19.3. Firewalls

Objective

19.3.1. Agencies operating bi-directional gateways implement firewalls and traffic flow filters to provide a protective layer to their networks in both discrete and virtual environments.

Context

Scope

19.3.2. This section covers information relating to filtering requirements for bi-direction gateways between networks of different security domains.

19.3.3. When a control specifies a requirement for a diode or filter the appropriate information can be found within Section 19.4 –Diodes and Section 20.3 – Content Filtering.

19.3.4. Additional information that also applies to topics covered in the section can be found in:

- Chapter 12 – Product Security which provides advice on the selection of evaluated products;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 22.2 – Virtualisation.

Inter-connecting networks within an agency

19.3.5. When connecting networks accredited to the same classification and set of endorsements within an agency the requirements of this section may not apply. When connecting networks accredited with different classifications or endorsements within an agency the information in this section applies.

Connecting agency networks to the Internet

19.3.6. When connecting an agency network to the Internet, the Internet is considered an UNCLASSIFIED and insecure network.

References

19.3.7. Further information on the Network Device Protection Profile (NDPP) and firewalls can be found at:

Reference	Title	Publisher	Source
NDPP	**Network Device Protection Profile (NDPP)**	(US) National Information Assurance Partnership	https://www.niap-ccevs.org/Profile/Info.cfm?PPID=293&id=293

Rationale & Controls

Firewall assurance levels

19.3.8.R.01. **Rationale**

The higher the required assurance level for a firewall, the greater the assurance that it provides an appropriate level of protection against an attacker. For example, an EAL2 firewall is certified to provide protection against a basic threat potential, whilst an EAL4 firewall is certified to provide protection against a moderate threat potential. A Protection Profile (PP) is considered to be equivalent to EAL2 under its Common Criteria Recognition Arrangement.

19.3.8.R.02. **Rationale**

If a uni-directional connection between two networks is being implemented only one gateway is necessary with requirements being determined based on the source and destination networks. However, if a bi-directional connection between two networks is being implemented both gateways will be configured and implemented with requirements being determined based on the source and destination networks.

19.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3970]

All gateways MUST contain a firewall in both physical and virtual environments.

19.3.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3973]

Agencies MUST check the evaluation has examined the security enforcing functions by reviewing the target of evaluation/security target and other testing documentation.

19.3.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3975]

Agencies MUST use devices as shown in the following table for their gateway when connecting two networks of different classifications or two networks of the same classification but of different security domains.

Your network	Their network	You require	They require
RESTRICTED and below	UNCLASSIFIED	EAL4 firewall	N/A
	RESTRICTED	EAL2 or PP firewall	EAL2 or PP firewall
	CONFIDENTIAL	EAL2 or PP firewall	EAL4 firewall
	SECRET	EAL2 or PP firewall	EAL4 firewall
	TOP SECRET	EAL2 or PP firewall	Consultation with GCSB
CONFIDENTIAL	UNCLASSIFIED	Consultation with GCSB	N/A
	RESTRICTED	EAL4 firewall	EAL2 or PP firewall
	CONFIDENTIAL	EAL2 or PP firewall	EAL2 or PP firewall
	SECRET	EAL2 or PP firewall	EAL4 firewall
	TOP SECRET	EAL2 or PP firewall	Consultation with GCSB
SECRET	UNCLASSIFIED	Consultation with GCSB	N/A
	RESTRICTED	EAL4 firewall	EAL2 or PP firewall
	CONFIDENTIAL	EAL4 firewall	EAL2 or PP firewall
	SECRET	EAL2 or PP firewall	EAL2 or PP firewall
	TOP SECRET	EAL2 or PP firewall	EAL4 firewall
TOP SECRET	UNCLASSIFIED	Consultation with GCSB	N/A
	RESTRICTED	Consultation with GCSB	EAL2 or PP firewall
	CONFIDENTIAL	Consultation with GCSB	EAL2 or PP firewall
	SECRET	EAL4 firewall	EAL2 or PP firewall
	TOP SECRET	EAL4 firewall	EAL4 firewall

19.3.8.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3996]

The requirement to implement a firewall as part of gateway architecture MUST be met separately and independently by both parties (gateways) in both physical and virtual environments.

Shared equipment DOES NOT satisfy the requirements of this control.

Firewall assurance levels for NZEO networks

19.3.9.R.01. **Rationale**

As NZEO networks are particularly sensitive, additional security measures need to be put in place when connecting them to other networks.

19.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3999]

Agencies MUST use a firewall of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for firewalls between networks of different classifications or security domains.

19.3.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4000]

In all other circumstances the table at 19.3.8.C.03 MUST apply.

19.3.9.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4001]

Agencies SHOULD use a firewall of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.