CLOUD GATEWAY

CONNECT

PSN CONNECT: SITE VPN TO PSN

SERVICE DEFINITION

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

About this document

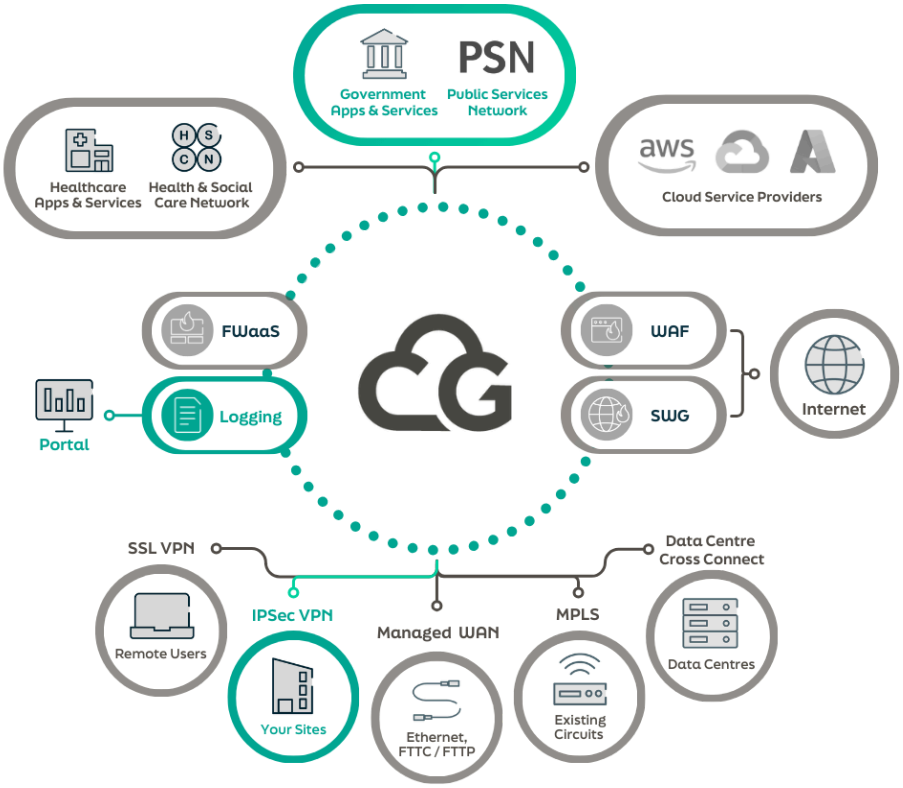
This document is designed to provide a straightforward, clear description of our **Site VPN to PSN** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is Site VPN to PSN?

Site VPN to PSN enables access to applications and resources on the Public Services Network (PSN) from one of your sites.

Using your own internet circuits and hardware, this service provides secure, scalable and resilient access to the PSN with no new devices required on site.

Traffic is secured via our Foundation Security component, which is included in this service. This set of configurable firewall capabilities manages and controls the traffic passing through the platform from the site to the PSN. By default, all traffic from the PSN to the site is blocked.



Ecosystem View

Diagram View

Basic operation

Site VPN to PSN is deployed over Cloud Gateway's core network, which provides private IP connectivity to the PSN network.

We provide you with a set of configurations and credentials, which allow you to build a pair of secure IPSec VPN tunnels from your Customer Premises Equipment (CPE) device(s), to our tenancy.

From there, we will connect the VPNs to our platform, and establish links to all the other endpoints on the network estate, depending on your needs.

To onboard, we need to know the encryption standards to be used on the IPSec VPN. This information will vary depending on the capability of your CPE.

We'll provide you with two public IP addresses for VPN termination.

If you're unsure and need assistance, we can provide guidance and support. Be aware that professional services time may carry a charge.

This service can only be used by users who require access to consume PSN services; it is not to be used to publish services to the PSN.

PSN Code of Connection (CoCo)

All organisations that require access to the PSN network are required to complete a set of policy documents making up the PSN Code of Connection. This must be completed before PSN Connectivity can be provisioned.

Information should be provided to Cloud Gateway in order for us to establish the connection.

Guidance on obtaining this can be found on our website https://www.cloudgateway.co.uk/knowledge-centre/customer-guides/psn-compliance-process/

VPN & Routing Configuration

IPSec VPN

Two IPSec VPN tunnels will be configured to each of your devices on site. These devices will remain owned and managed by you. Geographic separation gives the service resilience.

We need you to provide information about the device so that we can understand the VPN configuration parameters required. Each device is different. Ideally, the parameters will meet or exceed NCSC Foundation grade. However, if the device can't conform to these standards, we will work together to agree on an alternative method.

When using the NCSC Foundation crypto profile, Cloud Gateway prefers to use IKEv2 in place of IKEv1 (Internet Key Exchange).

Where possible, Cloud Gateway will configure a VTI (Virtual Tunnel Interface) type tunnel rather than static crypto-maps - also known as policy-based VPN. Both options are available, depending on the device capability.

Routing: VTI/BGP capable

In order to control traffic paths and allow for dynamic failover should there be any Priority 1 service affecting issues at any point during live service, BGP will be configured across the

VPN tunnels. BGP configuration parameters will dictate a primary route to our Point of Presence (PoP) for all traffic, with a secondary PoP as a backup for failover.

BGP AS-PATH prepend will be the main traffic path manipulation technique.

Improved Resilience

We can provide, on request, an enhanced resilience option by deploying multiple dual-resilient circuits to your site. Should both resilient legs of the primary circuit fail, your data traffic will be routed over a back-up circuit instead. Most commonly, we use a Layer 3 routing protocol (BGP) to automatically route traffic down the secondary link.

Within a single resilient circuit, the failover between one route and another is near-instant. When failing over between two separate circuits, a short service outage may be experienced. Traffic will not queue during this period.

Please speak with your account representative if you would like to find out more about improved resilience options.

Connecting to the PSN

PSN Connectivity connects our platform tenancy to the PSN networks. We can connect you to both PSN Assured (PSN-A) and PSN Protect (PSN-P).

Our PSN Connectivity Service has been through the PSN Assurance process, specifically Cabinet Office PSN-Compliance offering SRV_0454.

Cloud Gateway supports the connection of a customer via our Site to PSN service remote access service (SSL VPN), Internet IPSec VPN or NNI to their own virtualized instance of the Security Enforcement Core (SEC), with onward connection to AWS, Internet, other cloud providers and the proposed PSN connection. All connectivity goes through the SEC and must be configured to allow onward connections.

IP Addressing

Details of IP connectivity and addressing schemes for Site VPN to PSN are defined below:

- Site to PSN VPN traffic will be NAT translated to an allocated Cloud Gateway PSN IP (for PSN outbound access).

This service can support connectivity from your remote site to the PSN (outbound, for consuming PSN services). For inbound PSN connectivity, a different service will be required that allows the hosting of PSN facing services. Please ask us for details.

Security arrangements

A Security Incident is an event that compromises the confidentiality, integrity, or availability of information or information systems. It typically involves unauthorised access, use, disclosure, modification, or destruction of data, or interference with system operations.

Where network vulnerabilities are identified, Cloud Gateway will utilise its vulnerability management process and aim to address the vulnerability within the following timescales:

Severity	Base Score (CVE)	Remediation Target
None	0	N/A
Low	0.1 - 3.9	60 days
Medium	4.0 - 6.9	60 days
High	7.0 - 8.9	30 days
Critical	9.0 - 10	14 days

Foundation Security

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 site.

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'*

Acceptance testing

Acceptance criteria

The acceptance criteria for Site VPN to PSN, as part of the platform onboarding are:

- Basic connectivity testing from your Site to PSN endpoint(s)
- Failover test between Primary and Secondary VPN connection

Exclusions

The service does not include:

- Code of Connection. Cloud Gateway have a PSN certificate themselves as a PSN connectivity provider, you will require your own PSN certificate to access the PSN too.
- Internet or MPLS connectivity
- Hardware
- The licensing or right-to-use PSN applications
- When purchasing a Remote Access to PSN, you will receive a lighter version of the Cloud Gateway portal, with some capability restrictions. Therefore some portal features are excluded from this service.

Customer responsibilities

You are responsible for:

- Providing details of services that are required for traffic to PSN. We'll capture this during our engagement with you
- Providing a PSN connection compliance certificate to Cloud Gateway. This document proves you have completed the PSN CoCo
- Configuring the IPSec VPN tunnels on your own device(s) in accordance with the credentials we provide and any instructions we might give you
- Management of your own CPE (routing and firewall devices etc) located at your site
- Ensuring that your CPE devices are correctly configured for failover
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- Manually updating prefixes and detecting failures of VPN tunnels across the internet, if using non BGP/VTI routing configuration, and notifying Cloud Gateway of any updates made.
- Providing Rule Name, Source (IP), Destination (IP) and Service (Protocol/Port) for each firewall rule that is to be applied
- 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:

- Resilient IP connectivity to the PSN-A or PSN-P
- Ensuring you've completed the PSN CoCo prior to live service commencing
- All IP routing including failover and dynamic routing
- 24/7 proactive monitoring of the service
- Where network vulnerabilities are identified, Cloud Gateway will utilise its vulnerability management process and aim to address the vulnerability in accordance with the Security arrangements section
- Application and management of firewall rules gathered during onboarding process
- Providing VPN credentials and configuration instructions to you
- Providing access to a pair of highly available VPN endpoints
- Providing access to the Cloud Gateway Portal (subject to the Terms of Use)

Ordering and lead time

Ordering and volume

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

- 10Mbps
- 25Mbps
- 50Mbps

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 volume.

A standard service request charge applies to PSN services requiring a firewall change. A standard Service Request charge will also apply if you wish to remove access to any PSN services.

Lead time

Our Service Level Agreement (SLA) to deliver the service 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. Please be aware that third parties are involved in the process of you obtaining a PSN compliance certificate, therefore we recommend starting this process as early as possible to mitigate any risk of delay to your service provision. The SLA timer will be paused when there is a dependency on you or external parties to provide information or input.

Service management

Secure service administration

Secure service administration is carried out by appropriately cleared Service and Technical professionals, with clearance levels such as BPSS, SC or NPPV3 depending on client requirements.

Role separation is maintained to ensure individuals access only the information necessary for their duties.

Changes are managed using systems including the Service Management Platform and specialised platforms for technical components. A dedicated Service Desk team engages with both the system and end users, working alongside the engineering team to investigate issues and implement solutions.

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 populated via the Cloud Gateway Portal, alternatively they can be provided by our Service Desk. 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 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