AC.L2-3.1.14

Access Control

Remote Access Routing

"Route remote access via managed access control points."

Objectives

[a]

Managed access control points are identified and implemented.

[b]

Remote access is routed through managed network access control points.

Key Discussion Points

The Chokepoint Concept:
All remote traffic must pass through the managed access control point — it is the only place where monitoring, access enforcement, and session controls are applied to remote connections.

Document the Points:
[a] requires identifying and implementing managed access control points — the SSP must list them with a network diagram showing all remote access paths routing through them.

Split Tunneling Defeats This:
Split tunneling allows internet-bound traffic to bypass the corporate network — defeating this control and 3.1.12. VPN must be configured in full-tunnel mode.

Block Bypass Paths:
Firewall rules must block direct internet access to internal systems — every open RDP, SSH, or management port is an unmanaged access path that circumvents this control.

Assessment Methods

EXAMINE

Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; list of all managed network access control points; system configuration settings and associated documentation; system audit logs and records.

INTERVIEW

System or network administrators; personnel with information security responsibilities.

TEST

Mechanisms routing all remote accesses through managed network access control points.

AC.L2-3.1.14

ACCESS CONTROL — Remote Access Routing

Plain English

What this control is really saying:

All remote traffic must flow through the organization's firewall and VPN gateway — not around them. If an employee can reach internal systems by bypassing the VPN (through split tunneling, an open RDP port, or a personal remote access tool), this control is not met. The managed access control point is the chokepoint where monitoring and access enforcement actually happen.

How it is used:

- The corporate firewall and VPN gateway are the sole managed access control points — the SSP includes a network diagram showing all remote access flows passing through them.
- VPN is configured without split tunneling — all traffic, including internet browsing, routes through the corporate network so monitoring controls apply to all remote activity.
- Firewall rules block inbound RDP, SSH, and other direct access methods from the internet — remote access is only possible via the VPN gateway.
- Managed access control points are listed in the SSP with their network addresses, responsible owners, and the monitoring capabilities applied at each point.

Real World Example

The Scenario

Acme Defense has a Cisco firewall and VPN gateway. The IT admin configured VPN with split tunneling to reduce bandwidth costs. A developer also set up a direct SSH tunnel to an internal server for personal convenience.

What the assessor finds

VPN split tunneling means remote workers' internet traffic bypasses the corporate network and all monitoring controls. The unauthorized SSH tunnel bypasses the VPN and firewall entirely. Two remote access paths exist that are not managed access control points. No network diagram documents the routing architecture.

SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

Managed access control points identified in SSP with network diagram, VPN gateway as sole entry point with all other inbound paths blocked, split tunneling disabled, firewall rules block direct internet access to internal systems, all remote access paths documented and reviewed.

Common Gaps

What assessors actually find in the field:

✗ **Split tunneling enabled**

VPN uses split tunneling — internet traffic bypasses the corporate network entirely, circumventing all monitoring and access enforcement controls.

✗ **Direct internet ports open**

RDP and SSH ports are open on the perimeter firewall — direct connections from the internet to internal systems bypass the VPN gateway entirely.

✗ **No network diagram**

The organization cannot demonstrate managed routing because no network diagram exists — [a] cannot be evaluated without identifying the access control points.

✗ **Multiple unmanaged entry points**

Different departments set up their own remote access solutions — no single managed chokepoint exists and not all traffic is routed through it.

✗ **Consumer router as access point**

Employees connect through personal home routers that are not managed, monitored, or controlled by the organization — these are not managed access control points.