CMMC SC.L2-3.13.6

Deny Network Communications Traffic by Default

Implementation Playbook & Assessment Preparation Guide

NIST SP 800-171 Rev 2 | CMMC Level 2

The Requirement

> *"Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)."*

NIST 800-171A Assessment Objectives

[a] Network communications traffic is denied by default

[b] Network communications traffic is allowed by exception at managed interfaces

Both inbound AND outbound traffic must be blocked by default, with only explicitly approved communications permitted.

The Critical Distinction

Threat-Based Blocking ≠ Deny-By-Default

Threat-Based Blocking

Allow all traffic, block known bad

Logic: Is it malicious? If not, allow it.

Unapproved but safe destinations are accessible — requirement NOT met.

Deny-By-Default

Block all traffic, allow known good

Logic: Is it explicitly approved? If not, block it.

Only pre-approved destinations are reachable — requirement IS met.

Real-World Test

A compliant user with valid MFA tries to access a legitimate file-sharing service not approved for CUI.

The Most Common Misconception

Cloud, Zero Trust, and modern architectures do NOT exempt you from this requirement.

What OSCs Often Argue

- *"Our cloud provider handles this"*
- *"Zero Trust replaces deny-by-default"*
- *"Our monitoring/SIEM covers this"*
- *"Identity controls (MFA, SSO) satisfy it"*
- *"Deny-by-default would break operations"*
- *"We inherit this from our FedRAMP provider"*

What Assessors Evaluate

- Is traffic denied by default?
- Do you have an approved exception list?
- Is there a formal exception process?
- Does it cover BOTH directions?
- Can you prove unapproved traffic is blocked?
- Is your enforcement technically verifiable?

Architecture determines HOW you implement it, not WHETHER you implement it.

Five Mistakes That Lead to Findings

1

Identity ≠ Network Controls

MFA, SSO, and Conditional Access control who connects — not where systems can communicate.

2

Showing Only Threat-Based Blocking

Blocking malware and malicious URLs shows "block bad," not "deny everything except approved."

3

Justifications Instead of Evidence

Assessors need configuration proof, not multi-page arguments about why it's impractical.

4

Only Addressing Inbound Traffic

The practice requires BOTH directions. Outbound deny-by-default is frequently missed.

5

Monitoring Described as Enforcement

SIEM logging and alerting detects unauthorized traffic — deny-by-default prevents it.

What Assessors Look For

Four categories of evidence required during assessment

Default Deny Configuration

- Firewall rules showing default DROP/DENY
- DNS filter showing default block
- Application control config
- Proxy requiring explicit authorization

Approved Exception List

- Approved outbound destinations
- Approved applications & protocols
- Business justification per exception
- Approval authority documented

Exception Management Process

- Request process for new destinations
- Approval criteria & authority
- Review frequency for exceptions
- Audit trail of approvals

Enforcement Evidence

- Configuration exports/screenshots
- Logs showing blocked attempts
- Test results proving blocking
- Proof controls can't be bypassed

Implementation Approaches

Choose the approach that fits your architecture — the requirement stays the same.

Network / Perimeter

Firewalls, routers, security appliances with default outbound DENY

Host-Based Firewall

Endpoint firewalls managed centrally (e.g., via Intune or GPO)

Application Control

Only approved apps can execute and initiate network connections

DNS Filtering

DNS queries blocked by default with an approved domain allow-list

Proxy / API Gateway

All traffic forced through proxy or gateway enforcing allow-list

Cloud-Native Controls

Security groups, network ACLs, or cloud firewall with default DENY

A layered combination of multiple approaches provides defense-in-depth and is the recommended strategy.

The Shadow Rule Transition

A phased, data-driven approach to implementing deny-by-default without breaking the business.

1
PHASE

Shadow / Log All

Add a "Log All" rule at the bottom of your firewall stack. This logs every connection that would be blocked without actually blocking anything. Analyze 24-48 hours of data to identify legitimate traffic.

2
PHASE

Formalize Exceptions

Establish a formal Request-to-Rule SOP. Create allow rules for each identified legitimate service with documented business justification, SSP cross-reference, and management approval.

3
PHASE

Enforce Hard Deny

Replace the "Log All" rule with a hard "Deny All" for both inbound and outbound. Verify logging to SIEM. Continuously monitor deny logs for any missed legitimate services.

Handling Dynamic & Difficult Traffic

Cloud endpoints change frequently — these strategies keep deny-by-default manageable.

1 Vendor Service Tags & FQDN Filtering

Use pre-defined service objects (e.g., "Microsoft Update") and domain-based rules instead of static IPs. Cloud providers publish endpoint lists in JSON/XML for automation.

2 Automated Rule Updates

Pull vendor endpoint lists via scripts on a monthly cadence. Auto-push updated rules to firewalls and security groups. Govern automated updates through your formal Change Management process.

3 Proxies for Specialized Traffic

NTP: Route clients through an internal proxy; only allow the proxy to reach external time sources. CRL/OCSP: Use a transparent proxy to allow Certificate Authority URLs while blocking general browsing.

4 Formalize Dynamic Exceptions

Even automated processes need a Change Request authorizing the script. Maintain an audit trail proving updates are management-approved and mapped to mission-essential functions.

Evidence & Artifact Catalog

Artifact	What the Assessor Looks For	How to Extract / Generate
Firewall Running Config	Deny Any Any rule at the bottom of BOTH inbound and outbound ACLs	show running-config | include access-list (Cisco) show firewall policy (Fortigate)
Traffic Log Samples	Timestamps showing traffic hits on the Deny rule, proving active blocking	Export from SIEM, UniFi Controller Insights > Firewall Index
Authorized Ports List	Table in SSP matching Allow rules to documented business functions	Export firewall Allow rules to CSV Cross-map to business justifications
Change Mgmt Logs	Evidence that Allow rules were requested, approved, then implemented	Export Approved tickets from Jira/ServiceNow matching FW timestamps

Evidence Validation: The Mock Audit

Perform these three tests before the actual assessment to confirm "hard evidence" readiness.

Test 1: Unauthorized Egress Test

Action: From a CUI server, attempt to reach a known public IP via an unauthorized port (e.g., telnet 1.1.1.1 23).
Expected: Connection must time out or be actively refused.
Evidence: Screenshot of "Connection Timed Out" AND the corresponding SIEM Deny log entry.

Test 2: Unauthorized Ingress Test

Action: From an external non-VPN IP, run a port scan (Nmap) against your public gateway.
Expected: Only authorized ports (e.g., VPN 443) show as Open. All others show Filtered or Closed.
Evidence: Nmap scan report (PDF) demonstrating unauthorized services are closed.

Test 3: Shadow Discovery Test

Action: Review 24 hours of Deny rule logs to identify blocked legitimate traffic.
Expected: Find one blocked legitimate service (e.g., overlooked update) and document adding it via SOP.
Evidence: Documentation trail showing the process of discovering and formally approving an exception.

SSP Write-In Template

SC.L2-3.13.6 Implementation:

Network communications traffic is denied by default for both inbound and outbound directions through [firewall / security groups / host controls / service mesh].

Explicit allow rules are configured only for approved destinations and services.

Inbound: [Mechanism] denies all inbound connections except [list specific allowed services with ports/protocols].

Outbound: [Mechanism] denies all outbound connections except:

- Approved cloud service endpoints (per documented list)
- Required external APIs and services (per documented list)
- Update/patch services for OS and security tools
- [Other approved services with documented approval]

Exception Process: Requests for new outbound destinations require [role] review and approval with business justification. Approved exceptions are documented in [system/location] and implemented via [process/automation].

Maintenance: Approved destination list is reviewed [frequency] by [role]. Dynamic service endpoint changes are managed via [process]. All approved exceptions are audited [frequency].

Pre-Assessment Litmus Test

If a user/system tries to connect to an unapproved but legitimate service, what happens?

- ✓ It's blocked by default
- ✗ It's allowed and we'd see it in logs

Where is your list of approved outbound destinations?

- ✓ Documented and maintained
- ✗ We don't have a formal list

At what layer do you enforce deny-by-default?

- ✓ Network / Host / DNS / Proxy / etc.
- ✗ We rely on monitoring

Can you show blocked traffic to a non-malicious, unapproved destination?

- ✓ Yes, here are the logs
- ✗ We only block malicious traffic

Do these controls apply to BOTH inbound AND outbound?

- ✓ Yes, both directions
- ✗ We focus on inbound

Not Met? Use a POA&M

Plan of Action & Milestones for conditional certification (180-day remediation window)

1

Acknowledge the Gap

Be honest — don't argue it's met when it's not. Document the specific deficiency.

2

Document Remediation Steps

Detailed plan: what exactly you'll implement, technology choices, and configuration changes.

3

Provide Realistic Timeline

Must be within 180 days for conditional certification. Break into measurable milestones.

4

Identify Interim Controls

Compensating controls that reduce risk while the fix is in progress (they don't make it "met").

5

Assign & Track

Named responsible party, regular progress updates to assessor/C3PAO.

Compensating controls reduce risk but do NOT satisfy the practice. The gap must be remediated.

Key Takeaways

- Deny-by-default applies to BOTH inbound and outbound traffic — no exceptions.
- Cloud, Zero Trust, and managed services do NOT exempt you from this requirement.
- Identity controls (MFA, SSO) ≠ network controls — you need both.
- Monitoring and detection ≠ prevention — show traffic is blocked, not just logged.
- Document your approved exception list and maintain a formal management process.
- Test your implementation — prove unapproved traffic actually gets blocked.

"Am I actually denying traffic by default, or am I just blocking the bad stuff I detect?"