# Service Specific Terms

## Firewall Management Service

Vodafone Business Customers

## 1. The Service – Overview

1.1 The Vodafone Firewall Management service (the "**Firewall Management Service**") is a fully managed service aiming to provide the Customer with advanced firewall capabilities and improve the Customer's firewall management lifecycle. The Firewall Management Service aims to provision, manage and operate a firewall in a secured manner to protect Customer's Environment from malicious activity in accordance with Customer's security requirements. The term "Service" or "Services" in these Service Specific Terms means the Firewall Management Service.

## 2. Service Terms Structure

2.1 These Service Specific Terms include:

(a) the service specification, which sets out a description of the Service, may be updated from time to time and is made available at www.vodafone.co.uk/cloudservices/ (the "**Service Specification**");

(b) the service levels which set out the standards that will be applied to the provision of the Service (the "**Service Levels**");

2.2 The following documents further govern Vodafone's supply of the Service and form part of the Agreement:

(a) the Commercial Terms;

(b) the Order, which sets out the Service Elements selected by/for Customer;

(c) the Vodafone Business Marketplace Service Specific Terms (the **"VBM Service Terms"**) available at www.vodafone.co.uk/cloudservices/;

(d) the General Terms available at www.vodafone.co.uk/terms;

(e) any other documents referenced as incorporated in these Service Specific Terms; and

(f) any applicable policies and guidelines, as provided from time to time by Vodafone.

2.3 These documents apply in the order of precedence set out in the General Terms, save that the VBM Service Terms shall take precedence over the General Terms and all documents expressed to be of lesser precedence in the General Terms.

## 3. The Service

3.1 The Customer must select one of the following types of Service (each a **"Service Type"**, together the **"Service Types"**):

| Service Type | Description | Applicable Firewall Vendors |
|---|---|---|
| **New Build** | The provision and ongoing management of a new firewall instance to the Customer using the Applicable Firewall Vendors firewall solutions. | • Palo Alto – Prisma Access |
| **Takeover** | Takeover and ongoing management of the Customer's Existing Firewall solution. Takeover applies to the Applicable Firewall Vendors Existing Firewalls only. | • Cisco<br>• Checkpoint<br>• Fortinet<br>• Palo Alto<br>• Juniper (SD-WAN only). |

| | | |
|---|---|---|
| | | Note: Only in-support versions of the Applicable Firewall Vendors firewall will be managed by Vodafone. |
| **Replacement** | Replacing the Customer's Existing Firewall solution with a new firewall instance using one of the Applicable Firewall Vendors firewall solutions. | • Palo Alto – Prisma Access |

3.2 **Service Tiers:** The Service is available in one of the following two tiers (each a **"Service Tier"** and together the **"Service Tiers"**), one of which must be selected by Customer:

(a) **Tier 1:** provides all core NGFW features, pre-defined reporting and is supported by a standard SLA; or

(b) **Tier 2:** provides all core NGFW features, the ability to define Custom Reporting and is supported by a standard SLA. Tier 2 also provides architecture support to customise the solution for the Customer and a larger range of options for various services (i.e. higher number of Tickets, major upgrades, Custom Reporting etc).

3.3 **Optional Service Elements:** In addition to the Service Type and Service Tier selected by Customer, the Customer may also select any of the following Optional Service Elements:

(a) **Sandbox analysis:** Wild-Fire malware analysis service leverages cloud-based malware detection and multiple analysis techniques to identify and protect against unknown file-based threats while resisting attacker evasion techniques. Up to 12 Incidents per annum.

(b) **High availability (Takeover Service Type only):** deployment of a pair of firewalls with cluster configuration to maintain high availability in Active-Active or Active-Passive mode, providing redundancy and ensuring business continuity with failover in case of hardware failure;

(c) **Firewall Audit:** performance of a firewall rule review to ensure the firewall configuration and rule set, meets the business and compliance requirements of the Customer as per best security practices;

(d) **Pack of 10 Tickets:** additional pack of 10 Tickets provided where a Customer meets their Ticket quota (uses all of their Tickets).

3.4 The applicable Service Type, Service Tier and Optional Service Elements (if any) shall be set out in the Order and further detailed in the Service Specification.

## 4. Service Specific Conditions of Use

4.1 **Vodafone Business Marketplace** (the **"VBM"**)**:** The Service is made available to purchase through the VBM. The VBM Service Terms apply to the extent of the Customer's use of the VBM website. In the event of any conflict between the VBM Service Terms and the Firewall Management Service Terms, then the Firewall Management Service Terms shall take precedence. The Customer accepts that certain features and functionality detailed in the VBM Service Terms may be limited or not apply to the Service, including but not limited to the applicability of Charges and Subscription periods.

4.2 Customer may use the Service only in accordance with the terms and obligations:

(a) as indicated in the Order; and

(b) as defined in the Agreement.

4.3 Vodafone shall only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the responsibilities set out in the Agreement, Vodafone's performance of the Service may be delayed, impaired or prevented.

4.4 **Adequate Customer Personnel:** Customer must provide adequate personnel to assist Vodafone in delivery of the Service, upon reasonable request by Vodafone.

4.5 **Delays:** delays due to infrastructure, access right unavailability or other underlying dependencies could result in additional efforts and costs and impact the duration and timelines of the Service.

4.6 **Termination:** In addition to the termination rights set out in the General Terms, Vodafone shall be entitled to terminate the Service upon 30 days written notice to Customer where Vodafone's agreement with the Third Party Provider has terminated.

4.7 **Payment Card Industry:** Vodafone does not warrant that the Service will be payment card industry (**"PCI"**) requirements Compliant or that the Services will enable Customer to be compliant with Applicable Privacy Law.

4.8 **Palo Alto Third Party Provider Terms:**

(a) **Third-Party Products and Services:** Through its product(s), Palo Alto may make available to Customer third-party products or services (**"third-party apps"**) which contain features designed to interoperate with its products. To use such features, Customer must either obtain access to such third-party apps from their respective providers or permit Palo Alto to obtain access on Customer's behalf. All third-party apps are optional and if Customer chooses to utilise such third-party apps:

(i) all governing terms and conditions, including licensing and, shall be entered into between Customer and the applicable app provider;

(ii) Customer may be required to grant Palo Alto access to its account on such third-party apps; and

(iii) Customer instructs Palo Alto to allow the app provider to access Customer's data as required for the interoperation with the Palo Alto products.

(b) **Warranty:**

(i) With regard to any Palo Alto products used in the provision of the Service, Vodafone warrants that:

(A) hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

(B) software shall substantially conform to the Palo Alto Published Specifications for three (3) months from fulfilment; and

(C) subscriptions shall perform materially to the Palo Alto Published Specifications for the entire duration of the selected term.

(ii) As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable. All warranty claims must be made on or before the expiration of the warranty period specified herein, if any. Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you

(c) **Exclusions:** the warranty set forth above shall not apply if the failure of the Palo Alto product results from or is otherwise attributable to:

(i) repair, maintenance or modification of the applicable Palo Alto product by persons other than Palo Alto or its designee;

(ii) accident, negligence, abuse or misuse of the applicable Palo Alto product;

(iii) use of the applicable Palo Alto product other than in accordance with the Palo Alto Published Specifications;

(iv) improper installation or site preparation or Customer's failure to comply with environmental and storage requirements set forth in the Palo Alto Published Specifications including, without limitation, temperature or humidity ranges; or

(v) causes external to the applicable Palo Alto product such as, but not limited to, failure of electrical systems, fire or water damage.

(d) **Disclaimers:** except for the warranties expressly stated and to the fullest extent permitted by Applicable Law, the Palo Alto products are provided "as is". Vodafone and its Third Party Providers make no other warranties and expressly disclaim all other warranties, express or implied, including without limitation any implied warranties of merchantability, fitness for a particular purpose, and any warranties arising out of course of dealing or usage of trade. Vodafone and its Third Party Providers do not warrant that (i) the Palo Alto products will meet Customer's requirements, (ii) the use of the Palo Alto products will be uninterrupted or error-free, or (iii) the Palo Alto products will protect against all possible threats whether known or unknown.

## 5. Deliverables

5.1 The Deliverables are set out in the Service Specification.

5.2 Vodafone will use secure methods of transmission of the Deliverables to the Customer. If the Customer requires a specific technology to be used, the Customer is responsible for providing Vodafone with access to the technology for transmission.

5.3 The Deliverables are provided only for the Customer and the Customer may be permitted to disclose the Deliverables to its respective affiliates, directors, and employees.

5.4 The Deliverables are intended for Customer's own internal use only and not for any use by third parties nor for use in any legal proceedings. Vodafone disclaims any liability that may arise out of any third-party's review and/or use of such Deliverables, or arising out of, or in connection with, such Deliverables being used in legal proceedings. In no circumstances will Vodafone be required to provide expert testimony in connection with the provision of the Service or any Deliverables under this Schedule.

5.5 Customer agrees that it is responsible for:

(a) assessing the applicability to Customer's business and operations of the Deliverables and the Service, and any recommendations, advice or instructions provided by Vodafone in the course of providing the Service; and

(b) determining whether the Service and Deliverables provided by Vodafone, including any revised business processes implemented pursuant to each applicable Order:

(i) meet Customer's business requirements;

(ii) comply with all Applicable Laws; and

(iii) comply with Customer's applicable internal guidelines, long-term goals and any related agreements.

## 6. General Assumptions and Dependencies

6.1 There will be no changes to the scope of the Service set out in these Service Specific Terms.

6.2 The Customer will be accountable for final sign-off on key decisions and deliverables e.g. pre-engagement checklist, design documentation, transition etc at the respective Customer Sites.

6.3 The Customer point of contact will be accountable for identifying the stakeholders within the Customer environment relevant to the Service.

6.4 Where Customer has selected either the New Build or Replacement Service Type, if the Customer requests one of the following activities, the Customer shall provide the necessary trusted certificates:

(a) a custom page related to Customer's organisation to be displayed when a mobile user logs in; and

(b) the logs stored in the CDL to be forwarded to Customer's syslog or security operations centre (**"SOC"**) solution.

6.5 Customer is responsible for providing and maintaining the applicable certificates required for the Service.

6.6 SAML server/authentication details will be provided by the Customer for mobile users' authentication. If Customer does not have SAML server/ authentication infrastructure, local users will instead be created by Vodafone in the Prisma Access firewall and the user credentials will be shared with each User.

6.7 Where Customer has selected either the New Build or Replacement Service Type, User ID policies are applicable for those Customer Sites where Customer has an Active Directory server available. The same Active Directory server cannot be leveraged for other Customer Sites.

6.8 If using the Palo Alto – Prisma Access firewall:

(a) there are only two zones: Trusted and Untrusted. Outbound NAT will use Untrusted Zone IP Address, inbound NAT cannot be configured for Prisma Access – Remote Network; and

(b) logs for remote networks and mobile users will be forwarded to CDL.

6.9 Where Customer has selected the Takeover Service Type:

(a) if there is an IP conflict with Vodafone hosting infrastructure, Customer has to NAT its firewall IP/ internal network. Vodafone may provide guidance to the Customer on the action to be taken;

(b) the firewall logs storage and retention will be managed by the Customer; and

(c) Customer shall provide Vodafone with access to its centralised management tools in order to provide the Takeover Service Type.

6.10 SSL decryption is not provided as standard. If the Customer requires SSL decryption, the Customer must provide the required certificates and assumes all responsibility for the decryption of the SSL traffic.

6.11 The Services does not provide monitoring of Security Events, any Security Event mitigation or advice regarding security issues or threats.

6.12 Customer must promptly notify Vodafone of any changes to information, provided by Customer to Vodafone, in relation to the Service.

6.13 Customer shall:

(a) provide to Vodafone the High-level design for each of the Customer Sites where the Service needs to be deployed before commencement of the Low-Level Design phase; and

(b) respond to Vodafone inputs and requests in time (within 1 Working Day of receipt) to ensure the project is completed as per the planned schedule.

6.14 Customer agrees it is responsible for the connectivity of and between its networks unless otherwise mutually agreed by Vodafone and Customer in writing.

6.15 Customer, on behalf of itself and its third-party licensors, consents, authorises and grants to Vodafone the right to access the Customer's Environment and the right to retrieve data stored in or produced by the Customer's Environment in order to provide the Service. Customer agrees that if the Customer upgrades or otherwise changes the Customer's Environment, Customer will work with Vodafone in good faith to determine the impact to the Service.

6.16 Customer agrees that where it provides its approval this means that it has followed its own internal approval requirements and Vodafone can rely on such approval and is not required to confirm/check any such approval.

6.17 Customer acknowledges that it has knowledge and skill particular to its business practices and it will share such knowledge and skill and provide Vodafone with access to Customer subject matter resources, to facilitate the provision of the Service and Deliverables.

6.18 Subject to Vodafone's approval, where Customer has selected the Takeover Service Type and Customer requests additions and/or changes to its existing firewall solution (e.g. additional network zones, incidents, changes, etc), these will be subject to a separate charge and agreement, to be agreed with the Customer.

6.19 Standard design templates will be used for all Deliverables where possible. Where a Customer requirement is complex in nature and/or requires a non-standard approach, Vodafone may decide it is possible to support the Customer requirements which may be subject to a separate charge, to be agreed with the Customer and set out in the applicable Order.

6.20 Where Customer selects either the Takeover Service Type or the Replacement Service Type, communication during the Customer Site survey and installation phase will be in English. Vodafone shall provide all documentation in English.

## 7. Security Requirements

7.1 Customer agrees it retains full responsibility for: (i) ensuring that the security requirements comply with all applicable laws, industry self-regulatory codes, meet Customer's business requirements, and comply with Customer's applicable internal guidelines, long-term goals, and any related agreements; (ii) pursuing any enforcement or legal action with regard to such requirements; and (iii) reviewing and updating the security requirements to reflect technological developments. Nothing in this Agreement shall be interpreted to mean that Vodafone verifies that such security requirements comply with applicable laws, Customer's internal guidelines, and related agreements, or otherwise meet Customer's business requirements.

7.2 Compliance with Customer security policies shall not require Vodafone to provide any service beyond the scope of this Schedule.

7.3 Customer will not be entitled to make a claim against Vodafone for losses suffered or incurred by Customer to the extent such losses are the result of a security defect that: (i) exists in the Customer's legacy environment; or (ii) is introduced into the Customer's legacy environment by Customer or a third-party provided that such claim or loss is not attributable to or caused by: a) Vodafone negligence; or b) a Vodafone failure to perform the Services in line with terms of this Agreement.

## 8. Data Protection

8.1 Where the Customer shares Personal Data with Vodafone for the Processor Services, the Customer warrants and undertakes that it has complied with all necessary obligations imposed on it under Applicable Law including ensuring that it has either (i) obtained all necessary consents to transfer the Personal Data to Vodafone; or (ii) secured another lawful basis, in accordance with Applicable Privacy Law, to share such Personal Data with Vodafone for the processing envisaged by this Agreement and has provided appropriate privacy notices to the relevant data subjects (as required by Applicable Privacy Law) to enable it to share the Personal Data with Vodafone for the purposes envisaged by this Agreement.

8.2 For elements of this Service, Vodafone may act in the capacity as a Data Processor (**"Processor Services"**).

8.3 Vodafone (and its subcontractors):

(a) may Process User Personal Data for: (i) provision and monitoring of the Service; or (ii) any other purpose agreed between the parties subject to Customer's prior written consent. Additional instructions require prior written agreement and may be subject to Charges. Customer shall ensure that its instructions comply with Applicable Laws.

(b) may use User Personal Data to create statistical data and information about service usage and devices that does not identify a User.

(c) may engage another processor (a **"Sub-Processor"**) to carry out processing activities in the provision of the Services or to fulfil certain obligations of Vodafone under the Agreement. Vodafone shall inform the Customer of changes to Sub-Processors where Vodafone is required by Applicable Privacy Law by (i) providing at least ten (10) Working Days' prior notice, or (ii) listing the new or replacement Sub-Processor on www.vodafone.co.uk and/or at least ten (10) Working Days before Vodafone authorises and permits the new or replacement Sub-Processor access to User Personal Data in order to give the Customer the opportunity to reasonably object to such changes. Vodafone will enter into a contract or other legal act with the Sub-Processor and will impose upon the Sub-Processor substantially the same legal obligations as under this clause to the extent required by Applicable Privacy Law and that the Sub-Processor is

carrying out the relevant processing activities. Vodafone shall remain liable to the Customer for the performance of that Sub-Processor's obligations.

(d) may retain the User Personal Data for as long as is required to deliver the Service and shall destroy or return (at Customer's option) User Personal Data in its possession upon termination of the Agreement, save where Customer opts for Vodafone to retain User Personal Data subject to a new hosting agreement.

(e) shall limit access to User Personal Data to those necessary to meet Vodafone's obligations in relation to the Service and take reasonable steps to ensure that they: (i) are under an appropriate statutory obligation of confidentiality; (ii) are trained in Vodafone's policies relating to handling User Personal Data; and (iii) do not process User Personal Data except in accordance with the Customer's instructions unless required to do so by Applicable Law.

(f) shall (i) provide appropriate technical and organizational measures for a level of security appropriate to the risks that are presented by Processing; and (ii) comply with the security requirements contained in the Vodafone information security policies and/or based on ISO 27001;

(g) shall (i) provide Customer with such information, assistance and co-operation as Customer may reasonably require to establish compliance with Applicable Privacy Law including any personal data breach notification; (ii) without undue delay, notify Customer of any unauthorised access to User Personal Data of which Vodafone becomes aware, which results in loss, unauthorised disclosure or alteration to the User Personal Data; and (iii) where required by Applicable Privacy Law and requested by the Customer (prior to the processing), provide the Customer reasonable assistance to carry out a privacy impact assessment of the Services and any prior consultation of the relevant supervisory authority.

8.4 **Audit:** Customer shall with respect to any right of audit, including inspections, which they may have under Applicable Privacy Law relating to data protection, agree to exercise such right as follows: (a) no more than once per annum following the Agreement Start Date, request to meet (on a mutually acceptable date) with one or more senior representatives of Vodafone's security and/or audit department to review Vodafone's security organization and the best practice and industry standards which Vodafone meets or to which it aspires, including, without limitation, ISO 27001 (or equivalent), provided that such audit shall relate to the Services only. If the Transfer Contract Clauses apply (the model contract clauses set out in the European Commission's Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to data-processors established in third countries, under the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data as may be amended or replaced by the European Commission from time to time), nothing in this clause 8.4 amends or varies those standard clauses nor affects any data subject or supervisory authority's rights under those clauses; and (b) be responsible for reviewing the information made available by Vodafone and making an independent determination if the Services meet the Customer's requirements and legal obligations as well as its obligations under this clause.

8.5 **Transfer of User Personal Data out of the UK and EEA:** Vodafone may transfer User Personal Data to countries outside the European Economic Area only to the extent that (i) User Personal Data is transferred on terms substantially in accordance with the Transfer Contract Clauses for the transfer of Personal Data to processors established in third countries; (ii) that the transfer of User Personal Data does not put any member of Customer Group in breach of its obligations under Applicable Privacy Law; or (iii) it is required to do so by Union or Member State law to which it is subject; in such a case, Vodafone shall inform the Customer of that legal requirement before processing, unless that law prohibits such information.

8.6 **Law enforcement authorities:** Vodafone: (i) may receive legally binding demands from a law enforcement authority for the disclosure of, or other assistance in respect of, User Personal Data, or be required by Applicable Law to disclose User Personal Data to persons other than Customer; (ii) will not be in breach of its obligation to Customer in complying with such obligations to the extent legally bound; and (iii) shall notify Customer as soon as reasonably possible of any such demand unless otherwise prohibited.

8.7 **Enquiries from Users:** Vodafone shall, where the Customer is required under Applicable Privacy Law to respond to enquiries or communications (including subject access requests) from Users and taking into account the nature of the processing (i) without undue delay pass on to Customer any enquiries or communications (including subject access requests) that Vodafone receives from Users relating to their User

Personal Data or its Processing; and (ii) assist the Customer by appropriate technical and organizational measures, insofar as this is possible in the Customer's fulfilment of those obligations under Applicable Privacy Law

## 9. Delivery

9.1 Vodafone will make the Service available to Customer on the Service Commencement Date.

9.2 The Service shall be provided from the UK and India in English language.

## 10. Out of Scope Activity

10.1 Anything not specifically described in these Service Specific Terms is out of scope and is not included in the Service. In addition, and for avoidance of doubt, the following are not in scope for the Service:

(a) any procurement of firewall licenses and maintenance agreements for any of the in-scope Service. Customer shall be responsible for providing these items;

(b) any physical onsite support in Customer locations, where applicable;

(c) configuration of switches and other network devices;

(d) UAT and product training to Customer;

(e) ownership and maintenance of infrastructure in case of a virtual firewall;

(f) procurement of solution components;

(g) fixing product related bugs;

(h) providing a separate SIEM / log management solution;

(i) custom IPS signature fine tuning;

(j) remediation work as part of rule base review activity, to the extent the remediation works go beyond the firewall managed as part of the Service.

# Service Levels

## Firewall Management Service

Vodafone Business Customers

## 1. Service Levels

1.1 The Standard Service Levels are as follows:

| SLA ref | Service Level Description | Minimum Service Level | Measurement Period | Low Volumes (Y/N) |
|---|---|---|---|---|
| 1. | Incident Response Time of 30 minutes for Priority 1 Incidents | 95% | Month | Y |
| 2. | Incident Response Time of 60 minutes for Priority 2 Incidents | 95% | Month | Y |
| 3. | Incident Response Time of 1 Working Day for Priority 3 Incidents | 90% | Month | N |
| 4. | Incident Response Time of 3 Working Days for Priority 4 Incidents | 90% | Month | N |
| 5. | Incident Resolution Time of 4 hours for Priority 1 Incidents | 95% | Month | Y |
| 6. | Incident Resolution Time of 8 hours for Priority 2 Incidents | 95% | Month | Y |
| 7. | Incident Resolution Time of 3 Working Days for Priority 3 Incidents | 90% | Month | N |
| 8. | Incident Resolution Time of 5 Working Days for Priority 4 Incidents | 90% | Month | N |

1.2 Measurement of Service Levels

The following sets out the manner in which the Service Level Value for each of the Service Levels referred to in the table above will be calculated.

(a) **SLA 1:** Incident Response Time for Priority 1

SLA 1 = A / B * 100%

where:

**A** means the number of Priority 1 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month which have an Incident Response Time of 30 minutes or less

**B** means the total number of Priority 1 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month

(b) SLA 2: Incident Response Time for Priority 2

SLA 2 = C / D * 100%

where:

**C** means the number of Priority 2 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month which have an Incident Response Time of 60 minutes or less

**D** means the total number of Priority 2 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month

(c) SLA 3: Incident Response Time for Priority 3

SLA 3 = E / F * 100%

where:

**E** means the number of Priority 3 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month which have an Incident Response Time of 1 Working Day or less

**F** means the total number of Priority 3 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month

(d) SLA 4: Incident Response Time for Priority 4

SLA 4 = G / H * 100%

where:

**G** means the number of Priority 4 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month which have an Incident Response Time of 3 Working Days or less

**H** means the total number of Priority 4 Incidents for which an Incident Ticket is received by Vodafone in the relevant calendar month

(e) SLA 5: Incident Resolution Time for Priority 1

SLA 5 = I / J * 100%

where:

**I** means the number of Priority 1 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month which have an Incident Resolution Time of 4 hours or less

**J** means the total number of Priority 1 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month

(f) SLA 6: Incident Resolution Time for Priority 2

SLA 6 = K / L * 100%

where:

**K** means the number of Priority 2 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month which have an Incident Resolution Time of 8 hours or less

**L** means the total number of Priority 2 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month

(g) SLA 7: Incident Resolution Time for Priority 3

SLA 7 = M / N * 100%

where:

**M** means the number of Priority 3 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month which have an Incident Resolution Time of 3 Working Days or less

**N** means the total number of Priority 3 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month

(h) SLA 8: Incident Resolution Time for Priority 4

SLA 8 = O / P * 100%

where:

**O** means the number of Priority 8 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month which have an Incident Resolution Time of 5 Working Days or less

**P** means the total number of Priority 4 Incidents for which an Incident Ticket is Resolved by Vodafone in the relevant calendar month

## 2. Dependencies

The following sets out the Dependencies for each of the Service Levels referred to in Clause 1 (Service Levels).

2.1 **Customer Dependencies**

(a) The Customer Dependencies applicable to all Service Levels referred to in Clause 1.1 (Service Levels) are as follows.

(i) Vodafone can remotely access the Customer's systems.

(ii) The Customer's subject matter expert is available for testing.

(iii) The Customer has OEM contracts and premier support in place for hardware and parts replacement.

(b) SLA 5: Incident Resolution Time for Priority 1: The additional Customer Dependencies for SLA 5 are as follows.

(i) Downtime of the Customer's systems is provided (for a period directed as by Vodafone) for Incident resolution.

(c) SLA 6: Incident Resolution Time for Priority 2: The additional Customer Dependencies for SLA 6 are as follows.

(i) Downtime of the Customer's systems is provided (for a period directed as by Vodafone) for Incident resolution.

(d) SLA 7: Incident Resolution Time for Priority 3: The additional Customer Dependencies for SLA 7 are as follows.

(i) Downtime of the Customer's systems is provided (for a period agreed with the Customer) for Incident resolution.

(e) SLA 8: Incident Resolution Time for Priority 4: The additional Customer Dependencies for SLA 8 are as follows.

(i) Downtime of the Customer's systems is provided (for a period agreed with the Customer) for Incident resolution.

## 3. Incident Priority Levels and Definitions

3.1 Below is the "**Incident Priority Impact**" matrix which sets out the scoring used to determine the Priority of an Incident between Priorities 1, 2, 3, and 4, such matrix which is aligned to the ITIL framework.

3.2 Each Incident will be assessed in terms of its impact upon the business with which the business requires the Incident to be resolved or a work around to be implemented, by applying the below matrix. The Incident shall be assigned a Priority based on this assessment.

Table 1: Incident Priority Impact Matrix

| Priority Level | Impact |
|---|---|

| | 1 – Extensive / Widespread | 2 – Significant / Large | 3 – Moderate / Limited | 4 – Minor / Local |
|---|---|---|---|---|

The definitions of impact for assessing priority level with respect to the overall Customer base and the individual Customer are detailed below:

- **Priority 1 (Extensive / Widespread):** A complete breakdown or outage or a critical performance degradation causing service unavailability
- **Priority 2 (Significant / Large):** The functionality of the Service is affected to a large extent, a major performance degradation or loss of important function occurs, security is critically affected, or a breach of an applicable law occurs
- **Priority 3 (Moderate / Limited):** A minimal limitation to the functionality of the Service e.g. intermittent connectivity issue
- **Priority 4 (Minor / Local):** No limitation to the functionality but may impact the service if the issue is not resolved e.g. momentary spike in CPU/ memory utilization.

# Firewall Management Service

Vodafone Business Customers

## Appendix A - Ticket Management

**Service Requests**

The following are standard service requests that can be raised by Customers:

- Firewall rule base change to open access from given source to destination/application
- URL whitelisting
- New site to site VPN setup
- Provision of new VLAN/interface/sub interface on firewall
- File type/extension whitelisting/blacklisting
- Firewall OS upgrade/downgrade
- Remote Assistance in Hardware replacement which are hot swappable like PSU
- Remote Assistance in RMA/device replacement (on premise)
- Rebuild of firewall (cloud)
- Security profile configuration change related to AV/IPS/data filtering
- URL recategorization
- Add new application in existing rules
- Creation of new network object/host/range in existing rule
- Adding/removing static routes
- NAT changes

**Tickets that do not contribute to the Tier 1/Tier 2 volume quota**

Third Party Provider will process the following Service Requests without the ticket being counted towards a Customer ticket quota.

- New account creation for client to site VPN users
- User on/off-boarding on firewall
- (IOC block) URL/IP block list
- Password reset
- Firewall reboot/shutdown
- Firewall failover

# Firewall Management Service

Vodafone Business Customers

The following actions may require a request to be raised however Third Party Provider will process these requests without the ticket applying to a Customer ticket quota.

- If a Change Request is required to fix an issue already raised via another request, the Change Request ticket will not count towards a Customer ticket quota
- Flying/passing incident will not be debited from Customer Ticket quota, Example: If there's a network issue, but the firewall team was engaged to help in troubleshooting, if the resolution concluded that no action is required from firewall side a Ticket will not be debited.
- Sync/integration related incidents between Firewall/ Monitoring/ Reporting tools will not be debited from client allocated tickets.
- Change Requests created to formally capture any changes required during the 48hr hyper-care period after firewall deployment

# Firewall Management Service

Vodafone Business Customers

## 1. Definitions

1.1 The following definitions are applicable to the Service

| | |
|---|---|
| **Active-Active** | means more than one firewall running the same service at all times allowing all requests to be shared across all available processing capacity, usually to allow load balancing. |
| **Active Directory** | means the platform which stores information about objects on the network and makes this information easy for administrators and users to find and use. |
| **Active-Passive** | means having more than one firewall where at least one firewall (secondary) is not going to be active but is instead listening in standby mode to the active (or primary) firewall. The secondary firewall will act as a backup ensuring business continuity with seamless failover when a primary firewall fails. |
| **Applicable Firewall Vendors** | means those vendors listed in clause 3.1. |
| **CDL** | means Cortex Data Lake, the capability from Palo Alto that provides cloud-based logging for Prisma Access. CDL allows the Prisma Access service to collect and store logs for the provision of the Service. |
| **Change Request** | means addition, modification, or removal of anything that could have a direct or indirect effect on services to IT infrastructure, applications or any other critical component. |
| **Checkpoint** | means Checkpoint Software Technologies Ltd. |
| **Cisco** | means Cisco Systems, Inc |
| **Custom Reporting** | means the creation of customised operational report(s) within the NGFW to suit the pre-determined requirements of the Customer and to the extend technically and reasonably possible by the NGFW product. (e.g., customised reports). |
| **Deliverables** | means any deliverable, process or document to be provided by Vodafone in accordance with these Service Terms and as detailed in the Service Specification. |
| **Endpoint** | means the Customer's computers or laptops that host any one of Windows, Mac or Linux Operating systems (irrespective of the hardware used and the hosting location). |
| **Environment** | means the Customer's relevant systems, security controls, network infrastructure, and Endpoints. |
| **Existing Firewall** | means an individual firewall instance that the Customer requests to be managed as part of the Service. |
| **Fortinet** | means Fortinet or Fortinet Inc |
| **Group Company** | means an or a company or corporation within Vodafone Group (as the case may be). |

| | |
|---|---|
| **Incident** | means an event which causes, or may cause, an unplanned interruption to a firewall or a reduction in the quality of the Service. |
| **Incident Resolution Time** | means the period commencing at the time (rounded up to the next whole minute) at which the Incident Ticket in respect of an Incident has been Responded To and ending at the time (rounded down to the previous whole minute) that such Incident is Resolved. |
| **Incident Response Time** | means the period commencing at the time (rounded up to the next whole minute) at which Vodafone receives an Incident Ticket and ending at the time (rounded down to the previous whole minute) at which the Incident Ticket has been Responded To. |
| **Incident Ticket** | means a request issued by Customer to Vodafone via phone in relation to an Incident. |
| **Juniper** | means Juniper Networks Inc |
| **Lightweight Directory Access Protocol** or **LDAP** | means an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network. |
| **NAT** | means Network Address Translation, a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. |
| **NGFW** | means Next Generation Firewall, the current generation of firewalls which combine tradition firewall capabilities with other network device security features. |
| **Palo Alto** | means Palo Alto Networks Inc. |
| **Palo Alto – Prisma Access** | means a cloud-based firewall as a service (FWaaS) provided by Palo Alto that aims to protect remote users and business locations from threats while also providing the security services expected from a modern NGFW. |
| **Palo Alto Published Specifications** | means the user manual and other corresponding material published by Palo Alto and customarily made available to Users of the applicable Palo Alto product. |
| **Priority** | means, in respect of an Incident, the Priority level of such Incident as determined in accordance with the Service Levels. |
| **Resolved** | means, in respect of an Incident, its Incident Ticket has been resolved by Vodafone. |
| **Responded To** | means, in respect of an Incident Ticket, Vodafone communicates to the Customer that its Incident Ticket has been received. |
| **SAML** | means Security Assertion Markup Language, an open standard for exchanging authentication and authorisation data between parties (for example between an identity provider and a service provider) . |
| **Security Event** | means any act or attempt by people or malicious software to gain unauthorized access, disrupt service, or use systems or data in violation of Customer's policies. |

| | |
|---|---|
| **Service Level(s)** | the service levels that apply to the provision of the Service as set out in these Service Terms. |
| **Service Request** or **SR** | means the service requests listed in Appendix A raised from a User or on behalf of a User that initiates a service action as a part of normal service delivery. Service Requests cannot be used in response to a failure or degradation of services. |
| **SSL** | means Secure Sockets Layer, a standard protocol used to establish a secure communication connection between two devices (for example between a server and a client). A protocol which has been deprecated and replaced by a newer protocol Transport Layer Security (TLS). |
| Tenant | Means a virtual firewall, hosted by Palo Alto. A dedicated tenant is for a single customer. A shared tenant is between two or more Customers. |
| Third Party Provider | a third party contracted directly or indirectly by either Vodafone (including Vodafone Group) or Customer that provides a Service, a Third Party Service or that provides a service that connects to a Service. Third Party Providers may include incumbent providers. |
| **Ticket** | means a request issued by a Customer to Vodafone in relation to Incident management, Service Request management or Change Request management. |
| **Trusted Zone** | means internal interfaces (Private). |
| **Untrusted Zone** | means external interfaces (Public). |
| **Vodafone Business Marketplace ("VBM")** | means the platform set out at https://marketplace.vodafone.co.uk/home. |
| **Vodafone** | means (a) Vodafone Limited, a company incorporated in England with registration number 1471587, whose registered office is at Vodafone House, The Connection, Newbury, Berkshire, RG14 2FN, England; and/or (b) a Third Party Provider acting on behalf of Vodafone,.. |
| **Vodafone Group** | means Vodafone Group plc and each body corporate, partnership, or unincorporated association, in respect of which Vodafone Group plc owns (directly or indirectly) at least 15 per cent of:<br>(a) the issued share capital; or<br>(b) the ownership interests or units issued by such partnership or unincorporated association |
| **Wild-Fire** | means the platform from Palo Alto which provides sandbox capability allowing the inspection of unknown threats, files or email links and provides a verdict on its safety. |