Managed Firewall Service Definition

Version 6.3
August 2023

redcentric

AGILE • AVAILABLE • ASSURED

1 Service Overview

The Managed Firewall Service (MFS) is delivered on virtual firewalls on a shared platform, or where required, upon one or more dedicated hardware firewall appliances. The firewall(s) control traffic between devices on different networks providing a degree of perimeter protection. The firewall is configured to meet a Customer's specific requirements. Redcentric monitors the firewall for hardware failure and other alerts and staff manage the firewall configuration and provide advice on proposed configuration changes.

1.1 Feature Summary

- Based on cost-effective, highly available virtual-firewall platform
- Available at multiple locations for geographic diversity
- Dedicated single or high availability firewall appliance pairs also available
- Appliance firewalls can be deployed on a Customer's site or within a Redcentric data centre
- Layer-7, application aware firewalling as standard
- Unified Threat Management (UTM) functionality options
- Portal access to configuration, dashboard and reporting
- Support for site-to-site virtual private networks (VPN)
- Support for client VPNs for remote workers.
- Fully configurable rule-base managed by Redcentric's trained professionals.
- Customers receive advice and guidance on the effectiveness of the implemented rule-base, and any proposed changes.

Also available are dedicated appliance firewalls from specific vendors where some of the features above are not offered. Please see section 3 for details.

2 Service Description

2.1 Related Products

Redcentric offers several managed services that complement the MFS including an extensive connectivity portfolio and a variety of pay-as-you-use unified communications, compute, storage and hosting services. Redcentric's two-factor authentication service can be integrated with MFS to provide secure, remote access solutions for remote and home-working staff.

As an alternative to the managed service, Redcentric is happy to work with Customers to specify, deploy and configure devices including firewalls as part of a Professional Services project.

2.2 Firewall Platform

The platform delivers an extremely robust, flexible and cost-effective virtual firewall solution to meets the needs of most Customers. The platform is built using resilient components, as such Service Availability is very high. Additionally, the platform is present at several key locations, which supports disaster recovery design objectives.

Customers may elect to deploy dedicated firewall appliances where their requirements or policy dictates:

- Physical deployment of appliances is required at a Customer site
- Dedicated firewall appliance infrastructure is required
- Bandwidth throughput and/or other resources exceed those available on virtual firewalls

Please see Section 2.2.2 below for details.

2.2.1 Virtual Firewall Resource Specification

Redcentric currently offers three virtual firewalls sizes. Specifications are detailed below:

Resource	Size 1	Size 2	Size 3	Size 4
L7 Bandwidth throughput Mbps	50	200	500	1000
Sessions	60000	240000	500000	500000
IP Sec S2S VPN	25	50	100	200
Remote User VPN	5	10	15	30
Firewall Policy	1000	2000	4000	5000
Locally Configured Users	20	50	65	100

Other resources (e.g., proxy-services & address definitions, virtual-IP addresses etc.) are allocated on a fair-use basis. In the rare case that a Customer consumes one or more of these resources excessively, they will be given the option to reduce consumption, upgrade to a higher specification virtual firewall or migrate to dedicated appliance(s) at additional cost.

The platform does not support L2 transparent mode.

2.2.2 Alternative Dedicated Appliance Option

Redcentric will specify, design and deploy dedicated firewall appliances to meet specific Customer needs where virtual firewalls are unsuitable. Firewalls are chosen from a range that is compatible with the service options and portal capability as detailed in sections 2.3 and 2.4 respectively.

If the firmware or hardware version of your firewall appliance is forecast to become End of Support (EoS) / End of Life (EoL) during an initial contract term or a renewal of that contract term, Redcentric will no longer be able to provide security or critical firmware updates for that EoS or EoL dedicated firewall appliance.

In order to continue to receive security and critical updates, a hardware refresh of the dedicated firewall applicance will be required. Any hardware refresh, including the provision of new dedicated firewall appliance, is outside the scope of this Service and will be chargeable. A new dedicated firewall appliance can be provided by Redcentric for an additional charge.

2.2.2.1 Hardware Support

If a firewall appliance develops a fault, hardware support results in replacement of the faulty unit.

Redcentric aims to replace faulty hardware located within a Redcentric data centre within four hours and hardware at other locations within the UK next working day. This level of hardware support is included within the MFS charge. Expedited hardware replacement options are available to meet specific Customer requirements. Requirements and provision for expedited hardware replacement must be agreed in writing by both parties prior to finalising a Service Agreement.

2.2.2.2 Physical Deployment

Firewalls can be located on a Customer site or within a Redcentric data centre. If the firewall is to be deployed within a Redcentric data centre, by default it will be installed within a rack dedicated to managed devices. If the Customer subscribes to the Redcentric co-location service, the firewall(s) can be located in the Customer's colocation facility to simplify connectivity to multiple Demilitarised Zone (DMZ) devices.

If the firewall is to be deployed on a Customer site, a Redcentric engineer will visit the site and undertake installation, configuration and basic testing between 9:00am and 17:00pm.

2.2.3 Software and Subscription Licensing

Software subscription and licensing costs required to deliver the service are included in the charges for the MFS.

2.3 Service Versions

Regardless of the Customer's choice of virtual firewalls or dedicated appliance(s), Redcentric offers three service options, as detailed below:

- Standard
- Advanced
- Static-configuration

The Standard service delivers a high level of perimeter security based on Layer-7 application-aware firewalling performing network address translation with a level of denial-of-service capability (e.g. Mitigate sync. packet flooding).

The Advanced service builds on the Standard service by additionally offering three Unified Threat Management functions: Anti-virus, web filtering and intrusion detection. Please see sections 2.3.1, 2.3.2 and 2.3.3 for details.

The Static-configuration option is particularly cost-effective and suitable for environments where the rule-set is dictated by a governing body and rarely changes (e.g. where a firewall protects the interface to certain public sector networks). UTM functionality is not included. To minimise costs and service charges, fewer change requests are accepted for the static configuration option. No portal access is provided to the Customer as detailed in section 2.4. Redcentric recommends the standard or Advance service for all Customers using the firewall to protect their enterprise network edge.

2.3.1 Anti-virus (AV)

AV signature definition updates are periodically downloaded to the firewall automatically.

A single AV policy/profile will be defined which can be tailored and applied to certain traffic as required. This single policy/profile is sufficient for the majority of customers but Redcentric will create and administer additional policy/profiles as required. Creation and administration of additional policy/profiles is chargeable.

When the firewall detects that an AV signature has triggered, the Customer will be emailed immediately but no ticket is raised within the Redcentric ticketing system.

2.3.2 Web Filtering

Website category lists are managed and maintained centrally by the firewall vendor to provide the best possible service.

The Customer can dictate the action to be taken when users attempt access to disallowed sites. Options include denying access, permitting access after a warning message has been presented to the user, and generation of an email notification to the Customer. Redcentric does not raise tickets when a user attempts to access a disallowed site.

A single web filtering approved category list profile will be defined which can be tailored and applied to IP addresses and/or user groups as required. This single profile is sufficient for the majority of customers but Redcentric will create and administer additional category lists as required. Creation and administration of additional category lists is chargeable.

2.3.3 IDS/IPS

IDS definition updates are periodically downloaded to the firewall automatically.

Customers are encouraged to determine IDS policy carefully to maximise firewall performance. For example, if a customer has no devices with a particular operating system, the firewall should not be configured to check for exploits relating to that operating system. Where performance issues are related to poorly defined IDS policy, Redcentric consultants can provide system audit and advice as part of a Professional Service exercise.

A single policy containing some or all of the signatures will be defined which can be tailored and applied to certain traffic as required. This single policy is sufficient for the majority of customers, but Redcentric will create and administer additional policies as required, in which case additional charges may apply. The Customer can dictate whether traffic is to be allowed or blocked when an IDS signature triggers the system at the set-up stage. Events will be logged, a ticket raised within the Redcentric system for awareness only, and an email is sent to the Customer for further investigation.

2.4 Portal access

One major feature of the MFS is the customer access portal. The MFS customer access portal provides the following capabilities:

- View configuration, policies, objects and profiles
- Access near-real-time analytic dashboard
- Access and generate pre-defined reports
- Inspect real-time log view (application, attack etc.)
- Offers the ability to make minor configuration changes

Customers are issued with a portal user guide that explains how to access information and undertake tasks.

2.4.1 Account Set-up and Permissions

Redcentric staff set-up or modify Customer administrator portal accounts during initial set-up or throughout the Service Period.

2.4.2 Viewing Configuration

Customers can use the portal to view firewall rule-set, objects and addresses etc. Customers taking the Advanced service option can also view UTM configuration details.

2.4.3 Minor Configuration Changes

Redcentric support staff manage the configuration on the firewall, evaluating and implementing formal change requests submitted by the Customer as detailed in section 2.8. If required, Customer administrators may be issued credentials for the portal which will allow them to make configuration changes. The aspects of the configuration that can be modified by the Customer's administrator is limited to those that will not have major impact on the overall level of security the firewall provides. The list of aspects is subject to change but is currently limited to:

- Content-filter policy including modification of exception (AKA block/deny) lists
- Database of user credentials required for remote access VPNs

The Customer agrees to reasonable charges for fault investigation work where faults are traced to issues resulting from configuration changes made by the Customer.

2.4.4 Logging

The platform stores traffic log data so that it can be analysed and used in reports. The MFS recurring charge includes 25GB storage. For most Customers this storage volume is sufficient to retain a good level of log and analytical information for several months. Customers can optionally extend this volume for an additional charge.

By default, the platform will be configured with a 90%:10% allocation of log vs archive analytic data where old data is overwritten. Consequently, Redcentric makes no commitment to make log data available medium to long term.

2.4.5 Reporting

The following reports are configured on the platform:

- Bandwidth and Applications Report
- Cyber Threat Assessment
- Hourly Website Hits
- Top 20 Categories & Applications (Bandwidth)
- Top 20 Categories & Applications (Sessions)
- Top Allowed and Blocked with Timestamps

The Customer's administrator can run and access these reports via the portal.

Redcentric staff can set-up or tailor other reports limited by the capability of the platform, as a chargeable Professional Services exercise.

2.5 Customer Security Policy

Redcentric configures the firewall(s) with rules that meet the Customer's operational requirements. Redcentric recommends that prior to implementing any firewall solution, the Customer undertakes a full security review. One component of this security review should be the creation of a network security policy. The security policy can form the basis of the firewall rule-base and UTM configuration that will be implemented on the firewall(s).

Redcentric recommends that the firewall rule-base should be based on the premise that all traffic is to be denied both inbound and outbound. The rule-base should be written to permit only valid traffic according to the Customer's security policy. The configuration can be modified throughout the Service Period by approved personnel to meet changing requirements.

2.6 Address Translation and remote connections

2.6.1 Network and Port Address Translation

The firewalls are configured to translate addresses as part of the standard security implementation. Depending upon the number of addresses available and the required functionality, network address translation (NAT), port address translation (PAT), or a combination of the two may be deployed.

2.6.2 Site-to-site Virtual Private Networks

Redcentric supports secure, authenticated and encrypted connections/tunnels, commonly referred to as virtual private networks (VPNs) to firewalls, routers and other devices where compatibility exists.

Compatibility of VPN end-points varies between devices and manufacturers and compatibility assurance can only be offered when Redcentric designs, specifies and manages the devices at both ends.

2.6.3 Remote User Virtual Private Networks

Redcentric supports remote user VPNs using standards-based IP-sec and client based SSL protocol suites. Redcentric supplies a client that is supported on the major operating systems including Windows, MAC OS, Android and iOS. Redcentric supports basic remote user tunnels only - for example, posture-checking is not supported.

Users can be configured on the firewall for static username/password authentication. See virtual firewall resource specification (section 2.2.1) for the number of users supported. Maximum number of statically configured users on physical appliances is 100.

Use of static username/password is considered a weak authentication method by security professionals and Redcentric strongly recommends use of its two-factor authentication service for secure authentication of remote user VPNs.

User authentication may also be possible through integration with corporate directory structures (e.g. Lightweight Directory Access Protocol – LDAP). Such integration is undertaken as a Professional Services exercise.

2.7 Monitoring/Alarms

Redcentric polls managed firewalls regularly to check for availability and critical events (these include hardware failures, environmental alarms etc. where available). Service tickets are automatically generated on the Redcentric system when faults are detected. Additionally, the firewall platform is configured to send alerts to the monitoring platform. Tickets are managed by engineering professionals in Redcentric's operations centre 24x365.

2.8 Implementation of Change Requests

During the implementation phase, the Customer will be provided with a firewall change request form. This should be used to submit change requests throughout the Service Period.

The validation and subsequent implementation or rejection of change requests will be performed Monday to Friday between 8 am and 6 pm, with a target completion time of 48 hours for routine changes. Emergency changes are prioritised accordingly, and performance targets are detailed in Redcentric's Customer Welcome Pack.

In accordance with the Redcentric change request procedure, all change requests must be submitted by a designated and authorised Customer technical contact. If Redcentric's security engineer cannot validate the change requester against the authorised list, then Redcentric will place the change request on hold and attempt to contact one of the alternative authorised contacts. Redcentric must wait for the request to be ratified by a known authorised contact before proceeding with any firewall change. It is therefore essential that Customers provide accurate and current contact information for their designated and authorised staff.

It is extremely easy to weaken network security by submitting a seemingly innocuous change request. Redcentric staff review change requests based only on the information they have available, and therefore Redcentric cannot take responsibility for network weakness resulting from rule-base changes. If Redcentric support staff believe that a rule-base change request compromises the security of the Customer's network, Redcentric may ask the Customer to sign a disclaimer stating that they wish to go ahead regardless of the advice offered. In extreme cases, staff reserve the right to reject the change outright; for example, if the weakness could affect other Redcentric Customers.

2.9 Syslog

Both virtual and appliance firewalls can be configured to send Syslog feed to a customer's server. This is undertaken as a Professional Services exercise.

2.10 Professional Services Consultancy

Charges for the MFS do not include consultancy to help the Customer define the security policy or establish UTM configuration details. Also certain other functionality (e.g. IDS) generally requires a bedding-in and tuning process to minimise false alerts. Occasionally this may need to be repeated throughout the Service Period, for example if the Customer makes changes to their infrastructure or systems. Redcentric provides chargeable Professional Services consultancy to undertake this and other work mentioned throughout this definition on request.

2.11 Limit of Liability

Protocol and application vulnerabilities are identified and exploited regularly, and no firewall can offer absolute protection. Redcentric recommends that Customers make regular use of security scanning services and use the output along with log and report data as part of a continual security improvement cycle. It is essential that Redcentric is notified in writing of the intent to perform scans beforehand.

2.12 Customer Dependencies

The Customer is responsible for the following functions:

- Define firewall rule base and other security parameters
- Update Redcentric with changes to list of staff authorised to submit change requests

3 Tailored MFS solutions

The capabilities detailed in section 2 are based on a comprehensive set of products from a single vendor. Redcentric also specifies, deploys, monitors and manages firewalls from other vendors to meet specific Customer requirements. For these solutions, the features and capabilities detailed in sections 2.2 – 2.4 do not necessarily apply.

4 Implementation and Acceptance

4.1 Acceptance Criteria

The following are the Acceptance Criteria applicable to the MFS:

- Confirm Redcentric Support contact details have been supplied
- Check that Customer administrators can access the portal
- Check the LAN connections to the firewall(s) for speed and duplex mismatches and errors (where possible).
- Test IP connectivity by using permitted protocol traffic from permitted devices on each interface destined for permitted addresses on the other interfaces (e.g. test traffic on port 80 from a device on the internal network destined for a server on the outside network; repeat for server on the DMZ network if applicable)
- Use vulnerability scanning service to confirm traffic is permitted and denied according to required rule-base
- Test connectivity to/from devices which are connected to the firewall using secure tunnels if required
- Test functionality and notification mechanisms of UTM capabilities if chosen

5 Service Levels and Service Credits

5.1 Service Levels

The Service Level applicable to the MFS is as follows:

Applicable MFS service	Service Availability	Service Credit
Virtual firewall	=100%	none
	≥99.0% but <100%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS
Single firewall located in a Redcentric data centre	≥99.5%	none
	≥99.0% but <99.5%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS

Pair high availability firewalls located in a Redcentric data centre or on Customer site.	=100%	none
	≥99.0% but <100%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS
Single firewall installed on a Customer site	≥99.0%	none
	≥98.0% but <99.0%	5% of MS
	≥96.0% but <98.0%	15% of MS
	<96.0%	20% of MS
Portal access for analysis and visibility etc.	≥99.5%	none
	≥99.0% but <99.5%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS

5.2 Exclusions from Availability

In calculating Availability, in addition to the exclusions listed in clause 6.7 of the General Terms the following shall be excluded:

- Unavailability due to tasks required to implement and test change requests.
- Unavailability due to malicious activity of any kind. E.g., a Denial-of-Service attack (DOS)
- Unavailability due to Customer misconfiguration

5.3 Floor Service Level

The Floor Service Level applicable to the MFS in respect of Availability shall be 85% in any given Month.

5.4 Service Credits

The Service Credits applicable to the MFS shall be calculated as follows.

In the following table:

"≥" means "greater than or equal to"

"<" means "less than"

"MS" means the total Charges payable in respect of the MFS for the same Month

Applicable MFS service	Service Availability	Service Credit
Single firewall located in a Redcentric data centre	≥99.5%	none
	≥99.0% but <99.5%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS

Applicable MFS service	Service Availability	Service Credit
Pair high availability firewalls located in a Redcentric data centre or on Customer site.	=100%	none
	≥99.0% but <100%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS
Single firewall installed on a Customer site	≥99.0%	none
	≥98.0% but <99.0%	5% of MS
	≥96.0% but <98.0%	15% of MS
	<96.0%	20% of MS

6 Data Processing

6.1 Data Processing Scope

- Redcentric's Managed Firewall Service delivers a degree of IP network perimeter protection.
- Redcentric's Managed Firewall Service may involve the storage of summarised traffic and user activity.

6.2 Data Storage and Encryption

- Firewalls may be configured to encrypt traffic across certain networks.
- By the very nature of the Service, it is necessary for Redcentric to capture, inspect, analyse, and store the Customer's traffic/data.
- Redcentric would not have access to the content of the Customer's traffic/data in normal circumstances. Under certain circumstances, when managing a support ticket, Redcentric may further capture, inspect, analyse and/or store samples of the customer's traffic in order to investigate and diagnose specific problems. Such actions will only be undertaken at the request of and in conjunction with the Customer.
- The period for which data is stored in relation to the Managed Firewall Service is decided by the Customer.

6.3 Data Processing Decisions

- Redcentric does not make any data processing decisions in relation to the Redcentric Managed Firewall Service. Any processing of data over Customer systems when using Redcentric Managed Firewall Service 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 Redcentric Managed Firewall 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.

6.4 Sub-Processors

- Redcentric's Managed Firewall Service may make use of services provided by the selected firewall vendor (Eg. Fortinet, Cisco Sytems etc.). These services assist with the identification of security vulnerabilities, weaknesses, exploits, virus, worms etc.
- No other parties are involved in delivering the Redcentric Managed Firewall Service, and no other sub-processors are appointed by Redcentric.

6.5 Customer Access to Data

- The Customer controls its own platforms which use Redcentric's Managed Firewall Service to carry data, and the Customer therefore has full access to its own data.

6.6 Security Arrangements and Options

- The Redcentric Managed Firewall Service is hosted at both Redcentric and third-party locations. All locations meet physical security standard ISO27002 section 11.1 or equivalent.

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED