CLOUD GATEWAY

CONNECT

HEALTH CONNECT: SITE VPN TO HSCN

SERVICE DEFINITION

V2.0
Issue Date: 10/07/2025
Commercial in Confidence

About this document

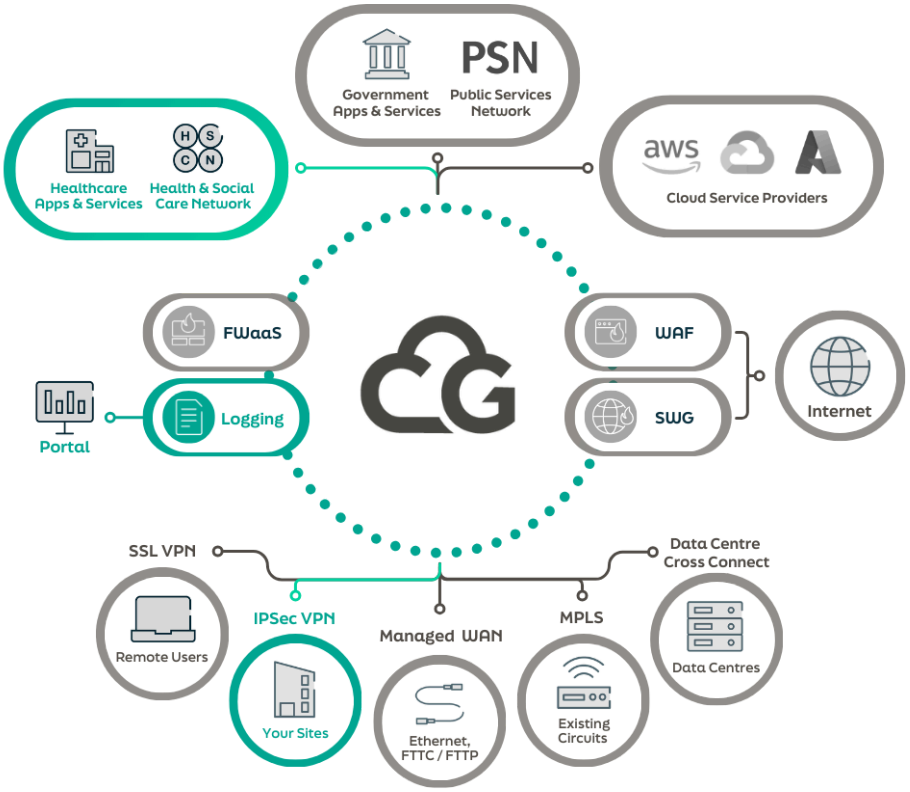
This document provides a straightforward, clear description of our **Site VPN to HSCN service**. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is Site VPN to HSCN?

Site VPN to HSCN enables access to applications and resources on the Health and Social Care Network (HSCN) from one of your sites.

Using your own internet circuits and hardware, this service provides secure, scalable and resilient access to the HSCN 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 HSCN to the site.



Ecosystem View

Diagram View

Basic operation

Site VPN to HSCN is deployed over Cloud Gateway's core network, which provides private IP connectivity to the HSCN 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. It's important that your IP schema is unique within the network and doesn't overlap with other services.

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 remote users who require access to consume HSCN services; it is not to be used to publish services to the HSCN.

ODS Code and Connection Agreement

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

Further information can be found here.

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. One of the tunnels will terminate in our London tenancy, the other will terminate in Manchester. 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 grade, 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 recommend the provision of multiple circuits to sites that require enhanced resilience and availability. Should the primary circuit fail, your data traffic will be routed over the back-up circuit instead. Most commonly, we use Layer 3 routing protocol to automatically route traffic down the secondary link.

For the majority of circuit combinations, an outage of up to 90 seconds may be experienced as the network detects failure and routes traffic via the alternative connection.

Connecting to the HSCN

We provide an IP connection to the HSCN network in line with the HSCN Compliance Framework.

IP Addressing

Details of IP addressing schemes for HSCN Connectivity are defined below:

1. You request an IP range (RFC1918) from NHS Digital or you may already have RFC1918 allocated by NHS Digital
2. We can use your RIPE range to advertise into HSCN (publically unique address from RIPE)
3. We can provide IP maximum of 1 (used for NAT into HSCN)

Note: where public RIPE addressing is allocated for use on HSCN, that address range must not be reachable via the public internet. The address block must not be dual allocated for use on both the public internet and the HSCN network.

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

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 HSCN, as part of the platform onboarding are:

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

Exclusions

The service does not include:

- Internet or MPLS connectivity
- When purchasing a Site VPN to HSCN, 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:

- Completing and evidencing the HSCN Connection Agreement and ODS Code
- Provision of IP addresses and/or FQDN (Fully Qualified Domain Name) of HSCN services that you require access to
- Requesting an IP address from NHS Digital if using more than one IP
- 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 the your sites
- Ensuring that your CPE devices are correctly configured for failover
- Ensuring there is no overlapping IP addressing between any networks connecting to the service
- 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
- 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:

- Ensuring our HSCN IP Connectivity is Resilient and ready for you to connect to
- Ensuring you've completed the HSCN Connection agreement prior to live service commencing
- All IP routing including failover and dynamic routing
- 24/7 proactive monitoring of the service
- Application and management of firewall rules gathered during onboarding process
- Providing 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 HSCN services requiring a firewall change. A standard Service Request charge will also apply if you wish to remove access to any HSCN 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. 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 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 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