SC.L2-3.13.5

System & Communications Protection

Public-Access System Separation [CUI Data]

"Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks."

Objectives

[a]

Publicly accessible system components are identified.

[b]

Subnetworks for publicly accessible system components are physically or logically separated from internal networks.

Key Discussion Points

DMZ Defined:
The DMZ (demilitarized zone) is the subnetwork containing publicly accessible components — internet-facing web servers, VPN gateways, and public APIs all belong there.

Identify First:
[a] requires identifying publicly accessible components before [b] can be satisfied — an accurate inventory of internet-facing assets is required.

Block DMZ to Internal:
The DMZ must be isolated from internal networks — by default, no traffic flows from the DMZ to internal CUI systems without explicit firewall permission.

Cloud Applies Too:
Cloud-hosted public services must also be separated from CUI cloud workloads — shared VPCs, accounts, or networks between public and CUI environments fail this control.

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.

SC.L2-3.13.5

SYSTEM & COMMS PROTECTION — Public-Access System Separation [CUI Data]

Plain English

What this control is really saying:

A web server sitting on the same flat network as your CUI systems means anyone who compromises the web server immediately has a foothold in the CUI environment. This control requires a DMZ — a separate subnetwork that holds publicly accessible components and is isolated from the internal network containing CUI.

How it is used:

- The company's public-facing web server and VPN gateway reside in a DMZ subnet — firewall rules block all DMZ-to-internal traffic except explicitly approved flows.
- The DMZ and internal networks use separate IP ranges — routing between them passes through the firewall, which enforces default-deny from DMZ to internal.
- Cloud infrastructure hosting public-facing services is in a separate account or VPC from the CUI environment — no peering allows direct access between the environments.
- The SSP and network diagrams document which components are publicly accessible and show the DMZ separation architecture — the diagram is current and reviewed annually.

Real World Example

The Scenario

Acme Defense hosts a public-facing job application portal on a server in their office. The server sits on the same network subnet as the CUI engineering workstations. No firewall segment or DMZ separates the web server from the CUI environment.

What the assessor finds

An attacker exploits a vulnerability in the web application and gains a shell on the web server. From there, they can reach all CUI workstations directly — the web server and CUI hosts are on the same subnet with no firewall between them. They exfiltrate 2,400 CUI design files.

SPRS Score Impact

3.13.5 carries a point value of 5. Placing public-facing systems on the same network as CUI means a web application vulnerability becomes a CUI exposure — the DMZ is the architectural control that breaks that attack chain.

What Good Looks Like

Publicly accessible components identified and documented, DMZ subnetwork implemented and physically or logically isolated from internal CUI network, DMZ-to-internal traffic blocked by default with only approved exceptions, DMZ architecture documented in SSP and network diagrams.

Common Gaps

What assessors actually find in the field:

✗ **No DMZ — flat network**

The public web server and CUI systems share the same flat internal network — a compromise of the web server gives direct access to CUI.

✗ **Public components not identified**

No inventory of publicly accessible components exists — the organization cannot verify what is exposed to the internet.

✗ **DMZ allows inbound to internal**

A DMZ exists but firewall rules permit connections from the DMZ to internal systems — the isolation is misconfigured.

✗ **VPN gateway on internal network**

The VPN concentrator sits on the internal CUI network — a compromised VPN endpoint has direct access to CUI without DMZ filtering.

✗ **Cloud not separated**

Cloud-hosted public services and CUI cloud workloads share the same cloud account and VPC — public-facing services have network proximity to CUI.