Every standard gateway capability, and where it is set in G8

For the team that arrives with a checklist: rate limiting, OAuth 2.0, Keycloak, LDAP, caching, logging, masking and the rest. Each row names the capability, what it does, the Plugin behind it and where its form is in the console. Every Plugin has a form drawn from the engine's own schema and a Raw JSON tab beside it; attach it to a Route, a Service or a Consumer, or to every request in an Environment as a Global rule.

Limits, identity and access

CAPABILITY	WHAT IT DOES	PLUGINS	WHERE IN THE CONSOLE
Rate limiting	Requests per window, request rate or concurrent connections, per client, Consumer or a key you choose; counters shared across gateway nodes in Redis.	limit-count, limit-req, limit-conn	Route › Plugins; Global rules
API keys	A key per Consumer, sent in a header or a query parameter; the key is shown masked after it is created.	key-auth	Consumer › Credentials; Route › Plugins
JWT and OAuth 2.0 access tokens	A JWT signed with a secret or a key pair, verified at the gateway; an OAuth 2.0 bearer token from your provider, verified as a JWT against the provider's keys or by introspection at the provider.	jwt-auth, openid-connect	Route › Plugins
OpenID Connect	Sign-in through your provider (Keycloak, Microsoft Entra ID, any OpenID Connect provider): a browser is sent to it, an API client sends a bearer token, and the identity reaches the backend in a header.	openid-connect	Route › Plugins
Keycloak authorization	Keycloak decides which paths a signed-in user may call, from the resources and permissions of its client.	authz-keycloak	Route › Plugins
LDAP and Active Directory	Credentials of API callers checked against your directory: a bind as uid=<user>,<base DN> for entries named by the account name (ldap-auth), or a search with a service account on sAMAccountName and then a bind, for Active Directory entries named CN=First Last (ldap-auth-advanced). The caller's DN must be on a Consumer credential, spelled exactly as the Plugin builds it.	ldap-auth, ldap-auth-advanced	Consumer › Credentials; Route › Plugins
SAML	SAML 2.0 sign-in in front of a Route.	saml-auth	Route › Plugins
Signed requests, basic authentication	HMAC-signed requests with a key per Consumer; username and password.	hmac-auth, basic-auth	Consumer › Credentials; Route › Plugins
Several methods on one Route	A list of authentication Plugins tried in order; the first that admits the request wins.	multi-auth	Route › Plugins
Policy engines and external authorization	A decision from Open Policy Agent or Casbin, or from a service of yours asked before the request passes.	opa, authz-casbin, forward-auth	Route › Plugins
Mutual TLS	Client certificates required from the CA you provide, with paths you skip; server certificates per hostname. A client without a certificate the CA signed completes the handshake and is answered 400 by the gateway before any Route matches, recorded in Traffic Explorer with gateway as the Upstream node.	Route and Certificates	Gateway › Certificates; Route
IP, User-Agent, Referer and URI rules	Allow or deny by address or network, by User-Agent, by Referer, by URI pattern.	ip-restriction, ua-restriction, referer-restriction, uri-blocker	Route › Plugins; Global rules
Request validation	Requests that do not match a JSON schema or your OpenAPI document are refused before the backend is called. A document fetched by URL must carry / or the gateway's address under servers, and is cached per worker for the time set in the Plugin's metadata, so change the URL when the document changes.	request-validation, oas-validator	Route › Plugins

Access, traffic, transformation and observability

CAPABILITY	WHAT IT DOES	PLUGINS	WHERE IN THE CONSOLE
CORS and CSRF	Cross-origin rules per Route; a CSRF token checked on changing requests.	cors, csrf	Route › Plugins
Web application firewall	Requests checked by a Chaitin SafeLine WAF you run before they reach the backend.	chaitin-waf	Route › Plugins; Global rules
Consumers and groups	A Route restricted to the Consumers, groups or Services you name.	consumer-restriction, acl	Route › Plugins
Caching	Upstream responses cached on disk or in memory, keyed on the parts of the request you choose; GraphQL responses too.	proxy-cache, graphql-proxy-cache	Route › Plugins
Rewriting	URI, method, host and headers rewritten before proxying; the response rewritten on its way back; bodies transformed with templates.	proxy-rewrite, response-rewrite, body-transformer	Route › Plugins
Masking	Headers, query arguments and JSON body fields masked in what your logger Plugins write, with data-mask; the backend and the client still see the real values. In G8's own request records, the headers, query arguments and body fields you name are masked before the record is stored; authorization, cookie and API-key headers by default.	data-mask; Traffic Explorer masks	Route › Plugins; Traffic Explorer › Settings › Masking
gRPC and GraphQL	REST to gRPC transcoding (the transcoder checks nothing; request-validation on the same Route is the contract), gRPC-Web, GraphQL to REST and GraphQL rate limits.	grpc-transcode, grpc-web, degraphql, graphql-limit-count	Route › Plugins
Canary releases	Traffic split between upstream versions by weight or by rules on the request.	traffic-split	Route › Plugins
Circuit breaker and health checks	A failing backend stops receiving requests until it recovers; active health checks take nodes out of rotation, passive ones mark nodes from real traffic. The console does not show node health: read which node answered in Traffic Explorer's Upstream node column, or ask Prometheus.	api-breaker; Upstream health checks	Route › Plugins; Upstream form
Mocking, fault injection, mirroring	A mocked response from the gateway; delays and errors injected for tests; traffic mirrored to a second backend.	mocking, fault-injection, proxy-mirror	Route › Plugins
Access logs	One record per request sent to the systems you run. The headers on the Traffic Explorer mask list arrive masked; a request body a logger includes does not, and data-mask is the mask for that. syslog sends only when its flush limit fills (4096 bytes by default), so lower it on a quiet Route.	elasticsearch-logger, kafka-logger, splunk-hec-logging, syslog, http-logger, loki-logger, clickhouse-logger, file-logger	Route › Plugins; Global rules
Metrics and traces	Request metrics scraped by your Prometheus; traces exported to Zipkin, SkyWalking or Datadog.	prometheus, zipkin, skywalking-logger, datadog	Route › Plugins; Global rules
Serverless backends	A Route answered by a function instead of a service.	aws-lambda, azure-functions, openwhisk, openfunction, serverless-pre-function, serverless-post-function	Route › Plugins
Other protocols	WebSocket, Kafka, Dubbo and MQTT in front of or behind the gateway; TCP and UDP on stream Routes.	websocket-proxy, kafka-proxy, http-dubbo, mqtt-proxy; stream Routes	Route; Stream routes
Housekeeping	The client address behind a proxy, compression, redirects, a request id on every call, buffering and body limits.	real-ip, gzip, redirect, request-id, proxy-buffering, client-control	Route › Plugins; Global rules
Secrets	Secrets kept in Vault, AWS Secrets Manager or GCP Secret Manager and referred to from the forms; a secret typed into a form is stored on the engine, shown only to roles that manage the object, and masked for everyone else and in the audit log.	Secret managers	Gateway › Secrets

Where the forms come from

Why the reference can name a form for every row.

Drawn from the engine’s schema

The console draws the form of each Plugin from the engine’s own schema, so a form never falls behind the engine; when an engine version differs, the build goes red until a person reviews the form.

Raw JSON beside every form

The people who prefer the configuration as JSON have it on the next tab, with the same validation.

Attached where it belongs

A Plugin on a Route applies to that Route; on a Service to every Route of the Service; on a Consumer to that caller everywhere; as a Global rule to every request in the Environment. The request path view of a Route shows which Plugins run and in what order.

Recorded before it is applied

Adding or changing a Plugin is a change to the object: a role check, an audit record opened before the engine is called, the engine’s own validation, and a completed record with before and after, secrets masked.

Step-by-step guides

Written on a real install, with the form fields, the refusals and the records they leave.

g8.dev/knowledge-base/rate-limiting-per-consumer-with-limit-count	A budget per Consumer, counted in Redis across nodes; the 429s in Traffic Explorer.
g8.dev/blog/keycloak-integration	OpenID Connect at the gateway and Keycloak authorization on a Route.
g8.dev/knowledge-base/promoting-gateway-configuration-from-staging-to-production	A Route copied to Production with the preview of what changes.
g8.dev/blog/openapi-to-mcp	An existing REST API served to AI agents as tools, behind the same Plugins.
g8.dev/platform/api-gateway	The capabilities with the console form that sets each one, and the full Plugin catalog with what every Plugin does.

NEXT STEP

Bring the rules your gateway applies today; we show the same configuration as forms in G8. Request a demo at g8.dev/request-a-demo or write to hello@g8.dev. Read next: G8 API Gateway Datasheet (2 pages), at g8.dev/downloads.

g8.dev/request-a-demo · hello@g8.dev