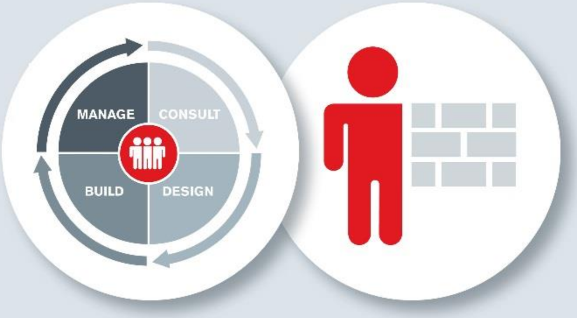

Co-Managed Firewall

Claranet can provide co-managed access to your physical firewall. Claranet will continue to manage the availability of your device and you will be able to access and amend policies when required.

Claranet are able to provide a Co-Managed service for accessing your firewall.

However, Claranet will not provide a "How to" service and recommend that all Co-Managed users have previous experience of Fortinet firewalls to NSE4 accreditation level.

Fortinet provide how-to videos via the firewall GUI. Following the link will allow you to gain access to a multitude of videos and documentation on configuration and in troubleshooting your firewall.

Setting up your firewall

Consult | Design

What Claranet will do

Accessing the firewall: Create a user profile for you to access the firewall graphical user interface or through the command line interface. Claranet will retain ownership of any physical device throughout the contract in all instances.

Features and functionality: Co-Management will provide write access to the majority of features:

Firewall & network configuration

- Policy configuration
- Address configuration
- Service configuration
- Schedule configuration
- Other configuration

Router configuration

- Static and dynamic routing protocols

Local User & Device configuration

- VPN Configuration (requires Claranet set up)
- IPSEC site to site VPN configuration
- Endpoint Security

You will have no access to following features which may compromise Claranet's ability to manage and monitor the firewall.

- System management configuration
- Maintenance such as firmware upgrades
- Firewall Admin management users and profiles
- Log configuration

Management: A management IP address, ports, username and password will be provided to you once the initial firewall configuration has been applied and the order has been set to "delivered". Claranet will only provide management access from RFC 1918 address space.

IPSEC VPN and SSL VPN: IPSEC and SSL dialup are not supported and chargeable if enabled. Please refer to Claranet's remote user access service.

What you will need to do

Policy changes: You will be responsible for any changes made to the firewall outside of the change request process and ensure that the firewall policy options you choose are suitable for your internal application. If changes result in Claranet accessing the firewall to fix issues then you will be charged.

Services provided

Claranet provides a Managed Firewall and a Co-Managed Firewall service depending upon your requirements including those relating to enhanced resiliency, throughput, performance, and specific data isolation.

Full details of these can be found in the Managed Firewall Service Description.

- **Customer Premise Equipment firewall (CPE)**
- **Small to medium physical firewall**
- **Medium physical firewall**
- **Medium to large physical firewall**
- **Large physical firewall**

Part of a larger solution

Claranet incorporates Firewall design and consultancy services as part of the Managed Hosting and Connectivity services.

Firewall Policy Survey

Defining your specification is a combined task between you and Claranet and details are discussed and captured in the Survey document.

Support

24x7x365 days per year once your service is up and running.

Claranet Online

You will be able to view details of your service and technical metrics through your Claranet Online login.

Claranet will continue to manage the firewall 24x7x365 in order to maintain its operation and availability. Where you require specific changes to be made to the configuration of your firewall, Claranet will continue to be responsible for making the changes if they are requested via a change request. You will be given your own login details to the firewall via the web. You will still be able to access Claranet Online to raise a ticket either to register an issue or to make a Request for Change, as well as access the device to make changes yourself. Full details of the change management process, ticketing, monitoring and the escalation of issues can be found in the Service Description. The parameters of the ongoing management of the service and the appropriate roles and responsibilities are outlined below.

What Claranet will do

Planned maintenance: Provide at least five working days' notice of any planned maintenance work or supplier planned engineering works (PEW) wherever possible.

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 utilisation. 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.

Break/fix service: Provide a break/fix service on all firewalls with hardware being replaced within 5 hours if needed.

Patching: You will not have permissions to update your firewall. Claranet will apply all critical patch updates on an as required basis. Where non-critical patches are released, Claranet can apply these at your request.

End of Life: Claranet will ensure that all services and products provided are of a high standard. If, for any reason, Claranet deem that a particular product or service may prove a technical or security risk to yourself or other customers, it reserves the right to cease providing or supporting that product or service.

What you will need to do

Co-Management: You will have access to change the configuration of the firewall. Details of what you can and cannot do are detailed above.

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

24x7 monitoring

Claranet will monitor key technical and service performance thresholds relating to your Co-Managed Firewall Service 24x7x365. Your service is measured on availability and you will be able to see at a glance, all aspects of the solution that Claranet provides. A full list of the technical and service metrics that are monitored and the frequency of the monitoring that are used to ensure your solution remains up and running, can be found in the Managed Firewall Service Description and can be viewed through Claranet Online. If changes made by you affect the uptime of the device then any Service Level Agreement offered by Claranet is void and Claranet will charge you to fix any issues caused

Logs

Co-Managed users will be able to access local logging and reporting features, such as Local Logs, FortiView local reports, Bandwidth and application usage, web usage, VPN usage, administration login and system events summary.

Service measurement availability (uptime)

Physical Standard Availability:	99.95%
Physical High Availability:	99.99%

Change requests

You can make unlimited changes yourself, or up to five rule-change requests using Claranet in each calendar month. Additional rule-change requests made by Claranet are then chargeable.

Account review

As part of your Co-Managed Firewall Service, Claranet will provide you with an annual technical and service review.

Managed services

Claranet will provide levels of availability monitoring and will work alongside you to create a pro-active approach to help you achieve your business outcomes.

Professional services

In addition to further technical, performance and service analysis, Claranet also provide experts in solution design, engineering, security, DevOps, Disaster Recovery, enterprise email migration, cloud transition and Project Management. Please see your Account Manager for further details.