SC.L2-3.13.6

System & Communications Protection

Network Communication by Exception

"Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)."

Objectives

[a]

Network communications traffic is denied by default.

[b]

Network communications traffic is allowed by exception.

Key Discussion Points

Default Deny:
The firewall must have an implicit deny-all at the end of its ruleset — if traffic matches no rule, it is blocked, not passed.

Permit by Exception:
Every allowed traffic flow must be explicitly permitted — no undocumented traffic can pass through the CUI system boundary.

Both Directions:
Inbound AND outbound — this control applies to traffic leaving the CUI environment as well as entering it.

Adds to 3.13.1:
3.13.1 requires monitoring, control, and protection of communications; 3.13.6 specifies the control posture — deny all, permit by exception.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries; system design documentation; boundary protection hardware and software; system configuration settings; enterprise security architecture documentation; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developers; personnel with boundary protection responsibilities.

TEST

Mechanisms implementing boundary protection capability.

Plain English

What this control is really saying:

Most firewalls are configured to allow everything and block known bad. This control flips that model: start by blocking everything, then explicitly permit only what is required. This way, no traffic enters or leaves your CUI environment unless it was deliberately approved — not just 'not blocked.'

How it is used:

- The firewall's default rule is an implicit deny — no traffic passes unless it matches an explicitly approved rule above the default.
- Approved firewall rules are documented with a business justification, the approving individual, and a review date — rules without justification are removed during quarterly review.
- Outbound rules restrict CUI workstations to approved destinations — general internet browsing goes through a proxy, not directly through the firewall.
- Firewall rules are reviewed quarterly — any rule that cannot be justified by a current business need is removed on a schedule.

SC.L2-3.13.6

SYSTEM & COMMS PROTECTION — Network Communication by Exception

Real World Example

The Scenario

Acme Defense's firewall has 47 inbound allow rules accumulated over eight years. The last two rules are explicit deny rules for specific known-bad IPs. There is no implicit deny at the end of the ruleset — any traffic not matching a rule passes through.

What the assessor finds

An assessor reviews the firewall ruleset and finds that traffic from any source to any destination on ports 80 and 443 is permitted inbound — because the default is allow, no explicit deny is required to block unwanted traffic, and no unwanted traffic is actually blocked.

SPRS Score Impact

3.13.6 carries a point value of 3. Default-allow is the most permissive possible starting point — it means every undocumented or unknown traffic flow is implicitly permitted. Deny-all, permit-by-exception means only approved traffic can reach CUI systems.

What Good Looks Like

Firewall default rule is implicit deny-all, all permitted traffic explicitly approved with documented justification, both inbound and outbound controlled, rules reviewed periodically, undocumented or unjustified rules removed.

Common Gaps

What assessors actually find in the field:

✗ **Default-allow posture**

The firewall blocks known bad traffic but allows everything else by default — only traffic matching a deny rule is blocked.

✗ **Implicit allow at end of ruleset**

There is no 'deny all' at the bottom of the ruleset — traffic that doesn't match any rule passes through rather than being blocked.

✗ **Rules not documented**

Many firewall rules exist with no comments or justification — nobody knows why they were created or whether they are still needed.

✗ **Outbound not controlled**

Inbound rules exist but all outbound traffic is unrestricted — CUI can be exfiltrated to any destination without control.

✗ **Rules never reviewed**

Firewall rules were set up years ago and have never been reviewed — obsolete rules remain, expanding the permitted traffic surface unnecessarily.