# Network Security Services

## Objective

Establish external and internal network perimeters and monitor network traffic.

## Key Considerations

* [ ] Ensure that egress/ingress points to and from GC cloud-based environments are managed and monitored. Use centrally provisioned network security services where available.
* [ ] Implement network boundary protection mechanisms for all external facing interfaces that enforce a deny-all or allow-by-exception policy.
* [ ] Perimeter security services such as boundary protection, intrusion prevention services, proxy services, TLS traffic inspection, etc. must be enabled based on risk profile, in alignment with GC Secure Connectivity Requirements and [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38.](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38).
* [ ] Access to Cloud storage shall be limited to authorized source IP addresses only (generally GC only).

## Validation

* [ ] Confirm policy for network boundary protection.
* [ ] Confirm policy for limiting number of public IPs.
* [ ] Confirm policy for limiting to authorized source IP addresses (e.g. GC IP addresses).

## Applicable Service Models

* IaaS, PaaS, SaaS

## References

1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.4
2. Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38.](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)
3. CSE Top 10 #1
4. Related security controls: AC-3, AC‑4, SC-5, SC‑7, SC‑7(5), SI-3, SI-3(7), SI-4