

NETWORK SERVICES TECHNICAL SPECIFICATIONS

Data transfer measurement & reporting	
Measurement	<p>Data transfer measurements are taken on the border switches at layer 3 in the network stack.</p> <p>Data transfer is measured on a per IP address basis for both inbound and outbound transfer.</p> <p>Data transfer is measured in bytes. A Kilobyte is defined as 1024 Bytes. A megabyte is defined as 1024 Kilobytes. A Gigabyte is defined as 1000 Megabytes.</p>
Calculation	<p>Data transfer that leaves enters or leaves the Anchor network is counted by the measuring system. Measurement of traffic occurs at our border routers to prevent local traffic being counted.</p>
Reporting	<p>An authenticated web based interface provides reporting on data usage for all allocated IP addresses.</p> <p>The following reports are provided for inbound/outbound transfer:</p> <ul style="list-style-type: none"> • Total daily summary • Total monthly summary • Daily per IP address • Monthly per IP address <p>CSV exports of all of the above reports are provided. A list of allocated IP addresses is provided.</p>
Network connection capacity	
Local network	100 Mbps switched network
Upstream providers	Primus: 100 Mbps, Uecomm: 100 Mbps, Pipe: 100 Mbps
Firewall services (Shared secure port, private secure port, secure segment)	
Firewall infrastructure	<p>The shared secure port is deployed on a redundant high availability Linux based device using IP tables. The firewall performs stateful packet inspection</p>
Firewall rules	<p>The default policy is to block all requests. Ports are only opened as explicitly requested by the client. Any valid IP tables configuration can be specified including source and destination based restrictions.</p> <p>Limits apply on the total number of rules that can be defined:</p> <ul style="list-style-type: none"> • Shared secure port: 50 rules • Private secure port: 100 rules • Secure segment: 50 rules multiplied by the number of servers provisioned.
Firewall rule changes	<p>Firewall rule change requests must be submitted to Anchor support.</p> <p>All changes are completed overnight to reduce the risk of service outage</p> <p>A maximum of 20 firewall rule changes per month can be made</p>

VPN Endpoint	
Protocols supported	<p>Support is provided for any remote device that can communicate with a standards based IPSec or L2TP device. This includes most firewalls and routers produced by most major manufacturers.</p> <p>IPSec support is only provided for X509 certificates. No support is provided for pre-shared key configurations.</p>
Implementation	Endpoints are terminated against a redundant high availability device running OpenSwan
Support services	Anchor is responsible for generation and provision of certificates. Installation and configuration of our endpoint. Provision of configuration details, advice and trouble shooting of the remote endpoint up until the point that a tunnel is established.
Load balancing	
Implementation	<p>The load balancing service is implemented on a redundant high availability device using the Linux Virtual Server (LVS) Project in conjunction with Ldirectord.</p> <p>The state of each node in the load balanced configuration is polled periodically (default is 10 seconds).</p>
IP Allocation	A public IP address is provided for the load balanced interface and each target interface.
Traffic distribution algorithms supported	Round-Robin Scheduling, Weighted Round-Robin Scheduling, Least-Connection Scheduling, Weighted Least-Connection Scheduling, Locality-Based Least-Connection Scheduling, Locality-Based Least-Connection with Replication Scheduling, Destination Hashing Scheduling, Source Hashing Scheduling, Shortest Expected Delay Scheduling, Never Queue Scheduling
Client requirements	<p>The client must provide Anchor with a URL which accurately describes the state of each server being load balanced to decide if the node is active.</p> <p>The client is requested to notify Anchor of any scheduled downtime on any nodes to avoid triggering false monitoring alerts.</p>