

SERVICE DESCRIPTION: VODAFONE SECURE INTERNET (VSI)

PART A – PRODUCT OVERVIEW

Vodafone Secure Internet (**VSI**) is a managed internet fire-wall product delivered over the Vodafone Private IP product (**PIP**) to a customer nominated site. VSI is a form of Unified Threat Management (**UTM**) and is designed to have multiple core security features and functionalities, including:

- firewall and intrusion prevention;
- application control;
- web content filtering;
- VPN;
- Antispyware;
- WAN optimization;
- two-factor authentication;
- anti-spam; and
- customer reporting,

These functions and features are more fully described in Part B.

VSI forms part of our cloud infrastructure and is designed to provide UTM-protected internet connectivity with several selectable VSI product options.

Please note that this Service Description contains **important information in section 13 (Part D) regarding your use of the reporting feature for the VSI product**. Please ensure that you have read and fully understood that section.

PART B – VODAFONE SECURE INTERNET

1. Your VSI Option

1.1 The VSI product is available in three levels of product capability called “**VSI Options**”, including:

- (a) VSI Standard (**VSI-S**);
- (b) VSI Flex (**VSI-F**); and
- (c) VSI Premium (**VSI-P**).

1.2 Your selected VSI Option is set out in the Pricing Schedule.

1.3 The features and functionality of the VSI Options are defined in the table below:

Feature	VSI-S	VSI-F	VSI-P
Firewall / VPN			
Allows outbound connections from customer’s network	X	X	X
Allows inbound connections to customer’s network (Customer Security Team support)		X	X
Allows connections to Vodafone cloud based services	X	X	X
Allows site to sites VPNs (5 sites bundled)		X	X
Traffic shaping			X
Integration to customers Active Directory			X

Antivirus / Antimalware			
Antivirus	X	X	X
Spyware	X	X	X
Scan downloaded documents			X
Unpack & scan downloaded zipped documents			X
Web Browsing			
URL filtering	X	X	X
Content filtering		X	X
Web reputation filtering	X	X	X
Application control at a user level			X
SSL content inspection		X	X
IPS / IDS			
Protection against malicious PDF files			X
Protection against malicious Office files			X
Protection against web browser vulnerabilities			X
Protection against Java vulnerabilities			X
Self-Service configuration			X
Remote Access			
SSL VPN Remote access from Windows Machines		X	X
SSL VPN remote access from MACs		X	X
SSL VPN from Smart devices		X	X
SSL VPN access from Unix systems		X	X
2 factor authentication– Fortitoken or X.509 certificate		X	X
Reporting			
Automated Weekly Security Analysis & Web Usage Report	X	X	X
Log View			X
Create and run own reports			X
Self Service			
Configure Web-Filter Categories			X
Configure Web-Filter White/Blacklists			X

2. Remote Access

Some of the VSI Options provide you with protected remote access for your staff and business partners with compulsory two-factor authentication capability which provides an additional layer of security. Those VSI Options also support VPN capability between you and your staff and business partners.

3. Reporting

- 3.1 Customer reporting is an integral part of the VSI product. The objective of the reporting feature is to provide you with usage information on a 24x7 basis in relation to your internet connection, in order for you to understand the security provided by the VSI product for the particular usage made of the internet by you, your staff and business partners (depending on your VSI Option).
- 3.2 If you are a VSI Standard customer you will be provided with our standard reports which will set out usage information on a 24x7 basis including information sorted by IP address. If you are a VSI Flex or a VSI Premium customer you will have access to the VSI Customer Portal and customisable reporting – see section 13.
- 3.3 The types of information you may access (depending on your VSI Option) includes:
- administration and system events;
 - details of threats, attacks, viruses, malware, botnets, data leaks and vulnerabilities discovered by VSI and against which VSI has provided protection;
 - internet usage analysis including “top” users, devices, applications, websites, web categories, browsed countries, IPS events, attacks and viruses – which may be sorted by various factors including bandwidth/usage, sessions, reputation, risk, visits, time frames, country and severity;
 - detailed information regarding active users, including internet usage, browsing time, websites accessed or blocked, attacks, virus infections and spam activity, among other information;
 - VPN usage information; and
 - bandwidth and traffic statistics and analysis.
- 3.4 Section 13 sets out more information on the scope of reporting for each VSI Option. Please speak to your Account Manager for more information on the scope of reporting for your chosen VSI Option.

4. Customer Portal (available for VSI Flex & VSI Premium Products Only)

- 4.1 If you are a VSI Flex or a VSI Premium customer, the Vodafone Business Customer Zone portal will provide you with the ability to configure and view your own customised reports.
- 4.2 In addition, if you are a VSI Premium customer you will be able to administer your remote users’ VPN access and manage your own URL filter through the configuration of black lists and white lists.

5. Platform Updates

- 5.1 VSI platform updates are automatically deployed according to what we and our partners consider to be the best frequency for each technology category. This will include updates in respect of:
- antivirus protection;
 - web filter;
 - IP reputation; and
 - attack, data type, suspicious URL, and data leak signatures.

6. Product Availability

- 6.1 The number of users and the type of use of VSI may prevent the full capacity being available to any one user.
- 6.2 VSI is designed to achieve a 99.92% target platform availability measured over a rolling 90 day period.

6.3 The target availability of the VSI platform excludes downtime due to the following:

- planned downtime;
- connectivity from the VSI platform to your nominated premises;
- upstream Internet connectivity. Due to the variable nature of the Internet, Vodafone cannot offer any assurance that any particular Internet based application or service will function as expected; and
- any other circumstances beyond our control or if any act or omission by you or a third party interferes with the platform.

7. Fault Management

Vodafone Helpdesk

The Vodafone Helpdesk is your primary point of contact. Through the Helpdesk, we will:

- provide you with a 24x7 fault logging facility;
- investigate and manage faults through to resolution;
- update you on progress with fault resolution;
- escalate unresolved faults to the appropriate Vodafone representative;

Fault Management

- We will use all reasonable endeavours to resolve any faults for which we are responsible in accordance with the resolution times specified in the table below. However, we do not guarantee that these resolution times will always be met.
- Faults will be assigned a priority rating depending on the impact that the fault is having on the Services based on the priority descriptions in the table below. We will determine that priority rating in consultation with you.

Proactive alarms

- Some designated Services and Equipment that are under continuous surveillance by us may automatically generate a range of alarm conditions. In that case we may, at our discretion, advise you of such faults and generate a “trouble ticket” for service response.
- In the case of priority one faults, we will use all reasonable endeavours to respond to those faults within 20 minutes of the alarm being generated, provided that the alarm is generated within Service Hours.

Definitions

- **Metro Sites** means those Sites that are within 65km of the CBDs of Auckland, Hamilton, Wellington, Christchurch, Dunedin.
- **Other NZ Sites** means areas outside of Metro and Regional sites.
- **Regional Sites** means your sites that are within 30km of Whangarei, Rotorua, New Plymouth, Napier/Hastings, Palmerston North, Nelson, Greymouth and Invercargill.
- **Resolution Time** means the period elapsed (during Service Hours) from the time you log the fault to the time that the affected Service is restored to normal operation.
- **Service Hours** means 24 hours per day, 7 days per week and 365 days per year.

PRIORITY	DEFINITION	RESOLUTION TIME	PROGRESS REPORTS
1. Critical Impact	A catastrophic fault, where a minimum of 50% of users at a particular Site cannot use a particular Service.	4 hours during Service Hours (or 8 hours during Service Hours where fault is assigned to a third party network operator for resolution). If a Site visit is required: Metro Sites: 4 hours during Service Hours or 8 hours during Service Hours where the fault is assigned to a third party network operator for resolution. Regional Sites: 80% within 8 hours, 90% within 16 hours. Other NZ Sites: 80% within 12 hours, 90% within 24 hours. Note: The above percentages refer to the percentage of P1 faults, which are resolved within the Resolution Time.	At 2 hour intervals during Service Hours following our initial response.
2. Major Impact	Up to 50% of users at a particular Site cannot use a particular Service.	8 hours during Service Hours. If a Site visit is required: Metro Sites: 4 hours during Service Hours or 8 hours during Service Hours where the fault is assigned to a third party network operator for resolution. Regional Sites: 80% within 8 hours, 90% within 16 hours. Other NZ Sites: 80% within 12 hours, 90% within 24 hours. Note: The above percentages refer to the percentage of P2 faults, which are resolved within the Resolution Time.	At 2 hourly intervals during Service Hours following our initial response.
3. Minor Impact	Repeated quality problems. Intermittent faults or degraded service. No major service impact.	5 Working Days	At 8 hourly intervals during Service Hours following our initial response.

Escalation Procedure

- Vodafone operates an automatic escalation process within our Fault Management Centre for all service issues.
- If you ask us to, the Vodafone representative who is coordinating resolution of the fault will escalate any unresolved faults to the following personnel:
 - Level 1 Group Team Leader - Complex Faults
 - Level 2 Group Manager - Complex Faults
 - Level 3 Department Manager – Fault Management Centre

Customer planned outages

Please provide us with reasonable notice of any activity that you are planning that may cause an interruption in the Services.

PART C - PRICING

8. Pricing Overview

- 8.1 Charges for the VSI product are aligned with both the subscribed bandwidth of the VSI product you purchase and the VSI Option (Standard, Flex or Premium) that you select.
- 8.2 Your Charges for VSI will include Monthly Recurring Charges (**MRCs**) which will be payable on an ongoing basis and also Non-Recurring Charges (**NRCs**) that are applicable to your VSI Option.

9. Monthly Recurring Charges

- 9.1 The MRCs for your VSI product are set out in the Pricing Schedule.

10. Non Recurring Charges

- 10.1 For simple installations we will charge the amounts set out in the Pricing Schedule for the cost of installing your Service (which includes building and implementing a configuration). If we consider that your installation is not simple, our NRCs for your installation will be on our Time and Materials Rates and we will consult with you to agree such costs (or the basis of such costs) prior to incurring them.
- 10.2 You agree to provide us with reasonable assistance during the installation phase.
- 10.3 We may provide you with a discount on your installation NRC as per the table set out in the Pricing Schedule depending on the Service Initial Term you select for your VSI Option.
- 10.4 Moves, Adds, Changes (**MACs**) to the VSI product will attract a NRC. Security services can be complex and it is difficult to predict the cost of implementing MACs in many cases. Our Charges for MACs will be on our Time and Materials Rates and we will agree such costs with you prior to incurring them.
- 10.5 However, our NRCs for simple MACs set out in the Pricing Schedule can be fixed where, in our opinion, the work that is required to be performed is simple and standard (**Simple MACs**).

PART D – OTHER TERMS AND CONDITIONS

11. Product Limitations

- 11.1 VSI is designed, implemented and maintained to provide a high level of on-going security. However, we do not offer guaranteed protection from external attacks, risks and/or viruses. It is advisable that you have robust and reliable security policies and procedures in place that are complimentary to the VSI product.

12. PIP Requirement

- 12.1 VSI requires a PIP connection from Vodafone to deliver the product. If you are an existing PIP customer, this may be a simple configuration change. If you do not have an existing PIP connection, a new PIP circuit will need to be ordered through your account manager.
- 12.2 You agree to provide us with reasonable assistance to develop or alter any configuration.

13. Privacy

- 13.1 This section contains important information relating to our collection and use of personal information about your Users in connection with the VSI product, and your access to such personal information in reports generated using VSI reporting services.
- 13.2 Subject to section 13.3, you acknowledge that personal information about your Users will be collected by us in accordance with our privacy policy available at Vodafone.co.nz/legal/policy/privacy, on a 24x7 basis for the purpose of:
 - (a) providing you with VSI services; and

(b) conducting our business operations.

In addition, depending on the VSI Option that you select, personal information may be accessed by you and used in reports that you generate using VSI reporting services, including, detailed information about internet usage on 24x7 basis under each of your User's computer login and assigned mobile devices.

- 13.3 We will not use User's personal information collected via traffic across the VSI platform for any marketing activities and for the avoidance of doubt, sections 2.7, 2.8 and 2.9 of our privacy policy will not apply to such personal information.
- 13.4 **Prior to using the VSI product, you must ensure that your Users have provided their express informed consent to the collection, use, disclosure of and access to their personal information to the extent, and for the purposes, set out above (including in relation to their internet usage on a 24x7 basis). Consent may be obtained in a variety of ways, including clearly setting out the possibility of such collection, use, disclosure of and access in your internet usage or similar policy that Users are bound to comply with (as part of their employment contract or otherwise). You must not access a User's personal information as part of any reporting to the extent that User has not given, or has retracted, its consent. You must ensure that persons who will generate reports using the VSI product are aware of the requirements in this section 5 prior to generating any such reports.**
- 13.5 If there is any complaint, claim or other proceeding made or brought against us in connection with your access to and/or use of personal information in connection with the VSI product
- we will be entitled to use any of your Confidential Information to the extent necessary (in our reasonable opinion) to enable us to fully address any such complaint, claim or proceeding and, if applicable, to the media; and
 - we may terminate or suspend any reporting functions of the VSI product and/or your access to the Vodafone Business Customer Zone portal (if applicable) for any period or indefinitely.
- 13.6 To protect personal information from unauthorised access, use and/or disclosure, you must maintain the confidentiality of any login, username, password or other security information relating to your use of VSI, including without limitation, your access to the Vodafone Business Customer Zone portal (**Security Information**). You must treat all Security Information as strictly confidential and not disclose it to any third parties. We are entitled to rely on the provision of your Security Information without further enquiry, as evidence of your identity. You must notify us immediately of any actual or suspected unauthorised use of your Security Information. Such notice will not release you from your obligations in respect of the Security Information, but we will use all reasonable endeavours to mitigate the effects of that unauthorised use.

14. Additional terms and conditions

- 14.1 You may be required to agree to Additional Terms and Conditions as a precondition to accessing and using the VSI product. We will notify you of any Additional Terms and Conditions either through an Account Manager or on the Vodafone Business Customer Zone portal. You acknowledge and agree that:
- (a) you may be required to agree to Additional Terms and Conditions; and
 - (b) your ability to access and use the VSI product may depend on your agreement to the Additional Terms and Conditions.

15. Definitions

In this Service Description the defined terms set out in the Agreement will apply and in addition:

Additional Terms and Conditions means additional terms and conditions that apply to your access to and use of the VSI product (including end user licence agreements, software terms and conditions or other similar instruments).

Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.

Hypertext Transfer Protocol or **HTTP** is an application protocol for distributed, collaborative, hypermedia information systems.

Intrusion Prevention System/Intrusion Detection System or **IPS /IDS** is a network security appliance that monitors network and/or system activities for malicious activity.

MAC has the meaning given in section 10.4.

Monthly Recurring Charges or **MRCs** have the meaning given in section 8.2.

Non-Recurring Charges or **NRCs** have the meaning given in section 8.2.

PIP has the meaning given in Part A.

Secure Sockets Layer or **SSL** is a secure protocol developed for sending information securely over the Internet.

Security Information has the meaning given in section 13.6.

Simple MAC has the meaning given in section 10.5.

Time and Materials Rates means Vodafone's then-current rates for the provision of professional services to business customers as updated from time to time.

Uniform Resource Locator or **URL** (also known as web address, particularly when used with HTTP), is a specific character string that constitutes a reference to a resource.

UTM has the meaning given in Part A.

Virtual Private Network or **VPN** is an extended private network across a public network, such as the Internet.

VSI Options has the meaning given in section 1.1.

Wide Area Network or **WAN** is a network that covers a broad area (i.e. any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports.

X.509 is an ITU-T standard for a public key infrastructure (**PKI**) and Privilege Management Infrastructure (**PMI**).