



SECUREME

Product Specification

© Spark New Zealand Trading Limited 2020

Spark owns copyright and all other intellectual property rights in this document.
You may not copy or redistribute any portion of this document without Spark's permission.

PRODUCT SPECIFICATION

Product Specifications provide standard details of the Services Spark provides to you.

SecureME

1. Introduction

This document contains product information for the SecureME Service. If you require more detailed technical information, please contact your Account Manager.

2. Service definition

2.1. Service overview

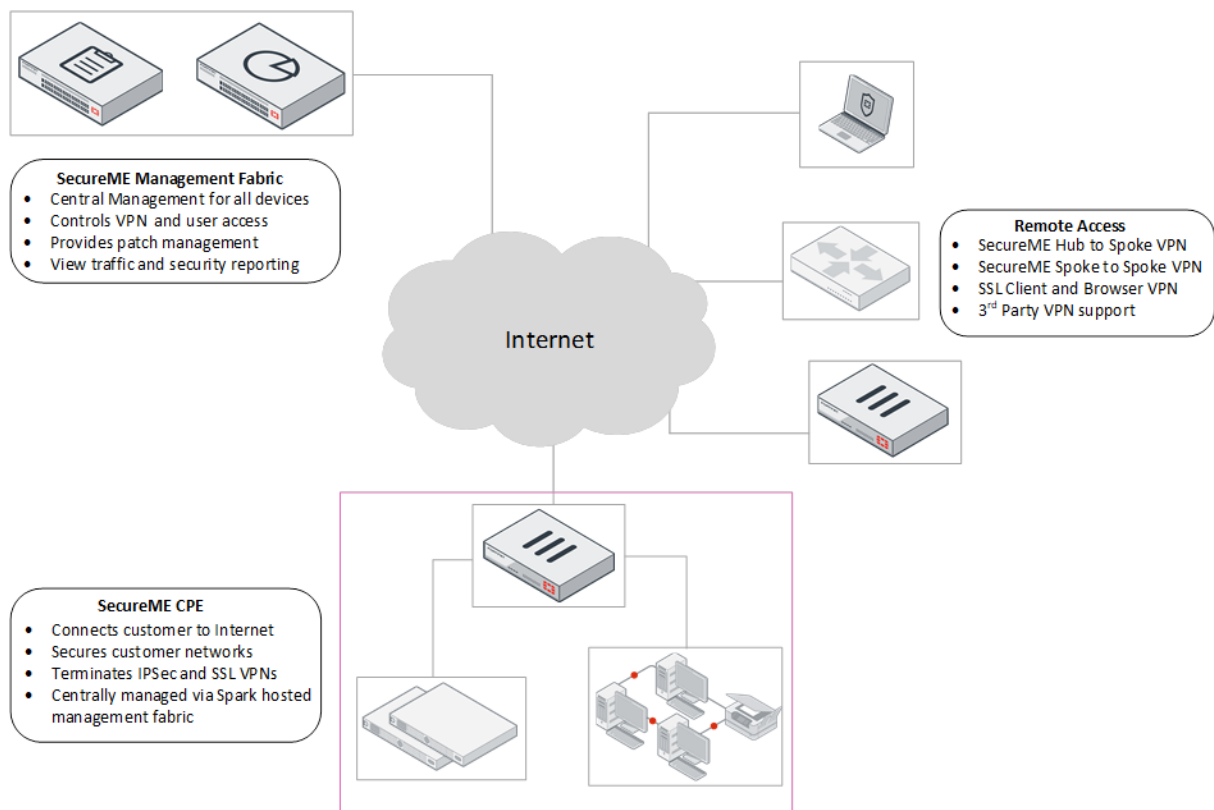
SecureME is a security service that has been built specifically for organisations with a business broadband connection. It enables you to have an onsite security appliance that provides firewall, internet content management, intrusion detection and VPN services.

The Service has been designed to allow users to administer and configure their own internet usage and security rules through a web interface. These rules and configuration settings are held centrally by the vendor which allows for very simple management and support procedures.

In order to receive the Service you are required to have your internet connectivity provided by Spark.

The Service has been built using Mako Networks Firewall Appliances (6500) ("Mako Appliance") and Fortinet Fortigate/FortiWiFi devices and hosted central management systems. The SecureME Service supports optional 3G/4G fail over, Ethernet connectivity and a range of VPN concentrator services (Dedicated 7550 (100VPN), 8875 (1000VPN) and Spark hosted Multi-tenanted concentrators).

The following diagram illustrates how the Service works.



2.2. Standard Service Features

The key features of our SecureME Service are:

- Supply and support – We and the relevant vendor will provide support for the hardware,
- Continuous update – as internet security threats are constantly evolving, the Service has been designed so that updates are automatically pushed out to the device. This removes the overhead from the site administrator of having to look out for and then install these updates as they are created. It also means that the site is as protected as we can make it.
- Reporting – Pre-defined reports providing detail on SD-WAN, Firewall and Security Threats will be available via the SecureMe reporting server. These reports can be generated ad-hoc or scheduled to run at regular time intervals where they can be emailed out as a PDF.
- Alerting – This function notifies the administrator of security threats. This can be in the form of detected attacks on the firewall (hacks) or from virus on the LAN introduced by a rogue PC.
- Security Features - The SecureMe device comes standard with the following security elements
 - Firewall – firewall protection for inbound, outbound, intranet and internet connections
 - Virtual Private Network – used for connecting to other sites or for remote access.
- Central Management – the administrator can control the device from anywhere in the world by using the administrative portal.
- Broadband router – The SecureME device contains a router suitable for terminating either ethernet, ADSL/VDSL or 3G/4G broadband connections.

2.3. Service Options

SecureMe MailGuard Email Sanitation:

This Service option provides an offsite filter for your clearing email for an entire domain. You can filter email for Spam, Viruses, Content, Size and Language. Email that meets the user-specified criteria can then be handled in various ways including header modification, forwarding to another recipient, moved to a queue to be manually inspected or deleted. This service is available using Mako equipment only.

Wireless Fail Over:

This Service option provides seamless fail over and fail back to the Spark 3G/4G network should a sites primary connection fail. Wireless Failover requires an appropriate 3G/4Gcapable device and is subject to 3G/4G data usage fees which are priced and charged in addition to the standard SecureME service. (This option is subject to the availability of 3G/4G coverage)

Dedicated SecureME Concentrators:

SecureMe concentrators support up to 1,000 concurrent VPNs depending upon the model provided. SecureME Concentrator Services are available to seamlessly connect multiple sites via secure SSL VPN to a centralised point for the consumption of specific services. A dedicated SecureME Concentrator can be deployed within a customer's network to aggregate branch office or site connections into the WAN.

SecureME Hosted Multi-tenanted Concentrator Service:

Suitable for 1-100 VPN connections or remote sites. This Service option allows for organisations to leverage resilient multi-tenanted concentrators which are connected to a carrier grade internet connection and hosted by Spark. The Service allows remote SecureME sites to securely connect into to an organisations Spark WAN Service environment and other Spark hosted services such as Ready Cloud without the need for a customer hosted dedicated concentrator service. (Customer is responsible for all hosting and connectivity costs within their environment)

Intrusion Detection Systems

SecureMe Intrusion Detection monitors the network for malicious activity or policy violations, using signatures of known attacks or deviations from normal activity. Any malicious activity or violation is collected and reported using the SecureMe alerting function.

Content Filtering (blocking of inappropriate websites)

SecureMe Content Filtering allows customers to set access permissions for websites by category or URL, ensuring compliance with company security policies.

2.4. Service management

The SecureME Central Management System is managed 24 hours x 7 days per week x 52 weeks per year.

Helpdesk support of your on-premise equipment is available 24x7.

The helpdesk has the following key capabilities:

- Specialist support staff – qualified to support the SecureME appliance
- Diagnostic tools – to enable them to quickly isolate the fault
- Helpdesk systems – to track calls and to pass them onto relevant 3rd parties to resolve

Hardware Support

Hardware support is available through the SecureME helpdesk. If the SecureME appliance is faulty the standard practice will be to initiate a swap out process. This will be co-ordinated by the helpdesk.

We aim to have a next Business Day delivery for the SecureME appliance provided the replacement device is requested prior to 2pm business days. Additional charges may apply to this support service.

As all of the configuration data is stored in the core SecureME Central Management System, when the new SecureME appliance arrives simply call the SecureME helpdesk and provide them with the replacement SecureME units serial number and it will be matched to the existing configuration and be up running with those rules within minutes of being connected.

2.5. Customer's Responsibilities

It is your responsibility to:

- Comply with this SecureME Product Specification.
- Ensure that everyone you are responsible for or that uses this service complies with this SecureME Product Specification.
- Comply with our Acceptable Use Policy (AUP) when using the System. We may change the AUP from time to time as required to protect the integrity of the service or ensure services can continue to be delivered to all of our customers.
- Ensure email alerts for broadband and 3G/4G Mobile data usage are configured correctly and monitored by your organisation's administrator.
- Pay for any broadband and 3G/4G mobile connection and data costs required or incurred while using this service.
- Provide all necessary information to the SecureME Helpdesk to ensure that the SecureME Service can be setup correctly.

- Provide security within the Customer Network, including:
 - physical security, including physical access to premises and access to computer systems
 - ensure that they keep secret their username and password to all SecureME System interfaces
 - security for trusted servers, applications, desktop computing devices, notebook and other mobile or remote computing devices
 - securing configurations and user authentication to servers, applications and other devices
 - virus scanning of all servers workstations (as well as regularly updating virus definitions)
 - strong encryption and password access to laptop and other mobile or remote computing devices
 - secure disposal of sensitive material, including password lists, computer configurations
 - user security policies that are given to end-users, clearly defining the user's responsibilities (such as not divulging usernames and passwords) and how the services can be used. It is particularly important to cover issues such as privacy of email and web content, which can be inspected and monitored using Safecom.
- Provide Customer Network support personnel, including:
 - an administrator or support person to communicate promptly with the SecureME helpdesk when issues arise
 - a technical resource that is able to work with the SecureME initial setup engineer and who is capable of performing the necessary tasks on your site for service implementations. The technical resource will ideally be a system administrator, who is technically skilled and understands IP routing. If you do not have a suitable resource available, then this will impact proposed costs and time frames for implementation of the solution.
- There are certain aspects of the firewall system that you will retain responsibility for:
 - **Pre-Implementation** – Provide input into the SecureME Technical Specification. Undertake pre-requisite work to bring your infrastructure up to an agreed level.
 - **Security Policies** – These belong to you and you retain the responsibility for the end-to-end security and firewall policies in place for their organisation. We can assist with the definition and development of these.
 - **Ownership of Hardware & Software** – You acknowledge that Spark retains ownership of the hardware and licensing supplied as part of the SecureME Service. Use of the software will be as per any software licence terms.
 - **Customer Site Hardware & Software Version Upgrades** – We will notify you when any upgrades are available and can assist in their implementation. You will also be responsible for keeping an unmanaged onsite spare current with every primary firewall change required.
 - **Other Network Devices** – The SecureME Service does not cover the management of any other network devices on your site and you will continue to monitor and manage these.
 - **Internet Access & Data Usage** – You will retain responsibility for providing Internet access, bandwidth, usage and availability to site(s).
 - **Authorised Support Contacts** – For security reasons, requests for assistance and fault reporting can only be accepted from your authorised contacts. This will require you to provide an initial central point of contact within the organisation before contacting us for support. It is your responsibility to update this list and to inform us of any changes.
 - **No Aggregation or Resale** – the Customer will not aggregate any third-party connections to the SecureME Service or otherwise try to resell the SecureME Service to anyone unless Spark's express written permission is first obtained. Spark shall not be obliged to agree to any such request under any circumstances.

Assistance provided by us on any of the above may be considered outside of the SecureME Service offering and will be subject to the charge structure within the MAC process.

2.6. Service Implementation

We and our vendors will work with you to setup the SecureME appliance. A list of tasks is provided below.

Spark and our Vendors	Your Responsibilities
Pre-Sales	
Assist you in understanding the solution and the value that it brings to the company. This presales activity will also cover the various aspects of the solution.	- Provide accurate information for business and technical requirements. - Sign our contract.
Initial Setup and Introduction	
Spark will contact you via telephone to setup the SecureMe device and provide initial technical introduction to the product.	- Provide accurate technical information. - Provide information relating to configuration to enable seamless SecureME appliance setup. - Ensure skilled technical expertise available to assist the Spark Support Team during the setup phase. - Develop a test plan to set the criteria for successful implementation of all functionality.
Help Desk – SecureME	
- Assist you with any SecureME related problems they may have from time to time. - Handshake you to our appropriate helpdesk for problems that are non-SecureME related.	Ensure support processes are communicated to all relevant internal parties.

You will be deemed to have accepted the Service once configuration of the SecureME system is completed. Your ongoing use of the Service is also deemed to constitute acceptance.

2.7. Service Boundaries

With the exception of installation queries, always contact the Spark helpdesk in the first instance if you experience issues with the SecureME Service. Spark will provide support to you for matters occurring within the service boundaries stated below.

The following service boundaries apply to the SecureMe Service:

- Customer Boundary** – We will ensure the correct functioning of the SecureME device within the Customer boundary. The external boundary is the WAN Ethernet port, ADSL/VDSL modem, or 3G/4G modem in the SecureME device. The internal boundary is the LAN 1 and LAN 2 Ethernet ports on your network.
- Server System Boundary** – Spark and its vendors are responsible for the management system housed at various locations around the world including Spark's Data centre facilities. Spark Vendors are not responsible for the Telco-provided internet connectivity of this server system.

The following are examples of, but are not limited to, matters that fall outside of these service boundaries:

- Configuration and support of Customer Network components including mail servers, workstations and network systems (routers, switches etc.)
- Configuration and support of Internet systems external to the SecureMe System such as web sites, email servers, search engines etc
- On-site support – this is not provided as part of the SecureME Services

3. Service Targets

This section lists the following:

- **Functional performance targets** – the performance targets for SecureMe service.
- **Provisioning/change performance targets** – performance targets for our implementation of and changes to the service.

3.1. Functional Performance Targets

Service Attribute	Attribute Definition	Service Target
1. Call Reception	The elapsed time for the SecureMe helpdesk to answer incoming telephone calls from you.	Call Response: Within 120 seconds.
2. Maintenance Window	The period when routine maintenance can be undertaken on the SecureMe System.	Weekly maintenance window for the SecureME Service Delivery Platform is between 2:00 am to 7:00 am, Sunday (NZST). Usual notification service levels to you apply for providing adequate notice to you.
3. Planned Outage Notification	Notice of any maintenance that could cause a service outage to you. Please note that not all maintenance will necessarily cause an outage to you	Weekly Maintenance Window: 5 days Outside Weekly Maintenance Window: 10 days Emergency Maintenance As much notice as possible will be given where emergency maintenance is required
4. Hardware Swap-out	Replacement of your SecureMe device in event of hardware failure whilst under warranty.	Next Business Day. Provided the replacement request is received prior to 2pm business days.
5. Restoration Hours	The elapsed time between Call Reception or alarm occurrence and you being notified that service is restored to the defined levels	Next Business Day

Definitions

Hours of Service	
Central Management Server Service Availability Target	99.9%
Spark hosted Multi-tenanted Concentrator Service Availability Target	99.9%
Helpdesk Service Hours:	24x7

Note: All times in this document refer to New Zealand Standard Time (NZST)

4. Fees and Invoicing

4.1. Invoicing

Your Fees may include one or more of the following:

- Monthly Fees
- Call Out Fees

Fixed Monthly Fees

Fixed monthly fees are invoiced in advance and cover the provision and management of the SecureME services included in your SecureME Service Schedule. Fixed monthly fees are applicable from the date that we advise you that the service is capable of being used between the designated service delivery points. We are not responsible for your non-use of the service due to implementation delays beyond the service delivery points. Billing for the SecureME service begins a maximum of seven days from the date the SecureME appliance is shipped to you.

Early Termination Fees

Early termination fees are calculated as the number of remaining contracted months x the contracted monthly rate per SecureME device.

3G/4G Mobile Data Charges

The customer is responsible for the payment of all and any 3G/4G data charges when using the SecureME 3G/4G capable Service. Mobile data charges are billed in addition to the SecureME Service.

Call Out Fees

Call out fees are invoiced to you should we have to provide onsite assistance to you in the support of the SecureME service. The SecureME service has been designed so that it can be installed, supported and run remotely. Your authorised customer network support personnel shall be capable of performing most on-site implementation, reducing the need for call outs.

5. SecureMe For Health

The following additional terms only apply where the customer has selected the SecureME for Health product. In addition to meeting any Spark requirements, the customer must qualify for and maintain all requisite authorisations mandated by the Ministry of Health, including but not limited to the supply of a certificate for the customer's SecureME connection. Should the customer fail to maintain any prerequisites for the use of the SecureME for Health Service Spark reserves the right to remove the customer's access to the SecureME for Health Service. In the event access is removed the customer's connection will revert to the SecureME standard service.

ACCEPTABLE USE POLICY (AUP)

Introduction

- a) This AUP applies to
 - i. you if you agree to take the Service and
 - ii. all other users of the Service including your employees and contractors. You and those users are together called the “Users” in this Policy.
 - b) Violations of this AUP, and the Acceptable Use Policies of other providers (see clause 5 below) can severely affect provision of various services. For example, spamming by Users can lead to denial of service attacks that disrupt not only the services to you but also the use by others of services on the Internet. Compliance is therefore particularly important.
 - c) Breach of this AUP by a User that utilises any of the services, through you, is considered to be a breach by you as well as by the User, whether or not you had knowledge or gave consent. It is important that you ensure compliance with this AUP.
 - d) Indirect or attempted violations of this AUP by Users are considered to be violations by you.
 - e) This AUP supplements but does not supersede the Service Schedule. In the event of a conflict between a term in this AUP and the Service Schedule, the Service Schedule prevails.
 - f) While we do not monitor or control communications, if we become aware of a violation of this AUP, we may take the following actions:
 - i. termination, suspension, blocking or filtering of sites, and
 - ii. co-operating with and notification of relevant authorities and parties including enforcement agencies and other internet service providers and carriers (“Third Parties”). We may need to communicate the Users’ personal information to such Third Parties.
- We may take any of these steps without informing the Users first and do this at our sole discretion when investigating any problem or complaint. However, where appropriate, we will endeavour to inform Users to give them an opportunity to comply voluntarily.
- g) The Users must inform us of any breaches of the AUP that comes to their attention. Your users should do so by contacting you and you should do so by contacting the Account Manager.

Changing the Acceptable Use Policy

We may change this AUP at any time by changing or removing existing requirements or adding new ones. Changes may take the form of a completely new AUP. We will tell you about any changes by e-mailing details of the changes.

Prohibited Uses

- a) **Illegal Uses** – Users must not use services in ways that constitute criminal or civil breaches of any statute, regulations, government requirements or any other law (including general or common law) of any country. Those breaches include, without limitation, breach of intellectual property rights (such as copyright, trademarks, patents, trade secrets and confidential information); defamation; breach of obscenity laws and laws as to objectionable publications, such as pornography and hateful materials; fraud; theft; misappropriation of money, credit card details or personal information; breaches of privacy obligations; and breaches of trade practices legislation, examples of which are the Fair Trading and Consumer Guarantees Acts (New Zealand) and the Trade Practices Act (Australia).
- b) **Security and Protection of the Network** – Users must not use services to breach, or attempt to breach, the security and operation of any network, equipment or any other system. This includes: hacking, cracking into, monitoring, or using systems without authority; scanning ports (including scanning for open relays); improper configuration of mail servers and FTP servers enabling distribution of spam or unlicensed material by others; interference of service to any user or network (or activities that might encourage such interference by others) including mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks; denial of service attacks or activities which might encourage denial of service attacks by others; unnecessarily excessive traffic (including excessive pings); distributing viruses, or other harmful material or software; any communications across the services which do not accurately identify (or disclose in a manner that is misleading) addresses, headers, names and other relevant details; and using our network in any way as a staging ground for any of those breaches or to disable or “crack” other systems.
- c) **Industry Codes** – Users must not use services in a way that breaches any material standard, code and content requirements produced by any relevant authority or industry body.
- d) **Threats** – Users may not use services to transmit content of a threatening nature including threats of death, physical harm and defamation.
- e) **Aggregation or Resale** – Users will not aggregate or resale any of the SecureME Services to any Third Parties.

Spam

Spam is not permitted. Spam includes (but is not limited to) sending:

- i. unsolicited e-mails without identifying an easy way for the recipient to stop receiving more e-mails from the originator of those e-mails;
- ii. unsolicited bulk e-mail (for example: sending a single message to more than 12 destinations (whether newsgroups, e-mail addresses or web sites) where there is no pre-existing business or personal relationship with the recipient(s);
- iii. messages or e-mails that could reasonably be expected to provoke complaints;
- iv. chain letters, pyramid schemes or hoaxes;
- v. e-mails and messages that do not accurately identify the sender's return address, header or domain name;
- vi. unsolicited e-mails and bulk mail from another provider, advertising or impacting upon the use of any of the services.

Other Provider's Policies

Users must not breach the AUPs (or similar guidelines and rules) of other internet providers including internet service providers and telecommunication carriers.

Responsible Use

Users must use the services in a responsible manner taking into account:

- i. the effect their use of the services may have on networks, equipment and other parties; and
- ii. compliance with "netiquette", newsgroup and internet conventions, as well as restrictions in rules, charters and similar Newsgroup, web site and e-mail mailing list material; and
- iii. the fact that such use must not interfere with the availability of any of the services to others or any other services including services offered by us and other internet providers and carriers to others.