

Annexe technique au Descriptif de Service Managed Applications Sécurité Managée

Table des matières

| | | |
|----------|---|----------|
| 1 | DESCRIPTION DETAILLÉE PAR SERVICE | 2 |
| 1.1 | MANAGED FIREWALL TIERS | 2 |
| 1.1.1 | Présentation du Service | 2 |
| 1.1.2 | Conditions de prix | 3 |
| 1.1.3 | Catalogue de change | 5 |
| 1.2 | MANAGED FIREWALL NATIF (VMWARE)..... | 6 |
| 1.2.1 | Description..... | 6 |
| 1.2.2 | Conditions de prix | 6 |
| 1.2.3 | Catalogue de change | 7 |
| 1.3 | MANAGED LOAD BALANCER NATIF (VMWARE)..... | 7 |
| 1.3.1 | Description..... | 7 |
| 1.3.2 | Conditions de prix | 8 |
| 1.3.3 | Catalogue de change | 8 |
| 1.4 | MANAGED LOAD BALANCER TIERS..... | 9 |
| 1.4.1 | Description..... | 9 |
| 1.4.2 | Conditions de prix | 10 |
| 1.4.3 | Changes catalogue – in Tokens, per act..... | 11 |
| 1.5 | MANAGED VPNSSL MUTUALISÉ | 11 |
| 1.5.1 | Présentation du Service | 11 |
| 1.5.2 | Conditions de prix | 12 |
| 1.5.3 | Catalogue de change | 12 |
| 1.6 | MANAGED OUTGOING PROXY | 13 |
| 1.6.1 | Présentation du Service | 13 |
| 1.6.2 | Conditions de prix | 13 |
| 1.6.3 | Catalogue de change | 14 |
| 1.7 | MANAGED LOAD BALANCER MUTUALISÉ..... | 14 |
| 1.7.1 | Présentation du Service | 14 |
| 1.7.2 | Conditions de prix | 15 |
| 1.7.3 | Catalogue de change | 16 |
| 1.8 | MANAGED LOAD BALANCER MUTUALISÉ POUR EXCHANGE ET MANAGED EMAIL SECURITY GATEWAY MUTUALISÉ POUR EXCHANGE | 16 |
| 1.8.1 | Présentation du Service | 16 |
| 1.8.2 | Conditions de prix | 17 |
| 1.8.3 | Catalogue de change | 17 |
| 1.9 | MANAGED IDS/IPS MUTUALISÉ..... | 18 |
| 1.9.1 | Présentation du service..... | 18 |
| 1.9.2 | Security Manager | 20 |

1 Description détaillée par service

1.1 Managed Firewall Tiers

1.1.1 Présentation du Service

Dans le cadre de ce service, nous assurons la gestion de votre Firewall tiers hébergé sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

- Cloud Avenue (Le Prestataire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Flexible Engine (Le Prestataire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - AWS (partenaire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Microsoft Azure (partenaire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Google Cloud (partenaire)

Le service de Managed Firewall Tiers est livré grâce à un cluster actif-passif de virtual appliance de notre partenaire technologique (Fortinet), avec les options de configuration VM suivantes en fonction du type de fonctionnalité et de la scalabilité souhaitées :

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

Le service Managed Firewall Tiers inclut les options suivantes :

- VPN IPSec (licence Forticare ou Advanced Threat Protection ou Unified Threat Protection requise)
- VPN SSL (licence Forticare ou Advanced Threat Protection ou Unified Threat Protection requise)
- IPS/IDS (option Extra logging et licence Advanced Threat Protection ou Unified Threat Protection requise)
- Web filtering (licence Unified Threat Protection requise)
- Proxy (licence Unified Threat Protection requise)
- Authentification multifactorielle (MFA) FortiToken avec revente de licence (sur devis)
- FortiAnalyzer dédié (licence FortiAnalyzer dédié requise)
- Option service co-managé (étude de faisabilité sur demande) – co-gestion de certaines fonctionnalités en collaboration avec le client. Cette option requiert une étude de faisabilité, et dans le cas où le client est éligible, les termes d'engagement de qualité de service pour les services co-managés seront appliqués.

L'option IDS/IPS fait l'objet d'une description spécifique en fin

1.1.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs avec une rétention jusqu'à 12 mois et une capacité de collecter jusqu'à 0,5 GB de logs par jour (firewall classique) ou 1,5 GB de logs par jour (IPS/IDS - option Extra logging requise). Les logs peuvent être consultés et exportés

sur demande. Le service n'est pas compatible avec des SIEM (Security Information and Event Management) externes à date.

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Activité interfaces réseau
- Configuration actif-passif, possibilité de déclenchement de la bascule
- Sauvegarde effectuée
- Uptime du firewall
- Healthcheck ICMP/SNMP
- Option IPS/IDS – IP/URL configurés/bloqués
- Option IPS/IDS – en complément des IP/URL choisis par le client, analyse des listes d'adresses IP référencées comme génératrices de spam ou de diffusion de logiciels malveillants gérés par Spamhaus et injection de nouveaux IP/URL suspects dans la configuration IPS/IDS jusqu'à plusieurs fois par jour
- Option IPS/IDS – type d'attaque (DDoS, malware etc.)

Utilisation des ressources

- CPU
- RAM
- Nombre de sessions
- Bande passante utilisée par les interfaces

Licence et mises à jour

- Numéro de série
- Version et veille sécurité

Alertes configurées

Conditions opérationnelles du service

- Utilisation de ressources
- Accessibilité cluster firewall
- Option IPS/IDS – astreinte pour dégradation du service FW et/ou de l'infrastructure (par exemple saturation bande passante du FW entraînée par un attaque DDoS. Dans ce cas le prestataire peut mettre le service offline jusqu'au moment où une solution est identifiée par le client)

1.1.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration firewall

Service restore

Restore de la configuration firewall avec vérification du service en suite.

1.1.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service Managed Firewall Tiers intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectuée par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel de « Run » couvrant les activités liées au maintien en condition opérationnelle du service Managed Firewall Tiers indexé sur le nombre d'instances gérés et les options configurées.
- D'un récurrent mensuel couvrant les licences de notre partenaire technologique nécessaires à l'opération du service Managed Firewall Tiers, indexé sur le nombre d'instances gérés et les options configurées.

Vous trouverez les prix récurrents mensuels de « Run » dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|---|---|--|
| Firewall – Socle | Managed Dedicated Fortigate Firewall (licence Forticare ou Advanced Threat Protection ou Unified Threat Protection requise) | Par cluster de 2 VM |
| Firewall – Options | VPNSSL – 1 tunnel (licence Forticare ou Advanced Threat Protection ou Unified Threat Protection requise) | Inclus dans l’offre “Managed Dedicated Fortigate Firewall” |
| Firewall – Options | VPNIPsec Fortigate – pack de 10 tunnels (licence Forticare ou Advanced Threat Protection ou Unified Threat Protection requise) | Par pack de 10 tunnels VPNIPsec |
| Firewall – Options | IPS/IDS (licence Advanced Threat Protection ou Unified Threat Protection requise) | Inclus dans l’offre “Managed Dedicated Fortigate Firewall” |
| Firewall – Options | Proxy (licence Unified Threat Protection requise) | Inclus dans l’offre “Managed Dedicated Fortigate Firewall” |
| Firewall – Options | Web Filtering (licence Unified Threat Protection requise) | Inclus dans l’offre “Managed Dedicated Fortigate Firewall” |
| Firewall – Offre spéciale administrateur IT | Cluster Firewall avec accès VPNSSL jusqu’à 5 utilisateurs max et reset de mot de passe tous les 60 jours (licence Fortinet incluse, pas possible de rajouter des options) | Par cluster de 2 VM |
| Firewall – Options | Authentification multifactorielle (MFA) FortiToken | Sur devis |
| Firewall – Options | FortiAnalyzer dédié | Par instance |
| Firewall – Options | Extra logging (jusqu’à 1 GB/day) | Par instance |

Vous trouverez la liste des licences disponibles dans le tableau ci-dessous.

| Licence | Unité |
|--|---------------------|
| Cluster Fortigate VM01 FortiCare (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM01 Advanced Threat Protection (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM01 Unified Threat Protection (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM02 FortiCare (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM02 Advanced Threat Protection (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM02 Unified Threat Protection (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM04 FortiCare (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM04 Advanced Threat Protection (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM04 Unified Threat Protection (jusqu’à 10 Virtual Domains) | Par cluster de 2 VM |

| | |
|--|---------------------|
| Cluster Fortigate VM08 Forticare (jusqu'à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM08 Advanced Threat Protection (jusqu'à 10 Virtual Domains) | Par cluster de 2 VM |
| Cluster Fortigate VM08 Unified Threat Protection (jusqu'à 10 Virtual Domains) | Par cluster de 2 VM |
| FortiAnalyzer dédié 5GB/jour et jusqu'à 3 TB en total (jusqu'à 10 Virtual Domains) | Par cluster de 2 VM |

Les tarifs du Service n'incluent pas :

- Le prix de l'infrastructure que vous devez souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

1.1.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|----------|--------------|-------------------|----------------|---|
| Firewall | SSL | 8/4/2 | 8/4/2 | Certificat installation/ modification/ suppression |
| Firewall | SSL | Sur Devis | Pas disponible | Création de profil SSL Inspection |
| Firewall | SSL | Sur Devis | Pas disponible | Modification/suppression de profile SSL Inspection |
| Firewall | SSL | 2 | Pas disponible | Suppression de profile SSL Inspection |
| Firewall | IPS/IDS | 6 | Pas disponible | Configuration (pour une IP destination) |
| Firewall | IPS/IDS | 4 | Pas disponible | Modification (pour une IP destination) |
| Firewall | IPS/IDS | 2 | Pas disponible | Suppression |
| Firewall | Flow | 2 | 2 | Ajout/Suppression/Modification de Policy/Object/Service |
| Firewall | WebFiltering | 4/2/2 | 4/2/2 | Création/Modification/Suppression de catégorie Custom |
| Firewall | Logs | 4 | Pas disponible | Demande d'extraction des flux/objets |
| Firewall | Logs | 2 | Pas disponible | Demande de logs |
| Firewall | Anti-Virus | Sur devis | Pas disponible | Création/Modification/suppression de Profile AV |
| Firewall | VM | 4 | Pas disponible | Changement de modèle de VM |
| Firewall | VM | 2 | Pas disponible | Changement de License |
| Firewall | VPN-Ipsec | 6 | Sur devis | Création |
| Firewall | VPN-Ipsec | 2 | 2 | Suppression |
| Firewall | VPN-Ipsec | 4 | 4 | Modification |
| Firewall | VPNSSL | 2 | 2 | Accès utilisateur - création/modification/suppression |
| Firewall | VPNSSL | 4 | 4 | Ajout/Modification de connecteur d'authentification LDAP |

| | | | | |
|----------|-----------|-----------|----------------|-----------------------------|
| Firewall | VPNSSL | 2 | 2 | Suppression configuration |
| Firewall | Routage | 2 | 2 | Routage / DNAT / SNAT |
| Firewall | Générique | Sur devis | Pas disponible | Création de connecteurs SSO |
| Firewall | Générique | Sur devis | Pas disponible | Modification Non-Standard |

1.2 Managed Firewall Natif (VMware)

1.2.1 Description

Dans le cadre de ce service, nous assurons la gestion de votre Firewall natif sur l'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire), avec une configuration pouvant atteindre jusqu'à 100 règles firewall par client.

Le service de Firewall managé est livré grâce à une fonctionnalité native de notre partenaire technologique (VMware) et il inclut les options suivantes :

- VPN IPSec

1.2.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs.

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Composants VMware NSX de la plateforme Cloud Avenue (plus de détails dans le descriptif de service Cloud Avenue)
- Healthcheck connectivité sortante

Alertes configurées

Conditions opérationnelles du service

- Coupure de la connectivité sortante

1.2.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration NSX et VCD.

Service restore

Procédure de restore de la configuration à la suite d'un reset du service.

1.2.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service « Managed Firewall Natif » intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectuée par le Prestataire, suite à laquelle un devis pour les frais d'accès est créé.
- D'un récurrent mensuel couvrant les activités liées au maintien en condition opérationnelle du service « Managed Firewall Natif » indexé sur le nombre d'instances gérées et les options configurées.

Vous trouverez les prix récurrents mensuels dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|--------------------|---|---------------------------------|
| Firewall - Socle | Firewall natif NSX | Par instance Firewall NSX |
| Firewall - Options | VPNIPsec Fortigate (pack de 10 tunnels) | Par pack de 10 tunnels VPNIPsec |

Les tarifs du Service n'incluent pas :

- Le prix de l'infrastructure que vous devez souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

1.2.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|----------|--------------|-------------------|----------------|---|
| Firewall | Flow | 4 | 4 | Ajout/Suppression/Modification de Policy/Object/Service |
| Firewall | Logs | 4 | Pas disponible | Demande d'extraction des flux/objets |
| Firewall | Logs | N/A | Pas disponible | Demande de logs |
| Firewall | VPN-Ipsec | Sur devis | Sur devis | Création |
| Firewall | VPN-Ipsec | 2 | 2 | Suppression |
| Firewall | VPN-Ipsec | 4 | 4 | Modification |
| Firewall | Routage | 2 | 2 | Routage / DNAT / SNAT |
| Firewall | Générique | Sur devis | Pas disponible | Modification Non-Standard |

1.3 Managed Load Balancer Natif (VMware)

1.3.1 Description

Dans le cadre de ce service, nous assurons la gestion de votre Load Balancer natif sur l'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Le service de Load Balancer Natif managé est livré grâce à une fonctionnalité native de notre partenaire technologique (VMware) et il inclut les options suivantes :

- Local Traffic Manager

1.3.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs.

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Composants VMware NSX de la plateforme Cloud Avenue (plus de détails dans le descriptif de service Cloud Avenue)
- Active health monitor (version standard et avancée)

- Temps de réponse de bout en bout, débit, nombre de séances actives et connexions (version avancée)

Alertes configurées

Conditions opérationnelles du service

- Réponse au healthcheck des VIP

1.3.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration du Load Balancer.

Service restore

Procédure de restore de la configuration à la suite d'un reset du service.

1.3.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service « Managed Load Balancer Natif » intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectué par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel couvrant les activités liées au maintien en condition opérationnelle du service « Managed Load Balancer Natif » indexé sur le nombre d'instances gérés et les options configurées.

Vous trouverez les prix récurrents mensuels dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|-----------------------|--------------------|--------------------------------|
| Load Balancer - Socle | Firewall natif NSX | Par instance Load Balancer NSX |

Les tarifs du Service n'incluent pas :

- Le prix de l'infrastructure que vous devez souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

1.3.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|---------------|---------------|-------------------|----------------|--|
| Load Balancer | LTM | 2 | Pas disponible | Modification LTM Pools, Nodes, Monitor, Certificat |
| Load Balancer | LTM | 4 | Pas disponible | Ajout d'un VS (Virtual Service) |
| Load Balancer | Load Balancer | Sur devis | Pas disponible | Modification avancée (au-delà de L4, scripting) |

1.4 Managed Load Balancer Tiers

1.4.1 Description

Dans le cadre de ce service, nous assurons la gestion de votre Load Balancer tiers hébergé sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

- Cloud Avenue (Le Prestataire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Flexible Engine (Le Prestataire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - AWS (partenaire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Microsoft Azure (partenaire)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Google Cloud (partenaire)

Le service de Managed Load Balancer Tiers est livré grâce à un cluster actif-passif de virtual appliance de notre partenaire technologique (Ivanti), avec les options de configuration VM suivantes en fonction du type de fonctionnalité et de la scalabilité souhaitée indiquées au tableau suivant.

| Bande passante | Configuration VM | Maximum de transactions SSL par seconde |
|-------------------|---------------------------|---|
| 10 Mb/s – 150Mb/s | 1 vCPU/2G Mem/32GB HDD | 2500 |
| 151Mb/s – 300Mb/s | 2 vCPU/4G Mem/32GB HDD | 5200 |
| 301Mb/s – 450Mb/s | 4 vCPU/8G Mem/64GB HDD | 10000 |
| 451Mb/s – 1Gb/s | 8 vCPU/16G Mem/128GB HDD | 20000 |
| 1+ Gb/s | 16 vCPU/32G Mem/128GB HDD | 38500 |

Le service Managed Load Balancer Tiers inclut les options suivantes :

- Local Traffic Manager
- Web Application Firewall.

1.4.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs.

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Activité interfaces réseau des virtual appliance et des Virtual Server configurés
- Configuration actif-passif, possibilité de déclenchement de la bascule
- Sauvegarde effectuée
- Uptime Load Balancer
- Healthcheck ICMP/SNMP

Utilisation des ressources

- CPU
- RAM

- Bande passante utilisée par les interfaces

Licence et mises à jour

- Numéro de série
- Version et veille sécurité

Alertes configurées

Conditions opérationnelles du service

- Utilisation de ressources
- Accessibilité cluster

1.4.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration du Load Balancer.

Service restore

Restore de la configuration du Load Balancer avec vérification du service en suite.

1.4.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service « Managed Load Balancer Tiers » intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectué par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel de « Run » couvrant les activités liées au maintien en condition opérationnelle du service Managed Firewall Tiers indexé sur le nombre d'instances gérés et les options configurées.
- D'un récurrent mensuel couvrant les licences de notre partenaire technologique nécessaires à l'opération du service Managed Firewall Tiers, indexé sur le nombre d'instances gérés et les options configurées.

Vous trouverez les prix récurrents mensuels dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|-----------------------|-----------------------------|---------------------|
| Load Balancer - Socle | Cluster Load Balancer Tiers | Par cluster de 2 VM |

Vous trouverez la liste des licences disponibles dans le tableau ci-dessous.

| Licence |
|---|
| Cluster Ivanti – pack de 100 Mbps de bande passante |

Les tarifs du Service n'incluent pas :

- Le prix de l'infrastructure que vous devez souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

1.4.3 Changes catalogue – in Tokens, per act

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|---------------|---------------|-------------------|----------------|--|
| Load Balancer | LTM | 2 | Pas disponible | Modification LTM Pools, Nodes, Monitor, Certificat |
| Load Balancer | LTM | 4 | Pas disponible | Ajout d'un VS (Virtual Server) |
| Load Balancer | WAF | 4 | Pas disponible | Modification simple par policy WAF |
| Load Balancer | WAF | Sur devis | Pas disponible | Ajout d'une url |
| Load Balancer | Load Balancer | Sur devis | Pas disponible | Modification avancée (au-delà de L4, scripting) |

1.5 Managed VPNSSL mutualisé

1.5.1 Présentation du Service

Dans le cadre de ce service, nous assurons la gestion d'un service VPNSSL intégré dans la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Le service de Managed VPNSSL mutualisé est livré grâce à un backbone de virtual appliance de notre partenaire technologique (Fortinet), qui permet à chaque utilisateur d'atteindre jusqu'à 10 Mbps de débit.

Le service Managed VPNSSL mutualisé inclut les options suivantes :

- Authentification multifactorielle (MFA) FortiToken avec revente de licence (sur devis).

1.5.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs avec une rétention jusqu'à 12 mois et une capacité de collecter jusqu'à 0,1 GB de logs par jour

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Activité tunnel VPNSSL client
- Uptime du service VPNSSL

Alertes configurées

Conditions opérationnelles du service

- Accessibilité au service Managed VPNSSL mutualisé

1.5.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration VPNSSL

Service restore

Restore de la configuration VPNSSL avec vérification du service en suite.

1.5.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service Managed VPNSSL Mutualisé intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectuée par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel de « Run » couvrant les activités liées au maintien en condition opérationnelle du service Managed VPNSSL Mutualisé indexé sur le nombre d'instances gérés et les options configurées.
- Des frais de sortie de données (vers internet ou entre différents sites de la plateforme) générés par l'utilisation du service, qui sont facturés selon les tarifs actuels de la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Vous trouverez les prix récurrents mensuels de « Run » dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|---|--|-------------------------|
| Firewall – Services de plateforme | Managed VPNSSL mutualisé | Par utilisateur déclaré |
| Firewall – Services de plateforme – Options | Authentification multifactorielle (MFA) FortiToken | Sur devis |

Les tarifs du Service n'incluent pas :

- Les demandes de changement.

1.5.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|----------|--------------|-------------------|----------------|---|
| Firewall | SSL | 4 | 4 | Certificat installation/modification/suppression |
| Firewall | SSL | 2 | Pas disponible | Création/Modification/suppression de profile SSL Inspection |
| Firewall | Logs | 2 | Pas disponible | Demande d'extraction des flux/objets |
| Firewall | Logs | Sur devis | Pas disponible | Demande de logs |
| Firewall | VPNSSL | 2 | 2 | Accès utilisateur - création/modification/suppression |
| Firewall | VPNSSL | 4 | 4 | Ajout/Modification de connecteur d'authentification LDAP |
| Firewall | VPNSSL | 2 | 2 | Suppression configuration |
| Firewall | Générique | Sur devis | Pas disponible | Création de connecteurs SSO |
| Firewall | Générique | Sur devis | Pas disponible | Modification Non-Standard |

1.6 Managed Outgoing Proxy

1.6.1 Présentation du Service

Dans le cadre de ce service, nous assurons la gestion de votre proxy d'évasion sur l'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Le service de Managed Outgoing Proxy est livré grâce à une fonctionnalité de notre partenaire technologique (Fortinet) et il inclut les options suivantes :

- Pack fonctionnalités avancées (Web & Video Filtering, Data Leak Prevention, AntiVirus etc. - sur devis)

1.6.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs avec une rétention jusqu'à 12 mois et une capacité de collecter jusqu'à 0,2 GB de logs par jour

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Bande passante utilisée par le groupe d'IP du client
- Option pack fonctionnalités avancées - analyse des listes d'adresses IP référencées comme génératrices de spam ou de diffusion de logiciels malveillants gérés par Fortinet et injection de nouveaux IP/URL suspects dans la configuration du Proxy d'Evasion jusqu'à plusieurs fois par jour
- Healthcheck HTTPS/SNMP
- Sauvegarde effectuée

Alertes configurées

Conditions opérationnelles du service

- Accessibilité au service Managed Outgoing Proxy

1.6.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration du proxy d'évasion

Service restore

Procédure de restore de la configuration à la suite d'un reset du service.

1.6.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service Managed Outgoing Proxy intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectuée par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel couvrant les activités liées au maintien en condition opérationnelle du service Managed Outgoing Proxy indexé sur le nombre d'instances gérés et les options configurées.

- Des frais de sortie de données (vers internet ou entre différents sites de la plateforme) générés par l'utilisation du service, qui sont facturés selon les tarifs actuels de la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Vous trouverez les prix récurrents mensuels dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|---|---|----------------------------------|
| Firewall – Services de plateforme | Managed Outgoing Proxy | Par pack de 10 serveurs protégés |
| Firewall – Services de plateforme – Options | Pack fonctionnalités avancées (Web & Video Filtering, Data Leak Prevention, AntiVirus etc.) | Sur devis |

Les tarifs du Service n'incluent pas :

- Les demandes de changement.

1.6.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|----------|----------------|-------------------|----------------|---|
| Firewall | Flow | 2 | 2 | Ajout/Suppression/Modification de Policy/Object/Service |
| Firewall | Logs | 2 | Pas disponible | Demande d'extraction des flux/objets |
| Firewall | Logs | 2 | Pas disponible | Demande de logs |
| Firewall | Outgoing Proxy | 2 | Pas disponible | Configuration (pour une IP destination) |
| Firewall | Outgoing Proxy | 2 | Pas disponible | Modification (pour une IP destination) |
| Firewall | Outgoing Proxy | 2 | Pas disponible | Suppression |
| Firewall | Générique | Sur devis | Pas disponible | Modification Non-Standard (sécurité avancée) |

1.7 Managed Load Balancer Mutualisé

1.7.1 Présentation du Service

Dans le cadre de ce service, nous assurons la gestion d'un Load Balancer tiers intégré dans la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Le service de Managed Load Balancer Mutualisé est livré grâce à un backbone de virtual appliance de notre partenaire technologique (Ivanti), qui permet à l'ensemble des Virtual Serveurs dédiés au client d'atteindre cumulativement jusqu'à 50 Mbps de bande passante.

Le service Managed Load Balancer Tiers inclut les options suivantes :

- Local Traffic Manager
- Web Application Firewall (étude de faisabilité et devis sur demande)

1.7.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Activité interfaces réseau des Virtual Server configurés
- Healthcheck ICMP/SNMP

Utilisation des ressources

- Bande passante utilisée par Virtual Server

Alertes configurées

Conditions opérationnelles du service

- Utilisation de ressources par Virtual Server
- Accessibilité service load balancer

1.7.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde quotidienne de la configuration du Load Balancer.

Service restore

Restore de la configuration load balancer avec vérification du service en suite.

1.7.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service Managed Load Balancer Mutualisé intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectué par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel de « Run » couvrant les activités liées au maintien en condition opérationnelle du service Managed Load Balancer Mutualisé indexé sur le nombre d'instances gérés et les options configurées.
- Des frais de sortie de données (vers internet ou entre différents sites de la plateforme) générés par l'utilisation du service, qui sont facturés selon les tarifs actuels de la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Vous trouverez les prix récurrents mensuels dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|--|---------------------------------|--|
| Load Balancer – Services de plateforme | Managed Load Balancer Mutualisé | Par client et pack de 50 Mbps de bande passante et 8 Virtual Servers |
| Load Balancer – Options services de plateforme | Web Application Firewall | Sur devis |

Les tarifs du Service n'incluent pas :

- Les demandes de changement.

1.7.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|---------------|---------------|-------------------|----------------|--|
| Load Balancer | LTM | 2 | Pas disponible | Modification LTM Pools, Nodes, Monitor, Certificat |
| Load Balancer | LTM | 4 | Pas disponible | Ajout d'un VS (Virtual Server) |
| Load Balancer | WAF | 4 | Pas disponible | Modification simple par policy WAF |
| Load Balancer | WAF | 4 | Pas disponible | Ajout d'une url |
| Load Balancer | Load Balancer | Sur devis | Pas disponible | Modification avancée (au-delà de L4, scripting) |

1.8 Managed Load Balancer mutualisé pour Exchange et Managed Email Security Gateway mutualisé pour Exchange

1.8.1 Présentation du Service

Dans le cadre de ce service, nous assurons la gestion d'un Load Balancer mutualisé et d'une passerelle de Messagerie Sécurisée intégrés dans la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire). Les services sont configurés et maintenus en condition opérationnelles pour assurer la compatibilité avec l'offre Managed Exchange.

Les services de Managed Load Balancer mutualisé et Managed Email Security Gateway sont livrés grâce à un backbone de virtual appliance de nos partenaires technologiques (Kemp et Fortinet), qui permettent à l'ensemble des Virtual Serveurs dédiés au service Managed Exchange d'atteindre cumulativement jusqu'à 50 Mbps de bande passante.

Le service Managed Load Balancer mutualisé pour Exchange inclut les options suivantes :

- Local Traffic Manager.

1.8.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Activité interfaces réseau des Virtual Server configurés du Load Balancer
- Healthcheck ICMP/SNMP du Load Balancer et de l'Email Security Gateway

Alertes configurées

Conditions opérationnelles du service

- Accessibilité du service Managed Load Balancer mutualisé pour Exchange et Managed Email Security Gateway mutualisé Exchange

1.8.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration du service Managed Load Balancer mutualisé pour Managed Exchange et Managed Email Security Gateway mutualisé pour Managed Exchange

Service restore

Restore de la configuration Load Balancer et Email Security Gateway avec vérification du service en suite.

1.8.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service Managed Load Balancer mutualisé pour Exchange et Managed Email Security Gateway mutualisé pour Exchange intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectué par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel de « Run » couvrant les activités liées au maintien en condition opérationnelle du service Managed Load Balancer mutualisé pour Exchange et Managed Email Security Gateway mutualisé pour Exchange indexé sur le nombre d'instances gérés et les options configurées.
- Des frais de sortie de données (vers internet ou entre différents sites de la plateforme) générés par l'utilisation du service, qui sont facturés selon les tarifs actuels de la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Vous trouverez les prix récurrents mensuels dans le tableau ci-dessous.

| Famille | Sous Famille | Unité de service |
|---|---|---|
| Load Balancer – Services de plateforme | Managed Load Balancer mutualisé pour Exchange | Par client et pack de 50 Mbps de bande passante |
| Email Security – Services de plateforme | Managed Email Security Gateway mutualisé Exchange | Par pack de 50 Boîtes aux lettres |

Les tarifs du Service n'incluent pas :

- Les demandes de changement.

1.8.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|---------------|---------------|-------------------|----------------|--|
| Load Balancer | LTM | 2 | Pas disponible | Modification LTM Pools, Nodes, Monitor, Certificat |
| Load Balancer | LTM | 6 | Pas disponible | Ajout d'un VS (Virtual Server) |
| Load Balancer | Load Balancer | Sur devis | Pas disponible | Modification avancée (au-delà de L4, scripting) |

1.9 Managed IDS/IPS Mutualisé

1.9.1 Présentation du service

Dans le cadre de ce service, nous assurons la gestion d'un IPS/IDS mutualisé dans la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire). Le service est configuré et maintenu en condition opérationnelle.

Le service de Managed IDS/IPS mutualisé est livré grâce à un backbone de virtual appliance de notre partenaire technologique (Palo Alto).

Voici les mécanismes IDS/IPS mis en place :

- Détection basée sur des signatures et comportementales
- Détection heuristique :
 - Target (serveur)
 - OS (Windows, Linux)
 - Severity (medium, High, critical)
 - Application (middleware MS et Web)
 - Protocol (tous port TCP/UDP)
- Détection anomalies
- Détection basée sur l'hôte (IP, catégorie, réputation, géographie etc.)
- Détection d'intrusion réseau (NIDS)
- Détection en temps réel, à posteriori
- Le déchiffrement des protocoles HTTPS est disponible. La liste des Ciphers supportés est disponible dans la documentation de l'éditeur Palo Alto

1.9.1.1 KPI & alerts

Monitoring et logging

Le Prestataire dispose d'un système de surveillance et d'enregistrement des logs avec une rétention jusqu'à 12 mois et une capacité de collecter jusqu'à 1 GB de logs par jour (IPS/IDS - option Extra logging obligatoire). Les logs peuvent être consultés et exportés sur demande. A date, le service n'est pas compatible avec un SIEM externe.

Métriques observées en phase de RUN

Conditions opérationnelles du service

- Activité interfaces réseau des Virtual Server configurés
- Healthcheck ICMP/SNMP

Utilisation des ressources

- Bande passante utilisée par Client

Alertes configurées

Conditions opérationnelles du service

- Accessibilité service IDS/IPS

Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration IDS/IPS

Service restore

Restore de la configuration IDS/IPS avec vérification du service en suite.

1.9.1.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au service IDS/IPS Mutualisé intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectuée par le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel de « Run » couvrant les activités liées au maintien en condition opérationnelle indexé sur le nombre d'instances gérées et les options configurées.
- Des frais de sortie de données (vers internet ou entre différents sites de la plateforme) générés par l'utilisation du service, qui sont facturés selon les tarifs actuels de la plateforme d'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).

Vous trouverez les prix récurrents mensuels dans le tableau ci-dessous :

| Famille | Sous Famille | Unité de service |
|---------------------------------|---------------------------|-----------------------------------|
| Firewall- Service de Plateforme | Managed IDS/IPS Mutualisé | Par client et pack de 40 serveurs |
| Firewall-Service de Plateforme | Extra Logging (1 Go) | Par pack de 40 serveurs |

Les tarifs du Service n'incluent pas :

- Les demandes de changement

1.9.1.3 Catalogue de change

| Famille | Sous Famille | Token Full France | Token Global | Libellé (complet) Demande de Service |
|----------|--------------|-------------------|----------------|---|
| Firewall | IPS/IDS | 6 | Pas disponible | Ajout Configuration (gestion de profil/@ip) |
| Firewall | IPS/IDS | 4 | Pas disponible | Modification (gestion de profil/@IP) |
| Firewall | IPS/IDS | 2 | Pas disponible | Suppression (gestion de profil/@ip) |

1.9.2 Security Manager

L'accompagnement du Security Manager apporte une lecture mensuelle des rapports d'alertes relevés par le service afin de permettre au Client de comprendre les différents indicateurs et éventuellement l'accompagner sur des plans d'actions à prévoir.

Le Security Manager effectue un rapport concernant les incidents remontés par le service dans le mois, rapporte les nouvelles grandes menaces et tendances visibles sur le marché de la sécurité informatique et propose éventuellement quelques plans d'actions en fonction des incidents et des menaces rapportés. Ce rapport est le support de la relecture effectuée par le Security Manager avec le Client par téléphone pendant une réunion d'une heure. A l'issue de cette réunion de relecture, le Client sera alors à même de faire des demandes de changements pour optimiser sa politique de sécurité.

| Famille | Sous Famille | Unité de service |
|-------------------------|--------------------------------|-----------------------------|
| Firewall-Accompagnement | Prestation de Security manager | Par client et pack de 20 VM |