SERVICE DESCRIPTION: SECURE ACCESS

PART A – PRODUCT OVERVIEW

The Secure Access – powered by Palo Alto Networks Service is a cloud-delivered security-as-a-service platform that provides secure access for your mobile users and branch office locations to all of your private or cloud hosted data and applications (the "**Service**").

Whether your applications are hosted in public Cloud SaaS (Software-as-a-Service), a corporate head office, or private data centre, the Service provides visibility into the use of applications and the ability to control which applications are available for your users.

The Service works together with the GlobalProtect agent or application on laptops and mobile devices, when a Remote user has internet connectivity, the GlobalProtect application locates the best gateway available for the user's location and sets up a IPSec/SSL VPN tunnel.

The service fully inspects all application traffic bidirectionally including SSL/TLS-encrypted traffic on all ports, whether communicating with the Internet, the cloud, the data centre, or between branches, the service also provides more security coverage consolidating multiple point products into a single converged platform that includes firewall as a service, Zero Trust Network Access (ZTNA), CASB (Cloud Access Security Broker), Cloud Secure Web Gateway (SWG), Virtual Private Network (VPN), all manged through a single console.

The service is built upon a massively scalable network, leveraging the combined infrastructure of Amazon Web Services (AWS) and Google Cloud, with more than 100 service access points across 76 countries and every continent. This allows the service to provide ultra-low latency, backed by industry leading SLAs, to ensure a great digital experience for end users.

PART B –SECURE ACCESS – POWERED BY PALO ALTO NETWORKS

1. YOUR SECURE ACCESS - POWERED BY PALO ALTO NETWORKS

The service will consist of the specific components outlined in the table below. Any Components marked as optional are not required for the Service and you will advise us of such optional components that you wish to be included with the Service.

Component	Description
Firewall as a Service	Secure Access – powered by Palo Alto Networks provides firewall-as-a-service (FWaaS) capabilities consolidated into a single service edge.
Cloud Secure Web Gateways	Secure Access – powered by Palo Alto Networks provides cloud secure web gateway (SWG) functionality for remote users across all web traffic protocols and applications in hybrid environments. It also provides URL and content filtering for users based on dynamic group monitoring, allowing you to implement granular behaviour-based policies. Integrated proxying gives users maximum flexibility for how they connect to the Secure Access – powered by Palo Alto Networks service. Advanced DNS security prevents command-and-control (C2) callback and DNS tunnelling attacks.
Zero Trust Network Access (ZTNA)	Zero Trust Network Access (ZTNA) authenticates and connects users to applications based on granular role-based access control (RBAC) and provides a single pane of glass to create and enforce policies. Secure Access – powered by Palo Alto Networks service supports both agent-based and agentless connection methods regardless of a user's location. Unlike standalone VPN or proxy solutions, Secure Access – powered by

Component	Description
	Palo Alto Networks performs single-pass traffic inspection for malware, data loss, and malicious behaviour after users connect.
Cloud Access Security Broker (CASB)	Secure Access – powered by Palo Alto Networks service natively provides inline visibility and control of software-as-a-services (SaaS) applications. With the addition of Secure Access – powered by Palo Alto Networks Service SaaS, API-based security and contextual controls can be introduced for sanctioned SaaS applications. These controls are implemented together in an integrated manner and applied throughout all cloud application policies.
Threat Prevention	Automatically generates protections across the attack lifecycle when a new threat is first discovered to all WildFire subscribers in seconds for most new threats.
Enterprise DLP Subscription Optional (Business Premium & Enterprise)	Includes a set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing. DLP on Secure Access – powered by Palo Alto Networks enables you to enforce data security policies and prevent the loss of sensitive data across mobile users and remote networks
Autonomous Digital Experience Management (ADEM) Optional (Business Premium & Enterprise)	Only available for Mobile users with GlobalProtect network security for endpoint. Provides native end-to-end visibility for SASE (Secure Access Secure Edge), you gain segment-wise insights across the entire service delivery path, with real and synthetic traffic analysis that enables autonomous remediation of digital problems when they arise.
Service Connections for Private Application Access (Enterprise)	Service connections enable both mobile users and users at your branch networks to access resources in your Head Office or Data Centre. Beyond providing access to corporate resources, service connections allow your mobile users to reach branch locations. • GlobalProtect app IPsec/SSL (for Users) • GlobalProtect Clientless VPN (for Users) • Explicit proxy (for Users) • Peering via Partner Interconnect (for Clean Pipe, VLAN attachment per tenant) • 2w/Local Edition • 5w/Worldwide Edition.
Additional Service Connections for Private Application Access Optional (Enterprise)	Service connections enable both mobile users and users at your branch networks to access resources in your Head Office or Data Centre. Beyond providing access to corporate resources, service connections allow your mobile users to reach branch locations.
Net Interconnect for Site-to-Site and User-to-Site Access Optional (Enterprise)	Secures remote network to remote network and mobile users to remote network connectivity
Global Edition	Provides deployment of Secure Access – powered by Palo Alto Networks in any of the over 100 locations available around the world. (The standard edition allows deployment in up to 5 of the over 100 locations around the world)

2. CLOUD MANAGEMENT PORTAL

2. 1 You will receive access to a web portal that allows you to manage the Secure Access service. This portal provides you the ability to:

(a) Deploy and Configure security rules for your mobile users and branch office locations

(b) Visibility and Reporting of threats, traffic, users and applications through dashboards and detailed logs

(c) Access security posture improvement recommendations based on assessments of your configuration vs best practice

PART C – PRICING

3. BILLING

3. 1 Refer to the Pricing Schedule for details of all applicable Service charges, including charges for the components (both required and optional) set out in section 1 of this Service Description. [Early Termination Charges may apply.]

PART D – IMPLEMENTATION

3. 2 In order to implement this service, Professional Services provided by us will work with your relevant teams to implement and on-board the solution. An implementation plan will be provided as part of the implementation processes. The high-level deliverables of this implementation include:

(a) Management of the implementation plan

(b) Design of policy and configuration documented

(c) Sign off design document

(d) Implementation in platform and activate licencing and administrator logins for you and us

(e) Joint implementation of design in platform

(f) Joint implementation of service connections to your data centres

(g) Joint implementation of connections to your cloud providers

(h) Joint implementation of branch office routers and/or user devices

(i) Pilot testing of branch office and/or user devices

(j) Training your administrators on the service

(k) Handover of as-built design documents and support to your administrators and our support teams

(l) Deployment of service to remainder of branch offices and user devices

PART E – SUPPORT

The Secure Access – powered by Palo Alto Networks service can be supported either as a Self-Service support model, or a Managed Service.

3. 3 The Self-Service support option will see you manage all configuration, monitoring of environmental events, monitoring of security events and management of incidents. If you require technical support you can log a request with One New Zealand and One New Zealand will assist you and you will be subject to charges under a time and materials basis, refer to the Pricing Schedule for details of applicable charges.

3. 4 The Managed Service support option will see you manage all configuration and monitoring of security events, One New Zealand will monitor and advise you of environmental events and management of incidents. If you require technical support for configuration changes you can log a request with One New Zealand and One New Zealand will assist you and you will be subject to MAC Charges, refer to the Pricing Schedule for details of applicable charges.

3. 5 The below table outlines the support deliverables based on the chosen support model:

Item	Self-Service	Managed Service
Secure Access platform management and maintenance of service provided to Customer	Yes	Yes
Planned and Unplanned outage notifications provided to Customer	Yes	Yes
Environmental alerts sent to Customer	Yes	Yes
Environmental alerts sent to One New Zealand	No	Yes
Environmental alerts investigated by Customer (capacity related)	Yes	Yes
Environmental alerts investigated by Customer (non-capacity related)	Yes	No
Environmental alerts investigated by One New Zealand (non-capacity related)	No	Yes
Incidents from Environmental alerts managed by Customer (capacity related)	Yes	Yes
Incidents from Environmental alerts managed by Customer (non-capacity related)	Yes	No
Incidents from Environmental alerts managed by One New Zealand (non-capacity related)	No* *Customer can engage One New Zealand for support, charged at Time and Materials	Yes** **Managed by One New Zealand with Customer supporting
Security alerts monitored by Customer*** ***Unless separate One New Zealand security monitoring service subscribed to	Yes	Yes
Security alerts investigated by Customer	Yes	Yes
Security Incidents from Security alerts managed by Customer	Yes	Yes
Configuration of Secure Access service by Customer	Yes	Yes
Configuration of Secure Access service by One New Zealand	Charged at Time and Materials or Statement of Work	Charged as a MAC fee or Statement of Work
Technical Support of how to make configuration changes to Secure Access service	Online Knowledgebase or Charged at Time and Materials	Online Knowledgebase or Charged as a MAC fee

Item	Self-Service	Managed Service
Dataplane upgrade scheduling and post upgrade test managed by Customer	Yes	No
Dataplane upgrade scheduling and post upgrade test managed by One New Zealand	No	Yes

4. ALERTS AND NOTIFICATIONS

4. 1 Environmental Alerts describe the status of the Secure Access environment, for example, if the service is down, a tunnel to one of your branch sites is down. Alert notifications can be sent via email to you to notify you of these environmental issues. If you have chosen the Managed Service support option, we will also receive these Environmental Alerts (non-capacity related) and where appropriate, contact you to advise of the issue.

4. 2 Planned and Unplanned Outage Notifications for the service can be viewed by visiting the website: https://status.paloaltonetworks.com and from there you can subscribe to updates of individual notifications.

5. DATAPLANE UPGRADES

5. 1 The Secure Access dataplane that enables traffic inspection and security policy enforcement on your network and user traffic. Where the dataplane requires a maintenance upgrade, a maintenance window will be required, as there may be brief interruption to your network traffic.

5. 2 You can subscribe to dataplane upgrade email alert notifications via the Cloud Management Portal. Once a notification is received, you can login to the Cloud Management Portal and choose from a list of preferred maintenance window timeframes for the upgrade to occur.

5. 3 If you have chosen the Managed Service support option, we will work with you to prepare for a dataplane upgrade, confirming configuration will allow for failover during the upgrade, scheduling the change and performing post upgrade checks that service is re-established and performing as expected.

6. INCIDENT MANAGEMENT

6. 1 Where you have been alerted to an outage of the service via an Environmental Alert, updates for this outage will be available as noted in Part E section 8.2 above.

6. 2 Where there is an outage to the entire service and no Environmental Alert has been received, you can contact our service centre 24/7 to log an incident. We will then log, triage and manage this incident through until it is resolved.

6. 3 Where there is an outage to your individual service due to the configuration of your service made by you, if you require technical support from us, you can contact our service centre 24/7 to log an incident. This will be managed as a service request and charges for this will apply, please refer to the Pricing schedule for details of applicable charges.

7. SERVICE REQUEST MANAGEMENT

7. 1 You can make configuration changes and deploy new branches or mobile users to your Secure Access service via the Cloud Management Portal.

7. 2 If you require technical support from One New Zealand to assist you with a configuration change or make a change for you, you can submit this request to us. Charges for this will apply, please refer to the Pricing schedule for details of applicable charges.

7. 3 Additional licencing can be requested by submitting a request to us and we will provide you with a quotation for the additional licences. Once approved by you, these licences will be procured and loaded onto your Secure Access instance for you to consume.

8. QUARTERLY HEALTH CHECK

8. 1 As part of the service, once the implementation is completed and the deployment is complete, we will schedule quarterly health checks with you.

8. 2 These health checks review the configuration of your currently policies and configuration of the service and a health check document will be provided to you outlining the findings and suggestions of changes to improve the security posture of the service.

PART F – SERVICE LEVELS

8. 3 The Secure Access – powered by Palo Alto Networks service aims to provide the following service levels. You can view the service level status of availability at any time by you by visiting the website: https://status.paloaltonetworks.com.

9. SERVICE AVAILABILITY

9. 1 The service aims to be available 99.999% during any calendar month.

9. 2 Service Availability is calculated by subtracting from 100% the percentage of minutes during any calendar month that the Service is not available, excluding downtime resulting from any planned outage where prior notice had been provided or any emergency outage making it impracticable to issue advanced notice and taking into account the Exclusions set forth in Part F - section 17 below.

Availability = (Total - Downtime - Excluded) x 100 / (Total - Excluded).

Total = Total number of minutes in a calendar month.

Downtime = Time the Service was down.

Excluded = Excluded time, including criteria specified in Part F section 17 (“Exclusions”).

10. SECURITY PROCESSING LATENCY

10. 1 The service aims to have a security processing latency of 10 milliseconds (ms) 99.99% of the time in any given hour.

10. 2 The latency of a transaction is measured from when the Secure Access – powered by Palo Alto Networks security engine receives the network data packets for a particular transaction to the point when the same Prisma Access security engine component attempts to transmit the same data packet.

10. 3 The Security Processing Latency Percentage is calculated by subtracting from 100% the percentage of minutes during any one-hour period that the security processing latency exceeds 10 ms, excluding downtime resulting from any planned outage where prior notice had been provided or any emergency outage making it impracticable to issue advanced notice and taking into account the Exclusions set forth in Part F - section 17 below.

Security Processing Latency = (Total - Exceeded - Excluded) x 100 / (Total - Excluded).

Total = Total number of minutes in an hour.

Exceeded = Time this SLA exceeded an hourly average of 10ms.

Excluded = Excluded time, including criteria specified in Part F section 17 (“Exclusions”).

11. THIRD-PARTY SAAS APPLICATION LATENCY

11. 1 The service aims to have a Third-party SaaS application latency noted below 99.99% of the time in any given calendar day (24 hours):

35 ms - Americas

35 ms - EMEA

75 ms – APAC.

11. 2 The latency of a transaction is measured solely from when the Secure Access – powered by Palo Alto Networks security engine transmits the network data packets to the third-party SaaS application, directly to when the SaaS application server responds to the same packet. The following SaaS applications are supported: Microsoft O365, Google G Suite, Salesforce, Box and Slack.

11. 3 Daily SaaS Application Latency Percentage is calculated by subtracting from 100% the percentage of minutes during one day (midnight-to-midnight) that the third-party SaaS application latency exceeds 35 ms for Americas and EMEA; 75 ms for APAC, excluding downtime resulting from any planned outage where prior notice had been provided or any emergency outage making it impracticable to issue advanced notice and taking into account the Exclusions set forth in Part F section 15 (“Exclusions”).

Third-party SaaS Application Latency = (Total - Exceeded - Excluded) x 100 / (Total - Excluded).

Total = Total number of minutes in a day.

Exceeded = Time this SLA exceeded 35 ms in Americas & EMEA; 75 ms in APAC.

Excluded = Excluded time, including criteria specified in Part F section 15 (“Exclusions”).

12. INCIDENT MANAGEMENT

12. 1 Where One New Zealand are managing an incident relating to the configuration of your service, either through notification of an Environmental Alert or notification by you via our service centre, we will assign a priority to the incident based on the urgency and impact to your business. We aim to respond to the incident and have engaged with you within 30 minutes of the notification.

13. EXCLUSIONS

13. 1 The Service Level specified in Part F shall not apply and the Service shall be deemed available where the loss of Service results from:

(a) Your equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology used by us to deliver this service);

(b) Failure of your Internet Service Provider, utility companies, or other vendor(s) you utilise or rely on to access the Service and/or to access the internet;

(c) Your misconfiguration of Service features or settings wholly under your control;

(d) Your failure to purchase adequate licenses to meet the volume or capacity at which it uses the Service, if the SLA would have been met if not for such failure;

(e) Any feature or portion of the Service marked as “Beta,” “Test,” “Preview,” or the like, indicating that the feature has not been made generally available (aka production);

(f) Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties including, but not limited to, force majeure events;

(g) Planned and unplanned maintenance windows;

(h) High Availability events and scaling events;

(i) Fetching of logs from Cortex Data Lake service;

(j) Route convergence time if using BGP (Border Gateway Protocol);

(k) 500 Mbps connections with SSL Decrypt enabled;

(l) For purposes of the Security Processing Latency, packets which have been given a QOS (Quality of Service) policy by you are excluded.

13. 2 For purposes of the Third-party SaaS Application Latency SLA:

(a) any application not specified in Part F section 15.2 shall be excluded;

(b) only connection responses from the application server shall be considered; responses from the third-party SaaS application itself or loading of application content shall be excluded;

(c) SaaS traffic backhauled to a service connection via policy-based forwarding (PBF), default routing, explicit proxies, or the like, shall be excluded; and

(d) SaaS applications that are not set up to be globally distributed are excluded.

PART G – OTHER TERMS AND CONDITIONS

14. PROVISION OF SERVICE

14. 1 On execution of this Service Description you acknowledge that a binding offer to acquire the Service has been made and cannot be cancelled. For the avoidance of doubt, this section does not limit your ability to terminate in accordance with 21.2 below.

15. SERVICE LIMITATIONS

15. 1 The Service is limited to the components as set out in this Service Description, and you acknowledge that the Service does not include any Incident or Security Event resolution activities, forensics or services.

15. 2 We make no guarantees or warranties that the Service will correctly detect and identify all:

(a) Security Events or Incidents;

(b) Instances of unauthorised access to your network;

(c) Malware;

(d) Vulnerabilities;

(e) Exploits; or

(f) other types of attacks or issues.

15. 3 Any changes required for the ongoing tuning of the Service may be charged to you as a MAC.

16. YOUR RESPONSIBILITIES

16. 1 You shall agree and adhere to the Palo Alto Networks End User Agreement which can be located at: (www.paloaltonetworks.com/legal/eula).

16. 2 You shall configure and provide us with access to your service where this is not already configured by us during implementation.

16. 3 You shall manage IP-VPN configuration of your branch office routers based on the agreed design developed during implementation and any subsequent changes you choose to make to the service configuration.

16. 4 You shall manage packaging and deploying of the GlobalProtect Agent software to devices.

16. 5 If you subscribe to the Autonomous Digital Experience Management add-on, you shall manage any events/alerts generated from this add-on.

17. TERM AND TERMINATION

17. 1 The term of this Service Description commences as of the Effective Date and continues until terminated by either party in accordance with this clause19.

17. 2 This Service Description may be terminated:

(a) by us for convenience upon providing 80 days' prior written notice to you; or

(b) by either party for a material breach of this Service Description upon the non-breaching party providing 30 days' written notice to the other party of a material breach and provided such breach is not cured within that 30-day period.

18. DEFINITIONS

In this Service Description, in addition to the terms defined elsewhere in the Agreement, the following defined terms will apply to this Service Description:

Environmental Events means an event causing loss or degradation of the service to you, for example loss of IP-VPN connectivity to one of your branch offices, loss of the Cloud Management Portal and is not a Security Event or Autonomous Digital Experience Management event.

Palo Alto Networks means Palo Alto Networks, Inc, and Palo Alto Network Services as applicable.

Security Event means an observable change to the normal behaviour of your system, environment, process, workflow or person occurrence that may pose a security risk to your systems or environment.

IPSec means IP Security

SSL means Secure Sockets Layer

TLS means transport layer security

Mbps means megabits per second.