19.1. Gateways

Objective

19.1.1. To ensure that gateways are properly configured to protect agency systems and information transferred between systems from different security domains.

Context

Scope

19.1.2. Gateways can be considered to be information flow control mechanisms operating at the Network layer and may also control information flow at the Transport, Session, Presentation and Application layers of the Open Systems Interconnection model (OSI). Specific controls for different technologies can be found in:

- Section 19.3 –Firewalls
- Section 19.4 – Diodes
- Section 18.6 – Peripheral (KVM) switches; and
- Section 19.5 – Session Border Controllers.

19.1.3. Additional information relating to topics covered in this section can be found in the following sections of this manual:

- 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 19.3 – 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 Gateways

19.1.4. This section provides a baseline for agencies deploying gateways. Agencies will need to consult additional sections of this manual depending on the specific type of gateways deployed.

19.1.5. For network devices used to control data flow in bi-directional gateways, Section 19.3 – Firewalls will need to be consulted. Section 19.4 – Diodes will also need to be consulted for one-way gateways. Additionally, for both types of gateways, Section 20.1 - Data Transfers and Section 19.2 - Cross-Domain Solutions, will need to be consulted for requirements on appropriately controlling data flows.

19.1.6. The requirements in this manual for content filtering, data import and data export apply to all types of gateways.

Gateway classification

19.1.7. For the purposes of this chapter, the gateway assumes the highest classification of the connected domains.

References

19.1.8. Further references can be found at:

Reference	Title	Publisher	Source
	Gateway / Cross Domain Solution Audit Guide, Australian Government	ASD	https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-gateways
	Good Practices for deploying DNSSEC, ENISA	ENISA	https://www.enisa.europa.eu/publications/gpgdnssec
ISO/IEC 27033-4:2014	**Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways**	ISO	https://www.iso.org/standard/51583.html
ISO/IEC 7498-1:1994	**The OSI model Information Technology – Open Systems Interconnection: The Basic Model**	ISO	https://www.iso.org/standard/20269.html
NIST Special Publication 800-41, September 2009	**Guidelines on Firewalls and Firewall Policy**	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf [PDF, 331 KB]

PSR references

19.1.9. Relevant PSR requirements can be found at:

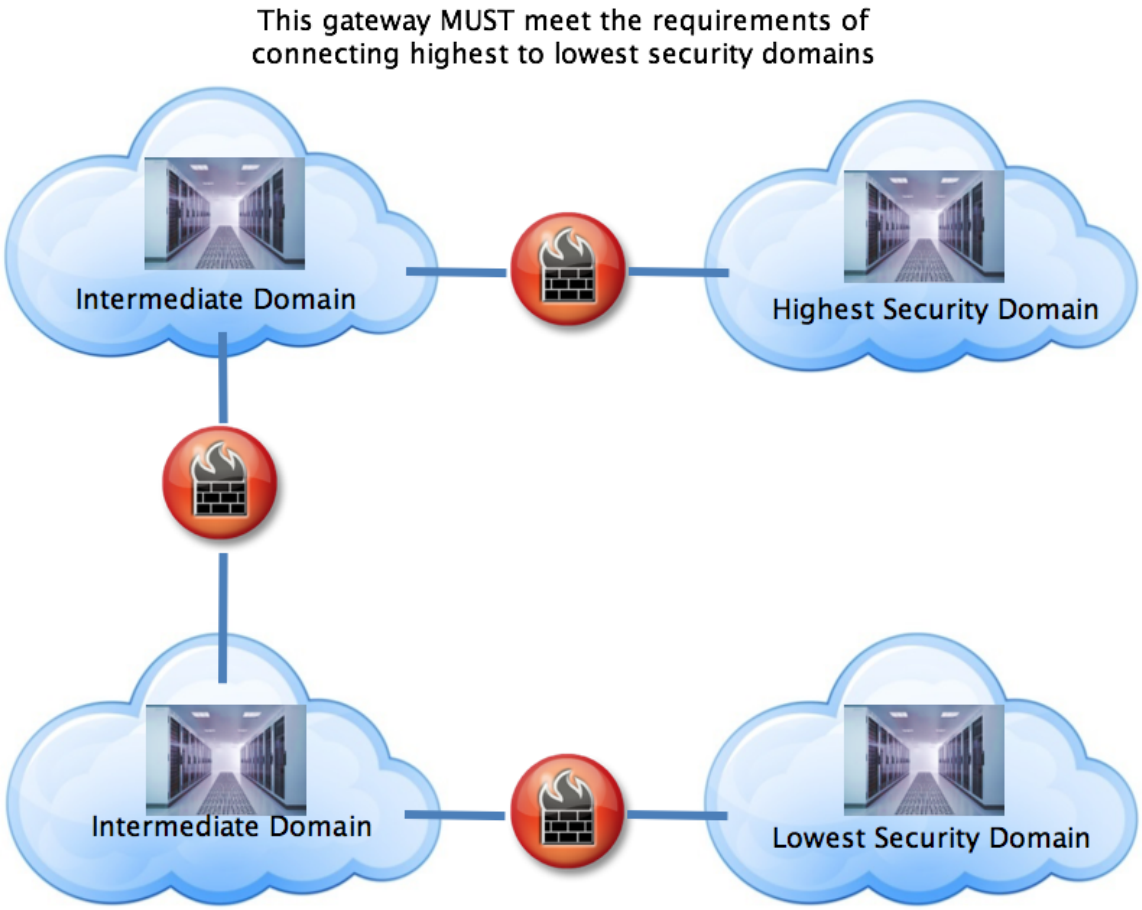
Reference	Title	Source
PSR Mandatory Requirements	GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements

Rationale & Controls

Gateways involving cascaded connections

19.1.10.R.01. **Rationale**

Protecting a cascaded connection path with the minimum assurance requirement of a direct connection between the highest and lowest networks ensures appropriate reduction in security risks of the extended connection. An illustration of a cascaded connection can be seen below.



19.1.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3538]

When agencies have cascaded connections between networks involving multiple gateways they MUST ensure that the assurance levels specified for network devices between the overall lowest and highest networks are met by the gateway between the highest network and the next highest network within the cascaded connection.

Using gateways

19.1.11.R.01. **Rationale**

Physically locating all gateway components inside a secure server room will reduce the risk of unauthorised access to the device(s).

19.1.11.R.02. **Rationale**

The system owner of the higher security domain of connected security domains would be most familiar with the controls required to protect the more sensitive information and as such is best placed to manage any shared components of gateways. In some cases where multiple security domains from different agencies are connected to a gateway, it may be more appropriate to have a qualified third party manage the gateway on behalf of all connected agencies.

Gateway components may also reside in a virtual environment – refer to Section 22.2 – Virtualisation and Section 22.3 – Virtual Local Area Networks

19.1.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3548]

Agencies MUST ensure that:

- all agency networks are protected from networks in other security domains by one or more gateways;
- all gateways contain mechanisms to filter or limit data flow at the network and content level to only the information necessary for business purposes; and
- all gateway components, discrete and virtual, are physically located within an appropriately secured server room.

19.1.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3551]

For gateways between networks in different security domains, any shared components MUST be managed by the system owners of the highest security domain or by a mutually agreed party.

Configuration of gateways

19.1.12.R.01. **Rationale**

Gateways are essential in controlling the flow of information between security domains. Any failure, particularly at the higher classifications, may have serious consequences. Hence mechanisms for alerting personnel to situations that may give rise to information security incidents are especially important for gateways.

19.1.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3562]

Agencies MUST ensure that 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;
- are managed via a secure path isolated from all connected networks (i.e. physically at the gateway or on a dedicated administration network);
- provide sufficient logging and audit capabilities to detect information security incidents, attempted intrusions or anomalous usage patterns; and
- provide real-time alerts.

Operation of gateways

19.1.13.R.01. **Rationale**

Providing an appropriate logging and audit capability will help to detect information security incidents and attempted network intrusions, allowing the agency to respond and to take measures to reduce the risk of future attempts.

19.1.13.R.02. **Rationale**

Storing event logs on a separate, secure log server will assist in preventing attackers from deleting logs in an attempt to destroy evidence of any intrusion.

19.1.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3578]

Agencies MUST ensure that all gateways connecting networks in different security domains:

- include a firewall of an appropriate assurance level on all gateways to filter and log network traffic attempting to enter the gateway;
- are configured to save event logs to a separate, secure log server;
- are protected by authentication, logging and audit of all physical access to gateway components; and
- have all controls tested to verify their effectiveness after any changes to their configuration.

Demilitarised zones

19.1.14.R.01. **Rationale**

Demilitarised zones are used to prevent direct access to information and systems on internal agency networks. Agencies that require certain information and systems to be accessed *from* the Internet or some other form of remote access, should place them in the less trusted demilitarised zone instead of on internal agency networks.

19.1.14.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3622]

Agencies MUST use demilitarised zones to house systems and information directly accessed externally.

19.1.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3623]

Agencies SHOULD use demilitarised zones to house systems and information directly accessed externally.

Risk assessment

19.1.15.R.01. **Rationale**

Performing a risk assessment on the gateway and its configuration prior to its implementation will assist in the early identification and mitigation of security risks.

19.1.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3626]

Agencies MUST perform a risk assessment on gateways and their configuration *prior* to their implementation.

Risk transfer

19.1.16.R.01.

Rationale

Gateways could connect networks with different domain owners, including across agency boundaries. As a result, all domain and system owners MUST understand and accept the risks from all other networks before gateways are implemented.

19.1.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3630]

All domain and system owners connected through a gateway MUST understand and accept the residual security risk of the gateway and from any connected domains including those via a cascaded connection.

19.1.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3633]

Agencies SHOULD annually review the security architecture of the gateway and risks of all connected domains including those via a cascaded connection.

Information stakeholders and Shared Ownership

19.1.17.R.01. **Rationale**

Changes to a domain connected to a gateway can affect the security posture of other connected domains. All domains owners should be considered stakeholders in all connected domains.

19.1.17.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:3637]

Once connectivity is established, domain owners MUST be considered information stakeholders for all connected domains.

19.1.17.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3640]

Once connectivity is established, domain owners SHOULD be considered information stakeholders for all connected domains.

System user training

19.1.18.R.01. **Rationale**

It is important that system users are competent to use gateways in a secure manner. This can be achieved through appropriate training before being granted access.

19.1.18.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:3648]

All system users MUST be trained on the secure use and security risks of the gateways before being granted access.

19.1.18.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3649]

All system users SHOULD be trained in the secure use and security risks of the gateways before being granted access.

Administration of gateways

19.1.19.R.01. **Rationale**

Application of role separation and segregation of duties in administration activities will protect against security risks posed by a malicious system user with extensive access to gateways.

19.1.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3660]

Agencies MUST limit access to gateway administration functions.

19.1.19.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3663]

Agencies MUST ensure that system administrators are formally trained to manage gateways by qualified trainers.

19.1.19.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3668]

Agencies MUST ensure that all system administrators of gateways that process NZEO information meet the nationality requirements for these endorsements.

19.1.19.C.04. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:3672]

Agencies MUST separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

19.1.19.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3676]

Agencies SHOULD separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

System user authentication

19.1.20.R.01. **Rationale**

Authentication to networks as well as gateways can reduce the risk of unauthorised access and provide an audit capability to support the investigation of information security incidents.

19.1.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3683]

Agencies MUST authenticate system users to all classified networks accessed through gateways.

19.1.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3685]

Agencies MUST ensure that only authenticated and authorised system users can use the gateway.

19.1.20.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3686]

Agencies SHOULD use multi-factor authentication for access to networks and gateways.

IT equipment authentication

19.1.21.R.01. **Rationale**

Authenticating IT equipment to networks accessed through gateways will assist in preventing unauthorised IT equipment connecting to a network.

19.1.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3695]

Agencies SHOULD authenticate any IT equipment that connects to networks accessed through gateways.

Configuration control

19.1.22.R.01. **Rationale**

To avoid changes that may introduce vulnerabilities into a gateway, agencies should fully consider any changes and associated risks. Changes may also necessitate re-certification and accreditation of the system, see Chapter 4 – System Certification and Accreditation.

19.1.22.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3702]

Agencies MUST undertake a risk assessment and update the SRMP before changes are implemented.

19.1.22.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3705]

Agencies MUST document any changes to gateways in accordance with the agency's Change Management Policy.

19.1.22.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3707]

Agencies SHOULD undertake a risk assessment and update the SRMP before changes are implemented.

Testing of gateways

19.1.23.R.01. **Rationale**

The testing of security measures on gateways will assist in ensuring that the integrity of the gateway is being maintained. An attacker who is aware of the regular testing schedule may cease malicious activities during such periods to avoid detection. Any test should, therefore, be unannounced and conducted at irregular intervals.

19.1.23.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3712]

Agencies SHOULD ensure that testing of security measures is performed at random intervals no more than six months apart.