**SERVICE SCHEDULE - CLOUD PLUS MANAGED FIREWALL**

The following terms apply to Data Access Services provided by Cloud Plus Pty Ltd (**“Cloud Plus”**) to the Client and form part of and are incorporated into the General Terms between Cloud Plus and the Client (the “Agreement”).

Terms which have a defined meaning in the Agreement shall have a corresponding meaning in this Service Schedule.

**SERVICE DESCRIPTION**

**Cloud Plus Managed Firewall** offers the Client access to a feature-rich managed firewall service that is hosted on industry leading enterprise-class hardware appliances, without the associated capital expenditure. Services are provisioned and maintained by highly skilled vendor certified technical resources from Cloud Plus.

The base configuration includes the Managed Firewall instance, a dedicated Internet VLAN and a dedicated internal VLAN. Additional VLAN’s can be added as required (e.g. the Client may need an Internet VLAN, Private Network VLAN, Internal Server VLAN and DMZ VLAN). And a wide range of optional features can be enabled to cater for the needs of the Client. These options are outlined briefly below.

If required, Cloud Plus can provide the Client with access to a web interface for administration and can tailor the access provided as required. For example, the Client may prefer that trained Cloud Plus staff make all changes but wants visibility of the configuration and logs. Or the Client may only want write access to the Content Filtering configuration as they make regular changes, whilst leaving Cloud Plus to manage the rest of the configuration.

Cloud Plus Managed Firewall is a core element of the security services that Cloud Plus offers its clients and it is strongly recommended that it be included in network and/or hosting solutions from Cloud Plus. With the appropriate options enabled to suit the Client’s requirements it forms a critical part of the Client’s overall security framework.

Connected directly to the core of the Cloud Plus MPLS network, the Cloud Plus Managed Firewall platform has high speed access to the Internet via Cloud Plus’ fault tolerant Tier-1 Internet backbone connections, Cloud Plus Private Network services and Cloud Plus Virtual Server infrastructure.

**SSL Remote Access VPN** is an option that enables secure encrypted remote access for individual users or machines via the Internet to a network residing behind Managed Firewall. The Client can either use the Fortinet SSL VPN client or the full Fortinet FortiClient, which includes a range of other features, to connect to the service.

**IPSec Site-to-Site VPN** is an option that enables secure encrypted connectivity between a network residing behind an IPSec capable device, such as a router or firewall, and a network residing beyond Managed Firewall. It is highly recommended that the Client uses a FortiGate firewall as the remote device. However, most IPSec capable devices from leading vendors (e.g. Cisco, Juniper and WatchGuard) will work with the service.

**Virus & Spam Filtering** is an option that helps protect against Internet based viruses on a suite of well-known services (HTTP, STMP, POP, IMAP, FTP and IM) and unsolicited (spam) email via common protocols (SMTP, POP, IMAP and a number of webmail services). All detected viral content is dropped at the firewall. With spam there is the option to either drop or tag at the firewall. As Managed Firewall does not have an email quarantine it is highly recommended that spam is tagged with a view to then handling it either on a mail server (e.g. Microsoft Exchange) or an email client (e.g. Microsoft Outlook). Then, if it is felt that mail has been incorrectly classified, the Client can view and/or recover email as required. There is facility to whitelist or blacklist particular IP or email addresses if necessary.

**Content Filtering** is an option that enables the ability to monitor and control access to content and applications. This helps the Client to effectively manage access to content that presents a security risk, is inappropriate for the workplace, places unwanted demands on network resources or opens up potential liability concerns. Traffic can be shaped or blocked on a 24x7 basis or based on time of day. And this can be done based on high level categories, application types, specific applications or specific URL’s / sites as required.

**Intrusion Prevention** is an option that helps to protect against attacks targeting services allowed through Managed Firewall to servers residing behind it. Anomaly-based defences protect against denial of service attacks and signature-based defences protect against known attacks and vulnerability exploits. It is highly recommended that the Intrusion Prevention option is enabled on Managed Firewall if it is being used to secure hosted services (e.g. web, email and DNS hosting).

**Server Load Balancing** is an option that provides the ability to distribute load across multiple back-end servers. There are various distribution methods including static (failover), round robin, weighted (to allow for servers with different performance levels) or based on health & performance metrics (either round trip time or number of connections). A variety of protocols are supported, including HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL or simply UDP/TCP or IP. Session persistence is supported based on the SSL session ID or an HTTP cookie. This option is only designed to cater for up to 20 concurrent sessions of SSL based protocols. Cloud Plus can provide other options if more sessions are required.

**PRICING**

Pricing for the Service and other charges under the Agreement shall be as notified by Cloud Plus (for example, in its proposal to the Client) and as otherwise notified or varied by Cloud Plus in accordance with the General Terms.

**ADDITIONAL TERMS – GENERAL**

1. For the purposes of this Agreement: **“Defined Abuse”** includes misuse of the Service including without limitation: (a) giving an unauthorized person the Client’s account and password details; (b) deliberately or recklessly disrupting Cloud Plus’ service; (c) engaging in the practice known as spamming; (d) using the Service in an unlawful manner; (e) using the Service to menace or harass others; (f) Denial-of-service attacks on other clients or any network; (g) using the Service to obtain unauthorized access to any network; or (h) as otherwise reasonably determined by Cloud Plus; and **“Denial-of-service attack”** includes behaviour of the Client that results in disruption of Cloud Plus’ service, disruption of other people’s access or their enjoyment of that access, including without limitation computer viruses and other harmful components, IRC harassment, e-mail bombardment, damage to internet-connected resources and channel flooding.
2. Whilst Cloud Plus may provide general information regarding options available to the Client within Managed Firewall, such information is not advice and is provided on an “as is” basis. Notwithstanding any communications between the parties, it is the responsibility of the Client to select the options that are most appropriate to its needs and the Client warrants to Cloud Plus that it has conducted all investigations and made all necessary inquiries in order to satisfy this requirement.
3. Cloud Plus may provide the Client with a unique login identification code, password and other login information required to enable connection to the Service. The Client must ensure that such information is not disclosed to any unauthorised person.
4. The Service may be subject to an SLA provided or published by Cloud Plus from time to time. Subject to the Agreement, Cloud Plus may vary any such SLA as required by providing the Client with at least 30 days’ notice.
5. The Client acknowledges and warrants to Cloud Plus that the Client is not acquiring any goods or service from Cloud Plus under the Agreement wholly or predominantly for personal, domestic or household use or consumption.
6. The Client agrees to use the Service only in accordance with any Acceptable Use Policy provided or published by Cloud Plus from time to time. Cloud Plus may vary any such Acceptable Use Policy by providing the Client with at least 30 days’ notice.
7. The Client must ensure that its use of the Service and all data transmitted via the Service (whether by the Client or another person):
   1. is free from computer viruses, trojans, worms, hacking tools and other harmful components;
   2. does not infringe the intellectual property rights of any person;
   3. complies with the terms of the Agreement;
   4. does not defame any person; and
   5. does not breach any law (including without limitation any law relating to pornographic, obscene or offensive material, vilification, unsolicited electronic messaging, consumer protection, confidential information, information security, national security and public safety
8. Cloud Plus will not be liable for any activity associated with the use of the Service and the Client warrants that it will fully indemnify and hold harmless Cloud Plus, its employees, contractors and suppliers in relating to any such matters (including the matters referred to in clause 7 above). Cloud Plus may cease providing the Service and retains the right to apply an early termination fee if appropriate and to refuse refund for the Service in such circumstances.
9. Cloud Plus will use its best endeavours to make the Service available to the Client 24 hours a day, 7 days a week. However, the Client acknowledges that the Service may be unavailable at times, due to various factors including but not limited to network maintenance, peak congestion, Service Equipment or line failure. The Client further acknowledges that Cloud Plus does not guarantee the speed, performance or quality of the Service, although certain credits or rebates may be available under an applicable SLA. References to speeds are maximum theoretical speeds and may not reflect actual performance.
10. Emergency maintenance and scheduled maintenance in relation to the Service may be required from time to time. Should this be necessary, Cloud Plus will provide as much notice as is reasonably practicable and will endeavour to conduct such maintenance at times that are unlikely to impact most clients.
11. Charges may include establishment, monthly recurring (which may be invoiced in advance), usage-based and other associated charges (including hardware, software and professional services).
12. Charges shall commence from the time Cloud Plus makes the Service available to the Customer, whether or not the Customer is ready to make use of the Service at that time.
13. If there is a data allowance associated with a given service and it is not used within the period for which it is provided, it does not roll-over into a subsequent period.
14. The Client acknowledges that devices connected to a network, and particularly those connected to the Internet, are subject to security threats. The Client agrees that Cloud Plus will not be held responsible or liable for ensuring the security, privacy or integrity (including threats arising from viruses, trojans, worms, hacking tools or any other harmful component) of any Client data held on devices connected to the Service either directly or indirectly or transmitted to another location using the service. The Client must fully indemnify and defend Cloud Plus in relation to any claim relating to the matters referred to in this paragraph.
15. Without limiting clause 14 above (and without making any warranty or representation), Cloud Plus recommends that the Client takes up all appropriate options within Managed Firewall and employs other security technologies in conjunction with the Service. Cloud Plus may agree to assist the Client in regards to the latter, as an additional service and subject to Cloud Plus’ then current rates.
16. In the event that the Service allows for the assignment of a public IP address block and the Client requires a block greater than a /30 (2 usable IP addresses), the Client will need to provide justification for its requirements in accordance with APNIC policy. This will result in an additional monthly fee.
17. Where the Service is being used to deliver Internet access with usage-based pricing Cloud Plus will charge an excess usage fee for downstream usage that exceeds the included usage associated with the service. Cloud Plus will not charge an excess usage fee for upstream usage unless it exceeds ten times the included downstream usage, however should this occur Cloud Plus will charge for excess usage in both directions.
18. The Client must use its best efforts to identify whether a fault is related to the Service is within the Client’s own network, systems or otherwise within the Client’s responsibility prior to contacting Cloud Plus for support. Should the Client request after-hours support and the fault be found not to be related to the Service, Cloud Plus may impose a professional service fee at Cloud Plus’ then current rates.
19. Nothing in this Schedule limits any limitation, exclusion or indemnity contained in the General Terms.
20. If the initial term for the Service is specified in the application forms it will be as specified. Where not specified in the application forms the initial term for the Service will be 36 months. The Agreement shall automatically renew for successive 12-month periods thereafter, provided either party may terminate the Agreement at the end of the then current term by notifying the other party in writing at least 60 days prior to the end of the then current term.
21. Cloud Plus Managed Firewall is not a stand-alone service and should be bought in conjunction with Cloud Plus Virtual Server and/or Cloud Plus Private Network services.

**Service Speed**

1. By default, the Internet VLAN on Managed Firewall is shaped to 10Mbps. It is possible to provide the Client with a higher speed of access to the Internet, however additional fees will apply depending on the speed of access that the Client requires (e.g. 20, 50 or 100 Mbps).

**Administrative Access**

1. If the Client has requested administrative access to Managed Firewall, Cloud Plus will provision this and provide the Client with the relevant access details. If the Client is provided with write access it warrants that Cloud Plus will not be held responsible for any configuration changes made by the Client.
2. Administrative access must be restricted by IP address/subnet. This may include private networks hosted by Cloud Plus, users connected via SSL remote access VPN sessions, sites connected via IPSec site-to-site VPN sessions and Internet connected sites with dedicated IP addresses.

**Configuration & Support**

1. Up to two hours of professional service time is allowed for provisioning a Managed Firewall service. Beyond the initial two hours, professional service fees will apply at the then standard hourly rate or as otherwise agreed between Cloud Plus and the Client in writing.
2. Once a service has been provisioned and handed over to the end client, Cloud Plus allows up to 30 minutes of professional service work per month to cater for ongoing changes and tuning of the configuration. If this period of time is exceeded in any given month, professional service fees will apply at the then standard rate or as otherwise agreed between Cloud Plus and the client in writing.

**On-Premise Managed Firewall**

1. Where appropriate it is possible for Cloud Plus to be delivered as an on-premise solution at a site belonging to the Client. In this case, the speed of access will be limited to the speed of the Internet access at that site and unless otherwise agreed in writing, the Client will be responsible for everything beyond the inside interface of the hardware appliance/s used to provide the service.
2. It is highly recommended that a pair of hardware appliances be deployed and configured for High Availability where an on-premise solution is required. If this should not be the case, Advanced Hardware Replacement will be required to ensure timely recovery from any potential hardware failure.
3. Additional fees will apply to provision an On-Premise Managed Firewall service as the hardware at the Client site will be dedicated to the Client and as one or more site visits may be required.
4. Unless otherwise agreed in writing the hardware appliances used to deliver an On-Premise Managed Firewall service will remain the property of Cloud Plus and must be returned to Cloud Plus at the end of the term.