Service Specification

Firewall Management Service

Business Customers

1. Introduction

1.1 Further details of the Service Types provided are as follows:

(a) **New Build Service Type and Replacement Service Type** – Prisma Access (SaaS solution powered by Palo Alto)

Provides the security, visibility, and control of Palo Alto Networks' next-generation firewall (NGFW) solution but within a cloud-based solution. All Users can connect safely and securely to cloud applications as well as the internet.

(b) **Takeover Service Type –** Firewall Management service for Customer-owned devices

The Service will manage the firewall hosted in the Customer's Environment or cloud to protect customer network communications from malicious activity, in accordance with Customer's security requirements. Leveraging the customer's investment in their existing firewalls while ensuring the configuration and rules are compliant to customer policy, and maintained to enterprise grade security standards, using the existing management console.

2. Service Packaging

2.1 Standard Technical Features: The Service offers the following core technical features for New Build and Replacement firewalls. For Takeover, the technical features will be as per the Customer's existing solution.

(a) **Application ID Inspection:** The Application ID inspection features on the NGFW, accurately identifies applications, including applications disguised as authorised traffic, using dynamic ports, or trying to hide under the veil of encryption. Application ID allows Customer to understand and control applications and their functions, such as video streaming versus chat, upload versus download, screen-sharing versus remote device control and implement defined policy. For avoidance of doubt, a Web Application Firewall is not provided as part of the Service. However, the Application ID features on the NGFW can be used to configure firewall rules.

(b) **User ID Policy:** The User ID policy enables the NGFW to identify Users in their locations. User ID policy creation is dependent on the presence of LDAP capabilities available outside the customer's internal network protected by this firewall.

(c) **Vulnerability Protection Profile:** The Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorised access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network. Vulnerability Protection profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. For the New Build Service Type and Replacement Service Type, while signature updates to the firewall will be done by Palo Alto, Vulnerability Protection Profile will be configured by Vodafone. For the Takeover Service Type, the Customer's existing process will be followed.

(d) **Anti-Virus:** The Antivirus profiles protect against viruses, worms, trojans, spyware downloads, etc. Using a stream-based malware prevention engine, which inspects the traffic the moment the packet is received. This profile scans for a wide variety of malware in executables, PDF files, HTML and JavaScript viruses, including support for scanning inside compressed files and data encoding schemes. For the New Build Service Type and Replacement Service Type, while signature updates to the firewall will be done by Palo Alto, Anti-Virus Profile will be configured by Vodafone. For the Takeover Service Type, the Customer's existing process will be followed.

(e) **Anti-Spyware:** The Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing detection of malicious traffic leaving

the network from infected clients. For the New Build Service Type and Replacement Service Type, while signature updates to the firewall will be done by Palo Alto, Anti-Spyware Profile will be configured by Vodafone. For the Takeover Service Type, the Customer's existing process will be followed.

(f) **URL Filtering:** The URL Filtering feature enables Customer to monitor and control how users can access the web over HTTP and HTTPS. It enables safe access to the internet by preventing access to known malicious sites, phishing sites as well as other restricted sites such as adult content sites. For the New Build Service Type and Replacement Service Type, while content updates will be provided by Palo Alto (or respective OEM), the template to capture the required configuration / URL categories will be provided by Vodafone. For the Takeover Service Type, the customer will provide the list during onboarding.

(g) **File Inspection:** This feature blocks specified file types in the specified flow direction – inbound, outbound or both. The profile can be set to alert or block an upload and/or download files. Custom configuration can be done to block pages when Users try to download a specified file type.

(h) **Data Filtering:** This feature prevents sensitive, confidential, and proprietary information from leaving a network. Predefined patterns, built-in settings and options to customise, make it easy to protect files that contain certain file properties (such as a document title or author), credit card numbers, regulated information from different countries (like social security numbers), and third-party data loss prevention (DLP) labels.

(i) **Signature updates:** Signature updates refresh the threat prevention signatures, which inspect all traffic for threats—regardless of port, protocol or encryption and automatically block known vulnerabilities, malware, exploits, spyware, command, and control.

2.2 Optional Service Elements

(a) The Optional Service Elements available to Customer are as follows:

(i) **Sandbox analysis:** Sandbox analysis (Wildfire by Palo Alto) subscription service will provide enhanced services to Customer requiring immediate coverage for threats, forward unknown file types and email link for further analysis. It assists by providing a prompt verdict of the files analysed.

(ii) **Firewall Audit:** Firewall rule review is performed to ensure that the firewall configuration and rule set, meets the business and compliance requirements of the organization. The audit will be performed bi-annually.

(iii) **High Availability (Takeover Service Type only):** High Availability is a deployment method. In this method, two firewalls are placed in a group and their configuration is synchronised to prevent a single point of failure. Setting up two firewalls in a High Availability pair provides redundancy and enables business continuity.

(iv) **Pack of 10 Tickets:** An additional pack of 10 Tickets can be purchased by Customer on expiry of its allocated Ticket quota. The Tickets can be used for Service Requests, Change Requests and/or Incident requests.

2.3 Service Tier Details

(a) The table below summarises the Service offering and any associated volume quota. Where Customer has selected the Takeover Service Type, the functionality offered shall be dependent on the Applicable Firewall Vendor firewall and as such the following Service offerings can and will only be provided by Vodafone to the extent technically and reasonably possible using the existing Applicable Firewall Vendor firewall.

Service Offering	Service Offering Features	Tier 1 Volume Quota Per Annum (where applicable)	Tier 2 Volume Quota Per Annum (where applicable)	Additional Information
Technical Features	*Anti-Virus*	Included	Included	See Attachment 1 for feature description
	Anti-Spyware	Included	Included	See Attachment 1 for feature description
	Application ID Inspection	Included Up to 5 custom applications in addition to the firewall's default applications	Included Up to 20 custom applications in addition to the firewall's default applications	Custom applications will be captured in a pre-defined template and customer will share the application port/ID See Attachment 1 for feature description
	User ID policy	Included Up to 150 policies	Included Up to 300 policies	For New Build Service Type and Replacement Service Type User ID policy for Mobile Users will work with SAML User ID policy for Remote Network will work with AD/LDAP if available locally See Attachment 1 for feature description
	Vulnerability Protection Profile	Included Using the firewall's default profile	Included With ability to customise the action	See Attachment 1 for feature description

Service Offering	Service Offering Features	Tier 1 Volume Quota Per Annum (where applicable)	Tier 2 Volume Quota Per Annum (where applicable)	Additional Information
			for critical/high severity signature	
	URL Filtering	Included And up to 100 custom URLs	Included And up to 500 custom URLs	The URL volumes listed here represent the quota for additional custom URLs that the customer may request after the build phase (using a pre-defined templates provided by Vodafone) See Attachment 1 for feature description
	File Inspection	Included Using the firewall's default profile	Included Up to 20 custom file types may be configured in addition to the firewalls default profile.	See Attachment 1 for feature description
	Data Filtering	Included Using the firewall's default profile	Included Up to 10 custom policies may be configured in addition to the default configuration.	See Attachment 1 for feature description
	Signature updates	Included Using the firewall's default profile with	Included Using the firewall's default profile with	See Attachment 1 for feature description

Service Offering	Service Offering Features	Tier 1 Volume Quota Per Annum (where applicable)	Tier 2 Volume Quota Per Annum (where applicable)	Additional Information
		automatic updates	automatic updates	
Service Management Features	*Incident management*	Up to 10 Tickets per Existing Firewall (Takeover Service Type) or per Site (New Build Service Type/Replacement Service Type)	Up to 18 Tickets per Existing Firewall (Takeover Service Type) or per Site (New Build Service Type/Replacement Service Type)	A Ticket can be raised and used for Incident management, Service Requests or Change Requests. If the quota is reached in a contract year, additional blocks of Tickets can be purchased as an Optional Service Element A list of requests that **do not** count towards the quota are detailed in Attachment 3. Any unused tickets will expire at the end of the contract year
	Service Request management			
	Change Request management			
	Reporting	Included The standard set of reports outlined in the Customer Deliverables Section.	Included The standard set of reports outlined in the Customer Deliverables section AND up to 5 Custom Reports	

Service Offering	Service Offering Features	Tier 1 Volume Quota Per Annum (where applicable)	Tier 2 Volume Quota Per Annum (where applicable)	Additional Information
	Support Window	Included *24*7*	Included *24*7*	
	SLA	Standard SLA	Standard SLA	
	Architecture Support	Not Included	Included Up to 5 man days effort	Applicable to Tier 2 only. See Attachment 1 for feature description
Maintenance Features	*Health and Availability Management*	Included	Included	See Attachment 2 for feature description
	Back-up Management	Included	Included	See Attachment 2 for feature description
	Policy Updates and FW Administration	Included	Included	See Attachment 2 for feature description
	Patch Management/Minor upgrades	Included	Included	See Attachment 2 for feature description
	Concurrent VPN (Remote Access)	Included Where an integration is not available the following will apply: Up to 50 users per Existing Firewall (Takeover Service Type) or Site (New Build Service	Included Where an integration is not available the following will apply: Up to 50 users per Firewall or Site	Dependency: For New Build Service Type and Replacement Service Type: Integration with Customer SAML solution to provision VPN Users See Attachment 2 for feature description

Service Offering	Service Offering Features	Tier 1 Volume Quota Per Annum (where applicable)	Tier 2 Volume Quota Per Annum (where applicable)	Additional Information
		Type/Replacement Service Type)		
	Hardware Capacity Management and Performance Monitoring	Included Applicable to Takeover Service Type only	Included Applicable to Takeover Service Type only	Not applicable for New Build Service Type or Replacement Service Type See Attachment 2 for feature description
	Major Version Upgrades	Included -but on request by Customer via a Service Request.	Included - two upgrades per annum	See Attachment 2 for feature description

3. Prisma Access Solution

3.1 Prisma Access provides firewall as a service (FWaaS) that aims to protects remote users and business locations from threats while also providing the security services expected from a modern NGFW.

3.2 All users, whether at corporate headquarters, branch offices, or on the road, connect to Prisma Access to safely use cloud applications as well as the internet. Prisma Access consistently inspects all traffic across all ports and provides bi-directional networking.

3.3 Prisma Access stores logs centrally within the Cortex Data Lake (CDL) environment. The logs are stored in the EU region and in an encrypted format. CDL is delivered as a cloud service.

3.4 Panorama is the centralized management tool used to configure security policy for Prisma Access.

3.5 Prisma Access provides both visibility into the use of applications on the network, and the ability to control user access to those applications. There are two options available as part of Prisma Access:

(a) Prisma Access for networks - Prisma Access for networks provides security services such as App-ID and threat prevention for remote networks, safely enabling commonly used applications and web access, which are available on internet and cloud hosted. Remote networks can be connected to Prisma Access via an industry-standard IPSec VPN-capable device. Prisma Access is ideally suited for any remote site with one or multiple internet links and provides secure internet access.

(b) Prisma Access for users- Prisma Access for users provides secure internet access including App-ID and threat prevention for mobile users as a service in the cloud. Global protect software agent will be installed on all the

mobile users' endpoints to provide secure internet access.

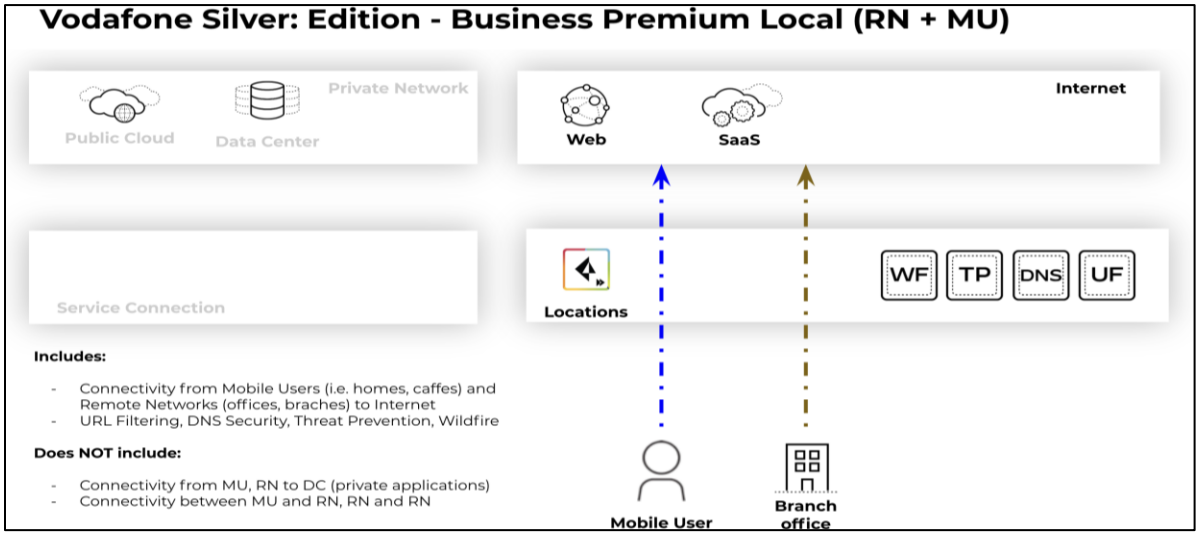

Figure 1: Palo Alto Prisma Access Silver Edition

3.6 Prisma Access details, features and specification is as follows:

Description	Prisma Access for Networks	Prisma Access for Users
Use Case	• Branch offices/retail • Virtual private clouds • Palo Alto Networks SD-WAN hub • Third-party SD-WAN security	• Mobile users with: ○ Laptops ○ Smartphones ○ Tablets • Zero Trust network access
Licensing	Based on bandwidth pool; each connection can be assigned up to 500 Mbps	Based on total number of unique users
Minimum Deployment Size	Bandwidth pool of 200 Mbps	200 users
Authentication	LDAP/Active Directory	SAML Authentication: Okta, Duo, Ping, Azure AD

3.7 It is to be noted that network-based license for Prisma Access is based on the total bandwidth used across all the sites. This bandwidth pool can then be divided across the different locations. A minimum bandwidth pool of 200 Mbps needs to be purchased. If Prisma Access is deployed for mobile users, the standard license allows the customer to deploy for upto 200 users. The remote users are protected to the same level as the corporate sites.

4. Service Description and Deployment Model

4.1 New Build Service Type – Green Field

(a) This Service Type is best suited for where Customer has a growing number of users, branch offices, data and services located outside the protection of traditional network security appliances, hence requiring a cloud-based infrastructure that converges networking.

(b) The following features will not be available for a shared tenant:

(i) Company domain name for mobile users' access portal

(ii) User ID based policy

(iii) Multiple Data Centers

(iv) Bandwidth requirement of 200Mbps or above

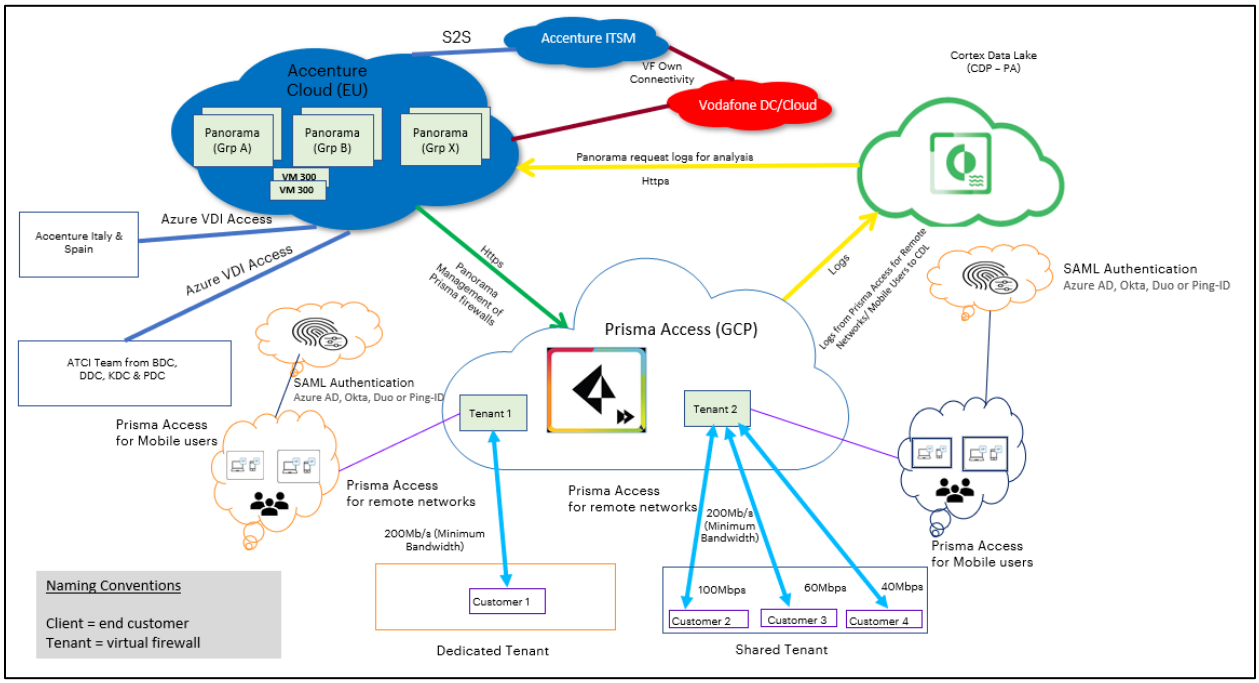

Figure 2: Deployment Model for Prisma Access Solution

(c) In Figure 2 above, Customer 1 has opted for dedicated tenant while Customers 3,4 and 5 have opted for a shared Tenant i.e. they would be sharing the 200 Mbps bandwidth.

(d) Criteria for Selecting dedicated tenant:

(i) Usage of Company domain name for Mobile users' access portal

(ii) User ID based policy

(iii) Bandwidth requirement 200Mbps or above

(iv) Dedicated policy package

(e) The main limitation of a shared tenant is that the policy package will be shared across all the customers in the shared tenancy. However, rules will be applied to specific customer based on their unique IP address range. Also, User ID agent can be configured for one customer only.

4.2 Takeover Service Type – Brownfield

(a) This Service Type is available where Customer has an existing investment in firewalls and wants to retain these devices but wish to outsource management and support. The Customer will retain ownership of the equipment, but the existing services are transitioned to Vodafone for management.

(b) During takeover, Vodafone will perform the assessment of existing firewall-set up and highlight risk (if any) for sign off. Proposed risk mitigation plan will be discussed and agreed with the Customer. Vodafone will connect to the Customer's Environment to remotely manage the firewalls. On-boarding activities will be executed by establishing secure S2S connectivity between Vodafone and the Customer. If there are any issues related to the firewall, Vodafone will raise the support requests on behalf of the Customer.

(c) Vodafone will leverage the Customer's centralised management tool, where applicable, to perform management activities. In cases where the Service can't be delivered due to hardware limitations, while Vodafone will work with the Customer to find an alternative approach, it might not be possible in all circumstances.

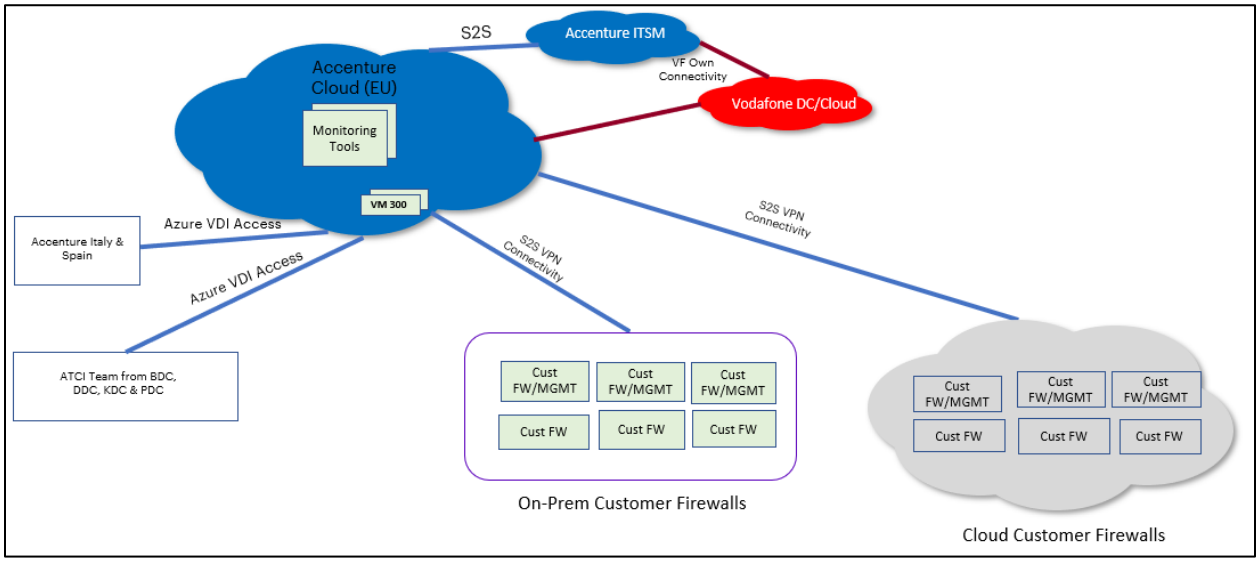

Figure 3: Deployment Model for Takeover Solution

4.3 Replacement Service Type – Brownfield

(a) Where Customer would like to replace an existing firewall with a new firewall, the Prisma access option, utilising the same solution as the New Build Service Type, shall be selected. The New build Service Type process will be followed to enable Prisma Access.

(b) The design document will cover the following:

(i) Existing Firewall architecture and configurations

(ii) Detailed Design for replacement firewall – Prisma Access

(iii) Existing rulesets and how these will be integrated into the new solution

(c) Once the design is agreed, a parallel solution, based on Prisma Access, will be built. Firewall rules to be built, based on Prisma Access configuration template, to de-risk the process by transitioning the existing configurations to the new Prisma Access.

(d) Testing of each of the security services will be performed using test window provided by the Customer to ensure that Prisma Access is operating correctly and that the rules are in place to block or allow traffic as per the original firewall.

(e) Once the test results are reviewed and approved, a switchover to Prisma Access will be scheduled, while leaving the old systems in-place (disconnected) to allow for rollback if required.

5. Service Delivery

5.1 Service Delivery Approach

(a) The following table outlines the service provisioning stages for the Service:

Provisioning Stage	Description
Establish Context	Gather initial requirements to agree on project scope.
Target State Assessment	Perform necessary due diligence to understand the Customer's Environment.
Target State	Define/update a target-state firewall architecture where appropriate.
Low Level Design	Define/update a corresponding low-level design.
Integration	Deployment of centralised management platform / tools and integration of Firewall
Firewall Deployment	Provision firewall features based on Tier 1 or Tier 2 Customer requirements and applicable Optional Service Elements.
Transition	Knowledge transfer to Customer
Operation	Perform applicable activities based on Tier 1 or Tier 2 Customer requirements and applicable Optional Service Elements.

(b) The following table sets out the key activities for each provisioning stage, and the associated Service provisioning documents. The Activities will apply to the Service unless detailed otherwise:

Activities	Description	Provisioning documents
Establish Context	• Review requirements and confirm dependencies • Define the firewall scope • Define roles and responsibilities Note – only those elements applicable to the Service will be included, e.g. they will not include information related to Customer's broader network and firewall plans and strategy	**Project Scoping Document*** • Firewall scope • Requirements and dependencies • Roles and responsibilities • High-level milestone plan
Target State Assessment	• Perform necessary due diligence to understand the Customer's Environment • Understand the Customer and Vodafone capacity requirement	
Target state	New Build Service Type / Replacement Service Type: • Validate bandwidth requirements of Customer • Define/update a target-state architecture, high level design (where appropriate) • Review with Customer stakeholders for sign off Takeover Service Type:	**High Level Design Document** • Target state objectives • High level architectural design

Activities	Description	Provisioning documents
	• Define integration strategy of the Customer firewall with Vodafone monitoring tools • Review with Customer stakeholders for sign off • Plan for knowledge transfer session with Customer • Understand the production environment and standard operating process • As-is firewall takeover	
Low Level Design	New Build Service Type / Replacement Service Type: • Define/update a corresponding low-level design • Define the Applicable Firewall Vendor firewall test plan based on the options selected by Customer (e.g shared OR dedicated tenant) Takeover Service Type: • Define/update a corresponding low-level design • Define the Firewall Connectivity Test Plan	**Low Level Design Document** • Low level architectural design with requirements traceability
Integration	New Build Service Type / Replacement Service Type:	**Device Configuration Files** • Device configuration files for the virtual appliance and integration parameters if request by Customer and for the purpose of Customer records, only. • Copy of exported policy rules for Customer records, only.

Activities	Description	Provisioning documents
	• Configure Applicable Firewall Vendor firewall, remote network and mobile users • Deployment of management platform for Applicable Firewall Vendor firewall • Connect tenant to firewall management platform where applicable • Purchase additional Cortex Data Lake ("CDL") capacity (if required) for storage of logs • Integrate Applicable Firewall Vendor firewall with CDL • Integrate CDL with management platform and monitoring tool, Syslog, etc. Takeover Service Type: • Deployment of tools and integration of Firewall • Firewall integration with availability/ monitoring tools, backup etc.	
Firewall Deployment	New Build Service Type / Replacement Service Type: • Provision firewall features based on Tier 1 or Tier 2 Customer requirements and applicable Optional Service Elements.	N/A

Activities	Description	Provisioning documents
	• Existing firewall configuration to be referred to build Applicable Firewall Vendor firewall • Update configuration management database • Test the firewall as per the agreed plan – Security policy, Inbound and outbound traffic flow, test the application • Prepare the standard operating process • Forty-eight-hour hyper care period to remedy any issue that arises, for example including, but not limited to, routing of any specific traffic and access issues related to specific users. Any resultant changes will initially be confirmed via email with the Customer, but subsequently formally captured in a Change Request Takeover Service Type: • Provision firewall features based on Tier 1 or Tier 2 Customer requirements and applicable Optional Service Elements. • Update configuration management database • Prepare the standard operating process • Forty-eight-hour hyper care period to remedy any issue that arises, for example including, but not limited to, routing of any specific traffic	

Activities	Description	Provisioning documents
	and access issues related to specific users. Any resultant changes will be, confirmed via email with the Customer, but subsequently formally captured in a Change Request	
Transition	• Knowledge transfer to Customer and Vodafone • Firewall admin access creation • Standard operating process document signoff • Create 30-60-90-day Plan	**Customer Service Manual** • Operations document with key contacts, and basic service management processes (e.g., basic testing procedures in the event of an unexpected firewall reset).
Operation	• Monitor CDL/firewall logs • Perform applicable activities based on Tier 1 or Tier 2 Customer requirements and applicable Optional Service Elements • Finetuning of access rules and security policy • Role based access control for firewall • Address all actions listed in 30-60-90-day Plan • Execute a service improvement plan • Perform service management activity (incident, change and service requests) • Action all Incidents within the defined SLA • Backup and restore management • Action all service and Change management request • Standard & Ad-hoc reporting • Update the standard operating process	

*Requirements to be provided in pre-engagement checklist and confirmed with the Customer at the beginning of the engagement.

6. Customer Deliverables

6.1 The following deliverables will be shared with customer as part of the Service:

Deliverables	Frequency	Firewall Service
System Health and Utilization report	Monthly	Takeover Service Type Only
Periodic Signature report	Quarterly	Takeover Service Type New Build Service Type Replacement Service Type
Periodic Network Activity report - Top 10 Rules, Destination, Attacker, Region	Weekly	Takeover Service Type (depended on available features in Customer Firewall and management tools) New Build Service Type Replacement Service Type
CR, Incident, Service report	Monthly	Takeover Service Type New Build Service Type Replacement Service Type
SLA report	Monthly	Takeover Service Type New Build Service Type Replacement Service Type
If Firewall Audit Optional Service Element is purchased: Periodic Security Ruleset (based on defined parameters) Optimization report Access violation and Compliance report	Biannually	Takeover Service Type New Build Service Type Replacement Service Type

Attachment 1 – Offerings Features Descriptions

The Service offers the following core technical features. For Takeover Service, the technical features will be provided to the extent technically and reasonably possible by the Applicable Firewall Vendors solution.

Application ID Inspection

The Application ID inspection features accurately identifies applications, including applications disguised as authorised traffic, using dynamic ports, or trying to hide under the veil of encryption. Application ID allows Customer to understand and control applications and their functions, such as video streaming versus chat, upload versus download, screen-sharing versus remote device control and implement defined policy. It is to be noted that a Web Application Firewall is not being provided. However, the Application ID features on the NGFW can be used to configure firewall rules.

User ID Policy

The User ID policy enables to the firewall to identify users in all locations, no matter their device type or operating system. Knowing who is using which applications on the network, and who may have transmitted a threat or is transferring files, can strengthen security policies and reduce incidents and potential security threats. User ID policy creation is dependent on the presence of LDAP capabilities available outside the customer's internal network protected by this firewall.

Vulnerability Protection Profile

The Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorised access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network. Vulnerability Protection profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. In the New Build and Replacement Service, while signature updates to the firewall will be done by Palo Alto, Vulnerability Protection Profile will be configured by Accenture. In the Takeover Service the Customer's existing process will be followed.

Anti-Virus

The Antivirus profiles protect against viruses, worms, trojans, spyware downloads, etc. Using a stream-based malware prevention engine, which inspects the traffic the moment the packet is received. This profile scans for a wide variety of malware in executables, PDF files, HTML and JavaScript viruses, including support for scanning inside compressed files and data encoding schemes. In the New Build and Replacement Service, while signature updates to the firewall will be done by Palo Alto, Anti-Virus Profile will be configured by Accenture. In the Takeover Service, the Customer's existing process will be followed.

Anti-Spyware

The Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing detection of malicious traffic leaving the network from infected clients. In the New Build and Replacement Service, while signature updates to the firewall will be done by Palo Alto, Anti-Spyware Profile will be configured by Accenture. In the Takeover Service, the customer's existing process will be followed.

URL Filtering

The URL Filtering feature enables Customer to monitor and control how users can access the web over HTTP and HTTPS. It enables safe access to the internet by preventing access to known malicious sites, phishing sites as well as other restricted sites such as adult content sites. In the New Build and Replacement Service, while content updates will be provided by Palo Alto (or respective OEM), the template to capture the required configuration / URL categories will be provided by Accenture. In the Takeover Service, the Customer will provide the list during onboarding.

File Inspection

This feature blocks specified file types in the specified flow direction – inbound, outbound or both. The profile can be set to alert or block an upload and/or download files. Custom configuration can be done to block pages when user tries to download a specified file type.

Data Filtering

This feature prevents sensitive, confidential, and proprietary information from leaving a network. Predefined patterns, built-in settings and options to customise, make it easy to protect files that contain certain file properties (such as a document title or author), credit card numbers, regulated information from different countries (like social security numbers), and third-party data loss prevention (DLP) labels.

Signature updates

Signature updates refresh the threat prevention signatures, which inspect all traffic for threats—regardless of port, protocol or encryption and automatically block known vulnerabilities, malware, exploits, spyware, command, and control (C2).

Architecture Support

Overall analysis of Customer infrastructure related to their inbound & out bound traffic flow. Perform Security assessment in line with best security practices. Assess Customer network & endpoint protection policy & share the findings. Participate in the design & architecture call and provide suggestions for improvement. Assist in defining Customer security standards & policy related to firewalls.

Attachment 2 – Maintenance Features Description

Maintenance Features

Health and Availability Management: Firewall will be integrated with monitoring tool which ensures firewalls health, availability & performance are monitored 24*7. In case firewall goes down or any spike is observed in any vital parameter (CPU/memory etc), an automated incident will be created in IT Service management tool to address the issues proactively, and the same is resolved before it can cause any potential impact to users/ service. For New Build and Replacement Service,

Back-up Management: Firewall will be integrated with a backup and restore management tool to ensure full configuration backup to avoid any human error. Tool will also generate the notifications regarding backup success/failure. Configuration backup is maintained on a daily basis as agreed with the Customer. This will empower administrators to recover quickly if any device failure happens.

Policy Updates and FW Administration: Policy will be created based on given requirements and will ensure that it always complies with the best security practices - e.g. Usage of secure port, avoid opening "wider subnet" or avoid putting "any" in source/destination/service field etc. Zero trust model will be in place related to any policy change along with 4 eye checks. RBAC (Role Based Access Control) will be in place to have authorized access of firewall, and access reconciliation/UER (User Entitlement Review) will be carried out regularly and will ensure that 'available users' access is approved by respective Leads.

Patch Management/Minor Upgrades: Accenture ensures that firewalls are running with the stable patch version to confirm the most accurate and effective protections are being applied. Minor upgrades are performed to remediate any vulnerabilities or known bugs identified in the current patch.

Concurrent VPN (Remote Access):

Takeover **-** Remote access VPN service will be configured to provide secure connection between remote/mobile users and office network. After establishing the secure access connection, the mobile users can virtually work on the company network.

New build/Replacement - Remote access VPN service will be configured to provide secure internet access for mobile users.

Hardware Capacity Management and Performance Monitoring: Firewalls are integrated with monitoring tool to capture the utilization of vital parameters and capacity analysis is performed based on utilization trend over a certain period. This allows to plan for the expansion or upgrade of firewall in the near future.

Major Version Upgrades: Accenture ensures that firewalls are running with stable OS version to ensure that the most accurate and effective protections are being applied. In a major version upgrade, the base version of the firewall will be changed to a stable/recommended version. Major upgrades are performed for bug-fixes and new feature releases by the Applicable Firewall Vendor. This feature is included for Tier 2 customers, however, Tier 1 customers are required to raise a Service Request ticket.

Attachment 3 – Ticket Management

Service Requests

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

- 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

Accenture 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

The following actions may require a request to be raised however Accenture 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