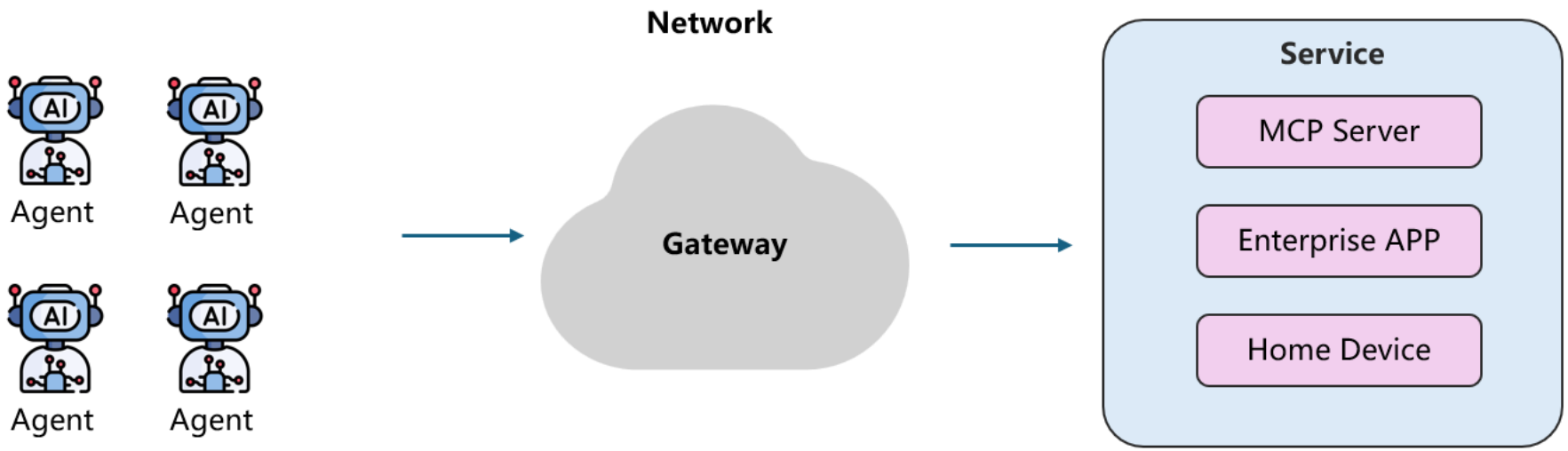
July 2026

Use Cases and Requirements for Network Admission of AI Agent Instances

Chao Shang, weiyu Jiang, Liang Xia, Bizhu Wang, Mengying Sun
Huawei, BUPT

Why agent admission is a network problem

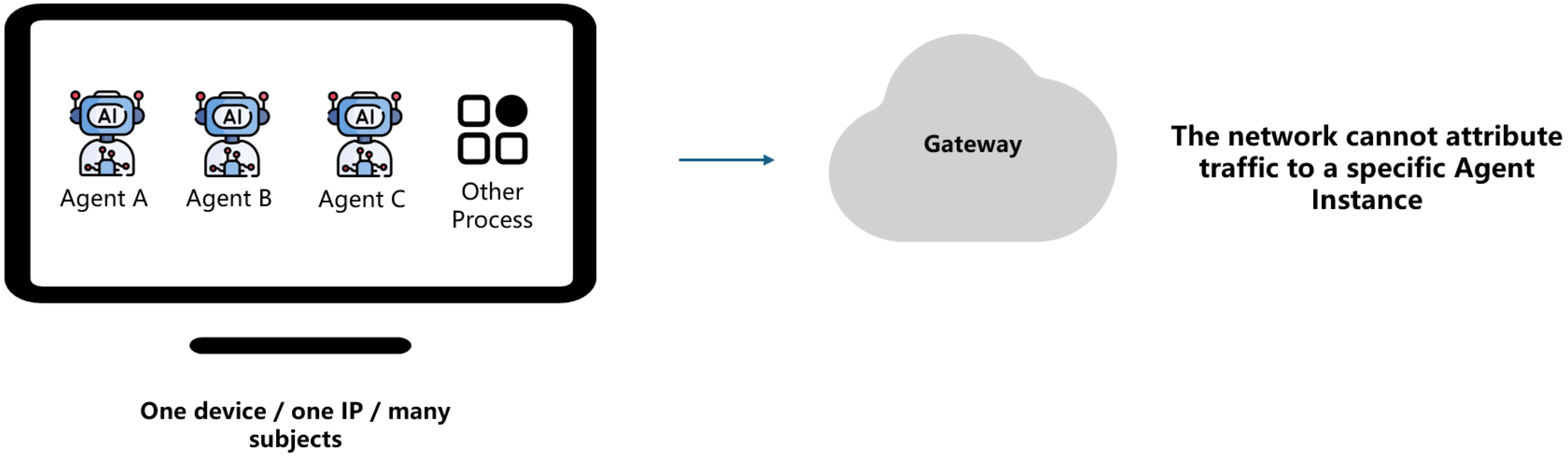


- Agents call internal resources, tools, external models, and peers
- Application proofs are checked after reachability exists
- Legacy and non-HTTP services may not understand Agent identity
- Many instances may share a host, IP, or gateway

Network admission adds an earlier control boundary; application authorization remains.

One IP address can represent multiple security subjects

Approved agents, unapproved agents, ordinary applications, and the user may share one attachment.

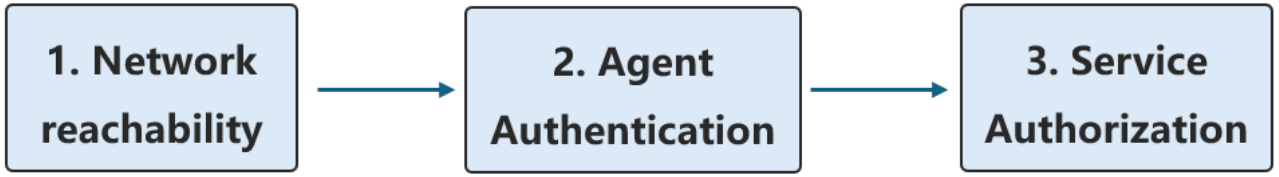


Implications

- Device admission does not authenticate each Agent Instance
- Source IP, source port, or a self-asserted Agent-ID is not proof
- Different agents need different reachability policy

Admission must precede general reachability

Current model

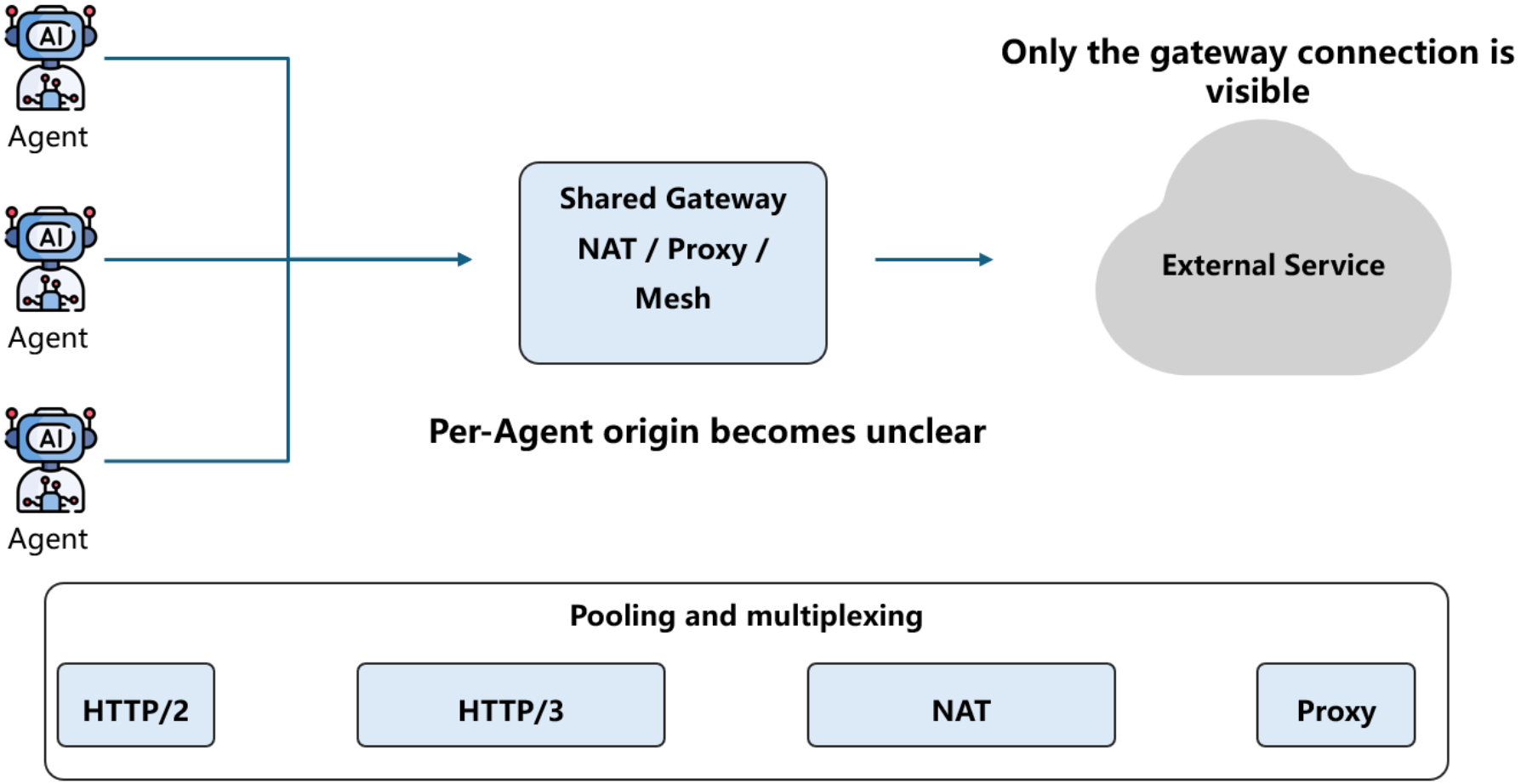


Why application-only is insufficient

- Reachability exists before credential verification
- Every destination must understand Agent identity
- Scanning and bypass remain possible
- Network EPs do not receive the result

The network is already exposed before the application decides.

Shared gateways can erase the originating Agent Instance



The gateway must preserve protected per-Agent context for every request.

The missing function:

A verifiable Agent Binding

1. Authenticated Agent Instance
    - A particular running instance or continuity domain
1. Credential-key possession
    - Fresh proof bound to the admission session
1. Optional runtime evidence
    - Bound to the same instance key and context
1. Enforceable Network Context
    - Protected from reuse by another process
1. Finite lifetime
    - Renewal, revocation, migration, and termination
1. Result: Agent Binding
    - Identity and traffic attribution become enforceable

Functional model: verify, bind, enforce

1. Agent Instance + Evidence

Proves possession of the instance key and supplies optional runtime evidence

2. Network Admission Function

Verifies credential, freshness, evidence, and policy; then installs an Agent Binding

3. Network Enforcement Point

Maps Agent-ID, key, and attributes to an enforceable Network Context

The security property depends on the integrity of the complete path from authenticated key to Network Context.

Six core requirements derived from the use cases

1

Agent Instance authentication

Authenticate a particular running instance with fresh proof of possession—not only its user, host, image, or platform.

2

Binding to enforceable traffic

Bind the successful result to protected Network Context and distinguish traffic when agents share an attachment.

3

Shared-gateway attribution

Isolate per-Agent state and preserve the originating instance across pooled connections and multiplexed streams.

4

Admission, lifetime, revocation

Use constrained pre-admission connectivity, finite lifetimes, renewal, and prompt removal on change or termination.

5

Non-bypass and layered authorization

Prevent alternate paths; network admission constrains reachability but never implies unrestricted application authority.

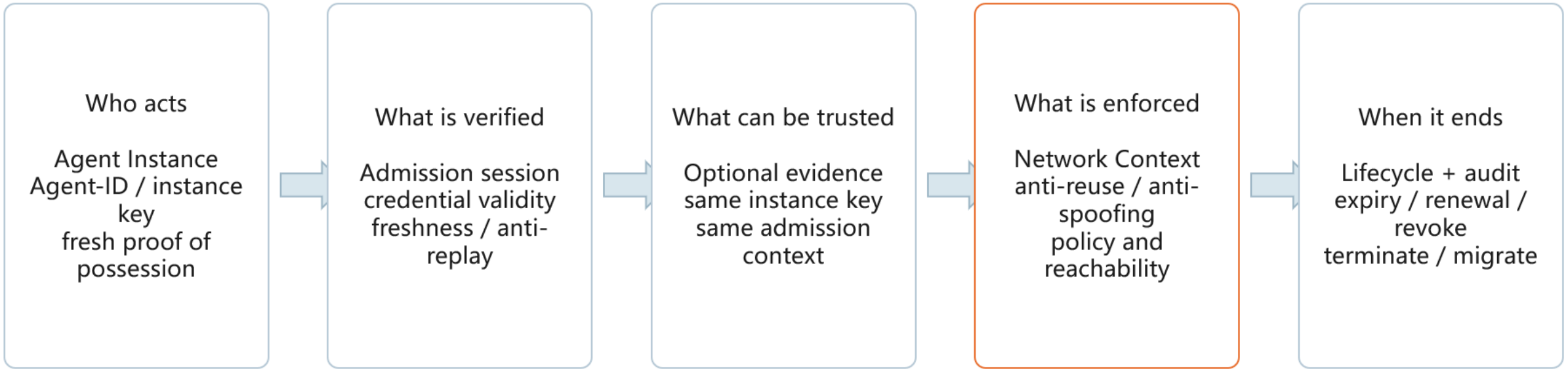
6

Evidence, audit, privacy

Bind evidence to the same key and context; record lifecycle events while minimizing identifier scope and retention.

A secure architecture must protect both the cryptographic proof and the local mechanism that creates and uses the binding.

Security depends on the complete binding path



Primary risk	A false association between an authenticated Agent-ID and traffic generated by another process, host, request, or stream.
Binding rule	Protect the complete path from instance key to Network Context; proof-of-possession helps only when the key and context are protected.
Privacy rule	Minimize identifier scope and retention; disclose only policy-required attributes and avoid unnecessary export of runtime evidence.

This draft defines requirements—not a new protocol

IN SCOPE

1. Define the problem

Operational use cases
Agent Instance terminology
Admission and attribution gaps

Clarifies why application authorization and network admission are complementary.

IN SCOPE

2. State requirements

Authentication and binding
Lifetime and revocation
Non-bypass, audit, and privacy

Creates criteria for evaluating future architectures and protocol profiles.

OPEN DESIGN SPACE

3. Realize the binding

Network Context choices
Distributed NAF / EP placement
Reuse of existing IETF mechanisms

No new Agent-ID format, authentication protocol, OAuth grant, or routing extension is defined.

Discussion: Are the requirements complete, and which existing mechanisms can realize the binding?