21.3. Content Filtering

Objective

21.3.1. The flow of data within gateways is examined and controls applied in accordance with the agency's security policy. To prevent unauthorised or malicious content crossing security domain boundaries.

Context

Scope

21.3.2. This section covers information relating to the use of content filters within bi-directional or one-way gateways in order to protect security domains.

21.3.3. Content filters reduce the risk of unauthorised or malicious content crossing a security domain boundary.

Rationale & Controls

Limiting transfers by file type

21.3.4.R.01. **Rationale**

The level of security risk will be affected by the degree of assurance agencies can place in the ability of their data transfer filters to:

- confirm the file type by examination of the contents of the file;
- confirm the absence of malicious content;
- confirm the absence of inappropriate content;
- confirm the classification of the content; and
- handle compressed files appropriately.

Reducing the number of allowed file types reduces the number of potential vulnerabilities available for an attacker to exploit.

21.3.4.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:4321]

Agencies MUST strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.

21.3.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4322]

Agencies SHOULD strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.

Blocking active content

21.3.5.R.01. **Rationale**

Many files are executable and are potentially harmful if activated by a system user. Many static file type specifications allow active content to be embedded within the file, which increases the attack surface.

21.3.5.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:4325]

Agencies MUST block all executables and active content from entering a security domain.

21.3.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4326]

Agencies SHOULD block all executables and active content from being communicated though gateways.

Blocking suspicious data

21.3.6.R.01. **Rationale**

The definition of suspicious content will depend on the system's risk profile and what is considered normal traffic. The table below identifies some filtering techniques that can be used to identify suspicious data.

Technique	Purpose
Antivirus scan	Scans the data for viruses and other malicious code.
Data format check	Inspects data to ensure that it conforms to expected/permitted format(s).
Data range check	Checks the data within each field to ensure that it falls within the expected/permitted range.
Data type check	Inspects each file header to determine the file type.
File extension check	Checks file extensions to ensure that they are permitted.
Keyword search	Searches data for keywords or 'dirty words' that could indicate the presence of classified or inappropriate 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 complies with the permitted classifications and endorsements.
Manual inspection	The manual inspection of data for suspicious content that an automated system could miss, which is particularly important for the transfer of image files, multi-media or content-rich files.

21.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4329]

Agencies MUST block, quarantine or drop any data identified by a data filter as suspicious until reviewed and approved for transfer by a trusted source other than the originator.

Content validation

21.3.7.R.01. **Rationale**

Content validation aims to ensure that the content received conforms to a defined, approved standard. Content validation can be an effective means of identifying malformed content, allowing agencies to block potentially malicious content. Content validation operates on an allow listing principle, blocking all content except for that which is explicitly permitted. Examples of content validation include:

- ensuring numeric fields only contain numeric numbers;
- other fields operate with defined character sets;
- ensuring content falls within acceptable length boundaries;
- ensuring XML documents are compared to a strictly defined XML schema.

21.3.7.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:4332]

Agencies MUST perform validation on all data passing through a content filter, blocking content which fails the validation.

21.3.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4333]

Agencies SHOULD perform validation on all data passing through a content filter, blocking content which fails the validation.

Content conversion and transformation

21.3.8.R.01. **Rationale**

Content conversion, file conversion or file 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 often be removed or disrupted enough to be ineffective.
Examples of file conversion and content transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a PDF file;
- converting a Microsoft PowerPoint presentation to a series of JPEG images;
- converting a Microsoft Excel spreadsheet to a Comma Separated Values (CSV) file; or
- converting a PDF document to a plain text file.

Some file types, such as XML, will not benefit from conversion. The conversion process should also be applied to any attachments or files contained within other files, for example, archive files or encoded files embedded in XML.

21.3.8.C.01.

Control System Classifications(s): All Classifications; Compliance: Should [CID:4336]

Agencies SHOULD perform content conversion, file conversion or both for all ingress or egress data transiting a security domain boundary.

Content sanitisation

21.3.9.R.01. **Rationale**

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. Extraneous application and protocol data, including metadata, should also be inspected and filtered where possible. Examples of sanitisation to mitigate the threat of content exploitation include:

- removal of document properties information in Microsoft Office documents;
- removal or renaming of JavaScript sections from PDF files;
- removal of metadata such as EXIF information from within JPEG files.

21.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4339]

Agencies SHOULD perform content and file sanitisation on suitable file types if content conversion or file conversion is not appropriate for data transiting a security domain boundary.

Antivirus scans

21.3.10.R.01. **Rationale**

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

21.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4348]

Agencies SHOULD perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines.

Archive and container files

21.3.11.R.01. **Rationale**

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. The content filtering process should recognise archived and container files, ensuring the embedded files they contain are subject to the same content filtering measures as un-archived files.

21.3.11.R.02. **Rationale**

Archive files can be constructed in a manner which can pose a denial-of-service risk due to processor, memory or disk space exhaustion. To limit the risk 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.

21.3.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4401]

Agencies SHOULD extract the contents from archive and container files and subject the extracted files to content filter tests.

21.3.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4402]

Agencies SHOULD perform controlled inspection of archive and container files to ensure that content filter performance and availability is not adversely affected.

21.3.11.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4403]

Agencies SHOULD block files that cannot be inspected and generate an alert or notification.

Allow listing permitted content

21.3.12.R.01. **Rationale**

Creating and enforcing an allow list of allowed content/files is a strong content filtering method. Allowing content that satisfies a business requirement only can reduce the attack surface of the system. As a simple example, an email content filter might allow only Microsoft Office documents and PDF files.

21.3.12.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:4406]

Agencies MUST create and enforce an allow list of permitted content types based on business requirements and the results of a security risk

assessment.

21.3.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4407]

Agencies SHOULD create and enforce an allow list of permitted content types based on business requirements and the results of a security risk assessment.

Data integrity

21.3.13.R.01. **Rationale**

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 or contains other data not authorised for release, for example by the addition or substitution of sensitive information.

21.3.13.R.02. **Rationale**

If content passing through a filter contains a form of integrity protection, such as a digital signature, the content filter should 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 or quarantined for further inspection.

Examples of data integrity checks include:

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

21.3.13.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:4411]

If data is signed, agencies MUST ensure that the signature is validated before the data is exported.

21.3.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4412]

Agencies SHOULD verify the integrity of content where applicable, and block the content if verification fails.

Encrypted data

21.3.14.R.01. **Rationale**

Encryption can be used to bypass content filtering if encrypted content cannot be subject to the same checks performed on unencrypted content. Agencies will need to consider the need to decrypt content, depending on:

- the security domain they are communicating with;
- whether the need-to-know principle is to be enforced;
- end-to-end encryption requirements; or
- any privacy and policy requirements.

21.3.14.R.02. **Rationale**

Choosing not to decrypt content poses a risk of encrypted malicious software communications and data moving between security domains. Additionally, encryption could mask the movement of information at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill.

21.3.14.R.03. **Rationale**

Some systems allow encrypted content through external/boundary/perimeter controls to be decrypted at a later stage, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

21.3.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4417]

Agencies SHOULD decrypt and inspect all encrypted content, traffic and data to allow content filtering.

Monitoring data import and export

21.3.15.R.01. **Rationale**

To ensure the continued confidentiality and integrity of systems and data, import and export processes should be monitored and audited.

21.3.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4420]

Agencies MUST use protective marking checks to restrict the export of data from each security domain, including through a gateway.

21.3.15.C.02. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must [CID:4421]**

When importing data to each security domain, including through a gateway, agencies MUST audit the complete data transfer logs at least monthly.

Exception Handling

21.3.16.R.01. **Rationale**

Legitimate reasons may exist for the transfer of data that may be identified as suspicious according to the criteria established for content filtering. It is important to have an accountable and auditable mechanism in place to deal with such exceptions.

21.3.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Should [CID:4424]**

Agencies SHOULD create an exception handling process to deal with blocked or quarantined file types that may have a valid requirement to be transferred.