REDCENTRIC

MANAGED IP-VPN GLOBAL SERVICE SERVICE DEFINITION

SD036 V5.0
Issue Date 31st May 2018

redcentric
business technology. managed.

1) SERVICE OVERVIEW

1.1) SERVICE OVERVIEW

The Redcentric Managed IP-VPN Global Service represents one of the connectivity options within the Redcentric Managed IP-VPN connectivity portfolio. It is aimed at businesses wishing to connect offices, data centres, disaster recovery sites etc. in non-UK locations to the rest of the UK corporate network. The Managed IP-VPN Global Service includes a high specification terminating router that acts as the demarcation point for the bandwidth service(s) delivered to site.

2) SERVICE DESCRIPTION

2.1) SERVICE DESIGN

Various delivery mechanisms are deployed which are largely determined by the availability of services from the in-country communications provider.

Redcentric typically deploys the Managed IP-VPN Global Service to a particular international location using one of the technical solutions detailed below. Details of the technical solution proposed for each international site will be provided in the Statement of Work for the Redcentric Managed IP-VPN Global Service.

2.1.1) Point-to-point circuit between the Customer's international site and the Redcentric core:

Redcentric sources a point-to-point circuit between the Customer's international site and the Redcentric core. Customer data from the international site traverses the supplier's network and is delivered to Redcentric's UK core. The number of bandwidth services available is determined by the circuit technology and the supplier's offering. The bandwidth across the supplier's network may be contended or uncontended. Traffic between two international Customer sites goes via the Redcentric UK core. A piece of Redcentric equipment (CPE – Customer Premises Equipment) is deployed on the Customer's premises and forms the demarcation of bandwidth services. The CPE is managed and polled by Redcentric so that failures are identified quickly.

2.1.2) Global packet-switched IP network between Customer Global site and Redcentric core:

Redcentric sources a private Internet Protocol (IP) traffic path between the Customer's International site and the Redcentric core. Customer data from the international site traverses the supplier's IP network and is delivered to Redcentric's UK core. The number of bandwidth services available is determined by the end circuit technology and the supplier's offering. The bandwidth across the network may be contended or uncontended. Traffic between two international Customer sites goes either directly or via the Redcentric UK core dependent upon design. Managed CPE is installed on the Customer premises and forms the demarcation for the bandwidth service(s). The CPE is polled by Redcentric so that failures are identified quickly.

2.1.3) Internet delivered to international Site with secured tunnel over Internet to the Redcentric core:

Redcentric uses a local supplier to provide an Internet connection at the Customer's international site. Customer data from the international location is encrypted as it traverses the Internet, and unencrypted as it enters the private IP network of a Redcentric supplier. The traffic is passed over the supplier's IP network and delivered to Redcentric's UK core. In most cases, Virtual Private Network (VPN) is the only bandwidth service available. Traffic between two international Customer sites would either go directly or via the Redcentric UK core dependent upon design. A Redcentric managed device is installed on the Customer premises and forms the demarcation for the bandwidth service(s).

2.2) SERVICE DELIVERY & LEAD TIMES

Delivery timescale for the Managed IP-VPN Global Service is determined by the in-country supplier and largely depends on existing infrastructure. Details of the anticipated delivery timescales will be provided in the Statement of Work for the Managed IP-VPN Global Service.

Two options exist for CPE installation:

- Redcentric will ship the CPE to the Customer's preferred UK site for the Customer to onward ship and self-install (with telephone assistance from Redcentric engineering staff during UK office hours).
- A Redcentric partner installs the CPE at the Customer's international site.

Details of the CPE deployment method will be provided in the Statement of Work for the Managed IP-VPN Global Service.

2.3) FAULTY CPE REPLACEMENT

Two options exist for faulty CPE replacement:

- Redcentric will ship a replacement, pre-configured unit to the Customer's preferred UK site for the Customer to onward ship and change-out. It is the Customer's responsibility to return faulty equipment back to Redcentric's UK head-office. The target timeframe for delivery of a replacement unit to the Customer's UK site is 24 hours.
- A Redcentric partner replaces faulty CPE at the Customer's international site.

Details of the faulty CPE replacement option will be provided in the Statement of Work for the Managed IP-VPN Global Service.

3) IMPLEMENTATION AND ACCEPTANCE

3.1) ACCEPTANCE CRITERIA

The following acceptance criteria will be demonstrated during the service delivery process and the Customer's signed approval will signify that the service as described in this Service Definition is ready for use:

- Check the LAN connection to the CPE for speed and duplex mismatches and errors (where possible).
- Test IP connectivity by pinging devices on remote sites
- Failover testing where resilient solution is offered and testing possible

4) SERVICE LEVELS AND SERVICE CREDITS

4.1) SERVICE LEVELS

The Service Level applicable to the Managed IP-VPN Global Service is as follows:

Service Level: Availability **Measurement Period: Month**	
Service Level	Varies according to the service level offered by the in-country supplier. By default, no Availability Service Level is offered. However, where an Availability Service Level is offered for specific connections, the applicable Availability Service Level will be provided in the Statement of Work for the Managed IP-VPN Global Service.

4.2) FLOOR SERVICE LEVEL

By default, no Floor Service Level is offered. However, where a Floor Level is offered on specific connections, the applicable Floor Service Level will be provided in the Statement of Work for the Managed IP-VPN Global Service.

4.3) SERVICE CREDITS

The Service Credits applicable to the Managed IP-VPN Global Service will be provided in the Statement of Work for the Managed IP-VPN Global Service.

5) DATA PROCESSING

5.1) DATA PROCESSING SCOPE

- The Managed IP-VPN Global Service facilitates secure transport of IP packets between locations.
- The Managed IP-VPN Global Service does not involve any storage or backing up of data.

5.2) DATA STORAGE AND ENCRYPTION

- Depending on the technical solution, Redcentric may deploy industry standard encryption protocols to help keep user traffic traversing shared or public connections private.
- Redcentric does not capture, inspect, analyse, store or share the customer's traffic/data under normal circumstances.
- Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the customer's traffic in order to investigate and diagnose a very specific problem, e.g. to help resolve a problem relating to IP packet corruption. Such diagnosis would involve the examination of a small sample of IP packets.

5.3) DATA PROCESSING DECISIONS

- Redcentric does not make any data processing decisions in relation to the Managed IP-VPN Global Service. Any processing of data over Customer systems when using the Managed IP-VPN Global Service for transit is instigated, configured and managed by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Managed IP-VPN Global Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4) SUB-PROCESSORS

- Customer data may traverse 3rd party, shared or public networks where Redcentric has limited or no direct control of data integrity, data confidentiality and/or reliability. Consequently for some designs, the Managed IP-VPN Global service makes use of data encryption to help maintain customer data confidentiality and integrity.
- No other third parties are involved in delivering the Managed IP-VPN Global Service, and there are no sub-processors appointed by Redcentric.

5.5) CUSTOMER ACCESS TO DATA

- The Customer controls its own platforms which use the Managed IP-VPN Global Service to carry data, and the Customer therefore has full access to its own data.

5.6) SECURITY ARRANGEMENTS AND OPTIONS

- The core Infrastructure delivering the Managed IP-VPN Global Service is hosted at both Redcentric and third party locations. All such locations meet physical security standard ISO27002 section 11.1 or equivalent.

HARROGATE (HEAD OFFICE)

Central House
Beckwith Knowle
Harrogate
HG3 1UG

THEALE

2 Commerce Park
Brunel Road
Theale
Reading
RG7 4AB

CAMBRIDGE

Newton House
Cambridge Business Park
Cowley Road
Cambridge
CB4 0WZ

READING

3-5 Worton Drive
Reading
RG2 0TG

LONDON

Lifeline House
80 Clifton Street
London
EC2A 4HB

HYDE

Unit B
SK14 Industrial Park
Broadway
Hyde
SK14 4QF

INDIA

606-611, 6th Floor
Manjeera Trinity Corporate
JNTU – Hitech City Road
Kukatpally, Hyderabad – 72

0800 983 2522
sayhello@redcentricplc.com
www.redcentricplc.com

redcentric
business technology. managed.

bsi.
ISO 9001 Quality Management FS 603185
ISO 22301 Business Continuity Management BCMS 603194
ISO/IEC 27001 Information Security Management IS 603187
ISO/IEC 20000-1 Information Technology Service Management ITMS 668453