SC.L2-3.13.9

System & Communications Protection

Connections Termination

"Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity."

Objectives

[a]
A period of inactivity to terminate network connections associated with communications sessions is defined.

[b]
Network connections associated with communications sessions are terminated at the end of the sessions.

[c]
Network connections associated with communications sessions are terminated after the defined period of inactivity.

Key Discussion Points

Define the Period:
[a] requires an organization-defined inactivity period — it must be documented in the SSP. 'Terminating after inactivity' without a defined timeframe fails [a].

Two Triggers:
[b] at session end (explicit logout) and [c] after inactivity — both apply. A system that terminates on logout but never on inactivity fails [c].

Internal + External:
This applies to internal and external networks — idle sessions on internal CUI systems also require termination, not just remote access connections.

Server-Side Required:
Client-side timeout is not sufficient — the server must enforce termination so a disconnected client doesn't leave an active server-side session.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing network disconnect; system design documentation; system security plan; system configuration settings; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developer.

TEST

Mechanisms supporting or implementing network disconnect capability.

Plain English

What this control is really saying:

An open network session is an open door. An idle VPN session, a forgotten remote desktop connection, or an unattended terminal with an active network connection — all of these represent opportunities for an unauthorized person to resume that session. This control requires that connections close automatically at session end and after a defined period of inactivity.

How it is used:

- Remote access server is configured with a 60-minute inactivity timeout — connections idle for 60 minutes are terminated regardless of whether the user session is still open.
- VPN gateway disconnects sessions when the client is inactive — the defined timeout period is documented in the SSP and verified against the current server configuration.
- Web applications that access CUI time out the browser session after a defined period — the application terminates the session token rather than relying on the browser to close.
- The inactivity period is defined in the system security plan — the value balances operational needs against security risk and is approved by the system owner.

SC.L2-3.13.9

SYSTEM & COMMS PROTECTION — Connections Termination

Real World Example

The Scenario

Acme Defense's remote access server has no inactivity timeout configured. Engineers connect to CUI systems via VPN and leave sessions open overnight. No automatic disconnection occurs.

What the assessor finds

An engineer left a VPN session open over a weekend. A visitor in the office on Saturday found the unattended workstation with an active CUI file server connection. The remote access server showed the session had been idle for 72 hours with no termination.

SPRS Score Impact

3.13.9 carries a point value of 1. An open idle network session is an attack surface — it allows session hijacking, unauthorized access by a second person, or persistence by an attacker who has already gained access.

What Good Looks Like

Inactivity timeout period defined in SSP, remote access servers configured to terminate idle sessions, sessions terminated at explicit logout, timeout period balances security and operational needs, configuration verified against documented setting.

Common Gaps

What assessors actually find in the field:

✗ No timeout configured

Remote access sessions and VPN connections never time out — idle sessions can persist indefinitely after a user walks away.

✗ Timeout period not defined

Sessions time out in practice but no specific inactivity period is defined in the SSP or policy — [a] is not met.

✗ Sessions not terminated at logout

Users close the application window but the underlying network connection remains active — logout does not terminate the session.

✗ Timeout too long

A timeout exists but it is set to 8 hours — an unattended workstation can be accessed by anyone for most of a workday.

✗ Only client-side timeout

The VPN client times out locally but the server does not enforce timeout — the session remains open on the server side after client disconnect.