

A10 AI Gateway: The Intelligent Control Plane for All AI Operations

Intelligent Routing, Budget Allocation, and Governance for Every LLM in Your Organization



The Fragmented AI Environment

AI adoption looks different across organizations and even within the same organization. Developers may build AI into applications and business systems, while other departments such as marketing and product teams may use personal AI tools to help with daily work that have no connection to any system IT manages. The result is a fragmented AI environment, making it difficult to understand who is using AI, how it's being used, the associated costs, and if it's being used efficiently.



A Centralized, Intelligent Controller for AI

A10 AI Gateway provides a centralized way to manage AI across the organization. It intelligently routes AI calls from users, apps, or AI agents to appropriate AI resources, providing greater AI usage control, cost optimization, security, and visibility over their AI workflow. The result is a more controlled, efficient, and secure approach to enterprise AI – helping organizations get the most value from AI by understanding exactly who is using it, at what costs, while maintaining the proper security measures.

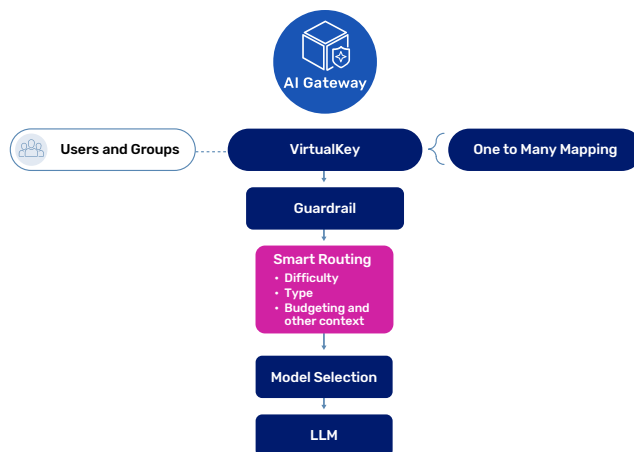


Figure 1: Example A10 AI Gateway AI traffic flow illustrating identity-based access and A10 proprietary smart routing technology.

Challenge

AI adoption is outpacing organizations' ability to manage it. Organizations are struggling to maintain consistent visibility, control costs, enforce security, and make sure users have reliable access to AI.

Solution

A10 AI Gateway brings all AI interactions into a single, governed environment, allowing for overall improvement in routing, cost management, AI key management, and visibility for efficient use of AI resources.

Benefits

- Identity-based AI access allocates spend and model access by user or team
- Reasoning-based Intelligent routing evaluates prompts on difficulty and type
- Centralized visibility and management, rate limiting



A10 AI Gateway Features and Benefits

With A10 AI Gateway, organizations gain:

- 1. Identity-based AI Access – Give the right users access to the right resources.** A10 AI Gateway enables organizations to apply AI access and routing policies based on individual users and groups, with the capability of syncing with existing local directory systems. Engineering users can, for example, be routed to specialized coding models, while other teams can be directed to models appropriate for their roles and needs. Organizations can also define individual access policies for users who require unique permissions, giving them precise control over AI usage, and cost.
- 2. Smart Routing – Match every request with the right model.** A10 AI Gateway goes beyond just metering, or static routing policies. It evaluates the complexity and type of each AI request via an 11-step decision tree, then with reasoning, it will logically and accurately route simple tasks to more cost-efficient models and complex, reasoning-intensive tasks to more capable models. Organizations can optimize performance and control costs by using the right model for every request.
- 3. Centralized AI traffic and cost management –** Core AI gateway functionality is present as well, with A10 AI Gateway acting as a centralized control plane and AI cost management tool for managing AI traffic, routing requests between different AI models and tools, and providing visibility into how AI is being used.

The Building Blocks of A10 AI Gateway

Identity, Access and Governance

- Virtual API keys issued per user and per team, each with its own budget and rate limits
- Per-key model access policies restricting which models and providers each identity may reach
- Secure provider credential vault – real provider keys are never exposed to callers

Routing

- Task complexity classification – simple vs. complex prompt routing
- Budget-triggered priority-chain cascade across configured model pools

- Consumer-configurable routing policy per virtual key or team

Cost, Budgeting and Rate Limiting

- Real-time, per-request cost tracking in dollars
- Per-model and per-team token budgets, with hard limits and soft-limit alerts
- Business-layer TPM / RPM rate limiting enforced per key or team

The New AI Gateway: An Intelligent Control Plane

As adoption of AI continues to accelerate, managing AI usage across users, applications, agents, and models becomes increasingly complex. Without a centralized approach, organizations can struggle to understand how AI is being used, and how to control costs, manage access, and ensure AI resources are used efficiently and securely.

An AI gateway provides a centralized control plane for the AI workflow, but not all AI gateways are created equal. The A10 AI Gateway goes beyond simply managing AI traffic by intelligently routing requests to the most appropriate model based on the needs of the request, while giving organizations the ability to manage AI access, usage, and costs at the individual and team levels.

The result is a more efficient, secure, and reliable approach to implementing AI, helping organizations maximize the value of every AI interaction while maintaining visibility and control over how AI is accessed and used.

About A10 Networks

A10 Networks (NYSE: ATEN) delivers secure application and network solutions that protect, optimize, and scale business-critical systems across on-premises, hybrid cloud, and edge environments. Our portfolio enables large enterprises, service providers, and cloud platforms worldwide to deliver performance, reliability, and protection against cyber threats, while preparing their networks for the demands of AI and next-generation applications. Founded in 2004 and headquartered in San Jose, California, A10 Networks serves over 7,000 global customers.

For more information, visit A10networks.com and follow us [@A10Networks](https://twitter.com/A10Networks).

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

©2026 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Logo, A10 Control, A10 Defend, A10 Harmony, Harmony, A10 Thunder, Thunder, ACOS, A10 SSL Insight, SSL Insight, SSLi, vThunder, ThreatX, ThreatX Protect, and TrojAI are trademarks or registered trademarks of A10 Networks, Inc. or its affiliates in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: A10Networks.com/a10trademarks.