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 this document 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; Priority: Must
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; Priority: Should
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: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Gateways:
- are the only communications paths into and out of internal networks
- by default, deny all connections into and out of the network
- allow only explicitly authorised connections
- apply the guidance in the Guidelines for data transfers and content filtering
- are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network)
- provide sufficient logging and audit capabilities to detect cyber security incidents, attempted intrusions and overuse/unalusual usage patterns
- provide real-time alerts.

**Gateway operation**

Providing sufficient logging and auditing capability to help detect cyber security incidents, including attempted network intrusions, enables an organisation to implement counter-measures to reduce the likelihood and consequence of future network intrusion attempts.

Storing event logs on a separate secure log server increases the difficulty for an adversary attempting to delete logging information to destroy evidence of a targeted cyber intrusion.

**Security Control: 0634; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must**

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

- filter all network traffic attempting to enter the gateway and log subsequently permitted traffic
- log network traffic attempting to leave the gateway
- are configured to save event logs to a separate secure log server
- 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.

**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; Priority: Must**

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; Priority: Must**

A security risk assessment is performed on gateways and their configuration before their implementation.
A security risk assessment is performed on all systems before they are connected to a gateway.

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.

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

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.

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

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.

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

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 (SOPs) 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.

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

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

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.

Once connectivity is established, system owners become information stakeholders for all connected security domains.

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 authorising systems
- Guidelines for cyber security incidents
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 this document 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

This document defines 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.
When connecting a highly classified network to any other network from a different security domain, a CDS is implemented.

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.

When designing and deploying a CDS, the ACSC is notified and consulted; and directions provided by the ACSC are complied with.

When introducing additional connectivity to a CDS, such as adding a new gateway to a common network, the ACSC is consulted on the impact to the security of the CDS; and directions provided by the ACSC are complied with.

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.

All CDS between highly classified networks and any other network implement isolated upward and downward network paths.

All CDS between highly classified networks and any other network implement protocol breaks at each layer of the OSI model.

All CDS between highly classified networks and any other network implement content filtering and separate independent security-enforcing components for upward and downward data flows.

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.

Due to the criticality of data import and export functions provided by CDS, organisations should regularly assess the performance of CDS data transfer policies against the security policies the CDS has been deployed to enforce.

All security-relevant events generated by a CDS are logged and regularly analysed.

A representative sample of security events generated by a CDS, relating to the enforcement of data transfer policies, is taken at least every 3 months and assessed against the security policies that the CDS is responsible for enforcing between security domains.

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 authorising systems
- 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 the basics of CDS can be found in the ACSC’s Introduction to Cross Domain Solutions publication at https://www.cyber.gov.au/publications/introduction-to-cross-domain-solutions.

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.

Security Control: 1528; Revision: 1; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
An evaluated firewall is used between official or classified networks and public network infrastructure.

Security Control: 0639; Revision: 8; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
An evaluated firewall is used between networks belonging to different security domains.

Security Control: 1194; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
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.

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.
Security Control: 0641; Revision: 7; Updated: Sep-18; Applicability: S, TS; Priority: Must
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.

Security Control: 0642; Revision: 7; Updated: Sep-18; Applicability: S, TS; Priority: Should
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.

Security Control: 0643; Revision: 5; Updated: Sep-18; Applicability: O, P; Priority: Must
An evaluated diode is used for controlling the data flow of unidirectional gateways between official or classified networks and public network infrastructure.

Security Control: 0645; Revision: 5; Updated: Sep-18; Applicability: S, TS; Priority: Must
A high assurance diode is used for controlling the data flow of unidirectional gateways between classified networks and public network infrastructure.

Security Control: 1157; Revision: 3; Updated: Sep-18; Applicability: O, P; Priority: Must
An evaluated diode is used for controlling the data flow of unidirectional gateways between official and classified networks.

Security Control: 1158; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A high assurance diode is used for controlling the data flow of unidirectional gateways between official or classified networks where the highest system is SECRET or above.

**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.

Security Control: 0646; Revision: 4; Updated: Sep-18; Applicability: S, TS; Priority: Must
An evaluated diode is used between an AUSTEO or AGAO network and a foreign network at the same classification.

Security Control: 0647; Revision: 6; Updated: Sep-18; Applicability: S, TS; Priority: Should
An evaluated diode is used between an AUSTEO or AGAO network and another Australian controlled network at the same classification.

**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.

**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.

**Transport Layer Security filtering**

Since Transport Layer Security (TLS) web traffic travelling over Hypertext Transfer Protocol Secure (HTTPS) 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.

**Transport Layer Security filtering**

- 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; Priority: Should
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 (DDNS) domains and other inappropriate domains).

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

Security Control: 0959; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
If whitelistin
ing 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; Priority: Should
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; Priority: Should
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; Priority: Should
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; Priority: Should
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; Priority: Should
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; Priority: Should
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.

A website whitelisting software application that allows for the management of whitelists can be obtained from http://whitetrash.sourceforge.net/.

Examples of client-side JavaScript controls are available at 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; Priority: Must
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; Priority: Must
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; Priority: Must
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; Priority: Must
An evaluated peripheral switch is used when sharing peripherals between official systems, or classified systems at 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; Priority: Should*

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*. 