Customer VPN VOIP Service

Overview

Magrathea can now offer Virtual Private Network (VPN) connectivity service to existing clients. The offering comprises of two dedicated client facing VPN routers located not only at different geographical locations, but also at different datacentre partners, to ensure the best level of resilience into the Magrathea network.

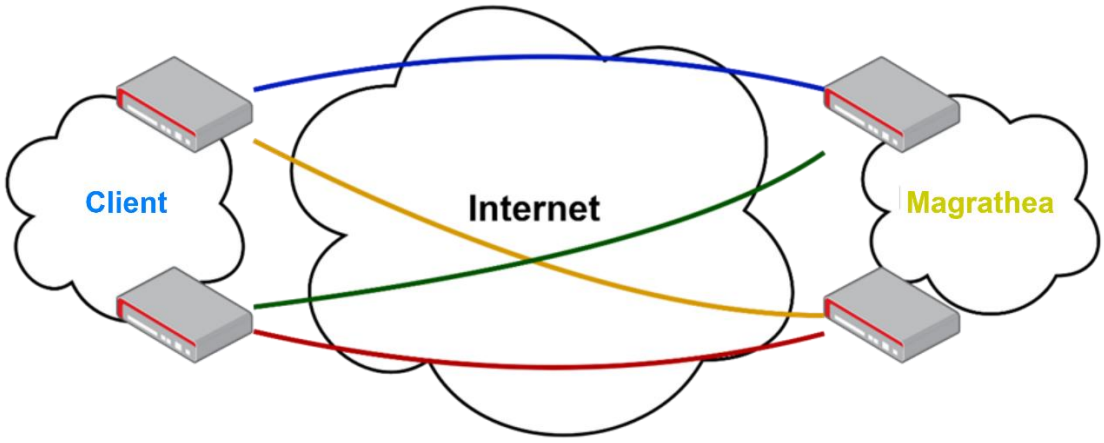
The service comprises of having a secure VPN connection (known as a tunnel) between the customer network and the Magrathea network, in order to route calls over the secure tunnel.

Although the traffic will still be routed over a public link, i.e. the Internet, using a VPN tunnel ensures that all traffic between Magrathea (one side of the tunnel) and the client (the other side of the tunnel) is encrypted, ensuring extra security on calls.

To ensure that the solution's resilience is maintained between both the Magrathea and the client's networks, Magrathea recommends where possible, that the customer also creates two unique VPN tunnels from/to two separate VPN appliances on the client's side. One should connect to each Magrathea VPN unit, thereby ensuring that the service remains operational should one of the tunnels/units experience any issues or outages.

Magrathea VPN tunnel setup revolves around IPsec and VPN tunnels IP routing over BGP (Border Gateway Protocol).

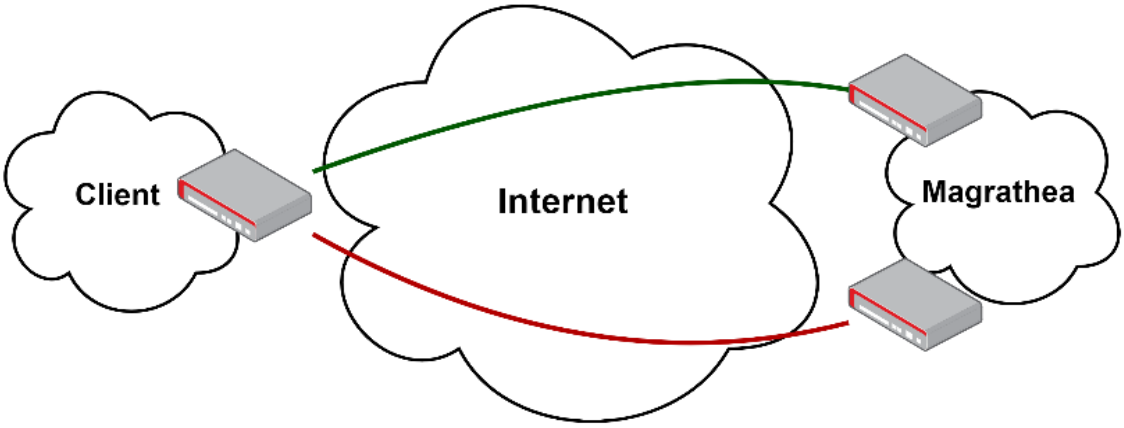
Below is a simple diagram of the ideal setup:



The grey boxes represent the independent VPN Routers on both the customer and Magrathea side and the coloured lines represent the individual VPN Tunnels that run between each of them.

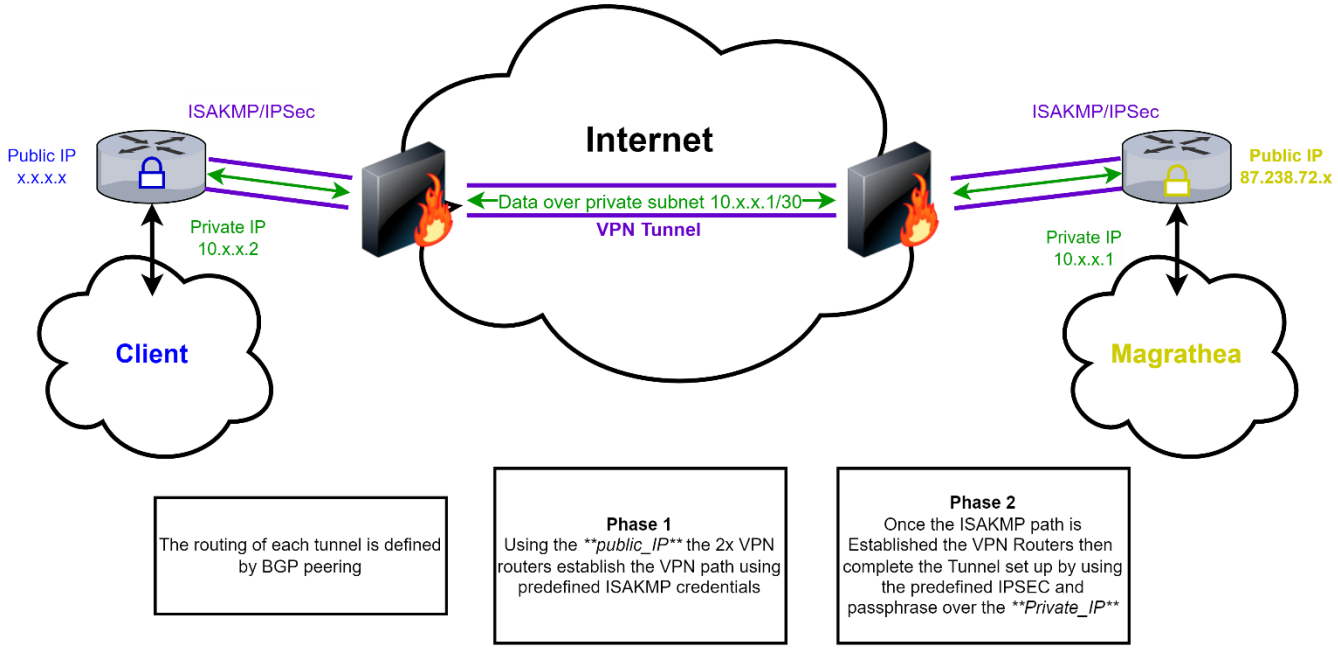
Single Router VPN tunnel connection

A single site VPN tunnel connection is also possible, therefore if the client only has a single VPN appliance on their side, two VPN tunnels would be configured from the client site, one to **each** of Magrathea VPN routers. This solution does not allow for redundancy on the customer side, so a failure of the VPN tunnels due to outage or failure of client's VPN appliance, will cause the traffic over the VPN tunnels to stop flowing, potentially causing interruption to call services.



Basic VPN tunnel connection

This is a simple diagram of the establishment of a VPN Tunnel:



Requirements

In order to set up the VPN tunnels the following information must be provided:

- The client will need to supply their endpoint (public) **static** IP address(es) that they wish to use to establish the VPN tunnels with Magrathea. These will be single IP addresses, normally IPv4 on the form of a.b.c.d. e.g - **87.238.73.137**

- The client needs to provide their BGP details, such as their AS name and Confederation ID, in order for Magrathea to configure BGP routing to occur over the VPN tunnels once they are established. e.g – **ASxxxxx – Confederation ID xxxxx**

- Magrathea and the client will need to use the same sets of encryption types in order to establish a successful VPN connection

  There are two phases of the VPN tunnel:

  Phase 1 – establishing the VPN tunnel (ISAKMP Internet Security Association and Key Management Protocol)

  Phase 2 – Encryption of data via the Tunnel. (IPSEC data encryption)

  As standard we suggest the following however alternatives can be negotiated if required:

  ISAKMP: SHA1 and AES128 encryption, with group 2.
  IPsec: SHA256 and AES256 encryption

Once the above is confirmed Magrathea will provide the following:

- Magrathea will provide the endpoint (public) **static** IP address for each of the VPN devices on the Magrathea network so the client can configure the VPN tunnels on their equipment.

- Magrathea will provide our BGP details, including the AS name and Confederation ID.

- Magrathea will create a unique passphrase to be used as part of the VPN validation
- Magrathea will create a new Private IP subnet for each VPN tunnel, this only needs to be a /30 range as only two IPs are needed (one IP on our side and one on the customers). A separate subnet needs to be allocated for each VPN tunnel.

- Magrathea will confirm and assist where possible in regards to the establishment of the VPN tunnels.

**Unfortunately, Magrathea are unable to provide specific configuration details for the client's equipment due to the vast array of VPN devices currently available, but we will assist and provide guidelines.*

Pricing

Initial set up fee: Please contact sales@magrathea-telecom.co.uk for pricing.
Ongoing charges: No ongoing charges
Additional support: If email/telephone support is required above a reasonable level required to set up this service, we can offer consultancy at £150 plus VAT per hour.
This is only available during normal working hours and support will be offered in line with Category B and C description on our SLA documentation. Please contact support@magrathea-telecom.co.uk to discuss if additional support is required.