REDCENTRIC

MANAGED FIREWALL SERVICE DEFINITION

SD007 V4.1
Issue Date 04 July 2014

redcentric
business technology. managed.

1) SERVICE OVERVIEW

1.1) SERVICE OVERVIEW

Redcentric's managed firewall service (MFS) is based on a hardware firewall appliance that controls traffic between devices on different networks. The firewall is configured to a Customer's specific requirements. The MFS is designed to offer passive defence, providing restrictions on the source and destination IP addresses and service ports that are allowed to pass through the firewall. Redcentric monitors the firewall for hardware failure and staff manage the firewall configuration and provide advice on proposed configuration changes.

The function of any firewall is to filter traffic coming into a network (also called border protection) based upon pre-determined criteria. No firewall can protect against all protocol or application weaknesses, and new software vulnerabilities are discovered regularly. All devices protected by a firewall should be administered with the same level of diligence as if the firewall were not present.

1.2) FEATURE SUMMARY

- Single device or high availability firewall pairs are available.
- Firewalls can be deployed on a Customer's site or within a Redcentric Data centre
- Support for site-to-site Virtual Private Networks (VPN)
- Support for remote client VPNs for home workers.
- Utilises Network Address Translation (NAT) to hide Customer network addresses from the Internet.
- 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.

2) SERVICE DESCRIPTION

2.1) CUSTOMER SECURITY POLICY

Redcentric provides, configures and maintains the managed firewall hardware, and configures the firewall(s) with bespoke rules configured to 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 that will be implemented on the firewall(s).

2.2) FIREWALL HARDWARE MODELS

Cisco Systems ASA devices are most commonly deployed as part of MFS. Cisco produce a number of appliances to meet the needs of Customers wishing to deploy firewall devices at small and home office sites through to very large corporate head offices.

Redcentric does not currently offer hardware options for VPN acceleration, intrusion detection or prevention services etc. Redcentric does not offer 'layer 7', application aware firewall functionality.

2.3) SOFTWARE LICENCES

All licensing costs required to deliver the MFS are included in the Charges for the MFS.

2.4) INSTALLATION/CONFIGURATION CONSULTANCY

The MFS includes basic security policy development by one of Redcentric's technical specialists. The objective is to document network objects and applications, and to determine the required network traffic restrictions and controls.

The standard consultancy time allocated to this work is four hours.

If the implementation has special requirements, such as proprietary equipment needing access through the firewall, additional consultancy may be required and will be charged accordingly.

2.5) DEFAULT SECURITY POLICY

The default firewall rule-base is based on the premise that all outbound traffic is to be permitted and all inbound traffic is to be denied. This can be overridden during the initial deployment or modified at any point in time using the firewall change request form (please see section 2.12 below).

2.6) VIRTUAL PRIVATE NETWORKS

Redcentric supports IP-Security (IP-sec) and Secure Socket Layer (SSL) VPN to Cisco firewalls and routers and other devices where compatibility exists. In such cases, the following applies:

Authentication based upon shared secret passwords.

IP-sec encryption using 56-bit Data Encryption Standard (DES). 3DES may be available subject to conditions being met.

Redcentric cannot guarantee the compatibility of VPNs unless Redcentric manages the firewalls at each end.

2.7) NAT AND PAT

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. It is not always necessary or desirable to translate the addresses of traffic on VPN tunnels.

2.8) LOGGING AND ANALYSIS

Basic logging information is captured and stored for one month on Redcentric's servers. This information is available on request and can be analysed by Customers and used to constantly improve security stance as part of their security policy. The MFS does not include analysis of alarm logs although this is available as an enhancement at additional charge.

2.9) MANAGEMENT

Redcentric manages all firewalls via a dedicated interface or sub-interface on the firewall. Within a Redcentric data centre, the management Virtual Local Area Network (VLAN) connects directly to the firewall. When a firewall is installed on a Customer site, it is a pre-requisite that the site is connected to the Redcentric network using the LANnet Service, which hosts the management link for the firewall.

2.10) SERVICE DELIVERY

Redcentric's service delivery staff will review the proposed rule-base with the Customer and provide feedback and/or recommendations as required. 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 it would usually be installed within a rack set aside for managed devices. If the Customer has subscribed to Redcentric co-location service, the firewall(s) can be located in the Customer's environment to simplify connectivity to multiple Demilitarised Zone (DMZ) devices if required.

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.

2.11) 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. The tickets are managed by engineering professionals in Redcentric's operations centre.

2.12) 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 during the contract term.

The validation and consequential 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 Service Plan (CSP).

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.

2.13) LIMIT OF LIABILITY

Security vulnerabilities can arise through many causes and no firewall can offer protection against all protocol vulnerabilities.

Redcentric recommends that Customers make regular use of security scanning services and applications to monitor network and application security. It is essential that Redcentric is notified in writing of the intent to perform such scans beforehand.

Redcentric does not offer Intrusion Detection Services (IDS) and Intrusion Prevention Services (IPS) as part of the MFS. Redcentric recommends that Customers deploy network and host IDS/IPS as part of their overall security policy.

2.14) CUSTOMER DEPENDENCIES

The Customer is responsible for the following functions:

- Define firewall rule base
- Update Redcentric with changes to list of staff authorised to submit change requests
- Arrange for vulnerability testing to be undertaken after installation, changes to the rule-base and periodically during the contract term.

3) IMPLEMENTATION AND ACCEPTANCE

3.1) ACCEPTANCE CRITERIA

The following are the Acceptance Criteria applicable to the MFS:

- Confirm Redcentric Support contact details have been supplied
- 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

4) SERVICE LEVELS AND SERVICE CREDITS

4.1) SERVICE LEVELS

The Service Level applicable to the MFS is as follows:

Service Level: Availability **Measurement Period: Month**	
Single firewall located in a Redcentric data centre	Not less than 99.5%
Pair high availability firewalls located in a Redcentric data centre or on a Customer site	Not less than 100%
Single firewall installed on a Customer site	Not less than 99%

4.2) EXCLUSIONS FROM AVAILABILITY

In calculating Availability, in addition to the exclusions listed in clause 5.7 of the General Terms the following shall be excluded:

Unavailability of the MFS due to tasks required to implement and test change requests.

4.3) FLOOR SERVICE LEVEL

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

4.4) 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
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

HARROGATE (HEAD OFFICE)

Central House
Beckwith Knowle
Harrogate HG3 1UG

THEALE

2 Commerce Park
Brunel Road
Theale, Reading
Berkshire RG7 4AB

CAMBRIDGE

Newton House
Cambridge Business Park
Cowley Road
Cambridge CB4 0WZ

READING

3-5 Worton Drive
Reading
Berkshire RG2 0TG

LONDON

John Stow House
18 Bevis Marks
London EC3A 7JB

INDIA

405-408 & 410-412
Block II, 4th Floor, White House
Kundan Bagh, Begumpet
Hyderabad 500016

0800 983 2522
info@redcentricplc.com
www.redcentricplc.com

redcentric
business technology. managed.