# MASTER SERVICES AGREEMENT

## SERVICE DESCRIPTION

## SERVICE DESCRIPTION: INTERNET PROXY SERVICES

### PART A – PRODUCT OVERVIEW

One New Zealand's Internet Proxy Service (the Service) is a service that comprises two parts. Firstly, it provides your users a secure method of browsing the Internet via their desktops, laptops, tablets or phones. Secondly, it optionally provides secure private access to internal applications whether they are running in your data centre or in the Public Cloud.

The Service is delivered as a Cloud Service and works by allowing users to connect to websites or applications that match your policy requirements. Web sites that your user's access are inspected for malicious content using a variety of techniques, including anti-malware engines, DNS security checks and our global reputation database. There is the option of Sandboxing and checking downloaded files before they are opened on your endpoint.

Data Loss Prevention capabilities include the use of standard or custom dictionaries, Cloud Access Security Broker Shadow IT reporting and the ability to control what file types are allowed in and out of your network. SSL Inspection can be used across all aspects of the service to inspect both inbound and outbound content.

The Service is globally accessible via a distributed network of access points, with one point of delivery (Service Node) located in New Zealand with many other nodes located around the world. Any of your users that need to travel globally will connect to the nearest node in the geographic region they are in. Each access point has optimised peering to reduce latency to cloud service providers such as Salesforce, AWS, Google, Microsoft M365 and other key SaaS platforms.

This service can also be extended to your servers and your internal applications within your organisations network.

The Service connects your users either using device configuration (PAC file), software agents on their devices or secure software configured tunnels (GRE or IPSEC) from your office locations.

### PART B – INTERNET PROXY SERVICES

### 1. INTERNET PROXY SERVICE – WEB BROWSING

1. 1 The Internet Proxy Service – Web Browsing provides the following features.

| Base Service Features | Description |
|---|---|
| URL and Content Filtering | Granular policy by user, group, location, time, and quota; dynamic content, classification for unknown URLs and Safe Search |
| File Type Control | True file type control by user, location, and destination |
| Inline Antivirus & Antispyware | Signature based antimalware and full inbound/outbound file inspection |
| Reputation-Based Threat Protection | Stop known botnets, command-and-control communications, and phishing |
| Standard Cloud Firewall | Granular outbound rules by IP address, port, and protocol (5-tuple rules) |
| Bandwidth Control | Ensure business apps like Office 365 are prioritized over recreational traffic |
| Standard Cloud Sandbox | Zero-day protection for .exe and .dll files from unknown and suspicious sites |
| Advanced Threat Protection | Page Risk and web IPS for content analysis of malware, call-backs, cross-site scripting, cookie stealing, and anonymizers |

| Base Service Features | Description |
|---|---|
| Cloud Application Visibility & Control | Discover, monitor, and control access to web applications |
| Mobile Application Reporting & Control | Visibility, granular policy control, and threat protection for mobile devices on or off the corporate network |
| Web Access Control | Ensure outdated versions of browsers and plugins are compliant |

1. 2 In addition there are the following advanced add-on features available by request.

| Service Add-on Features | Description |
|---|---|
| Data Loss Prevention & Exact Data Match | Inline scanning to prevent confidential data leaving the organization |
| Advanced Cloud Sandbox | Zero-day protection for all file types from all sites; ability to hold file delivery until confirmed sandbox clean; advanced reporting |
| Advanced Hosted Proxy | Hosted Proxy is a virtual appliance installed into your organisations network to provide connectivity to the Service. This option is useful where your organisation needs to access an Internet application that requires a dedicated/known IP address as a form of authentication or access control. |
| Log Streaming Server | The Log Streaming server is a virtual appliance installed into your organisations network to buffer, customise and stream log files to a SIEM or other log archiving solution. |

## 2. INTERNET PROXY SERVICE – PRIVATE ACCESS

| Base Service Features | Description |
|---|---|
| Global visibility for users and applications | Single pane of glass shows which users are accessing private, internal apps |
| Secure private application access to internal apps with Client Connector | Allows secure access to internal applications (whether public/private/hybrid cloud or data center environments) without exposing network or apps to the Internet |
| Multiple identity provider support | Enables simultaneous support of multiple IDP services |
| Application and server discovery | Wildcard policy shows application and server locations as they are requested by users |
| Microsegmentation by application | Granular access control for defined applications and segments |
| Device posture enforcement | Checks device fingerprint and certificate, as well as other postures |
| Continuous health monitoring | Application health is continuously monitored to ensure that ports are available and users can connect to the application. |

## 3. CONNECTION TO THE SERVICE

- In order to use these Services you require a connection to it. This can be provided in any combination of the following ways:
- The Agent software deployed onto your users' Desktop, Laptop or mobile devices.
- PAC settings configured for your mobile devices.
- A secure "site to site" GRE or IPSEC tunnel connecting your organisations network to the Service Node in Auckland and designated 'failover' site in Sydney or Melbourne.
- Through the optional Hosted Proxy add-on that residing within your organisations network.

## 4. CONFIGURATION MANAGEMENT AND MONITORING

4. 1 We will provide expert configuration and administration of the Service. All configuration information is stored in the cloud tenancy Platform. The Platform is natively redundant, highly available and includes an audit trail of all user access.

## 5. FAULTS AND CHANGES

5. 1 You can log a fault with this service by raising a new case via the One New Zealand Service Desk.

5. 2 You can request changes to the service by requesting a MAC via the One New Zealand Service Desk. Separate changes may apply for MAC's as defined below.

## 6. WEB SECURITY SERVICE PORTAL AND REPORTING

6. 1 We will provide you with access to a web portal where you can access your Internet Proxy Service for reporting and configuration actions.

6. 2 We will review the service with you each month. We will report on any points of interest that relate to the service that have any relevance to your organisation.

# PART C – PRICING AND BILLING

## 7. CHARGES

7. 1 Refer to the Pricing Schedule for details of the applicable Charges.

7. 2 Changes required for the ongoing tuning of the service will be charged as a MAC.

7. 3 The Early Termination Charges for the Web Security Service is the total cost of the service for all contracted users for the full term divided by the total number of months in the Service Initial Term multiplied by the number of months remaining in the Service Initial Term at the date of termination.

The Early Termination Charge w calculated as follows:

ETC = (AxB) x 50%

Where

A = number of months remaining in the Web Security Service Initial Term

B = Monthly Recurring Charge for the Web Security Service

## 8. BILLING

8. 1 Billing for this service will commence one month from when One New Zealand places the order with zScalar.

## 9. INSTALLATION

9. 1 The installation of the Service will be undertaken in stages. We will work with you to document the stages and timings in a Statement of Work that we both agree to. The Statement of Work may include, but will not be limited to, the following stages:

- Discovery and Planning Phase
- Confirming the High-Level Service Overview
- Provisioning the Service
- Operation and tuning of the Service.

9. 2 Part of the installation activity will include working with you to scope your deployment and determine which optional modules you require. We will work with you to provide the information you need to deploy the various software Agents and configure access from your network to the Service

9. 3 A Non-Reoccurring Charge for transition will be charged on a time and materials basis and we will consult with you to agree on the costs (or the basis of such costs) prior to incurring them.

## PART D – SUPPORT

### 10. SUPPORT

10. 1 Service Availability Targets

(a) The service availability targets for the following components of the Service are set out below:

| Item | Description | Service Target |
|---|---|---|
| Availability of the Service | Calculated per calendar month | 99.99% |
| The service target is calculated as follows:<br>Availability = [(A – B) – C/(A – B)] x 100<br>A = Total number of hours in the month.<br>B = Number of hours in a planned outage period in the month. | | |

(b) If there is a fault or outage which causes (or is likely to cause) a degradation in the quality of the Service (“Outage”), you must promptly investigate the cause of the Outage and notify us within 24 hours of such Outage.

(c) This availability target requires both a primary service location in New Zealand and a secondary service location in Australia to be used. There are no additional costs for the use of a secondary service location.

## PART E – OTHER TERMS AND CONDITIONS

### 11. SERVICE LIMITATIONS

The following limitations apply to the Web Security Service.

11. 1 The Service does not proxy UDP traffic, UDP traffic will be forwarded by the Service.

11. 2 The inspection of SSL or TLS traffic can only be provided at the protocol level. If there is additional encryption deployed at the application layer then the Service cannot be perform inspection at that level.

11. 3 IPv6 is not supported.

11. 4 We cannot guarantee that the Service will correctly detect and identify all:

- Security Events or Incidents;
- unauthorised access to your network;
- malware;
- exploits; or
- other types of attacks or issues.

11. 5 The installation of the software agents onto your users' devices is your responsibility. You must ensure the devices are maintained to the correct software, patching and operating system level.

11. 6 Where the software agents is deployed onto a users' device we may not support that device as part of the Service if you have not maintained the necessary firmware or software currency for that device.

11. 7 In the event that Zscaler discontinue the products or alter the commercial terms with One New Zealand that this Service Description is predicated on, One New Zealand reserve the right to revise this service description and the associated commercial terms with 80 days written notice to you.

11. 8 In the event your usage patterns (such as bandwidth, number of users or resilience requirements) change from what we have agreed on and documented in the installation statement of work we may revise the terms of the commercial agreement and apply additional charges.

11. 9 You are required to adhere to our standard Service on-boarding processes.

## 12. YOUR RESPONSIBILITIES

12. 1 You will need to setup your environment to support an approved method of authentication to the Service. Authentication integration is included in the installation fee. Professional Services may be required for the design.

12. 2 You will need to ensure that end user devices have a suitable connection to your organisations network or to the Internet in order to access the Service.

12. 3 You may need to change or update the end user device settings to all it to send web traffic to the Service.

12. 4 You are responsible for providing any certificates that may be required to enable the SLL/TLS inspection services.

12. 5 Internet and DNS hostname resolution is provided by the service. Your end user devices will need access to a DNS resolver in order to connect to the Service.

12. 6 If you require the optional Hosted Proxy or Log Streaming server then you will be responsible for providing hosting requirements. A separate installation fee and/or additional professional services may be required.

12. 7 You are responsible for reviewing and accepting the Zscaler "click-through" End User Agreement(s) for the relevant components we procure for you as part of this Service. The Zscaler End User Agreement(s) are available at https://www.Zscaler.com/legal.

## 13. 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:

WAN: wide-area network

DDoS: Distributed Denial of Service

SSL: Secure Socket Layer

TLS: Transport Layer Security

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

FTP: File Transfer Protocol

SAML: Security Assertion Markup Language

SMTP: Simple Mail Transfer Protocol

LDAP: Lightweight Directory Access Protocol

DNS: Domain Name System

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

UDP: User Datagram Protocol.