Guidelines for Gateway Management

Gateways

Purpose of gateways

Gateways act as information flow control mechanisms at the network layer and may also control information at the higher layers of the Open System Interconnect (OSI) model.

Deploying gateways

This section describes the security controls applicable to all gateways. Additional areas of these guidelines should also be consulted depending on the type of gateway deployed:

- For connections between different security domains, where at least one system is SECRET or higher, see the Cross Domain Solutions section of these guidelines.
- For devices used to control data flow in bi-directional gateways, see the firewalls section of these guidelines.
- For all gateways, see the Guidelines for Data Transfers and Content Filtering.

Applying the security controls

In all cases, gateways assumes the highest sensitivity or classification of the connected security domains.

Gateway architecture and configuration

Gateways are necessary to control data flows between security domains and prevent unauthorised access from external networks. Given the criticality of gateways in controlling the flow of information between security domains, any failure, particularly at higher classifications, may have serious consequences. As such, robust mechanisms for alerting personnel to situations that may cause cyber security incidents are especially important for gateways.

Security Control: 0628; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
All systems are protected from systems in other security domains by one or more gateways.

Security Control: 1192; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All connections between security domains implement mechanisms to inspect and filter data flows for the transport and higher layers as defined in the OSI model.

Security Control: 0631; Revision: 5; Updated: Jun-19; Applicability: O, P, S, TS
Gateways:
- are the only communications paths into and out of internal networks
- allow only explicitly authorised connections
- are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network)
- are protected by authentication, logging and auditing of all physical and logical access to gateway components
- have all security controls tested to verify their effectiveness after any changes to their configuration.

**Security Control: 1427; Revision: 2; Updated: Jun-19; Applicability: O, P, S, TS**

Gateways implement ingress traffic filtering to detect and prevent Internet Protocol (IP) source address spoofing.

**Gateway operation**

Implementing logging and alerting capabilities for gateways can assist in detecting cyber security incidents, attempted intrusions and unusual usage patterns. In addition, storing event logs on a separate secure log server increases the difficulty for an adversary to delete logging information in order to destroy evidence of a targeted cyber intrusion.

**Security Control: 0634; Revision: 7; Updated: Jun-19; Applicability: O, P, S, TS**

All gateways connecting networks in different security domains are operated such that they:

- log network traffic permitted through the gateway
- log network traffic attempting to leave the gateway
- are configured to save event logs to a secure logging facility
- provide real-time alerts for any cyber security incidents, attempted intrusions and unusual usage patterns.

**Demilitarised zones**

Demilitarised zones are used to prevent direct access to information and services on internal networks. Organisations that require certain information and services to be accessed from the Internet can place them in the less trusted demilitarised zone instead of on internal networks.

**Security Control: 0637; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS**

Demilitarised zones are used to broker access to services accessed by external entities, and mechanisms are applied to mediate internal and external access to less-trusted services hosted in these demilitarised zones.

**Gateway security risk assessment**

Performing a security risk assessment on the gateway architecture and the proposed configuration before implementation allows for the early identification and mitigation of security risks to the gateway environment and connected systems. In addition, gateways can connect networks in different security domains, including across administrative and organisational boundaries. By understanding and formally accepting security risks from all other networks before gateways are implemented, system owners can make informed decisions about changes to their gateway environment.

**Security Control: 0598; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

A security risk assessment is performed on gateways and their configuration before their implementation.

**Security Control: 1519; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS**

A security risk assessment is performed on all systems before they are connected to a gateway.

**Security Control: 0605; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

All system owners of systems connected via a gateway understand and accept security risks associated with the gateway and any connected security domains, including those connected via a cascaded connection.
The security architecture of a gateway, and security risks associated with all connected security domains, including those connected via a cascaded connection, is reviewed at least annually.

**Gateway configuration control**

Changes that could introduce security vulnerabilities or change security risks in a gateway should be appropriately considered and documented before being implemented.

**Security Control: 0624; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

Any associated security risk assessments are updated before changes are made to a gateway to ensure all relevant security risks have been documented and accepted.

**Security Control: 0625; Revision: 5; Updated: Aug-19; Applicability: O, P, S, TS**

All changes to a gateway architecture are considered prior to implementation, documented and assessed in accordance with the organisation’s change management process and supporting change management procedures.

**Gateway testing**

Testing security controls on gateways assists with understanding its security posture by determining the effectiveness of security controls. An adversary may be aware of regular testing activities. Therefore, performing testing at irregular intervals will reduce the likelihood that an adversary could exploit regular testing activities.

**Security Control: 1037; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

Gateways are subject to rigorous testing, performed at irregular intervals no more than six months apart, to determine the strength of security controls.

**Gateway administration**

Administrator privileges should be minimised and roles should be separated (e.g. separate network administration and security policy configuration roles) to minimise security risks posed by a malicious user with privileged access to a gateway.

Providing system administrators with formal training will ensure they are fully aware of, and accept, their roles and responsibilities regarding the management of gateways. Formal training could be through commercial providers, or simply through Standard Operating Procedures or reference documents bound by a formal agreement.

The system owner of the highest security domain of connected security domains is responsible for protecting the most sensitive information, and as such is best placed to manage any shared components of gateways. However, in cases where multiple security domains from different organisations are connected to a gateway, it may be more appropriate to have a qualified third party manage the gateway on behalf of all connected organisations.

**Security Control: 0611; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS**

Access to gateway administration functions is limited to the minimum roles and privileges to support the gateway securely.

**Security Control: 0612; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

System administrators are formally trained to manage gateways.

**Security Control: 1520; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS**

All system administrators of gateways are cleared to access the highest level of information communicated or processed by the gateway.

**Security Control: 0613; Revision: 4; Updated: Sep-18; Applicability: S, TS**

All system administrators of gateways that process Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) information are Australian nationals.
Roles for the administration of gateways are separated.

For gateways between networks in different security domains, a formal arrangement exists whereby any shared components are managed by the system managers of the highest security domain or by a mutually agreed third party.

**Shared ownership of gateways**

As changes to a security domain connected to a gateway potentially affects the security posture of other connected security domains, system owners should formally agree to be active information stakeholders in other security domains to which they are connected via a gateway.

**Gateway authentication**

Ensuring users and services are authenticated by gateways can reduce the likelihood of unauthorised access and provides an auditing capability to support the investigation of cyber security incidents.

Users and services accessing networks through gateways are authenticated.

Only users and services authenticated and authorised to a gateway can use the gateway.

Multi-factor authentication is used for access to gateways.

**ICT equipment authentication**

Authenticating ICT equipment to networks accessed through gateways assists in preventing unauthorised ICT equipment connecting to a network. For example, by using 802.1X.

ICT equipment accessing networks through gateways is authenticated.

**Further information**

Further information on topics covered in this section can be found in the following cyber security guidelines:

- **Guidelines for Cyber Security Incidents**
- **Guidelines for Physical Security**
- **Guidelines for Evaluated Products**
- **Guidelines for ICT Equipment Management**
- **Guidelines for System Hardening**
- **Guidelines for System Management**
- **Guidelines for System Monitoring**
- **Guidelines for Network Management**
- **Guidelines for Data Transfers and Content Filtering**.
Further information on preventing IP source address spoofing can be found in *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing* at https://tools.ietf.org/html/bcp38.

**Cross Domain Solutions**

**Purpose of Cross Domain Solutions**

Cross Domain Solutions (CDS) provide robust information flow control mechanisms at each layer of the OSI model in gateway environments where high levels of assurance are required. This section extends the preceding gateways section.

**Introduction to Cross Domain Solutions**

This section describes the security controls applicable to CDS. CDS systems should apply controls from both the gateways and Cross Domain Solutions sections. Furthermore, the *Guidelines for Data Transfers and Content Filtering* also applies to all gateways and CDS. Finally, additional sections of these guidelines should be consulted depending on the specific type of CDS deployed.

CDS are systems comprising security-enforcing functions tailored to mitigate the specific security risks of accessing or transferring information between security domains. A CDS may be an integrated appliance or, more commonly, be composed of discrete technologies or sub-systems, with each sub-system consisting of hardware and/or software components.

Personnel involved in the planning, analysis, design, implementation or assessment of CDS should refer to the Australian Cyber Security Centre (ACSC)'s *Introduction to Cross Domain Solutions* and *Guide to the Secure Configuration of Cross Domain Solutions* publications.

**Types of Cross Domain Solutions**

These guidelines define two logical types of CDS: Transfer CDS and Access CDS. These logical definitions are more closely aligned with how CDS are described and sold by vendors and system integrators. Vendors may also offer a combined Access and Transfer solution.

Regardless of logical configuration, the underlying mechanisms in each CDS will consist of a low to high data transfer path, a high to low data transfer path, or both. Data filtering and other security controls are then applied to mitigate threats applicable to the system’s operating context, including specific data paths and business cases.

A Transfer CDS facilitates the transfer of information, in one (unidirectional) or multiple (bi-directional) directions between different security domains.
An Access CDS provides the user with access to multiple security domains from a single device. Conceptually, an Access CDS allows remote interaction with one or multiple systems in a different security domain, such as a ‘virtual desktop’, and does not allow users to move data between security domains.

Applying the security controls

In all cases the gateway or CDS assumes the highest sensitivity or classification of the connected security domains.

Requirements to use Cross Domain Solutions

There are significant security risks associated with connecting highly classified systems to the Internet or to a lower classified system. An adversary having control of, or access to, a gateway or CDS can invoke a serious security risk.
Consultation when implementing or modifying Cross Domain Solutions

CDS environments can be complex to deploy and manage securely, as such, the likelihood of a network compromise is increased. Secure CDS implementations ensure that the security policy of each security domain involved is upheld in a robust manner across all physical and logical layers of the connection between domains.

Separation of data flows

CDS connecting highly classified systems to other potentially internet-connected systems should implement robust security enforcing functions, including content filtering and isolated paths, to ensure data flows are appropriately controlled.

Event logging

In addition to the security controls listed in the event logging and auditing section of the Guidelines for System Monitoring, CDS should have comprehensive logging capabilities to establish accountability for all actions performed by users. Effective logging practices can increase the likelihood that unauthorised behaviour will be detected.

User training

It is important that users know how to use a CDS securely. This can be achieved via training before access is granted, and reinforced by logon banners and awareness messages.
Further information

Further information on topics covered in this section can be found in the following cyber security guidelines:

- Guidelines for Cyber Security Incidents
- Guidelines for Physical Security
- Guidelines for Evaluated Products
- Guidelines for ICT Equipment Management
- Guidelines for System Hardening
- Guidelines for System Management
- Guidelines for System Monitoring
- Guidelines for Network Management
- Guidelines for Data Transfers and Content Filtering.


Further information regarding the planning, analysis, design, implementation or assessment of CDS can be found in the ACSC’s Guide to the Secure Configuration of Cross Domain Solutions publication available via request from the ACSC.

**Firewalls**

**Using firewalls**

Where an organisation connects to another organisation, both organisations should implement a firewall in their gateway environment to protect themselves from intrusions that originate outside of their environment. This requirement may not be necessary in the specific cases where shared network infrastructure is used only as a transport medium and link encryption is used.

**Firewalls for particularly important networks**

As AUSTEO and AGAO networks are particularly important, additional assurances should be put in place when connecting such networks to other networks.

An evaluated firewall is used between official or classified networks and public network infrastructure.

An evaluated firewall is used between networks belonging to different security domains.

The requirement to use a firewall as part of gateway infrastructure is met by both parties independently; shared ICT equipment does not satisfy the requirements of both parties.

In addition to the firewall between networks of different security domains, an evaluated firewall is used between an AUSTEO or AGAO network and a foreign network.
In addition to the firewall between networks of different security domains, an evaluated firewall is used between an AUSTEO or AGAO network and another Australian controlled network.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the Guidelines for Evaluated Products.

Diodes

Using diodes

A diode enforces one-way flow of network traffic thus requiring separate paths for incoming and outgoing data. This makes it much more difficult for an adversary to use the same path to both launch a targeted cyber intrusion and exfiltrate information afterwards.

Diodes for particularly important networks

While diodes between networks at the same classification are generally not needed, AUSTEO and AGAO networks require additional assurances to be put in place when connecting such networks to other networks.

Volume checking

Monitoring the volume of data being transferred across a diode ensures that it conforms to expectations. It can also alert an organisation to potential malicious activity if the volume of data suddenly changes from the norm.
Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the Guidelines for Evaluated Products.

Web content and connections

Web usage policy

If organisations allow users to access the Web they should define the extent of access that is granted. This can be achieved through a web usage policy and education of users.

Security Control: 0258; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
A web usage policy is developed and implemented.

Web proxies

Web proxies are a key component in detecting and responding to cyber security incidents. Thorough web proxy logs are also valuable in responding to user violation of web usage policies.

Security Control: 0260; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All web access, including that by internal servers, is conducted through a web proxy.

Security Control: 0261; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
A web proxy authenticates users and provides logging that includes the following details about websites accessed:

- address (uniform resource locator)
- time/date
- user
- amount of data uploaded and downloaded
- internal and external IP addresses.

Transport Layer Security filtering

Since Transport Layer Security (TLS) web traffic travelling over Hypertext Transfer Protocol Secure connections can deliver content without any filtering, organisations can reduce this security risk by using TLS inspection. In doing so, organisations may choose to allow websites that have a low risk of delivering malicious code and have a high privacy requirement, such as internet banking websites, to continue using end-to-end TLS encryption.

Security Control: 0263; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
If permitting TLS through internet gateways, either of the following approaches is implemented:

- a solution that decrypts and inspects TLS traffic as per content filtering security controls
- a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked or decrypted and inspected as per content filtering security controls.

Inspection of Transport Layer Security traffic

As encrypted TLS traffic may contain personally identifiable information, organisations are recommended to seek legal advice on whether inspecting such traffic could be in breach of the Privacy Act 1988.

Security Control: 0996; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Legal advice is sought regarding the inspection of TLS traffic by internet gateways.
Whitelisting websites

Defining a whitelist of permitted websites and blocking all unlisted websites effectively removes one of the most common data delivery and exfiltration techniques used by an adversary. However, if users have a legitimate requirement to access numerous websites, or a rapidly changing list of websites, organisations should consider the costs of such an implementation.

Even a relatively permissive whitelist offers better security than relying on blacklists, or no restrictions at all, while still reducing implementation costs. An example of a permissive whitelist could be whitelisting the entire Australian subdomain, that is ‘*.au’, or whitelisting the top 1,000 sites from the Alexa site ranking (after filtering Dynamic Domain Name System domains and other inappropriate domains).

Security Control: 0958; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Whitelisting is implemented for all Hypertext Transfer Protocol (HTTP) traffic communicated through internet gateways.

Security Control: 0995; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
If using a whitelist on internet gateways to specify the external addresses to which connections are permitted, it specifies whitelisted addresses by domain name or IP address.

Categorising websites

Websites can be grouped into categories and prohibited categories can be blocked via a web content filter.

Security Control: 1170; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
If websites are not whitelisted, categories are implemented for all websites and prohibited and uncategorised websites are blocked.

Blacklisting websites

Blacklists are collections of websites that have been deemed to be inappropriate due to their content or hosting of malicious content.

Targeted cyber intrusions commonly use dynamic or other domains where domain names can be registered anonymously for free due to their lack of attribution.

Security Control: 0959; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
If whitelisting of websites is not implemented, blacklisting of websites is implemented to prevent access to known malicious websites.

Security Control: 0960; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
If blacklisting websites, the blacklist is updated on a daily basis to ensure that it remains effective.

Security Control: 1171; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Attempts to access a website through its IP address instead of through its domain name are blocked.

Security Control: 1236; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Dynamic domains and other domains where domain names can be registered anonymously for free are blocked.

Web content filter

An effective web content filter greatly reduces the likelihood of malicious code infection or other inappropriate content from being accessed by users. Web content filters can also disrupt or prevent an adversary from communicating with their malicious code if deployed on an organisation’s network.

Some forms of content filtering performed by web content filters are the same as those performed by email or other content filters while other types of content filtering are specific to web-based content.

Security Control: 0963; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
A web content filter is used to filter potentially harmful web-based content.

**Security Control: 0961; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS**
Client-side active content, such as Java, is restricted to a whitelist of approved websites which may be the same as the HTTP whitelist or a separate active content whitelist.

**Security Control: 1237; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS**
Web content filtering controls are applied to outbound web traffic where appropriate.

**Further information**

Further information on web content filtering can be found in the *Guidelines for Data Transfers and Content Filtering*.

Examples of client-side JavaScript controls are available at [https://noscript.net/](https://noscript.net/).

**Peripheral switches**

**Using peripheral switches**

When accessing different systems through a peripheral switch, it is important that sufficient assurance is held in the operation of the switch to ensure that information does not pass between different security domains. As such, the level of assurance needed in a peripheral switch is determined by the difference in sensitivity or classification of systems connected to the switch.

There is no requirement for an evaluated peripheral switch when all connected systems belong to the same security domain.

**Security Control: 0591; Revision: 6; Updated: Sep-18; Applicability: O, P**
An evaluated peripheral switch is used when sharing peripherals between official and classified systems.

**Security Control: 1480; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS**
A high assurance peripheral switch is used when sharing peripherals between official or classified systems and highly classified systems.

**Security Control: 1457; Revision: 2; Updated: Sep-18; Applicability: S, TS**
An evaluated, preferably high assurance, peripheral switch is used when sharing peripherals between systems of different classifications.

**Security Control: 0593; Revision: 9; Updated: Apr-19; Applicability: O, P, S, TS**
An evaluated peripheral switch is used when sharing peripherals between systems of the same classification, that belong to different security domains.

**Peripheral switches for particularly important systems**

As AUSTEO and AGAO systems are particularly important, additional assurances should be put in place when such systems share a peripheral switch with other systems.

**Security Control: 0594; Revision: 4; Updated: Sep-18; Applicability: S, TS**
An evaluated peripheral switch is used when accessing a system containing AUSTEO or AGAO information and a system of the same classification that is not authorised to process the same caveat.

**Further information**

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the *Guidelines for Evaluated Products*.