SC.L2-3.13.7

System & Communications Protection

Split Tunneling

"Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling)."

Objectives

[a]

Remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

Key Discussion Points

What Split Tunneling Is:
Split tunneling lets a VPN user access internal resources AND the internet simultaneously — the internet traffic bypasses corporate security controls entirely.

Device + Server Enforce:
Both device-side (MDM-locked VPN config) and server-side (VPN server refuses split-tunnel clients) enforcement are needed — one alone is insufficient.

The Risk:
A compromised home network can reach the CUI environment through the active VPN session — the split-tunneled device bridges an uncontrolled external path to internal systems.

Users Can't Override:
The configuration must be locked so users cannot enable split tunneling — a policy prohibition without a technical control is not sufficient.

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.L2-3.13.7

SYSTEM & COMMS PROTECTION — Split Tunneling

Plain English

What this control is really saying:

When a remote employee's VPN allows split tunneling, their internet traffic bypasses all corporate security controls while they simultaneously access CUI systems. This control requires that all traffic be forced through the VPN tunnel — no direct internet path while connected to the CUI environment.

How it is used:

- VPN configuration on all company laptops disables split tunneling — when the VPN is active, all traffic (internet, internal, cloud) routes through the VPN tunnel.
- VPN client settings are locked via MDM — users cannot modify the split tunneling setting or disable the full-tunnel configuration.
- VPN server-side enforcement detects if a connecting device has split tunneling enabled and refuses the connection — a device-side setting alone is not sufficient.
- The configuration settings are documented in the SSP and verified against the MDM baseline on a quarterly schedule.

Real World Example

The Scenario

Acme Defense deploys a VPN for remote work. The VPN client is configured with split tunneling enabled. Remote employees use the VPN to access internal CUI systems while simultaneously browsing the internet directly through their home router.

What the assessor finds

A remote employee's home router is compromised by an attacker. The employee's laptop is split-tunneled — the attacker can reach the CUI network directly through the active VPN session while the employee's internet traffic bypasses all corporate monitoring.

SPRS Score Impact

3.13.7 carries a point value of 3. A remote device with split tunneling enabled is a dual-homed host — one interface touching the CUI network and one touching the uncontrolled internet. It creates an unmonitored path between the two.

What Good Looks Like

Split tunneling disabled in VPN configuration, setting locked via MDM and not user-modifiable, VPN server enforces full-tunnel requirement and refuses connections with split tunneling enabled, configuration documented in SSP and verified on schedule.

Common Gaps

What assessors actually find in the field:

✗ **Split tunneling enabled**

VPN is deployed but split tunneling is enabled — employees browse the internet directly while connected to CUI systems.

✗ **Device-side only, not enforced**

VPN configuration disables split tunneling on company laptops, but the VPN server does not verify — users can modify the setting without consequence.

✗ **Users can change the setting**

The split tunneling setting is not locked via MDM — technically proficient users can enable it and the change is not detected.

✗ **Personal devices not addressed**

BYOD users connect via VPN — no policy or technical control prevents split tunneling on personally owned devices.

✗ **Contractor VPNs not controlled**

Contractors use their own VPN clients — the organization has no visibility or control over split tunneling on contractor devices.