Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Gateways

Gateways

Purpose of gateways

Gateways act as data flow control mechanisms at the network layer and may also control data 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.

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 data 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: 6; Updated: Jun-20; 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)*
- *log all physical and logical access to their components*
- *are configured to save logs to a secure logging facility*
- *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 secure logging facility increases the difficulty for an adversary to delete logging data 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 data and services on internal networks. Organisations that require certain data 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 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 data, 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: 1; Updated: Jun-21; Applicability: O, P, S, TS
All system administrators of gateways are cleared to access the highest level of data communicated or processed by the gateway.

Security Control: 0613; Revision: 5; Updated: Jun-21; Applicability: S, TS
All system administrators of gateways that process Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) data are Australian nationals.

Security Control: 0616; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Roles for the administration of gateways are separated.

Security Control: 0629; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
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 stakeholders in other security domains to which they are connected via a gateway.

Security Control: 0607; Revision: 4; Updated: Jun-21; Applicability: O, P, S, TS
Once connectivity is established, system owners become 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.

Security Control: 0619; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Users and services accessing networks through gateways are authenticated.

Security Control: 0620; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Only users and services authenticated and authorised to a gateway can use the gateway.

Security Control: 1039; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
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.

Security Control: 0622; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
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***
- ***Guidelines for System Hardening***
- ***Guidelines for System Management***
- ***Guidelines for System Monitoring***
- ***Guidelines for Networking***
- ***Guidelines for Data Transfers***.

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

Introduction to cross domain security

A Cross Domain Solution (CDS) is a system comprising security-enforcing functions tailored to mitigate the specific security risks of accessing or transferring data 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.

This section describes the security controls applicable to a CDS and extends upon the security controls within the prior gateways section which are also applicable. Furthermore, the ***Guidelines for Data Transfers*** is also applicable to a CDS. Finally, additional sections of these guidelines should be consulted depending on the specific type of CDS deployed.

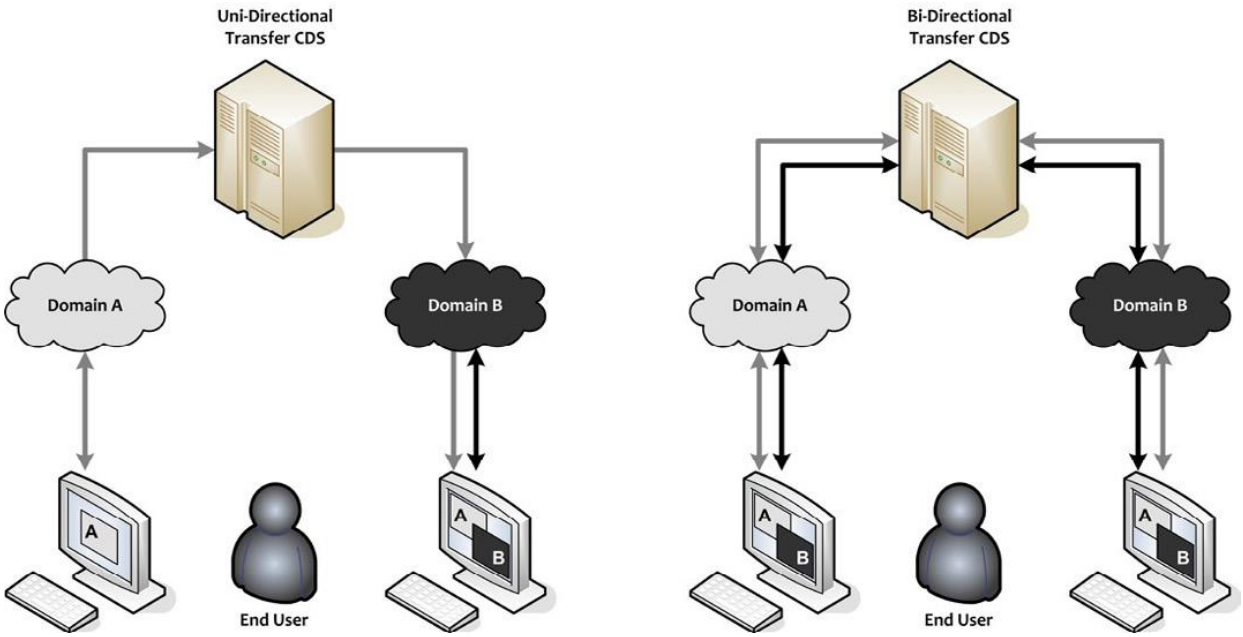
Personnel involved in the planning, analysis, design, implementation or assessment of a CDS should refer to the Australian Cyber Security Centre (ACSC)'s ***Introduction to Cross Domain Solutions*** and ***Fundamentals of Cross Domain Solutions*** publications.

Types of Cross Domain Solution

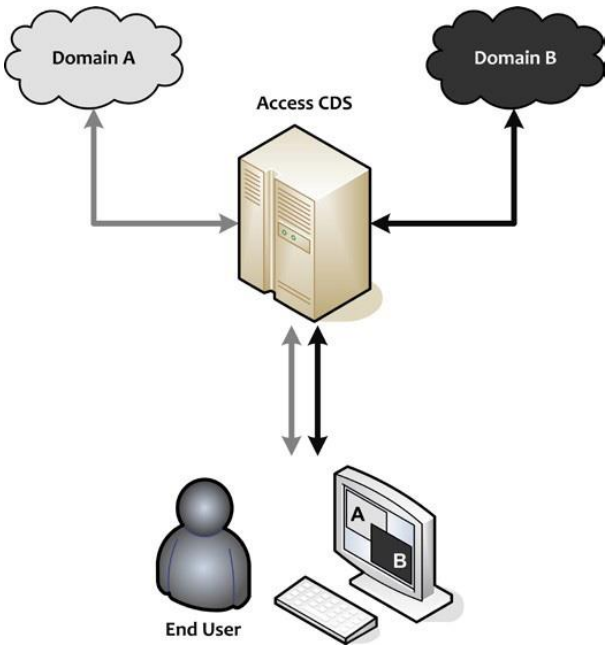
These guidelines define two logical types of CDS: a Transfer CDS and an Access CDS. These logical definitions are more closely aligned with how a CDS is described and sold by vendors and system integrators. Vendors may also offer a combined Access and Transfer solution.

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 data, 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.

When to implement a Cross Domain Solution

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.

Security Control: 0626; Revision: 4; Updated: Sep-18; Applicability: S, TS
When connecting a highly classified network to any other network from a different security domain, a CDS is implemented.

Consultation when implementing or modifying a Cross Domain Solution

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.

Security Control: 0597; Revision: 6; Updated: Sep-18; Applicability: S, TS
When designing and deploying a CDS, the ACSC is notified and consulted; and directions provided by the ACSC are complied with.

Security Control: 0627; Revision: 5; Updated: Sep-18; Applicability: S, TS
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

A 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.

Security Control: 0635; Revision: 5; Updated: Dec-19; Applicability: S, TS
A CDS between a highly classified network and any other network implements isolated upward and downward network paths.

Security Control: 1521; Revision: 1; Updated: Dec-19; Applicability: S, TS
A CDS between a highly classified network and any other network implements protocol breaks at each layer of the OSI model.

Security Control: 1522; Revision: 1; Updated: Dec-19; Applicability: S, TS
A CDS between a highly classified network and any other network implements 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***, a 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 a CDS, organisations should regularly assess the performance of a CDS's data transfer policies against the security policies the CDS has been deployed to enforce.

Security Control: 0670; Revision: 4; Updated: Sep-18; Applicability: S, TS
All security-relevant events generated by a CDS are logged and regularly analysed.

Security Control: 1523; Revision: 0; Updated: Sep-18; Applicability: S, TS
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.

Security Control: 0610; Revision: 6; Updated: Apr-19; Applicability: O, P, S, TS
Users are trained on the secure use of a CDS before access to the CDS is granted.

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***
- ***Guidelines for System Hardening***
- ***Guidelines for System Management***
- ***Guidelines for System Monitoring***
- ***Guidelines for Networking***
- ***Guidelines for Data Transfers***.

Further information on the basics of a CDS can be found in the ACSC's ***Introduction to Cross Domain Solutions*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/introduction-cross-domain-solutions.

Further information on the fundamentals of a CDS can be found in the ACSC's ***Fundamentals of Cross Domain Solutions*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/fundamentals-cross-domain-solutions.

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
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
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
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
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
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 data afterwards.

Security Control: 0643; Revision: 5; Updated: Sep-18; Applicability: O, P
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
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
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
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
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
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.

Security Control: 0648; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
A diode (or server connected to the diode) deployed to control data flow in unidirectional gateways monitors the volume of the data being transferred.

Further information

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

Web proxies

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.

Using web proxies

Web proxies are a key component in enforcing web usage policies and preventing cyber security incidents.

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.

Web proxy authentication and logging

Thorough web proxy logs are a valuable asset when responding to cyber security incidents and user violation of web usage policies.

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.*

Web content filters

Using web content filters

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 other types of content filters, while other forms of content filtering are specific to web content filters.

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: 7; Updated: Apr-20; Applicability: O, P, S, TS
Client-side active content, such as Java, is restricted to a list of allowed websites.

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.

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.

Security Control: 0263; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
For TLS traffic communicated through internet gateways, either of the following approaches are implemented:

- *a solution that decrypts and inspects all TLS traffic as per content filtering security controls*
- *a list of websites to which encrypted connections are allowed, with all other TLS traffic decrypted and inspected as per content filtering security controls.*

Inspection of Transport Layer Security traffic

As encrypted TLS traffic may contain personal 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.

Allowing access to specific websites

Defining a list of allowed websites and blocking all other 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 list of allowed websites offers better security than relying on a list of known malicious websites, or no restrictions at all, while still reducing implementation costs. An example of a permissive list could be the entire Australian subdomain, that is '*.au', or the top 1,000 websites from the Alexa website ranking (after filtering Dynamic Domain Name System domains and other inappropriate domains).

Security Control: 0958; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
A list of allowed websites, using either domain name or IP address, is implemented for all Hypertext Transfer Protocol (HTTP) and HTTPS traffic communicated through internet gateways.

Security Control: 1170; Revision: 3; Updated: Apr-20; Applicability: O, P, S, TS
If a list of allowed websites is not implemented, a list of allowed website categories is implemented instead.

Blocking access to specific websites

Collections of websites that have been deemed to be inappropriate due to their content or hosting of malicious content can be blocked to prevent them from being accessed.

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: 6; Updated: Apr-20; Applicability: O, P, S, TS
If a list of allowed websites is not implemented, a list of blocked websites is implemented instead.

Security Control: 0960; Revision: 6; Updated: Apr-20; Applicability: O, P, S, TS
If a list of blocked websites is implemented, the list 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.

Further information

Further information on content filtering techniques can be found in the content filtering section of these guidelines.

Further information and examples of client-side JavaScript controls are available at https://noscript.net/.

Content filtering

Content filtering techniques

Content filters reduce the likelihood of unauthorised or malicious content transiting a security domain boundary by assessing data based on defined security policies. The following techniques can assist with assessing the suitability of data to transit a security domain boundary.

Technique	Purpose
Antivirus scan	Scans the data for viruses and other malicious code.
Automated dynamic analysis	Analyses email and web content in a sandbox before delivering it to users.
Data format check	Inspects data to ensure that it conforms to expected and permitted formats.
Data range check	Checks the data in each field to ensure that it falls within the expected and permitted ranges.
Data type check	Inspects each file header to determine the actual file type.
File extension check	Inspects the file name extension to determine the purported file type.
Keyword search	Searches data for keywords or 'dirty words' that could indicate the presence of inappropriate or undesirable material.
Metadata check	Inspects files for metadata that should be removed prior to release.
Protective marking check	Validates the protective marking of the data to ensure that it is correct.
Manual inspection	The manual inspection of data for suspicious content that an automated system could miss, which is

	particularly important for the transfer of multimedia or content rich files.
Verification against file specification	Verifies that the file conforms to the defined file specification and can be effectively processed by subsequent content filters.

Content filtering

Implementing an effective content filter which cannot be bypassed reduces the likelihood of malicious content successfully passing into a security domain. Content filtering is only effective when suitable components are selected and appropriately configured with consideration of an organisation's business processes and threat environment.

When content filters are protecting classified environments as a component of a CDS, their assurance requirements necessitate rigorous security testing.

Security Control: 0659; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
When importing data into a security domain, by any means including a CDS, the data is filtered by a content filter designed for that purpose.

Security Control: 1524; Revision: 1; Updated: Dec-19; Applicability: S, TS
Content filters deployed in a CDS are subject to rigorous security assessment to ensure they mitigate content-based threats and cannot be bypassed.

Active, malicious and suspicious content

Many files are executable and are potentially harmful if executed by a user. Many file type specifications allow active content to be embedded in the file, which increases the attack surface. The definition of suspicious content will depend on the system's security risk profile and what is considered to be normal system behaviour.

Security Control: 0651; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
All suspicious, malicious and active content is blocked from entering a security domain.

Security Control: 0652; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Any data identified by a content filtering process as suspicious is blocked until reviewed and approved for transfer by a trusted source other than the originator.

Automated dynamic analysis

Analysing email and web content in a sandbox is a highly effective strategy to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.

Security Control: 1389; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Email and web content entering a security domain is automatically run in a dynamic malware analysis sandbox to detect suspicious behaviour.

Content validation

Content validation aims to ensure that the content received conforms to an approved standard. For example, content validation can be used to identify malformed content thereby allowing potentially malicious content to be blocked.

Examples of content validation include:

- ensuring numeric fields only contain numeric numbers
- ensuring content falls within acceptable length boundaries

- ensuring Extensible Markup Language (XML) documents are compared to a strictly defined XML schema.

Security Control: 1284; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Content validation is performed on all data passing through a content filter with content which fails content validation blocked.

Content conversion and transformation

Content conversion or transformation can be an effective method to render potentially malicious content harmless by separating the presentation format from the data. By converting a file to another format, the exploit, active content and/or payload can be removed or disrupted.

Examples of content conversion and transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a Portable Document Format (PDF) file
- converting a Microsoft PowerPoint presentation to a series of image files
- converting a Microsoft Excel spreadsheet to a comma-separated values file
- converting a PDF document to a plain text file.

Some file types, such as XML, will not benefit from conversion. Applying the conversion process to any attachments or files contained within other files (e.g. archive files or encoded files embedded in XML) can increase the effectiveness of a content filter.

Security Control: 1286; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Content conversion is performed for all ingress or egress data transiting a security domain boundary.

Content sanitisation

Sanitisation is the process of attempting to make potentially malicious content safe to use by removing or altering active content while leaving the original content as intact as possible. Sanitisation is not as secure a method of content filtering as conversion, though many techniques may be combined. Inspecting and filtering extraneous application and protocol data, including metadata, will assist in mitigating the threat of content exploitation. Examples include:

- removal of document properties in Microsoft Office documents
- removal or renaming of JavaScript sections from PDF files
- removal of metadata from within image files.

Security Control: 1287; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Content sanitisation is performed on suitable file types if content conversion is not appropriate for data transiting a security domain boundary.

Antivirus scanning

Antivirus scanning is used to prevent, detect and remove malicious code that includes computer viruses, worms, Trojans, spyware and adware.

Security Control: 1288; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Antivirus scanning, using multiple different scanning engines, is performed on all content.

Archive and container files

Archive and container files can be used to bypass content filtering processes if the content filter does not handle the file type and embedded content correctly. Ensuring the content filtering process recognises archived and container files will ensure the embedded files they contain are subject to the same content filtering measures as un-archived files.

Archive files can be constructed in a manner which can pose a denial of service security risk due to processor, memory or disk space exhaustion. To limit the likelihood of such an attack, content filters can specify resource constraints/quotas while extracting these files. If these constraints are exceeded the inspection is terminated, the content blocked and a security administrator alerted.

Security Control: 1289; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The contents from archive/container files are extracted and subjected to content filter checks.

Security Control: 1290; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Controlled inspection of archive/container files is performed to ensure that content filter performance or availability is not adversely affected.

Security Control: 1291; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Files that cannot be inspected are blocked and generate an alert or notification.

Allowing access to specific content types

Creating and enforcing a list of allowed content types, based on business requirements and the results of a risk assessment, is a strong content filtering method that can reduce the attack surface of a system. As a simple example, an email content filter might only allow Microsoft Office documents and PDF files.

Security Control: 0649; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
A list of allowed content types is implemented.

Data integrity

Ensuring the authenticity and integrity of content reaching a security domain is a key component in ensuring its trustworthiness. It is also essential that content that has been authorised for release from a security domain is not modified (e.g. by the addition or substitution of data). If content passing through a filter contains a form of integrity protection, such as a digital signature, the content filter needs to verify the content's integrity before allowing it through. If the content fails these integrity checks it may have been spoofed or tampered with and should be dropped.

Examples of data integrity checks include:

- an email server or content filter verifying an email protected by DomainKeys Identified Mail
- a web service verifying the XML digital signature contained within a Simple Object Access Protocol request
- validating a file against a separately supplied hash
- checking that data to be exported from a security domain has been digitally signed by a release authority.

Security Control: 1292; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The integrity of content is verified where applicable and blocked if verification fails.

Security Control: 0677; Revision: 4; Updated: Sep-18; Applicability: S, TS
If data is signed, the signature is validated before the data is exported.

Encrypted data

Encryption can be used to bypass content filtering if encrypted content cannot be subject to the same checks performed on unencrypted content. Organisations should consider the need to decrypt content, depending on the security domain they are communicating with and depending on whether the need-to-know principle needs to be enforced.

Choosing not to decrypt content poses a security risk that malicious code's encrypted communications and data could move between security domains. In addition, encryption could mask data at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill.

Where a business need to preserve the confidentiality of encrypted data exists, an organisation may consider a dedicated system to allow encrypted content through external, boundary or perimeter controls to be decrypted in an appropriately secure environment, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

Security Control: 1293; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
All encrypted content, traffic and data is decrypted and inspected to allow content filtering.

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 data 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 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: 5; Updated: Jun-21; Applicability: S, TS
An evaluated peripheral switch is used when accessing a system containing AUSTEO or AGAO data 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***.