# SC.L2-3.13.1

## System & Communications Protection

## Boundary Protection [CUI Data]

*"Monitor, control, and protect communications at the external boundaries and key internal boundaries of organizational systems."*

## Objectives

**[a]**
The external system boundary is defined.

**[b]**
Key internal system boundaries are defined.

**[c]**
Communications are monitored at the external system boundary.

**[d]**
Communications are monitored at key internal boundaries.

**[e]**
Communications are controlled at the external system boundary.

**[f]**
Communications are controlled at key internal boundaries.

**[g]**
Communications are protected at the external system boundary.

**[h]**
Communications are protected at key internal boundaries.

### Key Discussion Points

**Three Requirements:**
Monitor (visibility), control (enforcement), and protect (confidentiality/integrity) — all three apply to both external AND key internal boundaries.

**Define the Boundary:**
[a] and [b] must be met before [c] through [h] can be assessed — assessors cannot verify monitoring or control without a documented boundary definition.

**Internal Boundaries Too:**
Segmenting CUI from general IT is a key internal boundary requirement — a flat network with no internal controls fails [b], [d], and [f].

**Default Deny:**
Controlling communications means denying by default and permitting by exception — a firewall that allows all outbound traffic does not satisfy [e].

## 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; enterprise security architecture; system audit logs; system configuration settings.

### INTERVIEW

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

### TEST

Mechanisms implementing boundary protection capability.

# SC.L2-3.13.1

**SYSTEM & COMMS PROTECTION — Boundary Protection [CUI Data]**

## Plain English

### What this control is really saying:

Your network perimeter is the fence between your CUI and the internet. This control requires that you define where that fence is, watch what crosses it (monitoring), decide what is allowed (control), and secure what does cross (protection). It applies to both the external boundary and any internal boundaries — like the wall between your CUI environment and general IT.

### How it is used:

- A perimeter firewall enforces a default-deny posture — only explicitly permitted traffic flows are allowed inbound or outbound.
- An IDS/IPS monitors traffic at the external boundary and generates alerts on anomalous patterns — alerts are reviewed and responded to per the incident response plan.
- An internal firewall or VLAN segments the CUI environment from general office IT — traffic between segments is logged and controlled.
- Network traffic logs at both boundaries are retained per the audit logging policy — logs are reviewed for anomalies on a defined schedule.

## Real World Example

### The Scenario

Acme Defense has a firewall at the internet boundary. The CUI engineering workstations and the general office network share the same internal subnet. No internal segmentation exists. Firewall logs are generated but never reviewed.

### What the assessor finds

An assessor reviews 90 days of firewall logs and finds 14 connections from CUI workstations to known malware command-and-control IP addresses — none were blocked because outbound rules are default-allow. No alert was generated and no one reviewed the logs.

## SPRS Score Impact

3.13.1 carries a point value of 5. An undefined or unprotected boundary means the entire CUI environment is at risk from external threats — this is a foundational control that enables or undermines all other network security measures.

## What Good Looks Like

External and internal boundaries defined and documented, firewall enforces default-deny with approved exceptions, traffic monitored at both boundaries with log retention, IDS/IPS deployed at external boundary, CUI environment segmented from general IT, logs reviewed on schedule.

## Common Gaps

### What assessors actually find in the field:

✗ **No boundary defined**

The organization has no documented network boundary — assessors cannot determine what is in scope or where protections apply.

✗ **No internal segmentation**

CUI systems and general office IT share the same flat network — there is no internal boundary controlling data flow between them.

✗ **Firewall not monitored**

A firewall exists but logs are not reviewed — denied connections and anomalous traffic patterns go undetected.

✗ **Default-allow posture**

The firewall allows all outbound traffic by default — CUI can be exfiltrated without any control blocking or logging the transfer.

✗ **No IDS/IPS deployed**

No intrusion detection system monitors boundary traffic — malicious inbound connections are not detected until after exploitation.