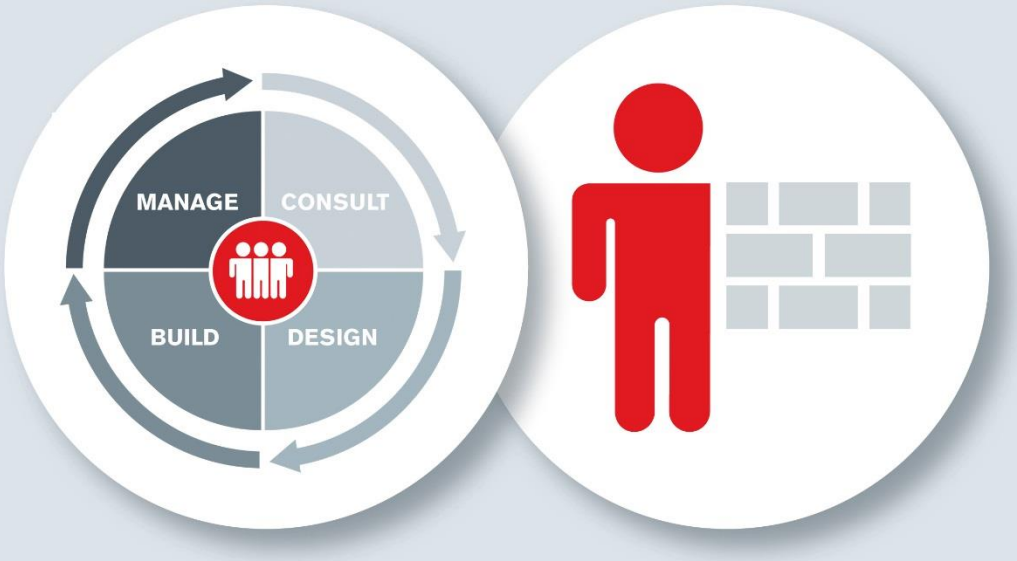
Claranet Service Description



Managed Firewall

Claranet provides a Managed Firewall service for both physical and virtual environments. We will provide you with a firewall and configure it to your specifications. Your service is monitored, measured on availability and supported 24x7.

Version 10.8

claranet
hosting | applications | networks

helping our customers
do amazing things

Contents

Service Description

This Service Description describes the service Claranet provides and details your responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and all terms used within this document are in accordance with the terms to be found in the Master Services Agreement.

Service overview

Claranet provides a Managed Firewall service for both physical and virtual environments. Claranet can provide dedicated platform firewall on a highly available shared virtualised firewall cluster and also physical firewall appliances to be installed either on your own premises or within our datacentres.

You discuss your requirements with Claranet's design team so we can ensure you have selected the right device, and Claranet can configure, despatch, install and maintain your appliance in accordance with the service level you require. Claranet can monitor all aspects of its function, keep you up to date on the performance levels as well as suggest how your system may benefit from any configuration changes and technological developments once it is in place. This document will take you through the various options available to you whether the firewall is part of your Managed Hosting service or part of a connectivity requirement and will outline exactly what each party is responsible for in the delivery of the Managed Firewall service in each of the **Consult | Design | Build | Manage** stages.

Components

Claranet provides a range of options within the Managed Firewall Service including both physical and virtual solutions. Every hosting solution requires a connection to the Internet via a direct and resilient connection to Claranet's own Autonomous System (AS) and if you are using Claranet's MPLS Service, this service can also be used to provide breakout from the MPLS network to the Internet.

Platform Firewalls

This is a service based on a platform firewall, dedicated to you, on a highly available shared virtualised firewall cluster. Claranet offer three variations of platform firewall that provide different levels of maximum traffic throughput. Details of these three options can be found in the **Appendix: Components.**

Platform firewalls provide a very cost-effective way to secure traffic and they run on a highly available Claranet platform firewall cluster. Each platform firewall is a software appliance on the Claranet platform firewall cluster. Your traffic is isolated and is not visible to any Customers.

What Claranet will do

Platform firewall: Provide a platform firewall and a connection out to the internet if required.

Loss of connection: Monitor the platform firewall for loss of connection and, in the event of a hardware failure, an appliance will be automatically restarted on another server by Claranet to ensure a fast recovery of the service in accordance with the Service Levels. Once the appliance is rebooted, any active sessions are lost. Your platform firewall is therefore not considered 'stateful'.

What you will do

Re-connection: You will re-establish a connection to the active sessions if lost. Details of how this can be achieved can be found in the **Appendix: Help and Support.**

Physical Firewalls

This service is based on a physical firewall appliance, dedicated to you and Claranet provides a range of physical firewall devices depending upon your specific requirements e.g. enhanced resiliency, throughput, performance, and specific data isolation. Full details of these options can be found in the **Appendix: Components.**

High Availability (HA) options

For each rack mountable firewall model a High-Availability (HA) option is available. In this option, two devices are deployed in the datacentre with synchronisation of the configuration, sessions and tunnels between the devices. This means that it in the event of one device failing, existing sessions are redirected to the other node with minimal loss of connection.

What Claranet will do

Physical firewall: Provide a physical firewall and a connection out to the internet if required.

Ownership: Retain ownership of the physical device throughout the contract in all instances.

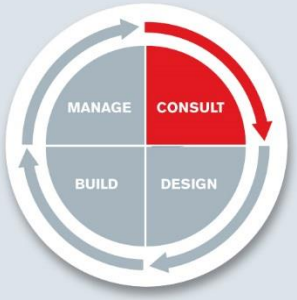
Features and functionality: Use the hardware to deliver the Service as described in this document but Claranet are not required to support all the features and functionality provided by the device vendor.

What you will do

Minimum specification: You will be responsible for defining any minimum specification.

Non-standard firewalls: You will be responsible for supporting any non-standard firewalls. Claranet may offer support to other firewalls with different specifications via a non-standard service process

Multiple Claranet datacentres: Utilise the MPLS Service if you are looking to consume services from multiple Claranet datacentres, as the Managed Firewall service does not include bandwidth between datacentres.



Consult

Claranet's consulting process ensures that you have the all right information, the right recommendations, and the right service options available to you to achieve your business outcomes.

Understanding your business is paramount to ensuring that you have the right solution for your business outcomes. In the Consult stage, Claranet will discuss your business requirements with you prior to recommending a solution. In most cases, the Managed Firewall service is part of a larger solution involving either the Managed Hosting service or one of the Connectivity services or both. Therefore, the Consult stage for the Managed Firewall is not treated independently and will be considered when reviewing the overall service and solution.

Depending on the complexity of requirements, one or more workshops between you and Claranet may be arranged in order to outline your requirements. These may be conducted by Solutions Consultants, Strategy Consultants, Solutions Architects and Enterprise Architects who will be applied at our discretion. It is in everyone's interests to ensure that the proposed solution will meet your requirements and one of our first roles is to focus on your business, your IT requirements and to produce a high level scoping report, the High Level Options Analysis. This will allow you to make an informed choice as to the recommended path.

What Claranet will do

Deliverable: The High Level Options Analysis report. A short, high-level scoping document.

High Level Options Analysis

What Claranet will do

Time to complete: The High Level Options Analysis is a consulting based service and is included up to a maximum of 2 days' work at Claranet's discretion. In some instances, the work required to produce a High Level Options Analysis could extend beyond this e.g. where the requirements need extensive discussion or the options are particularly complex. If this is the case, Claranet will agree with you a charge for the additional work required to produce a High Level Options Analysis to establish the requirement.

Technical Design: Technical work beyond this falls outside of the scope of the High Level Options Analysis and is carried out in the Design phase.

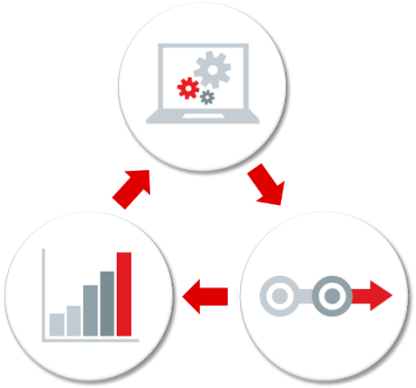
What you will do

Information sharing: Provide any requested information to allow Claranet to deliver a High Level Options Analysis. This will include full details of on-going technical contacts within your organisation. This information will form the basis of the Initial Configuration, so it is your responsibility to ensure the information provided is correct.

Packaged Consulting

Claranet has a number of pre-packaged assessments and audits that help to outline your readiness in respect of particular IT options. It may be that the completion of one or more of these packaged consultancy engagements is made as a result of the recommendations

made in the High Level Options Analysis report. The completion of these assessments follow a general pattern:



Current State
Performing a real life assessment of your current environment and understanding where your business needs, and your current technical setup, may diverge.

Future State
A vision of the future for your company, taking into account strengths, weaknesses, opportunities and threats.

Transformation
The enablement program to be undertaken as a priority to advance your organisation to the desired level of maturity.

What Claranet will do

Assessment options:

- Linux Infrastructure Maturity Assessment (LIMA)
- Infrastructure Maturity Assessment (IMA)
- Cloud Readiness Assessment
- Open Source Assessment

Pricing: This additional packaged consulting service is optional and is a chargeable event. Claranet provides three prices for each assessment depending on the size of your company and the complexity of your requirements: Small / Medium / Large.

Consulting

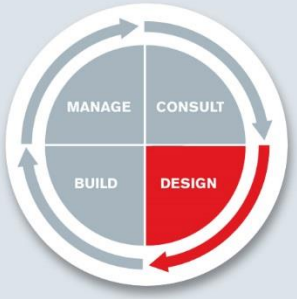
A packaged consulting approach can be of significant help to many organisations. However, Claranet also provide a specialist consulting service that can be used at any time (including pre-contract) to help you in areas outside of the packaged offering. This engagement is specific to you and can cover any area that is needed with regard to your business and technology.

What Claranet will do

Specialist consulting: Provide a range of specialist expertise in a variety of areas. This includes a detailed focus on your business in order to ascertain the scoping requirement or where you are unsure as to the direction your business should take in the ever-changing IT environment.

Outcomes: Provide a full and detailed report on your available options along with recommendations of the next steps to take.

Pricing: This additional consulting service is optional and is a chargeable event and is based on a consultancy day rate.



Design

The Claranet Managed Firewall Service is often included in a Claranet hosting or network solution. The choice as to which firewall service will meet your requirements is made in the Design stage.

The Managed Firewall service is part of a larger solution, either Managed Hosting or Connectivity. The Design stage of the larger solution, therefore encompasses any design features associated with the Managed Firewall service.

Claranet will undertake to identify which elements and options are required and how they should be configured to meet your requirements. Your solution will normally require the utilisation of a Solution Architect and the output of this process is a proposal document and a Statement of Works (SoW). This forms part of your agreement and will provide the technical specifications for your solution.

Typically the technical design of the solution will be completed prior to order, but further detail can be refined once the order has been placed. Any technical design work is conducted on a 'reasonable commercial endeavours' basis and will be based on assumptions made by you and Claranet.

What Claranet will do

Deliverable: A proposal document and a Statement of Works which forms part of your agreement which is detailed enough to allow a full quotation.

Standard level of design work: Produce design work on your proposed solution at a level commensurate with that of the market. It will be sufficient to allow further decisions to be made and may include input from a Claranet Sales Specialist. However, fully specifying a complex complete new hosting infrastructure is not part of the standard design work. If this is required at this stage, it can be completed using Claranet's Specialist Solution Design service.

What Claranet will do

Additional components: In the event that additional components are required outside of the SoW, Claranet will levy additional charges for the implementation and management of the modified solution. If this is the case, a new proposal and SoW document is produced. This must then be signed by you to acknowledge and accept the changes before any work is performed.

Additional load: Identify any substantial increment in either traffic or load on your solution. Claranet may also recommend that additional components are purchased to support the changes. If these recommendations are not taken this may affect your SLA and Service Credits.

In the **Design** stage, Claranet will ask you to complete a Firewall Policy Survey. The completion of this document is your responsibility and Claranet is not responsible for ensuring that the firewall policy options you choose are suitable for your internal application. However, Claranet is able to assist in designing a firewall policy suitable for your application. The Managed Firewall service is generally part of a hosting or network solution and this often provides for initial consultation etc. Additional support details can be found in the **Manage** section.

Sales specialist

As part of your standard Managed Hosting Service, or your Connectivity service, Claranet provides a sales specialist who has detailed knowledge within the particular field, or within your own specialist vertical industry, and will support your Account Manager and Solutions Architect with your proposal. Part of their role is also to help ensure that the proposed technical solution will fit your business and achieve the outcomes you are looking for.

Specialist solution design

At times, the complexity of your solution design will require additional or specialist design work in order to detail your requirements.

What Claranet will do

Specialist level of design work: Produce technical design work on your proposed solution in order to specify your firewall requirements fully. This may be completed by a Solutions Architect or a Claranet Technical Specialist in that particular field.

Pricing: This additional specialist solution design service is optional and is a chargeable event and is based on a day rate for the service.

The Firewall Policy Survey

Once your order is complete, Claranet's Project Office will send you a Firewall Policy Survey to complete. A copy of this Firewall Policy Survey is available.

What Claranet will do

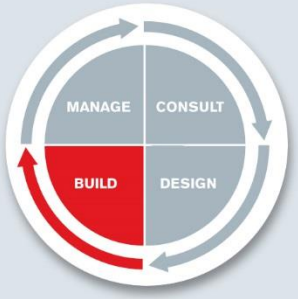
Default configuration: Implement a default configuration policy to your firewall if the Firewall Policy Survey is not completed. Details of the default configuration can be found in the **Appendix: Default configuration.**

Order completion: Commence the **Build** phase of the Managed Firewall service once your signed order is received.

What you will do

Minimum specification: Ensure that any minimum specification requirements are clearly and accurately completed in the Firewall Policy Survey as soon as possible.

Firewall policy options: Ensure that the firewall policy options you choose are suitable for your internal application.



Build

Once your order has been placed, Claranet will perform installation and configuration activities to build your solution in the Claranet datacentre.

The **Build** section covers the steps involving the configuration and installation of the Managed Firewall Service as part of the Managed Hosting or Connectivity services according to the agreed specifications. At the completion of this phase, the service is fully tested and handed over to you as part of the Handover Document. Once accepted, any future changes will be managed as part of In-Life Management, details of which can be found in the **Manage** section.

What Claranet will do

Delivery: Assume that delivery has taken place for physical firewalls that are installed into a Claranet Datacentre, when the firewall is fully functioning and handed over to you as part of the Test and Acceptance Process. Where the firewall is to be delivered to your premises, delivery is assumed once you have taken receipt of the firewall.

Order completion: Commence the **Build** section of the Managed Firewall service once your signed order is received.

Lead times

Part of the build process is to take into account the various lead times for the firewall selected.

Table: Lead times for firewall delivery. The time is taken from the signed order being received.

Firewall	Lead Time (working days)
Customer Premise Equipment - Firewall (CPE)	15
Small to medium firewall	10
Medium firewall	15
Medium to large firewall	15
Large firewall	15
Platform firewall	5

Installation

Installation of a physical firewall

Claranet will manage the process of installations into Claranet datacentres or the shipping and configuration of firewalls to be installed in your premises. As Claranet maintain all

firewalls in a dedicated area within its datacentres, Claranet cannot make any guarantees or commitments concerning the physical proximity between separate pieces of hardware that have been allocated to you.

What Claranet will do

Installation into a Claranet datacentre: Configure the appliance according to the specification you have requested in the Firewall Policy Survey, patch it accordingly, rack-mount it in to our datacentre and provide power.

Installation into your own premises: Ship the device with your configuration applied. Once received, and the device has been installed, the setup and configuration will be completed.

What you will do

Installation into your own premises: Install the firewall in an adequate space, supply power to the appliance and connect it to a router once it has arrived at your premises.

Connectivity to your premises: Ensure that Claranet is providing your site with WAN connectivity services (Internet / MPLS / VPN) and that appropriate switching infrastructure is already in place facilitating connectivity to the Claranet Managed Firewall. Claranet does not provide or manage LAN switching at your premises.

Notification: Notify Claranet that the firewall is connected once it has been installed.

Although you will have physical access to the appliance, you must not access the management console on the firewall. Any changes that need to be made, can be requested through the In-Life Claranet Change process to avoid potential issues of conflict or loss of service.

Installation of a platform firewall

Where you require the Managed Firewall Service based around a platform firewall:

What Claranet will do

Configuring: Configure the virtual appliance according to the specification you have requested in the Firewall Policy Survey, patch it accordingly, install it into our datacentre and provide the power.

Initial Build steps

Once the signed order has been received, Claranet's Project Office will contact you to inform you of the next steps including being assigned a Project Co-ordinator and an engineer. The engineer will be responsible for configuring the firewall in accordance to the information you have completed in the Firewall Policy Survey. As the Managed Firewall Service may be part of a hosting or network solution, you may also be provided with details of a contact within Claranet's Network Implementation Team or Claranet's Hosting Implementation Team as appropriate.

What Claranet will do

Support times: Provide support between 09:00 to 17:30 weekdays, excluding Bank Holidays. Your primary contact at this stage is your Project Co-ordinator within the Project office.

Engineer support: Assign you an engineer by the Project Office who will liaise with you regarding your firewall configuration and ship the device out.

Build progress update: Maintain a progress update schedule at every milestone of the project or once every 7 days.

Configuration agreement: Claranet will contact you to establish a second window for agreement on the final configuration, testing and acceptance.

VPN Connectivity

A VPN allows multiple Customer sites in different geographic locations to exchange data in a secure and private manner.

What Claranet will do

VPN Connections: Configure a Claranet firewall to terminate Virtual Private Network (VPN) connections where necessary.

IPSEC VPN and SSL VPN: Site-to-site IPSEC VPN is included in the price of the Managed Firewall service. However, SSL VPN or IPSEC dial-up VPNs are **not** provided as part of the Managed Firewall service and are subject to set up and configuration charges.

VPN traffic performance assurances: It is **not** possible to provide assurances and warranties with respect to the performance of traffic through VPNs particularly when the VPN connects to devices not managed by Claranet. If you require stringent performance requirements, you are advised to purchase Claranet Connectivity services.

Specialist engineering

It may be that your particular setup requires additional specialist engineering work. This will be quoted individually and could include specialist change requests, work on piloting projects or prototyping. This may be part of a larger overall hosting or connectivity requirement.

What Claranet will do

Specialist engineering: Provide a quotation for specialist engineering work based on a day rate.

Project Management

Some Claranet projects are small, simple and very straightforward and the management of these is part of the normal operation carried out by your Account Manager, the Solution Architect and Project Co-ordinator who are already built into the cost of delivering your standard service. Other Claranet projects are much more complex and require more comprehensive project management to bring together the many elements that are needed including the need for a Managed Firewall service as part of the solution. Claranet is conscious of the fact that the introduction of a Claranet Project Manager is a chargeable event but will suggest this when we believe it is justifiable and necessary. In addition, it may be that only a short time needs to be spent by a Claranet Project Manager in overseeing and authorising the Claranet project e.g. at the start of the project, where the project is then managed by a Project Co-ordinator, helping to keep your costs to a minimum.

What Claranet will do

Project Management: Allocate a Claranet Project Manager who is PRINCE2 qualified who will ensure that the project is initiated, implemented, carried out and closed according to PRINCE2 methodology and will be responsible for the overall control and management of the Claranet project. Full details of this can be found in the Project Management Service Description and from your Account Manager.

Testing and acceptance

Testing

The engineer configuring your firewall service will ensure that the testing process is as transparent as possible. If actions are identified as part of this process they will be included in your delivery plan and managed to closure by your Project Co-ordinator.

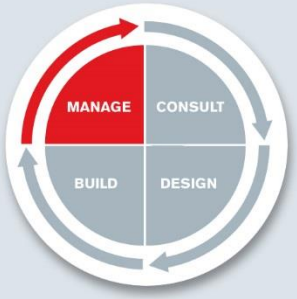
What Claranet will do

Testing: Test the firewall to ensure that it performs in terms of connectivity and speed in accordance with the Service Levels. The firewall will be connected to the internet and powered on.

Backing up the login details: Take a backup of the configuration and retain this along with details of the administration logins and password prior to acceptance.

Acceptance procedure and Handover Document

Once the firewall is installed and connected, the ongoing management is under the process of the In-Life Management process managed by our Service Operations Team. As part of the acceptance procedure, you will be provided with a Handover Document, a copy of which is available. This contains details of how to make the most of the support facilities and who to contact in case of a query or fault.



Manage

Your business is managed by our Service Operations team who provide a pro-active, ITIL aligned, service. You also have access to your customer portal, Claranet Online.

In-Life Management

A Managed Firewall is mandatory for each hosting solution and is used to secure network communications by preventing the transmission of unauthorised network traffic. The firewall policy contains a set of rules which define what types of traffic are permitted to pass through the firewall, in which direction, and through which network interfaces. Hosting servers, Internet access and MPLS networks are all connected into the firewall, and thus the firewall can then control the flow of data between them.

Additional rules can be added to the default policy, and supplementary policies can be created to separate out groups of rules. Once the firewall is up and running and the Handover Document is completed, Claranet will manage the firewall 24x7x365 in order to maintain its operation. The parameters of the ongoing management of the service and the appropriate roles and responsibilities are outlined in the areas below.

Access to the firewall

Access to firewall management interfaces and ports is carried out securely by Claranet via known and trusted IP ranges. Claranet retains all administration rights to managed firewalls and Claranet will retain control of the login accounts to the firewall.

Co-managed physical firewall

Claranet is able to provide co-managed physical firewalls. In this circumstance access is only provided locally or via a VPN.

Claranet will create a local user and group that will have limited system administrative access however you will be able to perform general firewall administration tasks such as policies and routing.

You are not permitted to change login details without approval from Claranet and so doing will void any Service Level Agreement in place.

Firewall administration will provide access to certain licenced features which may not be supported or supplied by Claranet such as SSL VPN or Unified Threat Management. If these features are activated you will be charged and no support will be provided.

Planned changes, emergency maintenance and patching

Claranet will contact you with regard to any planned maintenance. However, in order to ensure the continued operation of the service, it is necessary that rules relating to traffic routing are maintained and it may be necessary for Claranet to do this without notification to you. Similarly for security reasons, e.g. in the event that you are subject to an attack.

What Claranet will do

Notice: Provide at least five working days' notice of any planned maintenance work where an outage is expected or a reduction in the resiliency of infrastructure, wherever possible.

Supplier planned Engineering: Notify you of any supplier planned engineering works where it is likely that you will experience an outage within one day of receipt of the notification from our supplier wherever possible.

Notification: Notify your nominated contacts through two primary channels, Claranet Online and by email notification. An email is sent to the nominated contact and details are announced through the notifications in Claranet Online. The notification will contain the date and time of the maintenance, the reason, the service affected and the likely impact to you.

Problems occurring during planned maintenance: The Major Incident process will be invoked during the maintenance window where a rollback or issue mitigation process does not exist, or should the planned work extend beyond the planned maintenance window.

Emergency maintenance: Provide as much notice as possible and we will seek to ensure minimal disruption. Wherever possible, changes will be made at periods of low service utilization. It may be necessary to make changes to the configuration of your firewall, including traffic routing rules **without** prior notification to ensure the continued operation and security of the managed firewall.

Patching: Apply all critical patch updates on an as required basis. Where non-critical patches are released, Claranet can apply these at your request .Further details of the patching responsibilities and maintenance windows can be found in the Managed Hosting Service Description or the Connectivity Service Description.

Emergency outages: In some extreme cases, Claranet may require an emergency outage to rectify a problem. In such cases, Claranet will work with you to agree a mutually convenient time, but you agree that in such cases the problem cannot be rectified until the outage has taken place. These details can be maintained within Claranet Online.

What you will do

Contact list: You will be responsible for providing and maintaining the contact details including the levels of authorisation that any individuals may have. Claranet will only provide any reporting information and change requests, to those personnel in accordance with this information.

Changes requested by you

Where you require specific changes to be made to the configuration of your firewall, Claranet will be responsible for making the change as you are not permitted to access the firewall in order to change the configuration yourself. Change requests are made by raising a ticket through the Claranet Online portal and details of how to do this can be found in the **Appendix: Help and Support**.

What you will do

Co-Management: Unless specified prior to contract signing, you will have no access to change the configuration of the firewall as standard. You are responsible for any changes made, and any loss of service caused by changes are not covered under the Service Level Agreement.

Configuration printout: You can request a printout of the configuration policy of your firewall by requesting a ticket through the Claranet Online portal.

Change control process: It is your responsibility to familiarise yourself with the official Claranet change control process and to follow this process every time a change to the Service is required. Details of this process can be found in **Appendix: Help and Support.**

Change request impact: It is your responsibility to ensure that any changes will not directly cause a service outage or other disruption of the service.

Change of services: If you request a new service, a change of service type, additional users or a change in service features they must be requested via your Account Manager and may be subject to prevailing fees.

Number of change requests that can be made

You can make up to five rule change requests in each calendar month and Claranet reserve the right to charge you for any change requests that are made in excess of this amount. One change can include up to five rule amendments. A rule amendment is defined as:

a) the addition of one rule; or
b) the removal of one rule; or
c) the change to the specification of one rule

Further details on the response times and processes can be found in **Appendix: Help and Support**.

The addition of new services, a change of service type, the addition of new users or a change in service features must be requested via your Account Manager. Their contact

details can be found in the Handover Document that is provided to you once the service is live. These changes may be subject to new charges.

Monitoring of the firewall

Claranet will monitor key technical performance thresholds relating to your Managed Firewall Service 24x7x365.

Table: Technical Metrics – Performance and availability

Component	Type	Monitored By	Monitored Frequency (Minutes)	Action
Uptime / Availability	Alert	SNMP	5	Tivoli Alert raised
High CPU	Alert	SNMP	5	Tivoli Alert raised
High Memory	Alert	SNMP	5	Tivoli Alert raised
Conserve Mode	Alert	SYSLOG	5	Tivoli Alert raised
Allowed Traffic Logs	Informational	SYSLOG	Live	Log
Admin logs	Informational	SYSLOG	Live	Log
Change Logs	Informational	SYSLOG	Live	Log
CPU Graph	Informational	SNMP	5	Log
Memory Graph	Informational	SNMP	5	Log
Interface Bandwidth Graph	Informational	SNMP	5	Log
HA State Changes	Alert	SYSLOG	5	Tivoli Alert raised
System Event Logs	Informational	SYSLOG	Live	Log

When a threshold is breached

Where the monitoring system identifies that a threshold is breached, alarms are triggered to alert Claranet support staff to investigate the cause and resolve the issue.

What Claranet will do

Information delivery: Obtain the results for each of the metrics above and contact you according to your list of authorized contacts in the event that any results fall outside of the acceptable parameters. This information will also be displayed on the Claranet Online portal.

Archiving results: Retain an archive version of the monitoring results for up to 90 days which can be available to you on request through the Claranet Online portal.

Metrics exceeding the thresholds: In the event that a monitored metric exceeds the acceptable thresholds, Claranet will raise a support call to investigate the incident and contact you in accordance with the escalation details held for the firewall.

Monitoring on a non-Claranet network: Provide limited monitoring information if the firewall is installed on a non-Claranet network as Sys-logging will not be enabled. This is considered to be unsecured and Sys-logging is **not** enabled. No other monitoring will be enabled.

If a threshold is breached or a service affecting event occurs, the Claranet Operations team are notified to raise a ticket and take appropriate action to resolve the issue. This could include troubleshooting and resolving the problem, or notifying you that your application may be pushing a large amount of data. There are predefined response times to event notifications based on the severity of the issue. These are outlined below.

What Claranet will do

Severity response times: Respond to a threshold breach depending on the severity of the breach:

Major:
Claranet will acknowledge any alarms on the system within 30 minutes

Minor:
Claranet will acknowledge any alarms on the system within 60 minutes

Warning:
Claranet will acknowledge any alarms on the system within 1 day

Change to monitoring tools: Reserve the right to change its monitoring tools, methods, parameters and polling intervals over time

Where these storage thresholds have been breached for three consecutive calendar days, any downtime resulting directly or indirectly from insufficient storage will not be counted in the calculation of availability Service Levels.

Break/fix service

Claranet provides a break/fix Service on all firewalls as part of the Managed Firewall Service. In the case of a hardware failure on a Claranet firewall, as deemed by a Claranet engineer, Claranet will replace the firewall in accordance with the times below.

What Claranet will do

The starting point: Assume that the break/fix service level begins at the point when a Claranet engineer determines that a replacement firewall is required. Details of when the service level has been fixed can be found in the **Appendix: Help and Support.**

Replacement times in a Claranet datacentre: Replace the hardware within 5 hours of when a Claranet engineer deems that the hardware needs replacing where the firewall is in a Claranet datacentre.

Replacement times on your premises: Send an engineer to be onsite to replace the hardware within 5 hours of when it is deemed that the hardware needs replacing, where the firewall is installed on your premise.

Replacement times for firewalls outside the UK: When a Claranet engineer deems that the hardware needs replacing, the new device will be sent on a Next Business Day service. Due to Customs controls, Claranet cannot guarantee the delivery date.

Help and support

Service Desk support

What Claranet will do

Support times and Service Desk: Provide support 24x7x365 once the Managed Service has been handed over to you. Full details of how you can make the most of this service will be provided in your Handover Document.

Raising tickets: Changes to your firewall configuration can be made through the Claranet Online ticket request and details of this can be found in the **Appendix: Help and Support**.

Escalation: In the event that an escalation is required, Claranet provides a clear escalation process to allow you to contact the appropriate person within the company. Details of this can be found in the **Appendix: Help and Support**.

Service Levels

The Service Level determines the parameters by which the service is accountable. Many of the components of your service are designed to operate in a high availability configuration, with which there is an implied acceptance that from time to time an element of infrastructure may fail. Therefore for high availability options of components, unscheduled downtime is not considered to have occurred if one element fails and another element takes over the workload. Details of the metrics showing the expected service levels can be found in the **Appendix: Service Levels.**

Managed Service Options

As competition in your industry increases and product lifecycles become shorter, IT departments face constant pressure to respond efficiently. The ability to do this is often limited by workloads, IT expertise and budget restrictions causing delays and shortfalls. Claranet provide a flexible range of Managed Services levels around the main managed services e.g. Managed Hosting and Connectivity services, of which Managed Firewalls is a part, to allow you to select precisely the level suited to you and the level of your business expertise.

Standard Managed Service

With this level, Claranet will measure and monitor specific technical and service metrics associated with the Managed Firewall service you have purchased. Typically these metrics are based around availability and performance and are used to ensure that the service is available. Claranet will test the service around given thresholds and the results are communicated to you through Claranet Online and/or by email notification. It may be that Claranet acts automatically on this information to ensure the smooth running of your Service. Details of the specific metrics for the Managed Firewall service that are covered as Standard are detailed in this document within this section as well as in individual sections in the Appendix.

Appendices

Here you will find further information regarding the technical specifications of the service as well as standard procedures and agreements.

Appendix: Components

Physical Firewalls

Claranet provides a range of physical firewall devices upon request. Different options are available depending upon your specific requirements including those relating to enhanced resiliency, throughput, performance, and specific data isolation.

Table: Physical Firewall installed at a Claranet Datacentre

Physical Firewall Services	Rackmount option	Maximum Throughput (Mbps)	Maximum Concurrent Sessions
Small to medium firewall	rack mountable	2,500	3 million
Medium firewall	rack mountable	3,000	3.2 million
Medium to large firewall	rack mountable	8,000	6 million
Large firewall	rack mountable	16,000	6 million

Table: Physical Firewall installed on your premises

Physical Firewall Services	Rackmount option	Maximum Throughput (Mbps)	Maximum Concurrent Sessions
Customer Premise Firewall Equipment (CPE)	non-rackable	1,500	500,000

Platform firewalls

This is a service based on a platform firewall, dedicated to you, on a highly available shared virtualised firewall cluster which is a set of server hardware which was specified specifically for optimal network throughput. Your platform firewall will provide you with isolated traffic so that it cannot be seen by other customers. Claranet offer three variations of platform firewall that provide different levels of maximum traffic throughput.

Table: Platform firewall Service

Platform firewall Services	Maximum Throughput (Mbps)*	VLAN Security Zone limitations	Max Sessions	Policy count limitations	New Sessions per second	Maximum IPsec VPN throughput
Virtual Lite	100	3	75,000	200	2,000	10 Mbps
Virtual Core	250	6	150,000	200	4,000	20 Mbps
Virtual Advanced	500	12	300,000	200	7,000	40 Mbps

The table above is not provided as a guarantee as throughput is dependent on the configuration of policies to the firewall.

Internet connectivity

Every hosting solution requires a connection to the Internet via a direct and resilient connection to Claranet's own Autonomous System (AS), which utilises a mixture of private peering agreements and upstream IP transit from tier 1 carriers. A separate connection to the Internet is maintained by each of two core switches in the Claranet network, providing resilience in the event that a loss of service is experienced in either a core switch or an Internet feed. If you are using Claranet's MPLS Service, this service can also be used to provide breakout from the MPLS network to the Internet.

Speed

The speed represents the maximum rate at which traffic can be sent and received between the Internet and hosting servers and/or other devices on the MPLS network. The same connection is shared between all hosting servers and any devices on the MPLS network. Both the internet breakout and MPLS connections are supplied with bandwidth speeds of 20Mbps; 50Mbps or 100Mbps. Limitations on the speed of other components, such as Network Interface Cards (NICs) in servers and contention on network switches will mean that an individual server may not be able to consume the whole of the connection speed.

Customer Production Network

The Customer Production Network (otherwise known as the front-end network), is the network over which all your data will traverse, including remote management and traffic between servers. All devices in a solution are connected to the Customer Production Network.

On the Customer Production Network, Claranet will provision at least two dedicated private virtual network segments (VLANs) for each Customer utilizing 802.1Q VLAN tagging. The two VLANs are:

- Web Tier - for Internet access through a demilitarised zone (DMZ);
- Trusted Tier - for internal communication between servers within the solution.

What Claranet will do

Dedicated VLANS: Provision a Web Tier and a Trusted Tier dedicated VLANS for each customer.

Traffic isolation: Isolate the traffic so that it is not visible to any other customer.

IP addresses: Provide each VLAN with a /28 network of private IP addresses. Address space and assignments will be provided at time of implementation in the Handover Document. Further details can be seen below.

What you will do

Address changes: You will notify Claranet of any address ranges that should not be used because they may clash with ranges already used within any existing platforms that you may have.

IP addresses

What Claranet will do

Private IP addresses: Each physical or virtual server will be assigned the following private IP addresses:

- One internal (private) IP address from your private IP range and connected to the Customer Production Network;
- One internal (private) IP address from your private IP range for management and connected to the Management Network;
- One internal (private) IP address from your private IP range for backup and connected to the Management Network.

Public IP addresses: Supply you with two public IP addresses. Additional blocks of 8 IPv4 public IP addresses are available on request, though it is not always possible to provide blocks that are contiguous to existing ranges. The firewall provided can be configured to provide Network Address Translation (NAT) from public IP addresses to private network addresses.

Default configuration

Table: Default policy that will be deployed onto firewalls at the time they are initially provisioned, where the following definitions apply.

- **Any:** Any IP address 0.0.0.0/0;
- **Static**: Static IP address defined by you for remote access / any of your sites;
- **Web**: All IP addresses belonging to the web zone of solution;
- **DB**: All IP addresses belonging to the database zone of solution;
- **Patching**: All IP addresses belonging to Claranet's patching systems;
- **Automation**: All IP addresses belonging to any automation systems used by Claranet, including but not limited to PowerShell and orchestration tooling;
- **Relay**: Claranet SMTP relay for use with outbound SMTP mail;
- **Time**: Claranet's Network Time servers to maintain time synchronicity across servers

	Source	Destination	Service	Action
Inbound	Any	Web	HTTP (80)	Allow
	Any	Web	HTTPS (443)	Allow
	Static	Web	FTP	Allow
	Static	Web / DB	ICMP (Ping)	Allow
	Any	Any	Any	Deny
Outbound	Any	Any	Any	Allow
	Web / DB	Relay	SMTP	Allow
	Web / DB	Any	HTTP, HTTPS	Allow
	Web / DB	Time	NTP	Allow
Inter-Zone	Web	DB	SQL (1443)	Allow
	Web	DB	MySQL (3306)	Allow
	DB	Web	SMB	Allow
	Web	DB	ICMP (Ping)	Allow
	DB	Web	ICMP (Ping)	Allow
	Patching	Any	As required	Allow
	Automation	Any	As required	Allow

Appendix: Support

Help and Support

Change Control Process

Claranet's Change Management team are responsible for requests relating to any product and service configuration changes you wish to make. The team specialise in configuration and follow strict processes and ensuring that the changes are authorised. The Change Management team are also responsible for Claranet's Change Advisory Board (CAB), which discusses and approves changes raised internally. To make a change request, see the section below on "Raising a support ticket".

Raising a support ticket and a Request For Change (RFC)

Claranet provides two ways for your approved contacts to raise, track and update standard support tickets; through Claranet Online and by telephone. For security and audit reasons, you are required to make all requests for change through the customer portal and only portal users with the correct privileges can request a change. You will only see your services listed so please select the service relating to the request for change. In the event that the customer portal is unavailable, please contact Claranet by telephone, where an emergency procedure will be in place to log change requests on your behalf. Request for changes will not be accepted through this number at any other time.

What Claranet will do

Through Claranet Online: Support tickets raised through Claranet Online are assigned to the appropriate support team based on the service you need the support for. You will only see your services listed so please select the service relating to the incident or to the service request. The response time will start from as soon as your ticket has been submitted.

By telephone: It is not always convenient to raise support tickets through the portal and therefore you may choose to use the telephone instead. When choosing to raise a support ticket using the telephone you must provide proof of identity following Claranet's standard security procedure. The response time will start from as soon as your telephone call has ended.

Escalating a ticket

In the event that you need to escalate a ticket, Claranet is ready and available to help you quickly bring your issue to closure. Within each level of the escalation path the person you speak with is responsible for evaluating your situation, facilitating the resolution plan and acting as your sponsor. The benefits of the escalation procedure are:

- ITIL accredited staff owning your escalation
- A focus on service recovery
- Improved communication
- Consistent process

An escalation may be initiated when, after working through our standard support processes and with our teams, you are not satisfied with the level or timeliness of the service you have received. Additionally, an escalation should be initiated when there is tangible impact to your production environment, or there is high risk to your business operations.

What Claranet will do

Escalation Manager: Assign an Escalation Manager who will deal with your escalation and collaborate with you to develop a communication plan. A technical plan of action may be needed to ensure resolution of a technical issue. Your Escalation Manager works as your advocate internally and will become a virtual member of your own problem resolution team. Should you feel dissatisfied with the escalation process, please contact your Account Manager directly.

Service Delivery – Fix levels and response times

The circumstances where a fix service level is deemed to be met are:

- When the service has been fixed within the standard and expected response time
- Where you receive a telephone call (within the service level response time) resulting in a fix over the telephone
- Where you receive a telephone call and you defer the visit of an engineer to a specific time, the fix time is measured from the specific time you specify
- When a part which can be fitted by you arrives on site
- Where it is subsequently discovered that the issue giving rise to the telephone call falls outside the Services agreed to be provided by Claranet
- When the equipment has been returned to an acceptable operational status or an item of loan equipment has been supplied
- Where the fault relates to an excepted Service

What you will do

Efforts to resolve an issue: You are responsible for providing reasonable efforts support and information to Claranet to help in the resolution of any technical issues.

Service outage: In the event of a Service outage, you are responsible for complying as quickly as possible with any requests from Claranet for help with diagnostics. Any delay in resolving the fault due to you not being available or not complying with Claranet's requests may impact the validity of any Service Levels.

Table: Service Level Response Times – Request for Change

Priority	Service Level Response	Description
Standard	Initial response within 48 hours	Standard change request
Urgent	Initial response within 24 hours	Urgent change request

An Emergency Change Request can be actioned by contacting Service Operations once an Urgent change ticket has been raised via Claranet Online. Further information can be obtained through your Account Manager.

Service Levels

If Claranet fails to deliver the stated service level, Claranet agrees that you shall be entitled to receive, in lieu of all other remedies available to you, Service Credits as set forth in this section against the fees owing to Claranet under the Agreement.

Measure of availability

Any time in which the Claranet monitoring system is unable to receive or process monitoring data shall not be assumed to be unscheduled downtime. If you initiate a Service Credit request, this will put into a process where Claranet coalesce the systems monitoring data and logs with your own record of when and where an outage occurred. The Service Credits will be available for that agreed window. You have the option to dispute records with Claranet, where upon systems monitoring data can be provided to you.

Table: Technical Metrics –Availability showing credited downtime

Component	Source of availability data	Unscheduled downtime identified by	Exceptions	Service level
Physical Managed Firewall with Internet Breakout	SNMP test to firewall external IP address from Claranet monitoring platform every 5 minutes.	Every SNMP test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	SNMP tests are disabled during maintenance window	99.95% availability
Physical High Availability Managed Firewall with Internet Breakout	SNMP test to firewall external HA virtual IP address from Claranet monitoring platform every 5 minutes.	Every SNMP test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	SNMP tests are disabled during maintenance window	99.99% availability
Platform Managed Firewall with Internet Breakout	SNMP test to firewall external HA virtual IP address from Claranet monitoring platform every 5 minutes.	Every SNMP test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	SNMP tests are disabled during maintenance window	99.99% availability

In the event that you and Claranet agree that Claranet has failed to meet any service level guarantee during any given calendar month, Claranet will credit your account with a Service Credit. Service Credits shall apply only to the fee(s) for the affected service(s). Service Credits shall be deducted from the relevant monthly fee due in respect of the second month following the month in which an agreed Service Credit is claimed. The maximum amount of Service Credit a Customer can receive in each calendar month relating to this agreement is fixed to 50% of the fee for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in this agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the failure for which they are payable.

Compensation claims

Compensation claims must be submitted, in writing (email or letter), within 30 days from the service level guarantee breach to which they refer. All claims must be submitted to the appointed Account Manager and/or Service Manager. You agree to correct problems and to attempt to minimise the recurrence of problems for which you are responsible that may prevent Claranet from meeting the service level guarantees. Requests for support received by the Service Desk by means other than telephone or request ticket (for example, by fax) will be excluded when calculating service levels.

Exceptions

Claranet excludes responsibility for meeting any service levels to the extent that meeting the service levels is affected by the following items:

- if you are in default under the Agreement;

- in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
- in the event that the Service is disrupted due to unauthorised users or hackers;
- in the event that the Service is unavailable due to changes initiated by you whether implemented by you or Claranet on behalf of a customer;
- in the event that the Service is unavailable as a result of you exceeding system capacity;
- in the event that the Service is unavailable due to viruses;
- in the event that the Service is unavailable due to the your failure to adhere to Claranet's implementation, support processes and procedures;
- in the event that the Service is unavailable due to the acts or omissions of you, your employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel; or to your website at the request of a customer;
- in the event that the Service is unavailable due a Force Majeure Event;
- in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
- in the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet;
- in the event that the Service is unavailable due to your negligence or wilful misconduct of you or others authorised by you to use the Services provided by Claranet;
- in the event that the Service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by you;
- in the event that the Service is unavailable due to any failure local access facilities provided by you; and
- in the event that the Service is unavailable due to any failures that cannot be corrected because the you are inaccessible or because Claranet personnel are unable to access your relevant sites. It is your responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details.