CLOUD GATEWAY

CONNECT

TRANSIT ONLY CONNECTIVITY

SERVICE DEFINITION

V2.0
Issue Date: 14/10/2025
Commercial in Confidence

About this document

This document is designed to provide a straightforward, clear description of our **Transit-only Connectivity** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is Transit-only Connectivity?

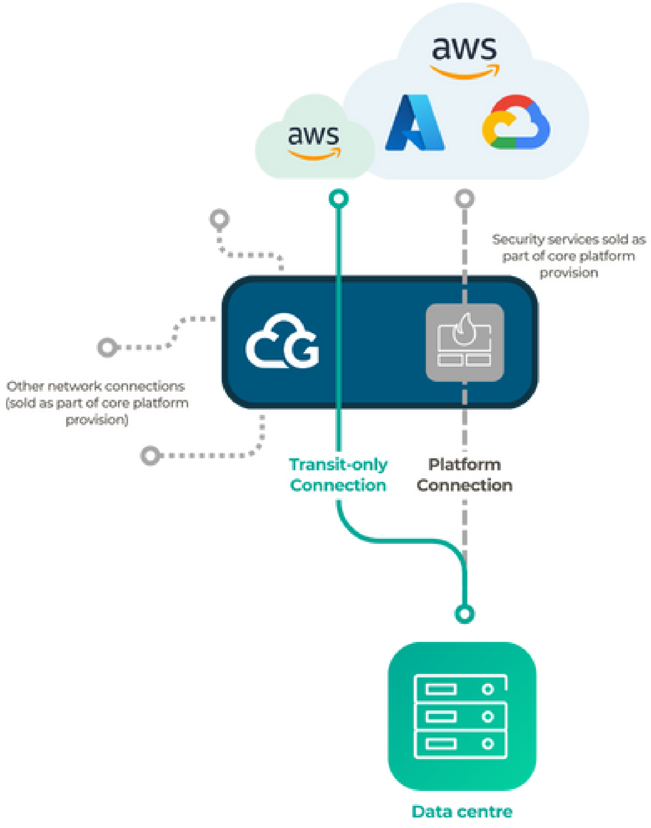
Transit-only Connectivity enables you to establish a network connection between your data centre presence and Cloud Service Providers (CSP). Traffic that traverses this service does not pass through our platform Secure Enforcement Core (SEC).

Transit-only Connectivity is deployed as an optional complementary service available as a part of your primary Cloud Gateway platform. This allows you to define what traffic should be controlled by security policy, and what traffic can be routed directly without inspection.

Additional connectivity and security services are subject to commercial agreement and not included with this service as standard. As part of the service, we will engage with you to provide technical guidance during the setup process.

Basic operation

The following diagram illustrates an example architecture, whereby Production traffic is routed via our Security Enforcement Core (SEC) to two Cloud Service Providers (CSPs) but a separate, high-bandwidth route is available for data migration purposes. Note this is within a single routing domain with unique IP addressing used for the Migration flow:


aws
aws
Security services sold as part of core platform provision
Other network connections (sold as part of core platform provision)
Transit-only Connection
Platform Connection
Data centre

The above diagram illustrates that Production traffic (in grey) is secured and subject to inspection, whereas Migration traffic (in green) is not subject to security policy. Note that, whilst we allow traffic to be routed to multiple Production CSPs via the Cloud Gateway SEC, this service limits the number of cloud connections to a single destination.

Transit-only Connectivity should be considered a separate service that does not impact your core platform deployment, even though traffic may originate from the same Data Centre presence. Transit-only Connectivity does not affect the bandwidth throughput of your core platform deployment. For example, if you purchase a 100Mbps platform, and subsequently purchase a 1Gbps Transit-only Connectivity service, the core 100Mbps platform throughput will not increase to 1Gbps.

Data Centre Connectivity

At the data centre, we can re-use any connectivity that we may have already provisioned as part of your core platform offering. We can continue to use IP addressing that is already present or, alternatively, provision the service using new IP addresses.

If there isn’t already a connection to re-use, or you need additional cross-connects to be installed, we can include our Data Centre Connectivity service in our proposal and solution design, including any relevant charges.

Cloud Connectivity

We will provision Cloud Connectivity to your chosen CSP via our private on-ramp, linking your data centre connection with the cloud, and bypassing the core platform SEC. The connection to the cloud will be resilient and configured for failover. We will connect to one cloud destination only - this will need to be different from any cloud environments that your platform already connects to.

Each cloud provider has a different method to establish network connectivity. As part of the service, we will engage with you to provide technical guidance during the setup process.

As with the data centre, there cannot be any duplication of IP addressing in order for the service to work. This means we will need to connect this service to a new cloud instance. You may still be able to use the same CSP account, but we need to ensure the addressing is unique.

Depending on the CSP, there are methods to move data within your cloud environment. This will be your responsibility. We recommend speaking to your CSP about this if you're unsure.

Acceptance testing

Acceptance criteria

The acceptance criteria as part of the platform onboarding are:

- To confirm that your Cloud Service Provider can be reached
- Traffic throughout is reported via the Cloud Gateway Portal
- Failover testing between our resilient routes to the destination cloud endpoint

Exclusions

The service does not include:

- Connectivity to or from other types of network connection. The service supports Data Centre Connectivity and Cloud Connectivity only. It is not compatible with other 'Connect' pillar services. e.g. VPN Site Connectivity
- Any form of managed security service delivered via our Security Enforcement Core, such as Foundation Security, FWaaS, SWG or WAF. This service simply provides a transit service which is additional to the core managed services, for use cases such as data migration
- Connectivity to multiple endpoints. This service provides no more than a resilient high bandwidth connection from a single data centre source to a single cloud destination
- Cloud services, virtual machines or cloud storage - this service provides network connectivity only. It does not include cloud-based services including, but not limited to, cloud data storage, virtual machines or applications
- As there is no security policy governing the traffic, the service will not generate any logs to be stored. Statistics from our network monitoring tools will be used to generate simple charts on the Cloud Gateway Portal

Customer responsibilities

You are responsible for:

- Ensuring the IP addresses for each of your cloud and data centre environments are unique and do not overlap with any other IP addresses in use on the Cloud Gateway service
- Setting up and preparing the cloud environment(s) to which the service is connecting
- Providing us with the name of the CSP(s) with which you wish to connect
- Following any instructions provided by us, or the CSP to establish network connectivity. Some steps in the setup process will rely on you, including (but not limited to) acceptance of invitations, and supplying service keys
- All negotiation, contracts and costs relating to your CSP, including (but not limited to) ingress and egress charges, any gateway-related charges, application running costs and data storage costs

Cloud Gateway responsibilities

We are responsible for:

- Design, installation, configuration and testing of the service
- Monitoring of the service, with an option for either normal business hours or 24/7 support
- Providing access to the Cloud Gateway Portal (subject to the Terms of Use) for reporting upon bandwidth utilisation

Ordering and lead time

Ordering and volume

We calculate your cost on a bandwidth basis. The following bandwidth volumes are available to purchase:

- 1Gbps
- 2Gbps
- 5Gbps
- 10Gbps

You can request an increase in bandwidth volume from our Sales Team, or via the Cloud Gateway Portal. During the service contract term, you will not be able to reduce the bandwidth.

The cost will usually be calculated and quoted as a separate cost in your proposal.

Lead time

We aim to deliver this service in 5 working days, however this may be subject to our supplier lead times in some circumstances, particularly when bandwidth connectivity of 5Gbps or more is required.

Service management

Service support

We have an experienced Service Desk team who are responsible for the day-to-day operational service between you and us.

The Service Desk team's primary responsibility is to provide a single point of contact within Cloud Gateway – to which issues surrounding satisfaction of service may be escalated and resolved.

Support escalations

We strive to ensure that all incidents, service requests, or simple advice and guidance requests from our customers are fulfilled efficiently and effectively within our published timescales.

If you feel that a request is not being managed effectively or would like to escalate a particular issue, this can be raised with our Service Management team.

Complaints

We take complaints seriously and ask that any customer wishing to raise a formal complaint does so in writing to service@cloudgateway.co.uk. Full details of our complaints procedure can be found within the Cloud Gateway Customer Service Pack, which you will receive during the onboarding process.

Reporting

Various types of reports can be provided. You can request these by contacting service@cloudgateway.co.uk, or raising a ticket via the Cloud Gateway Portal. Charges may apply.

Service levels

The service levels that apply to this service are available in our Service level Agreement (SLA).

Data processing

The data processing terms that apply to this service are available in the Cloud Gateway MSA, found here: https://www.cloudgateway.co.uk/compliance/msa/.

Security arrangements

- The core platform infrastructure that supports this component service is hosted in geographically diverse UK data centres. All data remains within UK sovereignty (with exception if endpoints connect to our platform via the internet)
- We are ISO27001 and ISO9001 accredited. We are also compliant with Cyber Essentials Plus

Log storage

- All traffic logs and policy controlled events are stored in our Log Aggregation Platform (LAP)

- Logs are retained for 62 days as standard, and are used to populate graphs and visualisations in the Cloud Gateway Portal

Business continuity and disaster recovery

Cloud Gateway maintains a comprehensive approach to operational resilience, ensuring continuity of service through robust business continuity and disaster recovery planning. Our internal continuity and disaster recovery plans are reviewed and tested regularly, and staff receive training to ensure they can respond effectively to a disruption.

Our infrastructure is designed for high availability across data centres. Network component configurations are backed up regularly and can be used to recover from disruptive scenarios. Supplier relationships are governed by rigorous due diligence, including reviews of the supplier’s own continuity and recovery practices. Data centres and hosting providers, where under our selection, are selected based on secure practices and continuity capabilities. Certifications held by the supplier are reviewed, such as ISO 22301, ISO 27001, ISO 9001 and ISO 14001.

Our operational model supports full remote working, whereby all staff are equipped to operate securely from the office, home or other locations.

CLOUD GATEWAY

cloudgateway.co.uk

+44 (0)20 3870 2444

sales@cloudgateway.co.uk

Cloud Gateway
The Ministry, Borough
79 Borough Rd, London SE1 1DN