CLOUD GATEWAY

PROTECT

FIREWALL-AS-A-SERVICE (FWAAS)

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 **Firewall-as-a-Service (FWaaS)**. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

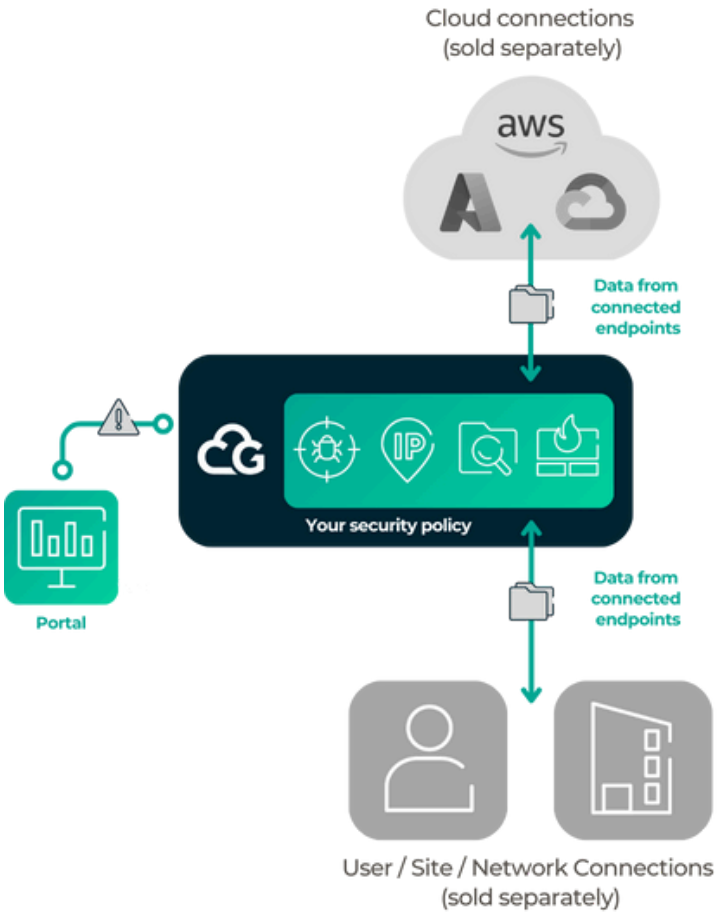
What is Firewall-as-a-Service (FWaaS)?

Firewall-as-a-Service (FWaaS) is a component service available as part of the Cloud Gateway platform. FWaaS provides configurable firewall Unified Threat Management (UTM) capabilities to manage and control the traffic passing through the platform from any/all connected endpoints.

Connectivity services are subject to commercial agreement and not included with FWaaS as standard. The rules assigned to the FWaaS are defined by you. As part of the service, we apply the security policy and manage it on your behalf.

FWaaS is comprised of:

- Layer 3 / Layer 4 Firewall
- Geo-IP Blocking & IP Reputation configurations
- Anti Virus & Anti Malware
- Intrusion Protection / Detection System (IPS / IDS)
- Deep Packet Inspection (DPI)



Basic operation

Layer 3 / Layer 4 Firewall

Layer 3 / Layer 4 firewall monitors and controls incoming and outgoing network traffic, based on predetermined security rules. It is designed to establish a barrier between your connected endpoints, whether internal or external traffic.

The below information is required in order to configure firewall policies to allow specific traffic through the platform:

- Rule Name - for example 'ACME RULE'
- Source (IP address) - for example '1.2.3.4/32'
- Destination (IP address) - for example '1.1.1.1/32'
- Service (Protocol/Port) - for example 'TCP/443'

DNS Inspection

DNS is the mechanism to resolve a human-friendly name to the computer-friendly IP address. For example, 172.217.169.4 is commonly known as www.google.com.

DNS filtering has the following features:

- Filters the DNS request based on the domain category rating
- Blocks the DNS request for the known botnet Command & Control domains
- Allows you to define their own domain category
- Enforces Google, Bing, and YouTube safe addresses for parental controls
- Allows you to define their own domain list to block or allow
- Allows you to define an IP block list to block resolved IPs that match this list
- Maps the resolved result to another IP that you define

Geo-IP blocking & IP Reputation

FWaaS can also filter and block communications from IP addresses that have a negative reputation, or that originate from specific geographic locations.

FWaaS takes data from a centralised threat intelligence service to determine where the traffic (based on IP address/ASN) is sourced. We can then configure traffic from chosen origin countries to be blocked as a group.

IP reputation uses the same threat intelligence service to determine if potentially malicious activity has been reported from a specific IP address. FWaaS can be configured to automatically block traffic from these IP addresses if required.

Anti Virus & Anti Malware

Anti Virus & Anti Malware deals with both established, lingering viral threats, and new, dangerous exploits. It utilises up-to-date threat intelligence data to ensure ongoing protection and mitigate zero-day and new exploits.

Intrusion Protection / Detection System (IPS / IDS)

Activating IDS and IPS creates a Unified Threat Management (UTM) system within the FWaaS, for complete network protection from any type of threat. IPS proactively affects traffic in flight as it traverses the network, whilst providing granular analytics that can be exported (via SIEM/SOC Integration Service) if required.

- IDS analyses and monitors network traffic for signs that indicate attackers are using a known cyberthreat to infiltrate or steal data from your network. The IDS system compares current network activity to a known threat database, to detect behaviours like security policy violations, malware, and port scanners
- IPS denies network traffic based on a predetermined security profile, if the packet being inspected represents a known security threat

Deep Packet Inspection (DPI)

By default, DPI is activated on FWaaS. To do this, we need you to deploy certificates to end user devices, to enable us to decrypt the traffic and inspect the packet.

DPI (also known as TLS intercept) allows the FWaaS to apply controls based on information within the payload, which may not otherwise be seen due to encryption.

This enables other security components to be more effective, as policies can be created based on the data inside the packet, whereas previously, we would just see an encrypted packet which may or may not include harmful intent.

Acceptance testing

Acceptance criteria

The acceptance criteria for FWaaS, as part of the platform onboarding are:

- Confirm you can reach destinations provided in the policy
- Confirm that logs are generated from the traffic passing through the policy

Exclusions

The service does not include:

- SIEM/SOC capabilities of any kind
- Management / maintenance of any other security devices you may have, which we have not provided
- Security for disconnected endpoints. Policy will only affect traffic that passes to/from endpoints connected to our platform
- Web Application Firewall (WAF) or SWG (Secure Web Gateway). These services are available as separate components of the platform

Customer responsibilities

You are responsible for:

- Providing Rule Name, Source (IP), Destination (IP) and Service (Protocol/Port) for each firewall rule that is to be applied
- For each rule provided, you should advise whether Anti Virus & Anti Malware, IPS/IDS and/or Geo-IP Blocking & IP Reputation should be enforced (per rule)
- Deploying certificates (provided by us) to end user devices to enable FWaaS to decrypt the traffic and inspect the packet (if DPI is required)
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- Ongoing maintenance, management and/or decommissioning of your other security capabilities
- Backups. You are responsible for backing up your own systems. We don't hold customer data. We will back up our own platform, and will store logs as detailed in the Log Storage section below

Cloud Gateway responsibilities

We are responsible for:

- Design, installation and configuration of FWaaS, in line with your requirements
- Application and management of firewall rules gathered during onboarding process
- Provision of certificates to you for the enablement of DPI (if required)
- Providing access to the Cloud Gateway Portal (subject to the Terms of Use)
- 24/7 proactive monitoring of the service

Ordering and lead time

Ordering and volume

We calculate your cost on a bandwidth basis. FWaaS is sold as a component of our platform, the cost will usually be combined with other components and quoted as a total service cost in the proposal. The bandwidth throughput capability of the security device will mirror the overall bandwidth capacity of the platform being purchased.

Lead time

Our Service Level Agreement (SLA) to deliver FWaaS is 5 working days. The lead time is measured from receipt of a valid Purchase Order (PO) and contract acceptance, to live service ready for any acceptance testing. The SLA timer will be paused when there is a dependency on you to provide information or input.

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 such as utilisation and traffic log reports are provided by the portal. You can request other reports 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 ISO 27001 and ISO 9001 accredited. We are also compliant with CyberEssentials 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