Technical Appendix
Managed Firewall & Managed Load Balancer

Table des matières

1 Detailed description per service

1.1 Managed Third Party Firewall

1.1.1 Service Presentation

As part of this service, we manage your third-party Firewall hosted on a Public Cloud IaaS infrastructure from the list below.

- Cloud Avenue (The Provider)
- Alpha (partially implemented, feasibility study available on demand) Flexible Engine (The Provider)
- Alpha (partially implemented, feasibility study available on demand) - AWS (partner)
- Alpha (partially implemented, feasibility study available on demand) - Microsoft Azure (partner)
- Alpha (partially implemented, feasibility study available on demand) - Google Cloud (partner)

The Managed Third Party Firewall service is delivered through an active-passive cluster of virtual appliances from our technology partner (Fortinet), with the following VM configuration options depending on desired functionalities and scale:

- VM01 = 1 vCPU 2GB Memory 32GB HDD
- VM02 = 2 vCPU 4GB Memory 64GB HDD
- VM04 = 4 vCPU 8GB Memory 64GB HDD
- VM08 = 8 vCPU 16GB Memory 128GB HDD

The Managed Third Party Firewall service includes the following options:

- VPN IPSec (Forticare or Advanced Threat Protection or Unified Threat Protection license required)
- VPN SSL (Forticare or Advanced Threat Protection or Unified Threat Protection license required)
- IPS/IDS (Extra logging option and Advanced Threat Protection or Unified Threat Protection license required)
- Web filtering (Unified Threat Protection license required)
- Proxy (Unified Threat Protection license required)
- Multifactor Authentication (MFA) with FortiToken and license resale (upon request)
- Dedicated FortiAnalyzer (dedicated FortiAnalyzer license required)
- Co-managed service option (feasibility study upon request) - joint management of certain features in collaboration with the client. This option requires a feasibility study, and in the event the client is eligible, the quality of service terms for co-managed services will apply

1.1.1.1 KPI & alerts

Monitoring and logging

The Provider has a logging and monitoring system in place for up to 12 months of retention and up to 0,5 GB/day (for classic firewalling) or 1,5 GB/day (for IPS/IDS - Extra Logging option required) of log collection. Logs can be accessed and exported upon request. The service is currently not compatible with external SIEM (Security Information and Event Management) systems as of the current date.

Monitored metrics during RUN phase

Operational service state

- Network interface activity
- Active-passive configuration, disaster recovery event
- Backup
- Firewall uptime
- Healthcheck ICMP/SNMP
- IPS/IDS Option - Configured/Blocked IP/URLs
- IPS/IDS Option - In addition to the IP/URLs chosen by the client, analysis of IP addresses listed as sources of spam or malicious software by Spamhaus and injection of new suspicious IP/URLs into the IPS/IDS configuration, up to several times a day
- IPS/IDS Option - Type of Attack (DDoS, malware, etc.)

Resource usage
- CPU
- RAM
- Number of sessions
- Used bandwidth per interface

Licenses and upgrades
- Serial number
- Versioning and security updates

Configured alerts

Operational service state
- Resource utilisation
- Access to firewall
- IPS/IDS Option - Standby for Service Degradation of FW and/or Infrastructure (for example, bandwidth saturation of the FW caused by a DDoS attack. In this case, the provider may take the service offline until a solution is identified by the client)

1.1.1.2 Backup and restore

Data backup and restore

The Provider performs firewall configuration backup

Service restore

Firewall configuration restore with consequent assessment.

1.1.2 Pricing conditions

The Service's pricing is composed by:

- Access fees for accessing the Managed Firewall Third Party service including all the implementation tasks mentioned in the Managed Application service description. To estimate these costs, an assessment of customer needs is carried out by the Provider, following which a quote for access fees is created.
- A monthly recurring "Run" fee covering the activities related to the maintenance in operational condition of the Managed Firewall Third Party service indexed on the number of managed instances and configured options.
- A monthly recurring fee covering the licenses of our technology partner needed to operate the Managed Firewall Third Party service, indexed to the number of managed instances and configured options.

You will find the monthly recurring "Run" prices in the table below.

Category	Description	Service Unit

Firewall – Cluster	Managed Dedicated Fortigate Firewall - for active & passive cluster (without license) incl. 1 IPsec tunnel (license Forticare or Advanced Threat Protection or Unified Threat Protection needed)	Per cluster of 2 VM
Firewall – Options	VPNSSL – 1 tunnel (license Forticare or Advanced Threat Protection or Unified Threat Protection needed)	Included in the "Managed Dedicated Fortigate Firewall" service unit
Firewall – Options	VPNIPsec Fortigate – 10 tunnels pack (license Forticare or Advanced Threat Protection or Unified Threat Protection needed)	Per pack of 10 tunnels VPNIPsec
Firewall – Options	IPS/IDS (license Advanced Threat Protection or Unified Threat Protection needed)	Included in the "Managed Dedicated Fortigate Firewall" service unit
Firewall – Options	Proxy (license Unified Threat Protection needed)	Included in the "Managed Dedicated Fortigate Firewall" service unit
Firewall – Options	Web Filtering (license Unified Threat Protection needed)	Included in the "Managed Dedicated Fortigate Firewall" service unit
Firewall – IT Admin special offer	Dedicated VPNSSL gateway up to 5 users and password reset every 60 days (Fortinet license included, not possible to add any options)	Per cluster of 2 VM
Firewall – Options	Multifactor Authentication (MFA) with FortiToken	Upon request
Firewall – Options	Dedicated FortiAnalyzer	Per instance
Firewall – Options	Extra logging (up to 1 GB/day)	Per instance

The list of available licenses can be found in the table below.

License	Unit
Cluster Fortigate VM01 FortiCare (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM01 Advanced Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM01 Unified Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM02 FortiCare (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM02 Advanced Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM02 Unified Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM04 FortiCare (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM04 Advanced Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM

Cluster Fortigate VM04 Unified Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM08 Forticare (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM08 Advanced Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM
Cluster Fortigate VM08 Unified Threat Protection (up to 10 Virtual Domains)	Per cluster of 2 VM
Dedicated FortiAnalyzer 5GB/Day and up to 3 TB retention (up to 10 Virtual Domains)	Per cluster of 2 VM

The Service rates do not include:

- IaaS infrastructure costs needed to run the service, which are billed separately
- Change requests

1.1.3 Change catalogue

Category	Subcategory	Token Full France	Token Global	Change request description
Firewall	SSL	8	8	Certificate install/modification/suppression
Firewall	SSL	16	Not available	Creation/Modification/suppression of profile SSL Inspection
Firewall	IPS/IDS	On quotation	Not available	Configuration (1 IP destination)
Firewall	IPS/IDS	8	Not available	Modification (1 IP destination)
Firewall	IPS/IDS	4	Not available	Suppression
Firewall	Flow	4	4	Add/Suppression/Modification of Policy/Object/Service
Firewall	WebFiltering	4	4	Creation/Modification/Suppression of custom category
Firewall	Logs	4	Not available	Flow/objects export request
Firewall	Logs	On quotation	Not available	Log export request
Firewall	Anti-Virus	8	Not available	Creation/Modification/suppression of AV Profile
Firewall	VM	8	Not available	Change of VM type
Firewall	VM	8	Not available	Change of License
Firewall	VPN-Ipsec	On quotation	On quotation	Creation
Firewall	VPN-Ipsec	8	8	Suppression

Firewall	VPN-Ipsec	8	8	Modification
Firewall	VPNSSL	4	4	User access - creation/modification/suppression
Firewall	VPNSSL	8	8	Creation/Modification of LDAP authentication connector
Firewall	VPNSSL	4	4	Configuration suppression
Firewall	Routing	4	4	Routing / DNAT / SNAT
Firewall	Générique	On quotation	Not available	SSO connector creation
Firewall	Générique	On quotation	Not available	Non-Standard change

1.2   Managed Native Firewall (VMware)

1.2.1   Description

As part of this service, we manage your native Firewall on the Public Cloud infrastructure IaaS Cloud Avenue (The Provider), with a configuration that can support up to 100 firewall rules per customer.

The Managed Firewall service is delivered through a native feature of our technology partner (VMware) and includes the following options:

- VPN IPSec

1.2.1.1   KPI & alerts

Monitoring and logging

The Provider has a system for monitoring and recording logs

Monitored metrics during RUN phase

Operational conditions of the service:

- VMware NSX components of the Cloud Avenue platform (further details in the Cloud Avenue service description)
- Outgoing connectivity health check

Configured alerts

Operational conditions of the service:
- Outgoing connectivity outage

1.2.1.2   Backup and restore

Data backup and restore

The Provider performs backup of the NSX and VCD configurations

Service restore

Procedure for restoring the configuration following a service reset.

1.2.2   Pricing conditions

The Service pricing consists of:

- Access fees for the "Managed Native Firewall" service, which includes all tasks mentioned in the implementation RACI. To estimate these fees, The Provider conducts a study of the client's needs, following which a quote for the access fees is created.
- Monthly recurring charges covering activities related to the operational maintenance of the "Managed Native Firewall" service, indexed based on the number of managed instances and configured options.

You will find the monthly recurring "Run" prices in the table below.

Category	Description	Service Unit
Firewall - Base	Native NSX firewall	Per NSX firewall instance
Firewall - Options	VPNIPsec Fortigate (pack de 10 tunnels)	Per pack of 10 tunnels VPNIPsec

The Service rates do not include:

- IaaS infrastructure costs needed to run the service, which are billed separately
- Change requests

1.2.3 Change catalogue

Category	Subcategory	Token Full France	Token Global	Change request description
Firewall	Flow	4	4	Add/Suppression/Policy Modification/Object/Service
Firewall	Logs	4	Not available	Flow/object export request
Firewall	Logs	On quotation	Not available	Logs export request
Firewall	VPN-Ipsec	On quotation	On quotation	Creation
Firewall	VPN-Ipsec	8	8	Suppression
Firewall	VPN-Ipsec	8	8	Modification
Firewall	Routing	4	4	Routing / DNAT / SNAT
Firewall	Générique	On quotation	Not available	Non-Standard change

1.3 Managed Native Load Balancer (VMware)

1.3.1 Description

As part of this service, we provide management for your native Load Balancer on the Cloud Avenue Public IaaS infrastructure (The Provider).

The managed Native Load Balancer service is delivered through a native feature from our technology partner (VMware) and includes the following options:

- Local Traffic Manager

1.3.1.1 KPI & alerts

Monitoring and logging

The Provider has a system for monitoring and recording logs

Monitored metrics during RUN phase

Operational conditions of the service:

- VMware NSX components of the Cloud Avenue platform (further details in the Cloud Avenue service description)
- Active health monitor (standard and advanced versions)
- End-to-end response time, throughput, number of active sessions, and connections (advanced version)

Configured alerts

Operational conditions of the service:
- Response to VIP Health Check

1.3.1.2   Backup and restore

Data backup and restore

The Provider performs backup of the NSX and VCD configurations

Service restore

Procedure for restoring the configuration following a service reset.

1.3.2   Pricing conditions

The Service pricing consists of:

- Access fees for the "Managed Native Load Balancer" service, which includes all tasks mentioned in the implementation RACI. To estimate these fees, The Provider conducts a study of the client's needs, following which a quote for the access fees is created.
- Monthly recurring charges covering activities related to the operational maintenance of the " Managed Native Load Balancer" service, indexed based on the number of managed instances and configured options.

You will find the monthly recurring "Run" prices in the table below.

Category	Description	Service Unit
Firewall - Base	Native NSX Load Balancer	Per NSX Load Balancer instance

The Service rates do not include:

- IaaS infrastructure costs needed to run the service, which are billed separately

- Change requests

1.3.3   Change catalogue

Category	Subcategory	Token Full France	Token Global	Change request description
Load Balancer	LTM	8	Not available	Modification LTM Pools, Nodes, Monitor, Certificate

Load Balancer	LTM	24	Not available	Add a **VS** (Virtual Server)
Load Balancer	Load Balancer	On quotatio	Not available	Advanced change (above L4 level, scripting)

1.4 Managed Third Party Load Balancer

1.4.1 Description

As part of this service, we provide management for your third-party Load Balancer hosted on a Public Cloud IaaS infrastructure from the list below.

- Cloud Avenue (The Provider)

- Alpha (partially implemented, feasibility study available on demand) Flexible Engine (The Provider)

- Alpha (partially implemented, feasibility study available on demand) - AWS (partner)

- Alpha (partially implemented, feasibility study available on demand) - Microsoft Azure (partner)

- Alpha (partially implemented, feasibility study available on demand) - Google Cloud (partner)

The Managed Third-Party Load Balancer service is delivered through an active-passive cluster of virtual appliances provided by our technology partner (Ivanti), with the following VM configuration options based on the desired functionality and scalability indicated in the following table.

Bandwidth	VM Configuration	SSL transactions per second max
10 Mb/s – 150Mb/s	1 vCPU/2G Memory/32GB HDD	2500
151Mb/s – 300Mb/s	2 vCPU/4G Memory/32GB HDD	5200
301Mb/s – 450Mb/s	4 vCPU/8G Memory/64GB HDD	10000
451Mb/s – 1Gb/s	8 vCPU/16G Memory/128GB HDD	20000
1+ Gb/s	16 vCPU/32G Memory/128GB HDD	38500

The Managed Third Party Load Balancer service includes the following options:

- Local Traffic Manager
- Web Application Firewall.

1.4.1.1 KPI & alerts

Monitoring and logging

The Provider has a system for monitoring and recording logs

Observed metrics during the RUN phase

Operational conditions of the service
- Network interface activity of the configured virtual appliances and Virtual Servers
- Active-passive configuration, possibility of triggering failover
- Backup state
- Load Balancer uptime
- Healthcheck ICMP/SNMP
Resource utilisation
- CPU
- RAM

- Bandwidth used by interfaces

License and updates
- Serial number
- Versioning and security updates

Configured Alerts

Operational conditions of the service
- Resource utilisation
- Cluster accessibility

1.4.1.2 Backup and restore

Data backup and restore

The Provider performs backup of the Load Balancer configuration

Service restore

Load Balancer configuration restore with service verification afterwards

1.4.2 Pricing conditions

The Service pricing consists of:

- Access fees for the "Managed Third-Party Load Balancer" service, including all tasks mentioned in the implementation RACI. To estimate these fees, The Provider conducts a study of the client's requirements, following which a quote for the access fees is generated.
- Monthly recurring fees for "Run" activities covering the maintenance and operational activities of the Managed Third-Party Load Balancer service, indexed based on the number of managed instances and configured options.
- Monthly recurring fees covering the licenses from our technology partner necessary for the operation of the Managed Third-Party Load Balancer service, indexed based on the number of managed instances and configured options.

You will find the monthly recurring "Run" prices in the table below.

Category	Description	Service Unit
Load Balancer - Cluster	Third Party Load Balancer cluster	Per cluster of 2 VM

The list of available licenses can be found in the table below.

License
Ivanti cluster – pack of bandwidth usage up to 100 Mbps

The Service rates do not include:

- IaaS infrastructure costs needed to run the service, which are billed separately

- Change requests

Business

1.4.3 Change catalogue

Category	Subcategory	Token Full France	Token Global	Change request description
Load Balancer	LTM	8	Not available	Modification LTM Pools, Nodes, Monitor, Certificates
Load Balancer	LTM	24	Not available	Add a **VS** (Virtual Server)
Load Balancer	WAF	On quotation	Not available	Simple change **per WAF policy**
Load Balancer	WAF	On quotation	Not available	Add one **url**
Load Balancer	Load Balancer	On quotation	Not available	Advanced change (above L4 level, scripting)

1.5 Shared Managed VPNSSL

1.5.1 Description

As part of this service, we provide management of an integrated VPNSSL service within the Cloud Avenue (The Provider) Public IaaS infrastructure platform.

The shared Managed VPNSSL service is delivered through a virtual appliance backbone from our technology partner (Fortinet), allowing each user to achieve throughputs of up to 10 Mbps.

The shared Managed VPNSSL service includes the following options:

- FortiToken Multifactor Authentication (MFA) with license resale (upon request).

1.5.1.1 KPI & alerts

Monitoring and logging

The Provider has a logging and monitoring system in place for up to 12 months of retention and up to 0,1 GB/day of log collection

Observed metrics during the RUN phase

Operational service conditions
- VPNSSL Client tunnel activity
- VPNSSL Service uptime

Configured Alerts

Operational conditions of the service
- Accessibility to the Shared Managed VPNSSL Service

1.5.1.2 Backup and restore

Data backup and restore

The Provider performs backup of the VPNSSL configuration.

Service restore

Procedure for restoring the configuration following a service reset.

1.5.2 Pricing conditions

The Service Pricing is composed of:

- Access fees for the Shared Managed VPNSSL service, which includes all tasks mentioned in the implementation RACI. To estimate these fees, The Provider conducts a client needs assessment, following which a quote for access fees is generated.
- A monthly recurring 'Run' fee covering activities related to the operational maintenance of the Shared Managed VPNSSL service, indexed based on the number of managed instances and configured options.
- Data egress charges (to the internet or between different sites on the platform) generated using the service, which are billed according to the current rates of the Cloud Avenue (The Provider) Public IaaS infrastructure platform).

You will find the monthly recurring 'Run' prices in the table below.

Category	Description	Service Unit
Firewall – Platform services	Shared Managed VPNSSL	Per declared user
Firewall – Platform services – Options	Multifactor Authentication (MFA)	Upon request

The Service rates do not include:

- Change requests.

1.5.3 Change catalogue

Category	Subcategory	Token Full France	Token Global	Change request description
Firewall	SSL	8	8	Certificate install/modification/suppression
Firewall	SSL	16	Not available	Creation/Modification/suppression of profile SSL Inspection
Firewall	Logs	4	Not available	Flow/objects export request
Firewall	Logs	On quotation	Not available	Log export request
Firewall	VPNSSL	4	4	User access - creation/modification/suppression
Firewall	VPNSSL	8	8	Creation/Modification of LDAP authentication connector
Firewall	VPNSSL	4	4	Configuration suppression
Firewall	Generic	On quotation	Not available	SSO connector creation
Firewall	Generic	On quotation	Not available	Non-Standard change

1.6 Managed Outgoing Proxy

1.6.1 Description

As part of this service, we provide management of your bypass proxy on the Cloud Avenue (The Provider) Public IaaS infrastructure.

The Managed Outgoing Proxy service is delivered through a feature provided by our technology partner (Fortinet) and includes the following options:

- Advanced feature pack (Web & Video Filtering, Data Leak Prevention, AntiVirus etc. – upon request)

1.6.1.1 KPI & alerts

Monitoring and logging

The Provider has a logging and monitoring system in place for up to 12 months of retention and up to 0,2 GB/day of log collection.

Observed metrics during the RUN phase

Operational conditions of the service
- Bandwidth used by the client's IP group
- Advanced feature pack option - analysis of IP address lists referenced as sources of spam or malicious software managed by Fortinet, and injection of new suspicious IPs/URLs into the Bypass Proxy configuration, performed up to multiple times per day
- HTTPS/SNMP Healthcheck
- Backup performed

Configured Alerts

Operational conditions of the service
- Managed Outgoing Proxy service accessibility

1.6.1.2 Backup and restore

Data backup and restore

The Provider performs backup of the Outgoing Proxy configuration

Service restore

Outgoing Proxy configuration restore with service verification afterwards

1.6.2 Pricing Conditions

The Service Pricing is composed of:

- Access fees for the Managed Outgoing Proxy service, which includes all tasks mentioned in the implementation RACI. To estimate these fees, The Provider conducts a client needs assessment, following which a quote for access fees is generated.
- A monthly recurring 'Run' fee covering activities related to the operational maintenance of the Managed Outgoing Proxy service, indexed based on the number of managed instances and configured options.
- Data egress charges (to the internet or between different sites on the platform) generated using the service, which are billed according to the current rates of the Cloud Avenue (The Provider) Public IaaS infrastructure platform).

You will find the monthly recurring 'Run' prices in the table below.

Category	Description	Service Unit
Firewall – Platform services	Managed Outgoing Proxy	Per pack of 10 protected servers
Firewall – Platform services – Options	Advanced feature pack (Web & Video Filtering, Data Leak Prevention, AntiVirus etc.)	Upon request

The Service rates do not include:
- Change requests.

1.6.3 Change catalogue

Famille	Sous Famille	Token Full France	Token Global	Libellé (complet) Demande de Service
Firewall	Flow	4	4	Add/Suppression/Modification of Policy/Object/Service
Firewall	Logs	4	Not available	Flow/objects export request
Firewall	Logs	On quotation	Not available	Log export request
Firewall	Outgoing Proxy	On quotation	Not available	Configuration (1 IP destination)
Firewall	Outgoing Proxy	8	Not available	Modification (1 IP destination)
Firewall	Outgoing Proxy	4	Not available	Suppression
Firewall	Générique	On quotation	Not available	Non-Standard change

1.7 Shared Managed Load Balancer

1.7.1 Description

As part of this service, we provide management of a third-party Load Balancer integrated into the Cloud Avenue (The Provider) Public IaaS Cloud infrastructure platform.

The Shared Managed Load Balancer service is delivered through a virtual appliance backbone provided by our technology partner (Ivanti), allowing all customer-dedicated Virtual Servers to collectively achieve up to 50 Mbps of bandwidth.

The Managed Third Party Load Balancer service includes the following options:

- Local Traffic Manager
- Web Application Firewall (feasibility study and quote available upon request).

1.7.1.1 KPI & alerts

Monitoring and logging

The Provider has a system for monitoring and recording logs

Observed metrics during the RUN phase

Operational conditions of the service
- Network interface activity of the configured Virtual Servers
- ICMP/SNMP Healthcheck

Resource utilisation
- Bandwidth used by Virtual Servers

Configured Alerts

Operational conditions of the service
- Virtual Server resource utilisation
- Shared Managed Load Balancer service accessibility

1.7.1.2 Backup and restore

Data backup and restore

The Provider performs backup of the Load Balancer configuration.

Service restore

Load Balancer configuration restore with service verification afterwards.

1.7.2 Pricing conditions

The Service Pricing is composed of:

- Access fees for the Shared Managed Load Balancer service, which includes all tasks mentioned in the implementation RACI. To estimate these fees, The Provider conducts a client needs assessment, following which a quote for access fees is generated.
- A monthly recurring 'Run' fee covering activities related to the operational maintenance of the Shared Managed Load Balancer service, indexed based on the number of managed instances and configured options.
- Data egress charges (to the internet or between different sites on the platform) generated using the service, which are billed according to the current rates of the Cloud Avenue (The Provider) Public IaaS infrastructure platform).

You will find the monthly recurring 'Run' prices in the table below.

Category	Description	Service Unit
Load Balancer – Platform services	Shared Managed Load Balancer	Per pack of 50 Mbps and 8 Virtual Servers
Load Balancer – Platform services Options	Web Application Firewall	Upon request

The Service rates do not include:
- Change requests.

1.7.3 Change catalogue

Famille	Sous Famille	Token Full France	Token Global	Libellé (complet) Demande de Service
Load Balancer	LTM	8	Not available	Modification LTM Pools, Nodes, Monitor, Certificates
Load Balancer	LTM	24	Not available	Add a **VS** (Virtual Server)
Load Balancer	WAF	On quotation	Not available	Simple change **per WAF policy**
Load Balancer	WAF	On quotation	Not available	Add one **url**
Load Balancer	Load Balancer	On quotation	Not available	Advanced change (above L4 level, scripting)

1.8 Shared Managed Load Balancer for Exchange and Shared Managed Email Security Gateway for Exchange

1.8.1 Description

Within the scope of this service, we ensure the management of a shared Load Balancer and an Email Security Gateway integrated into the Cloud Avenue (The Provider) Public IaaS Cloud infrastructure platform. These services are configured and maintained in operational condition to ensure compatibility with the Managed Exchange offering.

The Managed Shared Load Balancer and Managed Email Security Gateway services are delivered through a virtual appliance backbone provided by our technology partners (Kemp and Fortinet), allowing all Virtual Servers dedicated to the Managed Exchange service to collectively achieve up to 50 Mbps of bandwidth per customer.

The Managed Shared Managed Load Balancer for Exchange service includes the following options:

- Local Traffic Manager.

1.8.1.1 KPI & alerts

Monitoring and logging

The Provider has a system for monitoring and recording logs

Observed metrics during the RUN phase

Operational service conditions
- Virtual Server network interface activity
- Load Balancer and Email Security Gateway ICMP/SNMP Healthcheck

Configured Alerts

Operational conditions of the service
- Accessibility to the Shared Managed Load Balancer for Exchange and the Shared Managed Email Security Gateway for Exchange

1.8.1.2 Backup and restore

Data backup and restore

The Provider performs backup of the Shared Managed Load Balancer for Managed Exchange and Shared Managed Email Security Gateway for Managed Exchange

Service restore

Procedure for restoring the configuration following a service reset

1.8.2 Pricing Conditions

The Service Pricing is composed of:

- Access fees for the Shared Managed Load Balancer for Managed Exchange and Shared Managed Email Security Gateway for Managed Exchange services, which includes all tasks mentioned in the implementation RACI. To estimate these fees, The Provider conducts a client needs assessment, following which a quote for access fees is generated.
- A monthly recurring 'Run' fee covering activities related to the operational maintenance of the Shared Managed Load Balancer for Managed Exchange and Shared Managed Email Security Gateway for Managed Exchange services, indexed based on the number of managed instances and configured options.
- Data egress charges (to the internet or between different sites on the platform) generated using the service, which are billed according to the current rates of the Cloud Avenue (The Provider) Public IaaS infrastructure platform).

You will find the monthly recurring 'Run' prices in the table below.

Category	Description	Service Unit
Load Balancer – Platform services	Shared Managed Load Balancer for Managed Exchange	Par client et pack de 50 Mbps de bande passante
Email Security – Platform services	Shared Managed Email Security Gateway for Managed Exchange	Par pack de 50 Boîtes aux lettres

The Service rates do not include:
- Change requests.

1.8.3 Change catalogue

Category	Subcategory	Token Full France	Token Global	Change request description
Load Balancer	LTM	8	Not available	Modification LTM Pools, Nodes, Monitor, Certificates
Load Balancer	LTM	24	Not available	Add a **VS** (Virtual Server)
Load Balancer	Load Balancer	Sur devis	Not available	Advanced change (above L4 level, scripting)