintain a defence-in-depth security posture – built on the principles of a *modern defensible architecture* – demonstrate greater resilience to the impact of zero-day vulnerabilities. Importantly, this benefit extends beyond edge devices to the entire network environment.

This guidance recognises that network infrastructure forms a critical component of organisations' information technology (IT) environments. As such, organisations should take responsibility for managing, securing and maintaining their networks through a comprehensive, yet risk-informed, approach.

Introduction

This guidance focuses on strengthening the security of network devices – a foundational yet often under-addressed aspect of organisational cyber security. It provides executives and technical staff with the following resources:

- Two case studies – one real-world case study involving the containment of an exploited edge device using an n-day vulnerability, and one hypothetical scenario illustrating the critical importance of layered cyber security across the wider network environment.
- A prioritised set of strategic actions for network defence, shaped by the evolving threat landscape and aligned with cyber security guidance from ASD and international partners.
- Technical mitigations that directly reduce the risk of network attacks by addressing exploitable vulnerabilities, enhancing containment measures, and strengthening layered defences.
- Questions to continue the conversation, presented as assurance questions for executives and validation checks for technical staff.

By adopting this guidance, organisations can build a defence-in-depth security posture to minimise their network attack surface, strengthen their network resilience, and enhance their detection and response capabilities. The following resources offer targeted mitigations that help organisations proactively defend against network attacks by addressing known vulnerabilities and reinforcing critical security layers.

Case studies

The following case studies highlight the difference between an organisation with a strong cyber security posture and one without. They demonstrate how these differences impact incident response, business recovery and their overall security posture.

Case study 1: A disability support provider reports Citrix gateway compromise

In November 2023, a disability support provider reported to ASD that their network had been compromised using a vulnerability in their Citrix Netscaler Gateway. The vulnerability used was CVE-2023-4966, known as Citrix Bleed. It had already affected multiple Australian organisations. The vulnerability allowed malicious actors to bypass multi-factor authentication (MFA) and potentially obtain sensitive data or conduct session hijacking attacks.

The disability support provider's IT team had identified an unauthorised Citrix session from a non-Australian internet protocol (IP) address, and within 75 minutes had geo-blocked certain overseas IP ranges on their firewall to prevent further attacks. This rapid response demonstrated strong situational awareness and operational readiness. While Citrix allows multiple concurrent sessions per user by default, the disability support provider's IT administrator had previously changed insecure defaults and configured the Citrix Netscaler Gateway to only allow one session per user.

This proactive configuration restricted the malicious actor's ability to exploit the network, and no other fraudulent sessions or users were identified in event logs.

In this case, the disability support provider was proactive in disabling access to the Citrix Netscaler Gateway from outside of Australia within three hours of the unauthorised activity and resetting all passwords. No privilege escalation was identified and MFA was already enforced on most applications. There was minimal business impact with only two affected users. This outcome reflects effectiveness of layered security controls and a well-prepared incident response capability.

Lesson: This cyber security incident demonstrated the benefits of a strong cyber security posture. This was enabled by prior threat modelling, changing network device defaults and integration of a security information and event management (SIEM) solution to identify abnormal authentication. Well-defined cyber security incident response plans and a skilled network defender workforce also played a critical role. The provider's ability to detect, contain and recover from the incident with minimal disruption is a testament to their cyber maturity.

Note: While the geo-location of an IP address can help with initial cyber security event detection and analysis, it cannot reliably indicate the intent, identity or origin of malicious activity. For more information, refer to ASD's *Geo-blocking in context: Realities, risks and recommendations* publication.

Case study 2: 'The Company' – a hypothetical scenario showing the risk in security oversight

A digital-first enterprise, 'The Company', operated with a modern customer-facing presence but lacked foundational safeguards to protect its internal network and sensitive data. Key vulnerabilities included an unauthenticated customer data application programming interface (API), an unpatched VPN without MFA, and a flat network architecture that lacked internal segmentation.

The cyber security incident began with the compromise of a single user account associated with a legacy VPN. Without MFA in place, malicious actors were able to gain initial access to the corporate IT environment.

Once inside the corporate IT environment, the malicious actors quickly escalated their access due to the flat network design. Notably, the absence of segmentation allowed lateral movement across the network with minimal resistance. During this time, the malicious actors identified and accessed an unauthenticated API that exposed sensitive customer identity records.

Over the following weeks, the malicious actors exfiltrated large volumes of data without detection, taking advantage of the lack of centralised network logging and monitoring. The situation escalated when the malicious actors launched a ransomware attack, disrupting customer-facing services and internal business operations. Weak access controls, insufficient event logging, and missing web proxy enforcement (e.g. data loss prevention, authenticated access and deny policies) enabled undetected data exfiltration.

The Company chose not to engage with the malicious actors, and as a result, the malicious actors officially released the stolen data. The incident triggered widespread public concern, regulatory scrutiny, monetary loss and long-term reputational damage.

Lesson: Foundational security measures (e.g. patching, MFA and network segmentation) play a critical role in reducing network attack surfaces. When these controls are missing, the impact of a cyber security incident can quickly escalate.

Actions for network defence

This guidance organises actions for network defence into priority-based tiers, drawing from existing guidance provided by ASD and international partners. These tiers should be treated as guidance rather than strict requirements. Organisations should adjust prioritisation of actions according to their risk profile, architecture and threat environment.

The *Information security manual* (ISM) is a cyber security framework that organisations can apply, using their risk management framework, to protect their IT and operational technology systems and data from cyber threats. Chief information security officers (CISO), chief information officers (CIO), cyber security professionals and IT managers should use the ISM as their primary reference for detailed implementation of the below actions.

In addition, organisations should regularly monitor key cyber threat intelligence feeds to inform decision making, such as ASD's *alerts and advisories* and the Cybersecurity and Infrastructure Security Agency's *Known Exploited Vulnerabilities Catalog*.

Priority	Actions
Critical	• Patch internet-facing network devices • Implement phishing-resistant multi-factor authentication • Change default credentials and disable insecure protocols/services • Secure management interfaces • Apply event logging best practices
High	• Maintain secure backups • Enforce egress rules • Implement network segmentation and segregation
Medium	• Deploy a network detection and response solution • Enable just-in-time privileged access • Implement network access control

Priority	Actions
Foundational	• Maintain a network device register • Monitor configuration integrity • Establish baselines for network device health and traffic • Establish baselines for network control and forwarding plane activity • Review service and local accounts • Implement secure supply chain practices • Maintain a cyber security incident response plan • Conduct ongoing security awareness training

Critical priority actions

Patch internet-facing network devices

Goal: Apply patches, updates or other vendor mitigations to internet-facing network devices to mitigate vulnerabilities commonly targeted by malicious actors. The most common internet-facing network devices include routers, switches, firewalls and VPN concentrators.

Implementation guidance: Apply patches, updates or other vendor mitigations for internet-facing network devices within 48 hours of release when vendors assess vulnerabilities as critical or when working exploits exist. For non-critical vulnerabilities without known exploits, apply patches, updates or other vendor mitigations within two weeks of release.

Many vendors perform thorough testing of patches prior to their release. However, this testing is not always perfect and organisations are likely to, at some point, face the release of faulty patches or experience faults when attempting to apply patches to applications or operating systems.

It is recommended that organisations account for the possibility of faults during patching by understanding the impact of a faulty patch and establishing clear patch management procedures.

Organisations are encouraged to perform vulnerability scanning of internet-facing devices regularly to identify and address patching gaps.

For more guidance and considerations associated to patching, consider visiting *Patching applications and operating systems*.

Implement phishing-resistant multi-factor authentication

Goal: Enforce phishing-resistant MFA for all remote access and privileged accounts to prevent unauthorised access due to compromised passwords. Recommended MFA methods include FIDO2 security keys, smart cards and passkeys.

Implementation guidance: Protect access by privileged accounts and all forms of remote network access using MFA to reduce the risk of credential compromise and unauthorised access.

Change default credentials and disable insecure protocols/services

Goal: Change, disable or remove default user accounts and credentials for network devices, including any pre-configured accounts, during initial setup. Disable insecure protocols/services to eliminate common attack vectors.

Implementation guidance: Change all vendor-supplied default accounts and credentials and disable insecure or legacy services/protocols (e.g. telnet and SNMPv1/SNMPv2), where possible.

Disable legacy services, such as Cisco's smart install, unless explicitly required, as malicious actors actively exploit them. Use the *MITRE ATT&CK framework* to identify high-risk protocols, such as Universal Plug and Play (UPnP) or the zero-touch provisioning protocol. Disable any services that are not in use to reduce unnecessary exposure, even if they are not legacy.

Secure management interfaces

Goal: Isolate network management interfaces to reduce the attack surface by preventing unauthorised access to management interfaces of network devices and services.

Implementation guidance: Organisations should ensure that management interfaces (e.g. SNMP, Secure Shell and management APIs) for network devices are not exposed to the internet. These interfaces should be isolated within dedicated out-of-band management networks or zones, accessible only though secure entry points, such as jump hosts, Privileged Access Workstations or Secure Access Workstations.

Isolating management traffic from regular network traffic (also referred to as separating the control plane from the data plane) reduces the exposure of sensitive management functions and ensures only authorised operational staff and cyber security staff can access these critical interfaces.

Additionally, organisations should actively scan for exposed or misconfigured management interfaces and ensure that device control planes are not accessible to standard users.

Apply event logging best practices

Goal: Apply event logging best practices to enable the timely detection of malicious activity and preserve forensic evidence for cyber security incident response activities.

Implementation guidance: Implement a centralised, secure event logging solution to enable event log aggregation and then forward select processed event logs to analytic tools, such as a SIEM or extended detection and response solution. Organisations should retain event logs in a searchable manner for at least 12 months.

Event logs are a critical source of visibility across the network. It enables detection of unauthorised access and lateral movement. While this guidance focuses on internal infrastructure, edge device logging should also be considered as part of a defence-in-depth approach.

For more information, refer to ASD's *Best practices for event logging and threat detection* and *Priority logs for SIEM ingestion: Practitioner guidance* publications.

High priority actions

Maintain secure backups

Goal: Maintain and test secure and resilient backups to ensure a viable recovery capability exists in the event of a significant cyber security incident. In the context of network infrastructure, organisations should regularly back up configuration settings for network devices. If malicious actors delete running configurations and associated backups, the impact could be severe, potentially requiring a rebuild of the organisation's core network environment.

Implementation guidance: Perform and retain backups in accordance with business criticality and continuity requirements. Backups should be synchronised to enable consistent restoration, protection from modification or deletion through appropriate access controls, and retained in a secure and resilient manner (e.g. immutable storage). Organisations should use separate access credentials for backup administration that are not linked to the primary corporate identity store. Schedule and test restoration procedures regularly to confirm recovery time objectives are achievable.

Enforce egress rules

Goal: Restrict outbound network traffic to reduce the risk of data exfiltration and malicious command-and-control activity.

Implementation guidance: Configure egress rules to deny all outbound traffic by default, only permitting services and destinations that support business functions. Organisations should implement web proxy rules to enforce security controls (e.g. content filtering and Transport Layer Security inspection) and apply organisational restrictions to outbound traffic.

As an interim safeguard, consider a Protective DNS (Domain Name System) solution to block access to known malicious domains. Organisations may also implement data loss prevention controls to monitor and restrict sensitive data leaving their networks.

For more advice on securing outbound services, such as email, web proxies and recursive DNS, refer to ASD's *Gateway security guidance package: Gateway technology guides*.

Implement network segmentation and segregation

Goal: Implement network segmentation and segregation to inhibit malicious actors from moving laterally across networks.

Implementation guidance: Place high-value assets, such as identity services, in dedicated network segments. Enforce strict access controls between network segments using a default-deny policy, allowing only the traffic essential to administration-related operations. For instance, edge devices should never initiate remote desktop protocol connections to domain controllers, as this violates segmentation principles and introduces unnecessary risk.

For more information, refer to ASD's *Implementing network segmentation and segregation* publication.

Medium priority actions

Deploy a network detection and response solution

Goal: Deploy a network detection and response (NDR) solution to deliver behavioural analysis and threat detection capabilities on network infrastructure where traditional security visibility is limited.

Implementation guidance: Deploy an NDR solution to monitor traffic and telemetry from network devices, identify malicious activities and generate alerts. Focus the deployment on key network components guided by a risk assessment.

Enable just-in-time privileged access

Goal: Implement just-in-time (JIT) privileged access to minimise the time window in which malicious actors can misuse privileged credentials.

Implementation guidance: Use a privileged access management solution to grant time-bound privileged access to network devices. Automatically rotate credentials after each use.

For further information, refer to the UK National Cyber Security Centre's *Protecting system administration with PAM* and *Secure system administration* publications.

Implement network access control

Goal: Implement network access control to prevent unauthorised or non-compliant devices from connecting to the network.

Implementation guidance: Implement an 802.1X-based network access control solution. Redirect network devices that fail to meet security policy to a quarantined network segment for remediation.

For further information, refer to ASD's *Guidelines for networking* advice within the ISM.

Foundational actions

Maintain a network device register

Goal: Identify and record all network devices connected to the network.

Implementation guidance: Regularly reconcile the network device register with network scan data. Investigate any discrepancies immediately to ensure accuracy and compliance. Reliable network device visibility is a core foundation of modern defensible architectures, supporting informed decision-making and effective risk management. A reliable network device register enables organisations to understand asset relationships and prioritise protections accordingly.

Monitor configuration integrity

Goal: Monitor configuration integrity to detect unauthorised changes to network device configurations. Treat unexplained configuration change as a potential indicator of compromise.

Implementation guidance: Implement and configure network devices to generate alerts for modifications to baseline configurations. Use automated methods, such as frequency analysis for network configuration baselining, to identify patterns, anomalies and potential issues effectively.

Establish baselines for network device health and traffic

Goal: Establish baselines for network device health and traffic to detect anomalies that may indicate a compromise.

Implementation guidance: Monitoring telemetry from network devices, such as central processing unit (CPU) and memory utilisation, can provide valuable insights into network device health and performance. Establishing baselines for network device health and traffic helps in understanding expected behaviour. Significant deviations from these baselines, including unexpected spikes in CPU or memory load, should prompt further investigation to identify potential issues or threats.

Conduct telemetry and traffic assessments before and after maintenance activities on a regular basis (e.g. firmware upgrades and restarts). Unexpected changes in baseline behaviour may indicate a compromise or misconfiguration.

Establish baselines for network control and forwarding plane activity

Goal: Establish baselines for network control and forwarding plane activity to support the detection of unexpected or unexplained changes in network routing and traffics flows. Monitoring for anomalies, such as sudden route changes or unusual forwarding behaviour, can help identify potential misconfigurations or malicious activity.

Implementation guidance: Configure a network monitoring system to generate an alert in response to unscheduled changes in routing protocol states. This differs from an NDR solution, which is focused more on data plane traffic.

Malicious actors can potentially manipulate routing protocols (e.g. Open Shortest Path First [OSPF] and Border Gateway Protocol) and forwarding plane protocols (e.g. Multiprotocol Label Switching) to enable lateral movement, intercept traffic or exfiltrate data. To detect such activity, it is important to establish a baseline of normal control and forwarding-plane behaviour (e.g. adjacencies, convergence events and route announcements). Use simple monitoring techniques, including frequency analysis, to identify patterns and expected behaviours over time. Treat any deviation (e.g. an unexpected OSPF state change on a core link) as potential cyber security events, and investigate them accordingly.

Review service and local accounts

Goal: Review service and local accounts to detect the misuse of non-user accounts.

Implementation guidance: Prohibit interactive logins by service accounts and generate alerts when attempted.

Ensure service and local accounts only perform predictable actions. Investigate any account logins that are not associated with an authorised or planned change. Assign a second person with operational knowledge of service and local accounts to review account activity. Use statistical analysis to highlight unusual behaviour but rely on human judgment to determine whether an activity is suspicious or not.

Implement secure supply chain practices

Goal: Ensure cyber security requirements are embedded throughout the supply chain lifecycle for all new network devices.

Implementation guidance: Organisational supply chain policies should require that network devices are Secure by Design and Secure by Default. This includes the use of cryptographically signed firmware and the provision of a software bill of materials (SBOM) from vendors. Where available, a cryptographic bill of materials (CBOM) can further support an organisation's transition to post-quantum cryptography. Cyber security practices such as these should be applied not only during procurement but also across vendor selection, contracting, delivery and maintenance phases to ensure end-to-end supply chain integrity.

For further information on supply chain cyber security, refer to ASD's *Managing cyber supply chains*.

Maintain a cyber security incident response plan

Goal: Maintain and regularly test a cyber security incident response plan to support a structured and effective response to cyber security incidents. Although cyber security incident response may not be entirely predictable, having a documented plan helps ensure consistency, efficiency and reduced stress during a network compromise.

Implementation guidance: Conduct scheduled tabletop exercises to test the cyber security incident response plan and ensure team readiness and familiarity. Organisations should confirm that network infrastructure is properly scoped into the plan to support effective response and recovery efforts.

Conduct ongoing security awareness training

Goal: Provide ongoing security awareness training to reduce human-factor risk and improve the cyber security culture of the organisation.

Implementation Guidance: Make security awareness training regular and relevant to the role of staff members.

For further information, refer to ASD's *Guidelines for personnel security* advice within the ISM.

Questions to continue the conversation

The following questions can assist executives and technical teams in discussing the importance of business security and resilience through network defence:

- **Vulnerability management:** What is our process to have critical vulnerabilities in internet-facing network devices patched, updated or otherwise mitigated within 48 hours? Who owns each step? How do we verify if the mitigation has been applied effectively? Do we have adequate event logs and telemetry to identify if any network device had been exploited?
- **Network device resilience:** What were the outcomes of our most recent backup recovery exercise? Did this include network device configuration settings? Would network device recovery be possible with the backups we have today?
- **Containment:** Which firewall rules prevent a compromised network device from reaching production systems? What architectural changes could be made to provide greater defence-in-depth?

- **Supply chain risk:** What contractual assurances exist to ensure third-party providers are not using unsupported or high-risk vendor hardware for our network infrastructure? How do we verify compliance?

Summary

Network infrastructure remains a primary target for malicious actors. Compromised routers, switches, firewalls and VPNs can provide persistent access into networks. This network defender guidance highlights the most important actions organisations can take to strengthen the defence of their network infrastructure.

By adopting these measures, organisations reduce exposure to both state-sponsored and criminal cyber threats, and improve their ability to detect, contain and eliminate cyber security incidents.

Network defence is achieved with a balanced commitment to awareness, precision and action.

Further information

Further information on cyber security incident response planning is available within ASD's *Cyber security incident response planning: Executive guidance* and *Cyber security incident response planning: Practitioner guidance* publications.

Further information on gateway security is available within ASD's *Gateway security guidance package* and the *Guidelines for gateways* section of the ISM.

Further information on edge device security is available within the *Securing edge devices* series, published in collaboration with international partners. This series includes:

- *Mitigation strategies for edge devices: Executive guidance*
- *Mitigation strategies for edge devices: Practitioner guidance*
- *Security considerations for edge devices*
- *Guidance on digital forensics and protective monitoring specifications for producers of network devices and appliances*

Further information on network device security is available from ASD's international partners in the following websites and publications:

- *#StopRansomware Guide*
- *Secure by Design*
- *Zero Trust Maturity Model*
- *Network Infrastructure Security Guide*
- *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System.*

Contact details

If you have any questions regarding this guidance, you can write to us or call us on 1300 CYBER1 (1300 292 371).

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

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