Network Working Group
Internet-Draft
Intended status: Informational
Expires: 13 September 2026

C. Shang
X. Liang
W. Jiang
Huawei

12 March 2026

Campus Agent Identification and Scope-Down Access Control
draft-shang-campus-agent-scope-down-00

Abstract

AI agents operating in enterprise campus networks execute user-delegated tasks by invoking multiple tools and services, often without continuous user supervision. Traditional authorization models assume stable applications and human-driven interactions, creating a mismatch when applied to autonomous agents that can chain actions across heterogeneous systems.

Campus environments also contain heterogeneous and legacy services across diverse protocols, making per-service agent-aware authorization difficult to deploy consistently. This document describes the problem space for campus agent access control and argues that agents require task-bound privilege reduction ("scope-down") and that enforcement can be provided by in-path network devices in order to preserve compatibility with existing systems.

Table of Contents

1. Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). The list of current Internet-Drafts is available at:

https://datatracker.ietf.org/drafts/current/ (https://datatracker.ietf.org/drafts/current/)

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.

2. Copyright Notice

3. Introduction

Enterprise campus networks increasingly carry traffic generated by AI agents acting on behalf of users. These agents may retrieve internal documents, query knowledge bases, invoke APIs, and automate workflows across multiple services.

Unlike conventional applications, agents may be instantiated per task and autonomously chain operations based on intermediate results. Permissions that are safe for human operation may therefore become unsafe when exercised by an autonomous actor operating at machine speed.

Existing standards such as OAuth 2.0 [RFC6749] and JSON Web Tokens [RFC7519] provide identity and delegation primitives. However, these mechanisms alone do not address task-bound privilege reduction or enforcement in heterogeneous campus environments.

Deployable campus agent security therefore requires two capabilities:

* recognition of agent-generated traffic

* enforcement of task-bound privilege scope

4. Example Campus Network Architecture

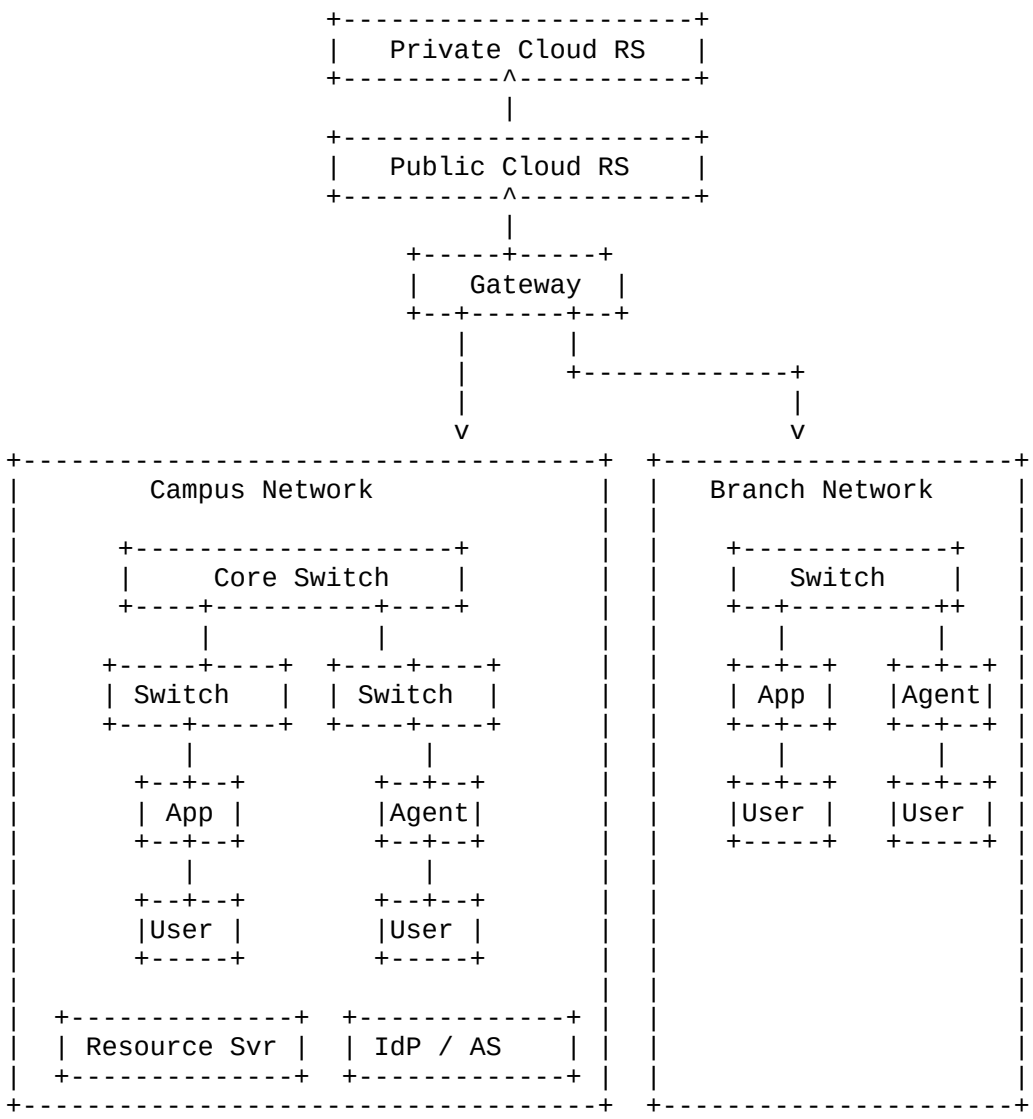


Figure 1

5. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

Agent: Software that performs tasks on behalf of a user or principal and may autonomously invoke services or tools.

Agent Identifier (Agent-ID): A verifiable identifier associated with a specific agent instance.

Principal: The human user or entity on whose behalf the agent operates.

Authorization Server (AS): The OAuth authorization server issuing tokens.

Resource Server (RS): A server hosting protected resources.

In-Path Network Device (ND): A network device positioned on the traffic path capable of enforcing policy decisions.

6. Problem Statement

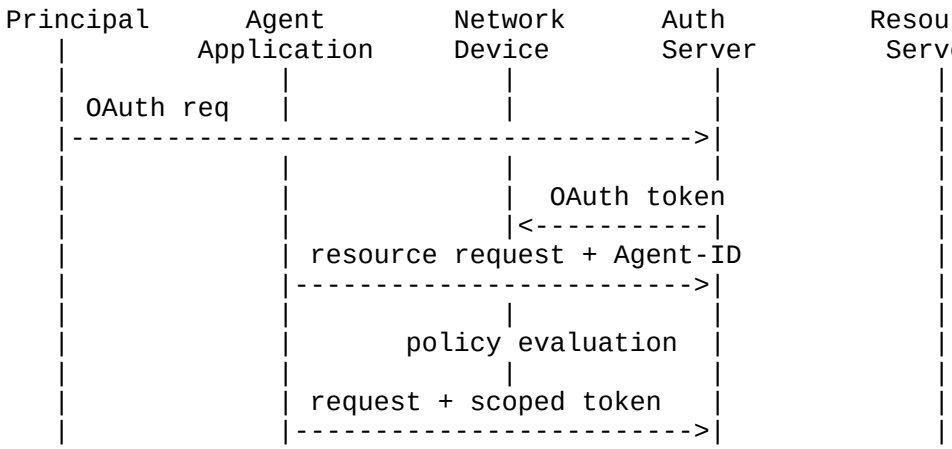
Traditional authorization models assume stable applications and human-driven workflows. Agents violate these assumptions by dynamically selecting targets and chaining tools across systems.

Without task-bound constraints, agent-driven workflows introduce several risks:

* over-broad aggregation of internal data across multiple systems
* cross-boundary exfiltration when generated output is transmitted externally
* unsupervised tool chaining across services without user review
* machine-scale amplification of data access or operations

Campus environments also contain heterogeneous services and legacy protocols, making it operationally infeasible to require each service to implement agent-aware authorization.

7. Architecture



8. Deployment Models

Different deployment models are possible.

Model A: Network Device performs token validation and policy enforcement without issuing new tokens.

Model B: Network Device obtains a reduced-scope token through OAuth Token Exchange [RFC8693] or via Authorization Server policy decisions.

This document does not define a new OAuth grant type or token format and relies on existing OAuth mechanisms.

9. Security Considerations

Deployments must address several threats.

Agent identity spoofing: Deployments *MUST* ensure that Agent-ID cannot be forged or reused across devices.

Token replay: Deployments *SHOULD* bind tokens to the Network Device as audience and *MAY* use mutual TLS or channel binding to reduce replay risk.

Network bypass: Network architectures *SHOULD* enforce that agent traffic cannot bypass the Network Device through fabric policies, VRF isolation, or ACL enforcement.

Intent mis-modeling: Scope-down mechanisms ensure that authorization does not expand privilege beyond the original delegation but cannot eliminate risks caused by incorrect intent interpretation.

10. Privacy Considerations

Deployments may log Agent-ID and authorization decisions for auditing.

Operators *SHOULD* minimize collection of unnecessary personal data and avoid storing sensitive token contents.

Deployments *SHOULD* consider using short-lived or per-task Agent-IDs and *SHOULD* distinguish Principal identifiers from Agent-IDs in audit logs.

11. IANA Considerations

This document makes no requests of IANA.

12. Acknowledgements

The authors thank members of the research community for discussions on agent identity and authorization models in campus networks.

13. References

13.1. Normative References

[RFC2119]

[RFC8174]

[RFC6749]

[RFC7519]

[RFC8693]

[RFC9068]

14. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC8693] Jones, M., Nadalin, A., Campbell, B., Ed., Bradley, J., and C. Mortimore, "OAuth 2.0 Token Exchange", RFC 8693, DOI 10.17487/RFC8693, January 2020, <https://www.rfc-editor.org/info/rfc8693>.

[RFC9068] Bertocci, V., "JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens", RFC 9068, DOI 10.17487/RFC9068, October 2021, <https://www.rfc-editor.org/info/rfc9068>.

Authors' Addresses

Chao Shang
Huawei
Email: chao.shang@huawei.com

Liang Xia
Huawei
Email: frank.xialiang@huawei.com

Weiyu Jiang
Huawei
Email: jiangweiyu1@huawei.com