



# Information Security Manual

Published: 16 June 2022

## Guidelines for Networking

### Network design and configuration

#### Network documentation

It is important that network documentation is developed and accurately depicts the current state of networks, as this can assist in troubleshooting network problems as well as responding to and recovering from cyber security incidents. As such, network documentation should include, at a minimum, high-level network diagrams showing all connections into networks and logical network diagrams showing all critical servers, high-value servers, network devices and network security appliances. Finally, as network documentation could be used by an adversary to assist in compromising networks, it is important that it is appropriately protected.

**Control: ISM-0516; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Network documentation includes high-level network diagrams showing all connections into networks and logical network diagrams showing all critical servers, high-value servers, network devices and network security appliances.*

**Control: ISM-0518; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Network documentation is updated as network configuration changes are made and includes a 'current as at [date]' or equivalent statement.*

**Control: ISM-1178; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Network documentation provided to a third party, or published in public tender documentation, only contains details necessary for other parties to undertake contractual services.*

#### Network encryption

While physical security can provide a degree of protection against unauthorised physical access to network infrastructure, unauthorised access to unencrypted data can still be gained via other means, such as compromised network devices. For this reason, it is important that all data communicated over network infrastructure is encrypted, even within appropriately secure areas. Note, however, some protocols do not have encrypted equivalents. In such situations, where practical and feasible, an organisation should consider transitioning to the use of alternative protocols that support encryption.

**Control: ISM-1781; Revision: 0; Updated: Jun-22; Applicability: All; Essential Eight: N/A**

*All data communicated over network infrastructure is encrypted.*

## Network segmentation and segregation

Network segmentation and segregation is one of the most effective controls in preventing an adversary from easily propagating throughout networks once initial access has been gained. To achieve this, networks can be segregated into multiple network zones in order to protect servers, services and data. For example, administrative infrastructure used for managing critical servers, high-value servers and regular servers should be segregated from each other. In addition, all administrative infrastructure should be segregated from other assets on networks.

**Control: ISM-1181; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Networks are segregated into multiple network zones according to the criticality of servers, services and data.*

**Control: ISM-1577; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*An organisation's networks are segregated from their service providers' networks.*

## Using Virtual Local Area Networks

Virtual Local Area Networks (VLANs) can be used to implement network segmentation and segregation as long as networks belong to the same security domain. In such cases, if a data spill occurs the impact will be less than if a data spill occurred between two networks of different classifications or between an organisation's network and public network infrastructure. Should an organisation choose to risk manage implementing VLANs between networks belonging to different security domains, such as at the same classification, additional controls for network devices will apply, such as not sharing VLAN trunks and terminating VLANs on separate physical network interfaces.

For the purposes of this topic, Multiprotocol Label Switching is considered to be equivalent to VLANs and is subject to the same controls.

**Control: ISM-1532; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*VLANs are not used to separate network traffic between an organisation's networks and public network infrastructure.*

**Control: ISM-0529; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*VLANs are not used to separate network traffic between networks belonging to different security domains.*

**Control: ISM-0530; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Network devices managing VLANs are administered from the most trusted security domain.*

**Control: ISM-0535; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Network devices managing VLANs belonging to different security domains do not share VLAN trunks.*

**Control: ISM-1364; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Network devices managing VLANs terminate VLANs belonging to different security domains on separate physical network interfaces.*

## Using Internet Protocol version 6

The use of Internet Protocol version 6 (IPv6) can introduce additional security risks to networks. As such, an organisation exclusively using Internet Protocol version 4 (IPv4) should disable IPv6. This will assist in minimising the attack surface of networks and ensure that IPv6 cannot be exploited by an adversary.

To aid in the transition from IPv4 to IPv6, numerous tunnelling protocols have been developed to allow interoperability between IPv4 and IPv6. Disabling IPv6 tunnelling protocols on networks that do not require such functionality will prevent an adversary from bypassing traditional network defences by encapsulating IPv6 data inside IPv4 packets.

Stateless Address Autoconfiguration is a method of stateless Internet Protocol (IP) address configuration in IPv6 networks. Notably, it reduces the ability of an organisation to maintain effective logs of IP address assignments on networks. For this reason, stateless IP addressing should be avoided.

**Control: ISM-0521; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*IPv6 functionality is disabled in dual-stack network devices unless it is being used.*

**Control: ISM-1186; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*IPv6 capable network security appliances are used on IPv6 and dual-stack networks.*

**Control: ISM-1428; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Unless explicitly required, IPv6 tunnelling is disabled on all network devices.*

**Control: ISM-1429; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*IPv6 tunnelling is blocked by network security appliances at externally-connected network boundaries.*

**Control: ISM-1430; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Dynamically assigned IPv6 addresses are configured with Dynamic Host Configuration Protocol version 6 in a stateful manner with lease data stored in a centralised event logging facility.*

## Network access controls

If an adversary has reduced opportunities to physically connect unauthorised network devices to networks, they also have reduced opportunities to compromise networks. Network access controls can not only prevent unauthorised physical access to networks, but also prevent personnel from carelessly bridging networks by connecting one network to another network. Furthermore, network access controls can also be useful for limiting the flow of network traffic between network segments.

**Control: ISM-0520; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Network access controls are implemented on networks to prevent the connection of unauthorised network devices.*

**Control: ISM-1182; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Network access controls are implemented to limit network traffic within and between network segments to only those required for business purposes.*

## Default accounts for network devices

Network devices can come pre-configured with default credentials. For example, wireless access points with an account named 'admin' and a password of 'admin'. Ensuring default accounts are disabled, renamed or have their credentials changed can assist in reducing the likelihood of their exploitation by an adversary.

**Control: ISM-1304; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Default accounts for network devices are disabled, renamed or have their credentials changed.*

## Disabling unused physical ports on network devices

Disabling unused physical ports on network devices reduces the opportunity for an adversary to connect to networks if they can gain physical access to network devices.

**Control: ISM-0534; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Unused physical ports on network devices are disabled.*

## Functional separation between servers

Implementing functional separation between servers reduces the likelihood that a server compromised by an adversary will pose an increased security risk to other servers.

**Control: ISM-0385; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Servers maintain effective functional separation with other servers allowing them to operate independently.*

**Control: ISM-1479; Revision: 0; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Servers minimise communications with other servers at both the network and file system level.*

## Network management traffic

Implementing security measures specifically for network management traffic provides another layer of defence should an adversary find an opportunity to connect to networks. In addition, this also makes it more difficult for an adversary to enumerate networks.

**Control:** *ISM-1006; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A*

*Security measures are implemented to prevent unauthorised access to network management traffic.*

## Use of Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices. The first two iterations of SNMP were inherently insecure as they used trivial authentication methods. Furthermore, changing all default SNMP community strings on network devices, and limiting their access to read-only, is strongly encouraged.

**Control:** *ISM-1311; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A*

*SNMP version 1 and 2 are not used on networks.*

**Control:** *ISM-1312; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A*

*All default SNMP community strings on network devices are changed and write access is disabled.*

## Using Network-based Intrusion Detection and Prevention Systems

A Network-based Intrusion Detection System (NIDS) or Network-based Intrusion Prevention System (NIPS) can be an effective way of identifying and responding to network intrusions. In addition, generating event logs and alerts for network traffic that contravenes any rule in a firewall ruleset can help identify suspicious or malicious network traffic entering networks due to a failure of, or configuration change to, firewalls.

**Control:** *ISM-1028; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A*

*A NIDS or NIPS is deployed in gateways between an organisation's networks and other networks they do not manage.*

**Control:** *ISM-1030; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A*

*A NIDS or NIPS is located immediately inside the outermost firewall for gateways and configured to generate event logs and alerts for network traffic that contravenes any rule in a firewall ruleset.*

## Blocking anonymity network traffic

Inbound network connections from anonymity networks, such as the Tor network, to an organisation's internet-facing services can be used by an adversary for reconnaissance and malware delivery purposes with minimal risk of detection and attribution. As such, this network traffic should be blocked. However, an organisation might choose to support anonymous connections to their websites to cater for individuals who want to remain anonymous for privacy reasons. In such cases, it is suggested that network traffic from anonymity networks be logged and monitored instead. Additionally, outbound network connections to anonymity networks can be used by malware for command and control or data exfiltration purposes and should be blocked.

**Control:** *ISM-1627; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A*

*Inbound network connections from anonymity networks to internet-facing services are blocked.*

**Control:** *ISM-1628; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A*

*Outbound network connections to anonymity networks are blocked.*

## Protective Domain Name System Services

A protective Domain Name System (DNS) service can be an effective way of blocking requests made by an organisation's users, or an adversary on an organisation's network, to known malicious domains – either as part of an

initial compromise or subsequent command and control activities. DNS event logs captured by a protective DNS service can also be useful for investigating any exploitation attempt or successful compromise of a network by an adversary.

In selecting a protective DNS service, many commercial offerings exist. In addition, the Australian Cyber Security Centre (ACSC) also offers a free protective DNS service for all levels of government.

**Control: ISM-1782; Revision: 0; Updated: Jun-22; Applicability: All; Essential Eight: N/A**

*A protective DNS service is used for networks.*

## Further information

Further information on wireless networks can be found in the wireless networks section of these guidelines.

Further information on gateways can be found in the gateways section of the [Guidelines for Gateways](#).

Further information on encrypting communications can be found in the cryptographic fundamentals section of the [Guidelines for Cryptography](#).

Further information on network segmentation and segregation can be found in the ACSC's [Implementing Network Segmentation and Segregation](#) publication.

Further information on network security zones can be found in the Canadian Centre for Cyber Security's [Baseline Security Requirements for Network Security Zones \(Version 2.0\)](#) publication.

Further information on implementing network segmentation and segregation for system administration purposes can be found in the system administration section of the [Guidelines for System Management](#).

Further information on functional separation of servers using virtualisation can be found in the virtualisation hardening section of the [Guidelines for System Hardening](#).

Further information on event logging can be found in the event logging and monitoring section of the [Guidelines for System Monitoring](#).

Further information on blocking anonymity network traffic can be found in the ACSC's [Defending Against the Malicious Use of the Tor Network](#) publication.

Further information on Domain Name System services can be found in the ACSC's [Domain Name System Security for Domain Owners](#) and [Domain Name System Security for Domain Resolvers](#) publications.

Further information on selecting a protective DNS service can be found in the United States' National Security Agency and Cybersecurity & Infrastructure Security Agency's [Selecting a Protective DNS Service](#) publication.

Further information on network design and configuration can be found in the United States' National Security Agency's [Network Infrastructure Security Guidance](#) publication.

## Wireless networks

### Wireless networks

This section describes the controls applicable to wireless networks and extends upon the prior network design and configuration section.

#### Choosing wireless devices

Using wireless devices, such as wireless access points, wireless adapters and wireless network cards, which have been certified against a Wi-Fi Alliance certification program, provides an organisation with the assurance that they conform to wireless standards and are guaranteed to be interoperable with other wireless devices on wireless networks.

**Control: ISM-1314; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A**

*All wireless devices are Wi-Fi Alliance certified.*

## Public wireless networks

When an organisation provides a public wireless network for general public use, connecting the public wireless network to, or sharing infrastructure with, any other organisation networks can create an entry point for an adversary allowing them to target organisation networks in order to steal data or disrupt services.

**Control: ISM-0536; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Public wireless networks provided for general public use are segregated from all other organisation networks.*

## Administrative interfaces for wireless access points

Administrative interfaces allow users to modify the configuration and security settings of wireless access points. Often, by default, wireless access points allow users to access administrative interfaces over fixed network connections or wireless network connections. To assist in reducing the attack surface for wireless access points, the administrative interface should be disabled for wireless network connections.

**Control: ISM-1315; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*The administrative interface on wireless access points is disabled for wireless network connections.*

## Default settings

Some wireless access points come with default Service Set Identifiers (SSIDs) or weak default configuration settings. As default SSIDs are often documented on the internet, along with default accounts and credentials, it is important to change default SSIDs of wireless access points along with default credentials and weak configuration settings.

When changing default SSIDs, it is important that new SSIDs do not bring undue attention to an organisation's wireless networks. In doing so, SSIDs of wireless networks should not be readily associated with an organisation, the location of their premises or the functionality of wireless networks.

A method commonly recommended to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, SSIDs are still broadcast in probe requests, probe responses, association requests and re-association requests. As such, it is easy to determine SSIDs of wireless networks by capturing these requests and responses. By disabling SSID broadcasting, an organisation will make it more difficult for users to connect to wireless networks. Furthermore, an adversary could configure a malicious wireless access point to broadcast the same SSID as a hidden SSID used by a legitimate wireless network, thereby fooling users or devices into automatically connecting to the adversary's malicious wireless access point instead. In doing so, the adversary could steal authentication credentials in order to gain access to the legitimate wireless network.

**Control: ISM-1316; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Default SSIDs of wireless access points are changed.*

**Control: ISM-1317; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*SSIDs of non-public wireless networks are not readily associated with an organisation, the location of their premises or the functionality of wireless networks.*

**Control: ISM-1318; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*SSID broadcasting is not disabled on wireless access points.*

**Control: ISM-1709; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Default accounts and credentials of wireless access points are changed.*

**Control: ISM-1710; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Configuration settings for wireless access points are hardened.*



## Media Access Control address filtering

Devices that connect to wireless networks generally have a unique Media Access Control (MAC) address. Using MAC address filtering can prevent rogue devices from connecting to wireless networks. However, an adversary may be able to determine MAC addresses of legitimate devices and use this information to gain access to wireless networks. As such, MAC address filtering introduces management overhead without any tangible security benefit.

**Control:** ISM-1320; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A

*MAC address filtering is not used to restrict which devices can connect to wireless networks.*

## Static addressing

Assigning static IP addresses for devices accessing wireless networks can prevent rogue devices connecting to wireless networks from being assigned routable IP addresses. However, an adversary may be able to determine IP addresses of legitimate devices and use this information to gain access to wireless networks. As such, configuring devices to use static IP addresses introduces management overhead without any tangible security benefit.

**Control:** ISM-1319; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A

*Static addressing is not used for assigning IP addresses on wireless networks.*

## Confidentiality and integrity of wireless network traffic

As wireless networks are often capable of being accessed from outside the perimeter of secured spaces, all wireless network traffic requires suitable cryptographic protection. For this purpose it is recommended that Wi-Fi Protected Access 3 (WPA3) be used as it provides equivalent or greater security than its predecessor Wi-Fi Protected Access 2 (WPA2). WPA3 has also prohibited the use of various outdated and insecure cipher suites.

WPA3-Enterprise supports three enterprise modes of operation: enterprise only mode, transition mode and 192-bit mode. Preference is given to WPA3-Enterprise 192-bit mode as this mode incorporates changes that satisfy the United States' Commercial National Security Algorithm Suite requirements and ensures no algorithms with known weaknesses are used. However, if any other WPA3-Enterprise modes are used then Authentication and Key Management suite 00-0F-AC:1 should be disabled (if this option is available).

**Control:** ISM-1332; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: N/A

*WPA3-Enterprise 192-bit mode is used to protect the confidentiality and integrity of all wireless network traffic.*

## 802.1X authentication

WPA3-Enterprise uses 802.1X authentication which requires the use of an Extensible Authentication Protocol (EAP). A number of EAP methods supported by both WPA2 and WPA3 are available.

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) is considered one of the most secure EAP methods and is widely supported. It uses a Public Key Infrastructure to secure communications between devices and a Remote Access Dial-In User Service (RADIUS) server through the use of X.509 certificates. While EAP-TLS provides strong mutual authentication, it requires an organisation to have established a Public Key Infrastructure. This involves deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses their wireless networks. While this introduces additional costs and management overheads, the security advantages are significant.

**Control:** ISM-1321; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A

*802.1X authentication with EAP-TLS, using X.509 certificates, is used for mutual authentication; with all other EAP methods disabled on supplications and authentication servers.*

**Control:** ISM-1711; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: N/A

*User identity confidentiality is used if available with EAP-TLS implementations.*

## Evaluation of 802.1X authentication implementation

The security of 802.1X authentication is dependent on four main elements and how they interact with each other. These four elements include supplicants, authenticators, wireless access points and authentication servers. To provide assurance that these elements have been implemented correctly, they should have completed an evaluation.

**Control: ISM-1322; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: N/A**

*Evaluated supplicants, authenticators, wireless access points and authentication servers are used in wireless networks.*

## Generating and issuing certificates for authentication

When issuing certificates to devices in order to access wireless networks, an organisation should be aware that certificates could be stolen by malicious code. Once compromised, certificates could be used on other devices to gain unauthorised access to wireless networks. An organisation should also be aware that in only issuing certificates to devices, any actions taken by users will only be attributable to specific devices.

When issuing certificates to users in order to access wireless networks, it can be in the form of certificates that are stored on devices or certificates that are stored on smart cards. While issuing certificates on smart cards provides increased security, it comes at a higher cost. However, users are more likely to notice missing smart cards and alert their security team, who are then able to revoke their credentials, which can minimise the time an adversary has access to wireless networks. In addition, to reduce the likelihood of stolen smart cards from being used to gain unauthorised access to wireless networks, multi-factor authentication can be implemented through the use of personal identification numbers on smart cards. This is particularly important when smart cards grant users any form of administrative access.

**Control: ISM-1324; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Certificates are generated using an evaluated certificate authority or hardware security module.*

**Control: ISM-1323; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: N/A**

*Certificates are required for both devices and users accessing wireless networks.*

**Control: ISM-1327; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A**

*Certificates are protected by encryption, user authentication, and both logical and physical access controls.*

## Caching 802.1X authentication outcomes

When 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated upon successful authentication of devices. This PMK is then capable of being cached to assist with fast roaming between wireless access points. When devices roam away from wireless access points they have authenticated to, they will not need to perform a full re-authentication should they roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate devices to neighbouring wireless access points that devices might roam to. Although requiring full authentication for devices each time they roam between wireless access points is ideal, an organisation can choose to use PMK caching and pre-authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

**Control: ISM-1330; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*The PMK caching period is not set to greater than 1440 minutes (24 hours).*

## Fast Basic Service Set Transition

The WPA3 standard specifies support for Fast Basic Service Set Transition (FT) (802.11r). FT is a feature designed to improve user mobility and combat lag introduced by the need to authenticate to each wireless access point. However, FT requires authenticators to request and send keys to other authenticators within a security domain. If any of these keys are intercepted, all security properties are lost. Therefore, it is imperative that communications are appropriately secured. As such, FT should be disabled unless it can be confirmed that authenticator-to-authenticator communications



are secured by a suitable ASD-Approved Cryptographic Protocol that provides confidentiality, integrity and mutual authentication.

**Control: ISM-1712; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*The use of FT (802.11r) is disabled unless authenticator-to-authenticator communications are secured by an ASD-Approved Cryptographic Protocol.*

## Remote Authentication Dial-In User Service authentication

Separate to the 802.1X authentication process is the RADIUS authentication process that occurs between authenticators and a RADIUS server. RADIUS is what is known as an authentication, authorisation and accounting protocol, and is intended to mediate network access. However, RADIUS is not secure enough to be used without protection. To protect credentials communicated between authenticators and a RADIUS server, communications should be encapsulated with an additional layer of encryption, such as RADIUS over Internet Protocol Security or RADIUS over Transport Layer Security.

**Control: ISM-1454; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A**

*Communications between authenticators and a RADIUS server are encapsulated with an additional layer of encryption using RADIUS over Internet Protocol Security or RADIUS over Transport Layer Security.*

## Interference between wireless networks

When wireless networks are deployed in close proximity, there is the potential for interference to impact their availability, especially when operating on commonly used 802.11b/g (2.4 GHz) default channels of 1 and 11. Sufficiently separating wireless networks through the use of frequency separation can help reduce this security risk. This can be achieved by using wireless networks that are configured to operate on channels that minimise overlapping frequencies or by using both 802.11b/g (2.4 GHz) channels and 802.11n (5 GHz) channels. It is important to note though, if implementing a mix of 2.4 GHz and 5 GHz channels, not all devices may be compatible with 802.11n and able to connect to 5 GHz channels.

**Control: ISM-1334; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Wireless networks implement sufficient frequency separation from other wireless networks.*

## Protecting management frames on wireless networks

An effective denial-of-service attack can be performed by exploiting unprotected management frames using inexpensive commercial hardware. The 802.11 standard provides no protection for management frames and therefore does not protect against spoofing or denial-of-service attacks. However, the 802.11w amendment specifically addresses the protection of management frames on wireless networks and should be enabled for WPA2. Note, in WPA3 this feature is built into the standard.

**Control: ISM-1335; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*Wireless access points enable the use of the 802.11w amendment to protect management frames.*

## Wireless network footprint

Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power can be deployed to achieve the desired footprint for wireless networks. This has the benefit of providing service continuity should wireless access points become unserviceable. In such cases, the output power of nearby wireless access points can be increased to cover the footprint gap until the unserviceable wireless access points can be replaced.

In addition to minimising the output power of wireless access points to reduce the footprint of wireless networks, the use of Radio Frequency (RF) shielding can be used for an organisation's facilities. While expensive, this will limit wireless communications to areas under the control of an organisation. RF shielding on an organisation's facilities also has the

added benefit of preventing the jamming of wireless networks from outside of the facilities in which wireless networks are operating.

**Control: ISM-1338; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power are deployed to achieve the desired footprint for wireless networks.*

**Control: ISM-1013; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A**

*The effective range of wireless communications outside an organisation's area of control is limited by implementing RF shielding on facilities in which SECRET or TOP SECRET wireless networks are used.*

## Further information

Further information on [Wi-Fi technologies](#) and associated [certification programs](#) are available from the Wi-Fi Alliance.

Further information on evaluated products can be found in the evaluated product acquisition section of the [Guidelines for Evaluated Products](#).

Further information on encrypting communications can be found in the cryptographic fundamentals section of the [Guidelines for Cryptography](#).

Further information on the United States' [Commercial National Security Algorithm Suite](#) is available from the United States' National Security Agency.

## Service continuity for online services

### Cloud-based hosting of online services

Using cloud service providers can allow an organisation to build highly resilient online services due to the increased computing resources, bandwidth and multiple separate physical sites made available by the cloud server providers. An organisation can achieve the same results using their own infrastructure. However, doing so may require significant upfront costs and may still result in a limited capability to scale dynamically to meet increased demand. In case of a denial-of-service attack, cloud-based hosting can also provide segregation from self-hosted or other cloud-hosted services ensuring that other systems, such as email, are not affected.

**Control: ISM-1437; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Cloud service providers are used for hosting online services.*

### Location policies for online services

When using cloud service providers, an organisation will need to consider whether they should lock their data to specific regions or availability zones. In choosing to do so, an organisation will have an expectation that their data will not be relocated to different regions or availability zones by cloud service providers.

**Control: ISM-1578; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*An organisation is notified by cloud service providers of any change to configured regions or availability zones for online services.*

### Availability planning and monitoring for online services

It is important that connectivity between an organisation and their cloud service providers meets requirements for bandwidth, latency and reliability. In support of this, an organisation and their cloud service providers should discuss any specific network requirements, performance characteristics or planned responses to availability failures, especially when a requirement for high availability exists. Furthermore, an organisation and their cloud service providers should discuss whether dedicated communication links or connections over the internet will be used and whether any

secondary communications links will provide sufficient capacity to maintain operational requirements should the primary communication link become unavailable.

Furthermore, capacity monitoring should be performed in order to manage workloads and monitor the health of online services. This can be achieved through continuous real-time monitoring of metrics, such as latency, jitter, packet loss, throughput and availability. In addition, feedback should be provided to cloud service providers when performance does not meet service level agreement targets. To assist with this, anomaly detection can be performed through network telemetry that is integrated into security monitoring tools.

**Control: ISM-1579; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Cloud service providers' ability to dynamically scale resources due to a genuine spike in demand or a denial-of-service attack is tested as part of capacity planning processes for online services.*

**Control: ISM-1580; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.*

**Control: ISM-1441; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Where a requirement for high availability exists for online services, a denial of service mitigation service is used.*

**Control: ISM-1581; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Continuous real-time monitoring of the availability of online services is performed.*

## Using content delivery networks

Similar to cloud-based hosting, the use of content delivery networks (CDNs) can allow an organisation to create highly resilient online services by leveraging the large bandwidth, geographically dispersed hosting locations, traffic scrubbing and other controls offered by CDNs.

The use of CDNs is particularly effective when serving static bandwidth intensive media, such as images, sound or video files. However, the services offered by CDNs can include more than basic content hosting, such as web response caching, load balancing, web application security and denial of service mitigations.

Care should be taken when configuring the use of CDNs to ensure that the IP addresses of an organisation's web servers are not identifiable by an adversary, as this could allow for protections to be bypassed. Additionally, appropriate controls should be applied to only allow communication between an organisation's web servers, CDNs and authorised management networks.

**Control: ISM-1438; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Where a high availability requirement exists for website hosting, CDNs that cache websites are used.*

**Control: ISM-1439; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*If using CDNs, disclosing the IP addresses of web servers under an organisation's control (referred to as origin servers) is avoided and access to the origin servers is restricted to the CDNs and authorised management networks.*

## Denial of service strategies

Denial-of-service attacks are designed to disrupt or degrade online services, such as website, email and Domain Name System services. To achieve this goal, an adversary may use a number of methods to deny access to legitimate users of online services. This includes using multiple computers to direct a large volume of unwanted network traffic at online services in an attempt to consume all available network bandwidth, using multiple computers to direct tailored network traffic at online services in an attempt to consume the processing resources of online services, or hijacking online services in an attempt to redirect legitimate users away from those services to other services that the adversary controls.

Although an organisation cannot avoid being targeted by denial-of-service attacks, there are a number of measures they can implement to prepare for and potentially reduce the impact if targeted. This includes engaging with their

cloud service providers to identify the denial of service detection technologies that may be available for their use. For example, real-time capacity reporting dashboards that provide out-of-band and real-time alerts based on organisation-defined thresholds can assist with the rapid identification of denial-of-service attacks.

Finally, not all online services offered by an organisation may be business critical. Understanding what online services can be disabled or offered with reduced functionality during denial-of-service attacks can help an organisation reduce or eliminate the impact on essential services. Overall, preparing for denial-of-service attacks before they occur is by far the best strategy as it is very difficult to respond once they begin and efforts at this stage are unlikely to be effective.

**Control: ISM-1431; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*Denial-of-service attack mitigation strategies are discussed with cloud service providers, specifically:*

- *their capacity to withstand denial-of-service attacks*
- *any costs likely to be incurred as a result of denial-of-service attacks*
- *thresholds for notification of denial-of-service attacks*
- *thresholds for turning off online services during denial-of-service attacks*
- *pre-approved actions that can be undertaken during denial-of-service attacks*
- *any arrangements with upstream service providers to block malicious network traffic as far upstream as possible.*

**Control: ISM-1458; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*The functionality and quality of online services, how to maintain such functionality, and what functionality can be lived without during a denial-of-service attack, are determined and documented.*

## Domain name registrar locking

The use of domain name registrar locking can prevent a denial of service caused by unauthorised modification of a domain's registration details or unauthorised deletion or transfer of a domain.

**Control: ISM-1432; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Domain names for online services are protected via registrar locking and confirming domain registration details are correct.*

## Monitoring with real-time alerting for online services

An organisation should perform automated monitoring of online services with real-time alerting to ensure that a denial-of-service attack is detected and responded to as soon as possible.

**Control: ISM-1435; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Availability monitoring with real-time alerting is implemented for online services to detect denial-of-service attacks and measure their impact.*

## Segregation of critical online services

Denial-of-service attacks are typically focused on highly visible online services, such as an organisation's core website, in order to have a publicly noticeable impact. By segregating online services, such as using one internet connection for email and internet access, and a separate internet connection for web hosting services, the impact of a denial-of-service attack can be limited.

**Control: ISM-1436; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Critical online services are segregated from other online services that are more likely to be targeted.*

## Preparing for service continuity

An organisation's full-featured website may have higher processing or resource demands due to database integration or the presence of high-resolution images and videos. These additional resource requirements may make the website more susceptible to denial-of-service attacks. As such, depending on the nature of a denial-of-service attack, replacing the full-featured website with a minimal impact static version can help provide a level of service which would otherwise not be possible.

**Control: ISM-1518; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*A static version of a website is pre-prepared that requires minimal processing and bandwidth in order to facilitate at least a basic level of service when under a denial-of-service attack.*

## Further information

Further information on business continuity and disaster recovery planning can be found in the Chief Information Security Officer section of the [Guidelines for Cyber Security Roles](#).

Further information on mitigating denial-of-service attacks can be found in the ACSC's [Preparing for and Responding to Denial-of-Service Attacks](#) publication.