19.2. Cross Domain Solutions (CDS)

Objective

19.2.1. Cross-Domain Solutions secure transfers between systems of differing classifications or trust levels with high assurance over the security of systems and information.

Context

Scope

19.2.2. This section describes the use and implementation of Cross Domain Solutions (CDS).

19.2.3. CDS provide information flow control mechanisms at each layer of the OSI model with a higher level of assurance than typical gateways. This section extends the preceding Gateways section. CDS systems must apply controls from each section.

19.2.4. 19.2.1. Additional information relating to topics covered in this section can be found in the following chapters and sections:

- Section 4.4 – Accreditation Framework;
- Section 8.2 – Servers and Network Devices;
- Section 8.3 – Network Infrastructure;
- Section 8.4 – IT Equipment;
- Chapter 12 – Product Security;
- Section 16.1 – Identification, Authentication and passwords;
- Section 16.6 – Event Logging and Auditing;
- Section 19.1 – Gateways;
- Section 19.3 – Firewalls;
- Section 19.4 – Diodes;
- Section 19.5 – Session Border Controllers;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 20.3 – Content Filtering.

Deploying Cross Domain Solutions

19.2.5. Consult the section on Firewalls in this chapter for devices used to control data flow in bi-directional gateways.

19.2.6. Consult the section on Diodes in this chapter for devices used to control data flow in uni-directional gateways.

19.2.7. Consult the Data Transfers and Content Filtering sections for requirements on appropriately controlling data flows in both bi-directional and uni-directional gateways

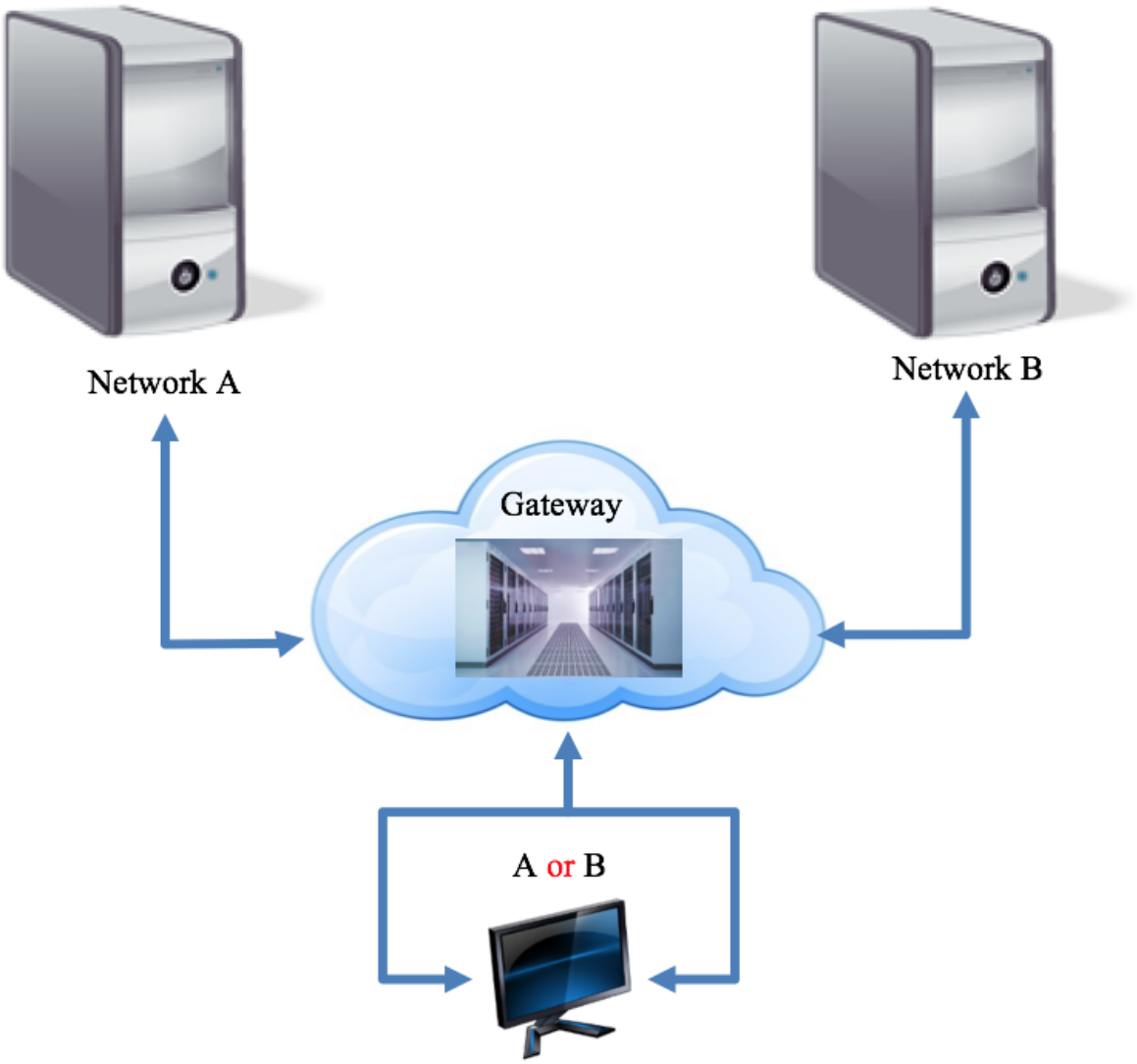
Types of gateways

19.2.8. This manual defines three types of gateways:

- access gateways;
- multilevel gateways; and
- transfer gateways.

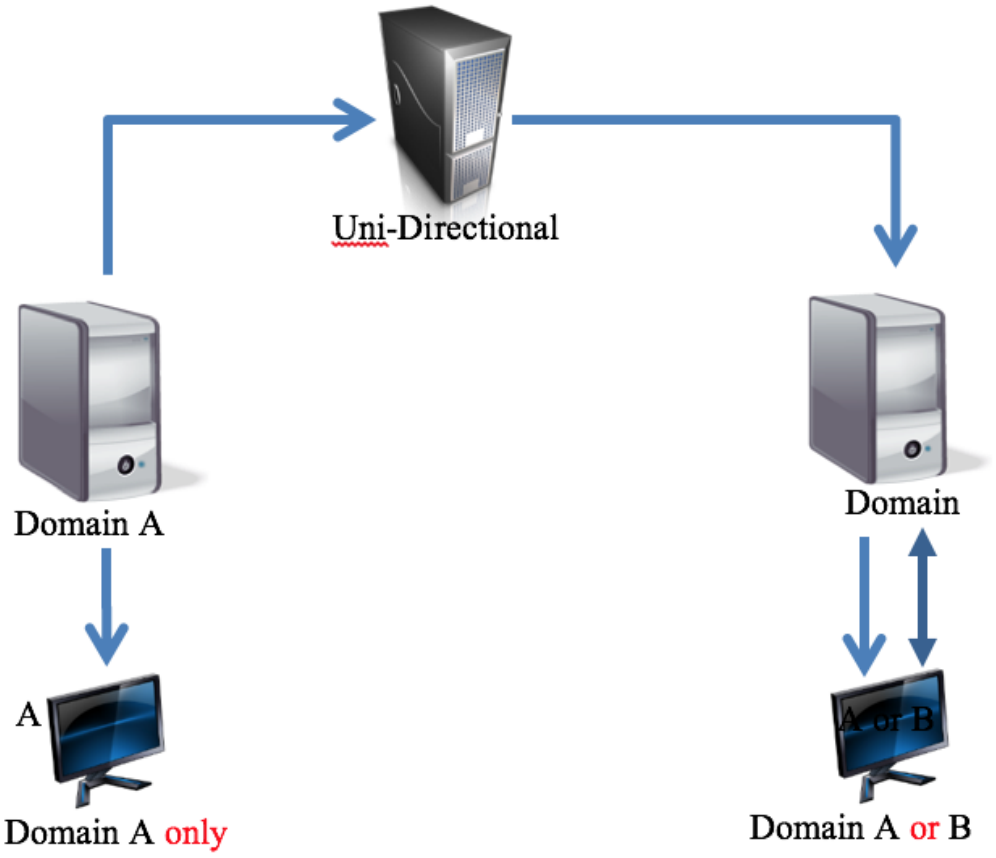
Access Gateway

19.2.9. An access gateway provides the system user with access to multiple security domains from a single device.

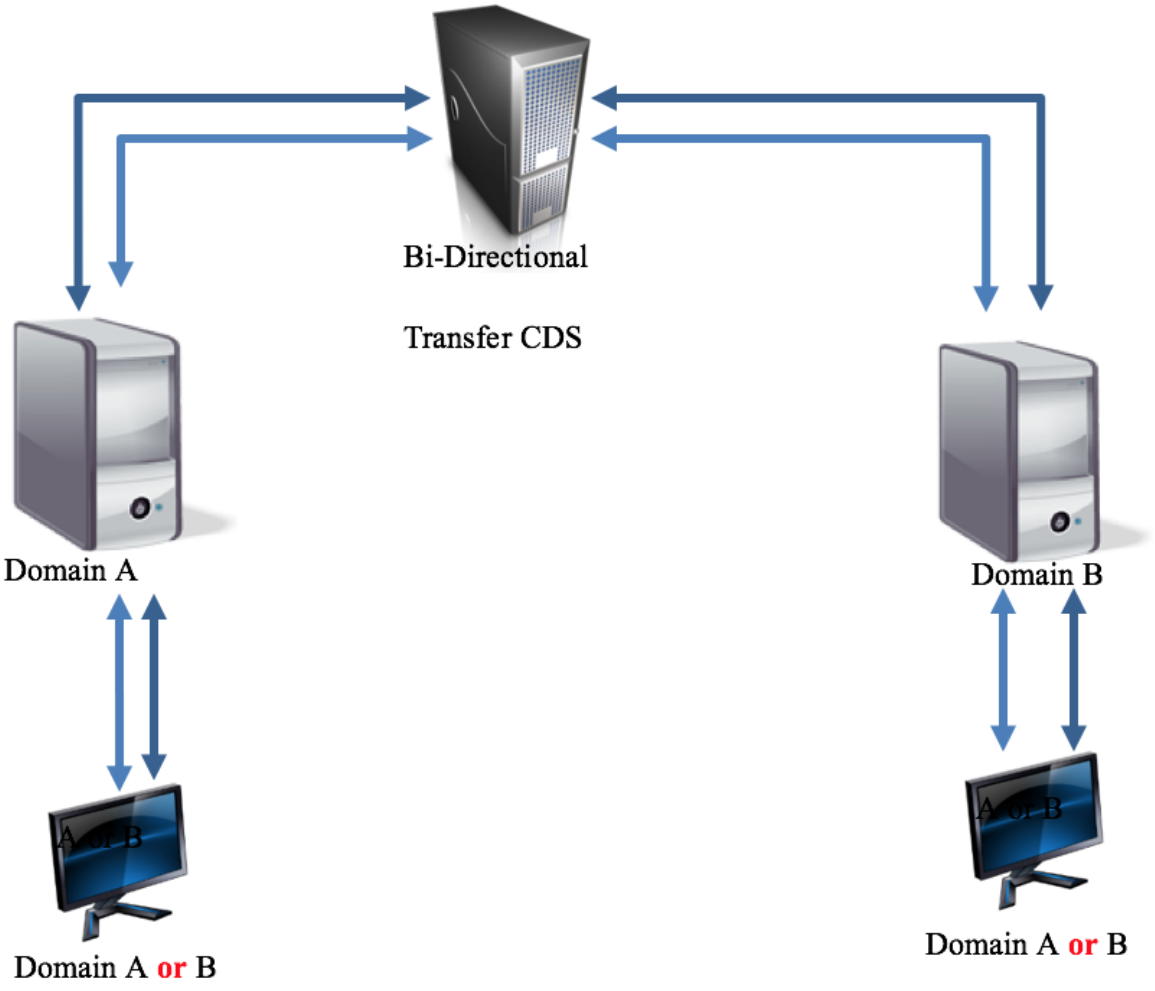


19.2.10. A transfer gateway facilitates the transfer of information, in one or multiple directions (low to high or high to low) between different security domains. A traditional gateway to the Internet is considered a form of transfer gateway.

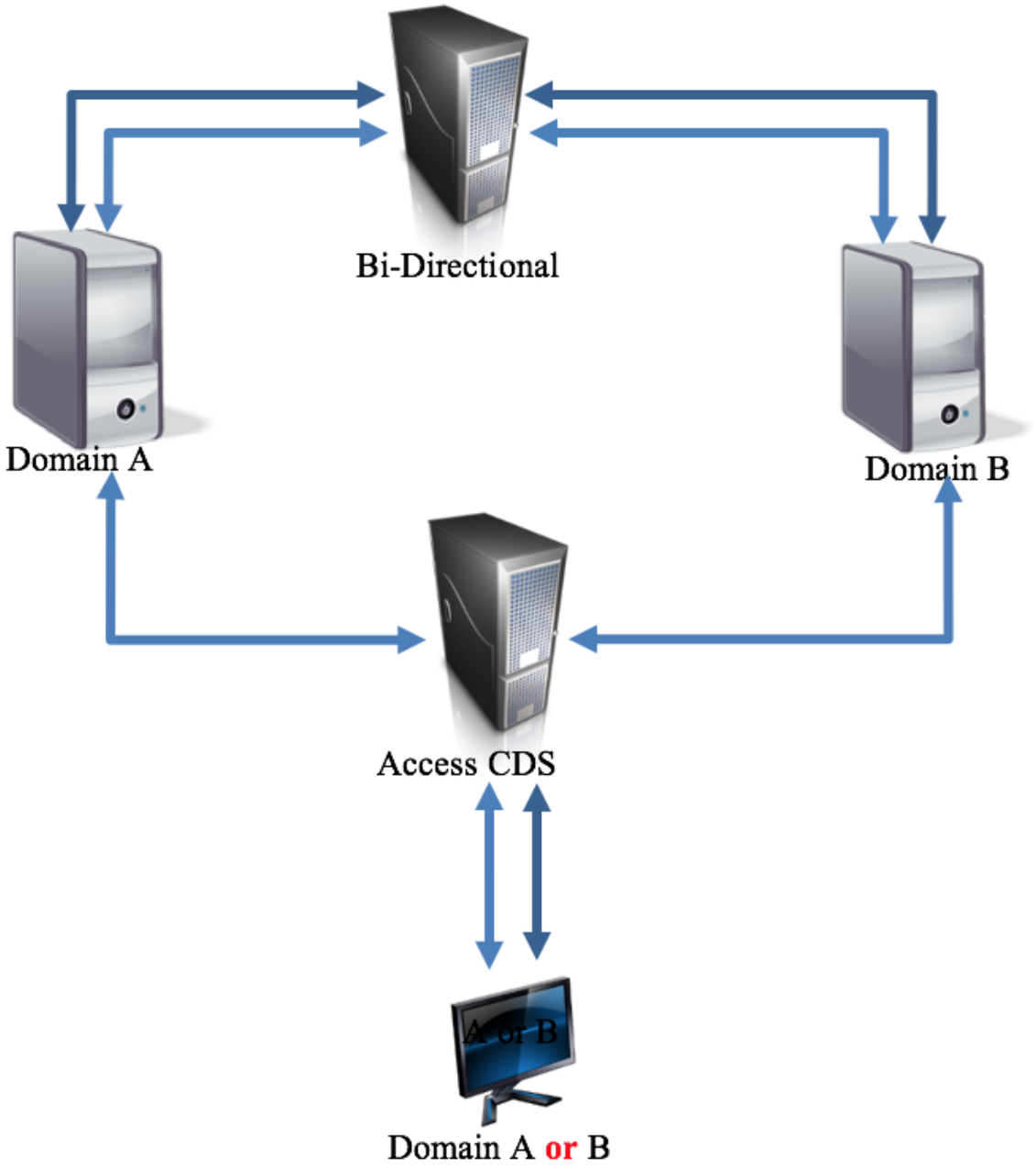
19.2.11. The following illustrates a Uni-Directional Transfer Cross Domain Solution.



19.2.12. A Bi-Directional Cross Domain Solution enables access, based on authorisations, to data at multiple classifications and releasability levels.



19.2.13. A Multi-Level Transfer Cross Domain Solution enables access, based on authorisations, to data at multiple classifications and releasability levels.



References

19.2.14. Additional guidance can be found at:

Reference	Title	Publisher	Source
	Cross Domain Solutions	ASD	Introduction to Cross Domain Solutions | Cyber.gov.au Fundamentals of Cross Domain Solutions | Cyber.gov.au
	Security principles for Cross Domain Solution	NCSC UK	Security principles for cross domain solutions - NCSC.GOV.UK
	Cross Domain Security Primer	CSE Canada	Cross domain security primer (ITSB-120) - Canadian Centre for Cyber Security
Sse-100-1	**Information Assurance Guidance For Systems Based On A Security Real-Time Operating System Systems Security Engineering**	NSA	Available at: National Security Agency Information Assurance Guidance for Systems Based on a Security Real-Time Operating System: Systems Security Engineering: National Security Agency: 9781508545705: Amazon.com: Books
	Solving the Cross-Domain Conundrum, **Colonel Bernard F. Koelsch United States Army, 2013**	US Army War College	ADA589325.pdf (dtic.mil)
	Inside Microsoft 365 Defender: Solving cross-domain security incidents through the power of correlation analytics - Microsoft Security Blog	Microsoft	Inside Microsoft 365 Defender: Solving cross-domain security incidents through the power of correlation analytics - Microsoft Security Blog
	Shedding Light on Cross Domain Solutions	SANS	https://www.sans.org/reading-room/whitepapers/dlp/shedding-light-cross-domain-solutions-36492

Rationale & Controls

Gateway classification

19.2.15.R.01. **Rationale**

The trust level or classification of systems directs users and systems administrators to the appropriate handling instructions and level of protection

required for those systems. This aids in the selection of systems controls.

19.2.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3870]

For the purposes of this Manual, the CDS MUST be classified at the highest classification of connected domains.

Allowable gateways

19.2.16.R.01. **Rationale**

Connecting systems to the Internet attracts significant risk and so highly classified systems are prohibited from being *directly* connected to each other or to the Internet. If an agency wishes to connect a highly classified system to the Internet the connection will need to be cascaded through a system of a lesser classification that is approved to connect directly to the Internet.

19.2.16.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:3880]

Agencies connecting a TOP SECRET, SECRET OR CONFIDENTIAL network to any other network MUST implement a CDS.

19.2.16.C.02. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must Not** [CID:3887]

Agencies MUST NOT implement a gateway permitting data to flow directly from:

- a TOP SECRET network to any network below SECRET;
- a SECRET network to an UNCLASSIFIED network; or
- a CONFIDENTIAL network to an UNCLASSIFIED network.

Implementing Cross Domain Solutions

19.2.17.R.01. **Rationale**

Connecting multiple sets of gateways and Cross Domain Solutions (CDS) increases the threat surface and, consequently, the likelihood and impact of a network compromise. When a gateway and a CDS share a common network, the higher security domain (such as a classified agency network) can be exposed to malicious activity, exploitation or denial of service from the lower security domain (such as the Internet).

19.2.17.R.02. **Rationale**

To manage this risk, CDS should implement products that have completed a high assurance evaluation, see Chapter 12 – Product Security. The AISEP Evaluated Product List (EPL) includes products that have been evaluated in the high assurance scheme but is not an exhaustive list.

Where CDS are not listed on the AISEP EPL, the GCSB can provide guidance on product selection and implementation on request.

19.2.17.C.01. **Control System Classifications(s): Secret, Confidential; Compliance: Must** [CID:3926]

When designing and deploying a CDS, agencies MUST consult with the GCSB and comply with all directions provided.

19.2.17.C.02. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:3927]

Agencies connecting a typical gateway and a CDS to a common network MUST consult the GCSB on the impact to the security of the CDS and comply with all directions provided.

Separation of data flows

19.2.18.R.01. **Rationale**

Gateways connecting highly classified systems to lower classified, or Internet connected systems need to incorporate physically separate paths to provide stronger control of information flows. Typically this is achieved through separate pathing and the use of diodes. Such gateways are generally restricted to process and communicate only highly-structured formal messaging traffic.

19.2.18.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:3929]

Agencies MUST ensure that all bi-directional gateways between TOP SECRET and SECRET networks, SECRET and less classified networks, and CONFIDENTIAL and less classified networks, have separate upward and downward paths which use a diode and physically separate infrastructure for each path.

Trusted sources

19.2.19.R.01. **Rationale**

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such the CISO and the ITSM.

19.2.19.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must [CID:3932]**

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

19.2.19.C.02. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must [CID:3933]**

Trusted sources MUST authorise all data to be exported from a security domain.

Operation of the Cross Domain Solution

19.2.20.R.01. **Rationale**

The highly sensitive nature of the data within cross domain solutions requires additional audit and logging for control, management, record and forensic purposes. This is in addition to the audit and logging requirements in Section 16.6 – Event Logging and Auditing.

19.2.20.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must [CID:3936]**

All data exported from a security domain MUST be logged.