

Description de Service Technique Managed Firewall et Managed Load Balancer

Table des matières

1	DESCRIPTION DETAILLEE PAR SERVICE	2
	MANAGED FIREWALL TIERS	2
	1.1.1 <i>Présentation du Service</i>	2
	1.1.2 <i>Conditions de prix</i>	3
	1.1.3 <i>Catalogue de change</i>	4
	MANAGED FIREWALL NATIF (NSX).....	5
	1.1.4 <i>Description</i>	5
	1.1.5 <i>Conditions de prix</i>	6
	1.1.6 <i>Catalogue de change</i>	6
	LOAD BALANCER TIERS.....	6
	1.1.7 <i>Description</i>	6
	1.1.8 <i>Conditions de prix</i>	8
	1.1.9 <i>Changes catalogue – in Tokens, per act</i>	8
2	GLOSSAIRE.....	9

1 Description détaillée par service

Managed Firewall Tiers

1.1.1 Présentation du Service

Dans le cadre de ce service, le Prestataire assure la gestion du Firewall tiers du Client hébergé sur une infrastructure de Cloud Public IaaS de la liste ci-dessous.

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

Le service de Managed Firewall Tiers est livré grâce à un cluster actif-passif de virtual appliance 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 (licence Advanced Threat Protection ou Unified Threat Protection requise)
- Web filtering (licence Unified Threat Protection requise)
- Proxy (licence Unified Threat Protection requise)

1.1.1.1 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
- Configuration actif-passif, possibilité de déclenchement de la bascule
- Sauvegarde effectuée
- Uptime du firewall
- Healthcheck ICMP/SNMP

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

1.1.1.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde de la configuration du 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 Fortinet nécessaires à l'opération du service Managed Firewall Tiers, indexé sur le nombre d'instances gérées et les options configurées.

Les prix récurrents mensuels de « Run » sont listés dans le tableau ci-dessous.

Famille	Sous Famille	Unité de service
Firewall – Socle	Cluster Firewall tiers (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 "Cluster Firewall tiers"
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 "Cluster Firewall tiers"

Firewall – Options	Proxy (licence Unified Threat Protection requise)	Inclus dans l'offre "Cluster Firewall tiers"
Firewall – Options	Web Filtering (licence Unified Threat Protection requise)	Inclus dans l'offre "Cluster Firewall tiers"
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

Les licences disponibles sont listées dans le tableau ci-dessous.

Licence
Cluster Fortigate VM01 FortiCare
Cluster Fortigate VM01 Advanced Threat Protection
Cluster Fortigate VM01 Unified Threat Protection
Cluster Fortigate VM02 FortiCare
Cluster Fortigate VM02 Advanced Threat Protection
Cluster Fortigate VM02 Unified Threat Protection
Cluster Fortigate VM04 FortiCare
Cluster Fortigate VM04 Advanced Threat Protection
Cluster Fortigate VM04 Unified Threat Protection
Cluster Fortigate VM08 Forticare
Cluster Fortigate VM08 Advanced Threat Protection
Cluster Fortigate VM08 Unified Threat Protection

Les tarifs du Service n'incluent pas :

- Le prix de l'infrastructure que le Client doit 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	8	Certificat installation/modification/suppression
Firewall	SSL	16	Pas disponible	Création/Modification/suppression de profile SSL Inspection
Firewall	IPS/IDS	Sur devis	Pas disponible	Configuration (pour une IP destination)
Firewall	IPS/IDS	8	Pas disponible	Modification (pour une IP destination)
Firewall	IPS/IDS	4	Pas disponible	Suppression
Firewall	Flow	4	4	Ajout/Suppression/Modification de Policy/Object/Service
Firewall	WebFiltering	4	4	Création/Modification/Suppression de catégorie Custom
Firewall	Logs	4	Pas disponible	Demande d'extraction des flux/objets

Firewall	Logs	Sur devis	Pas disponible	Demande de logs
Firewall	Anti-Virus	8	Pas disponible	Création/Modification/suppression de Profile AV
Firewall	VM	8	Pas disponible	Changement de modèle de VM
Firewall	VM	8	Pas disponible	Changement de License
Firewall	VPN-Ipsec	Sur devis	Sur devis	Création
Firewall	VPN-Ipsec	8	8	Suppression
Firewall	VPN-Ipsec	8	8	Modification
Firewall	VPNSSL	4	4	Accès utilisateur - création/modification/suppression
Firewall	VPNSSL	8	8	Ajout/Modification de connecteur d'authentification LDAP
Firewall	VPNSSL	4	4	Suppression configuration
Firewall	Routage	4	4	Routage / DNAT / SNAT
Firewall	Générique	Sur devis	Pas disponible	Création de connecteurs SSO
Firewall	Générique	Sur devis	Pas disponible	Modification Non-Standard

Managed Firewall Natif (NSX)

1.1.4 Description

Dans le cadre de ce service, le Prestataire assure la gestion du Firewall natif du Client sur l'infrastructure Cloud Public IaaS Cloud Avenue (Orange Business).

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

- VPN IPSec

1.1.4.1 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

- Interruption du service NSX
- Coupure de la connectivité sortante

1.1.4.2 Backup and restore

Data backup and restore

Le Prestataire procède à la sauvegarde des configurations NSX et VCD.

Service restore

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

1.1.5 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, puis 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 le Client doit souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

1.1.6 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	Sur devis	Pas disponible	Demande de logs
Firewall	VPN-Ipsec	Sur devis	Sur devis	Création
Firewall	VPN-Ipsec	8	8	Suppression
Firewall	VPN-Ipsec	8	8	Modification
Firewall	Routage	4	4	Routage / DNAT / SNAT
Firewall	Générique	Sur devis	Pas disponible	Modification Non-Standard

Load Balancer Tiers

1.1.7 Description

Dans le cadre de ce service, le Prestataire assure la gestion du Load Balancer tiers du Client hébergé sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

- Cloud Avenue (Orange Business)

- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Flexible Engine (Orange Business)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - AWS (hyperscaler)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Microsoft Azure (hyperscaler)
- Alpha (certaines fonctionnalités en cours d'implémentation, étude de faisabilité sur demande) - Google Cloud (hyperscaler)

Le service de Managed Load Balancer Tiers est livré grâce à un cluster actif-passif de virtual appliance Ivanti, avec les options de configuration VM suivantes en fonction du type de fonctionnalité et de la scalabilité souhaitée, telles qu'indiquées dans le 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.

1.1.7.1 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

1.1.7.2 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 firewall avec vérification du service en suite.

1.1.8 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, puis 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 gérées et les options configurées.
- D'un récurrent mensuel couvrant les licences Ivanti nécessaires à l'opération du service Managed Firewall Tiers, indexé sur le nombre d'instances gérés et les options configurées.

Les prix récurrents mensuels sont listés dans le tableau ci-dessous.

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

Licences disponibles sont listées 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 le Client doit souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

1.1.9 Changes catalogue – in Tokens, per act

Famille	Sous Famille	Token Full France	Token Global	Libellé (complet) Demande de Service
Load Balancer	LTM	8	Pas disponible	Modification LTM Pools, Nodes, Monitor, Certificat
Load Balancer	LTM	24	Pas disponible	Ajout d'un VS (Virtual Server)
Load Balancer	WAF	16	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)

2 Glossaire

Fortinet désigne le partenaire technologique du Prestataire pour la fourniture du Service Firewall managé

Ivanti désigne le partenaire technologique du Prestataire pour la fourniture du Service de Load Balancer managé