



**Chambre de Commerce et d'Industrie de région pays de la Loire (CCIR)**

Établissement public administratif

1 rue Françoise Sagan – 44800 SAINT-HERBLAIN

<https://www.paysdelaloire.cci.fr>

SIRET 184 401 289 00022 – TVA n° FR 75 184 401 289

**CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)**

**Marché « Firewall et Sécurité »**

**N° marché : 2025 GCPF 1075**



## Sommaire :

<b>1</b>	<b>Contexte .....</b>	<b>3</b>
1.1	Objet du marché .....	3
1.2	Organisation des CCI .....	3
<b>2</b>	<b>Description de l'existant .....</b>	<b>3</b>
2.1	Inventaire des composants firewalls existants et licences associées .....	3
2.2	Schéma de l'architecture Internet .....	4
2.3	Accès Internet .....	5
2.4	Firewall DataCenter .....	5
2.5	Métriques de l'infrastructure et dimensionnement .....	5
2.5.1	Firewall internet PA-3220 .....	6
2.5.2	Firewall central PA-3260 .....	8
2.5.3	User-ID Agent .....	11
2.6	Caractéristiques techniques de l'architecture .....	11
2.6.1	Filtrage applicatif .....	11
2.6.2	Routage .....	11
2.6.3	Déchiffrement .....	11
2.6.4	Qualité de service .....	11
2.6.5	Identification .....	11
2.6.6	Système de détection des menaces connues .....	12
2.6.7	Filtrage URL .....	12
2.6.8	Rapports et analyse .....	12
2.6.9	Administration .....	12
2.6.10	Failover .....	13
2.6.11	VPN .....	13
2.6.12	Plug-In VCENTER .....	13
2.6.13	Supervision via API .....	13
2.6.14	Assistance à l'analyse de configuration .....	14
<b>3</b>	<b>Projet de remplacement de l'infrastructure .....</b>	<b>14</b>
3.1	Déplacement de fonctionnalités .....	14
3.2	Contraintes techniques de migration .....	15
3.3	Connectiques de l'infrastructure proposée .....	15
3.4	Contraintes de planning de migration .....	15
3.5	Contraintes budgétaires .....	16
3.6	Prestations .....	16
3.7	Maintenance .....	16
3.8	Reprise de matériel .....	16
3.9	Délais de livraison .....	17
3.10	Marché à bons de commande .....	17

3.11	Remise constructeur / éditeur .....	17
3.12	Evolution technologique .....	17

## 1 Contexte

### 1.1 Objet du marché

L'objet du marché est de remplacer les équipements firewalls actuellement en place, et dont les contrats de support et licences arrivent à leur terme.

### 1.2 Organisation des CCI

Les CCI Pays de la Loire et CCI Bretagne détiennent chacune un datacenter. Les 2 datacenters fonctionnent entre eux en mode PRA.

18 entités CCI du grand Ouest utilisent ces environnements pour leurs besoins communs ou locaux.

Les investissements du datacenter PDLL (DC PDLL) sont réalisés par la CCI Pays de la Loire.

Les investissements du datacenter BZH (DC BZH) sont réalisés par la CCI Bretagne.

Dans des offres optimisées de type bundle, le titulaire devra pouvoir facturer son offre en fonction d'une clé de répartition fournie par les CCI au moment de la mise au point du marché.

La cotation proposée sera globale et ne tiendra pas compte des clés de répartition.

## 2 Description de l'existant

### 2.1 Inventaire des composants firewalls existants et licences associées

L'architecture actuelle est construite autour de deux niveaux de Firewall :

- 2 Palo Alto PA-3220 version 11.1.6-h10 Actif/Passif, frontal internet (sécurité périmétrique)

Licence	Expiration
Pan-DB URL Filtering	08/12/2025
Advanced URL Filtering	08/12/2025
DNS Security	08/12/2025
Support	08/12/2025

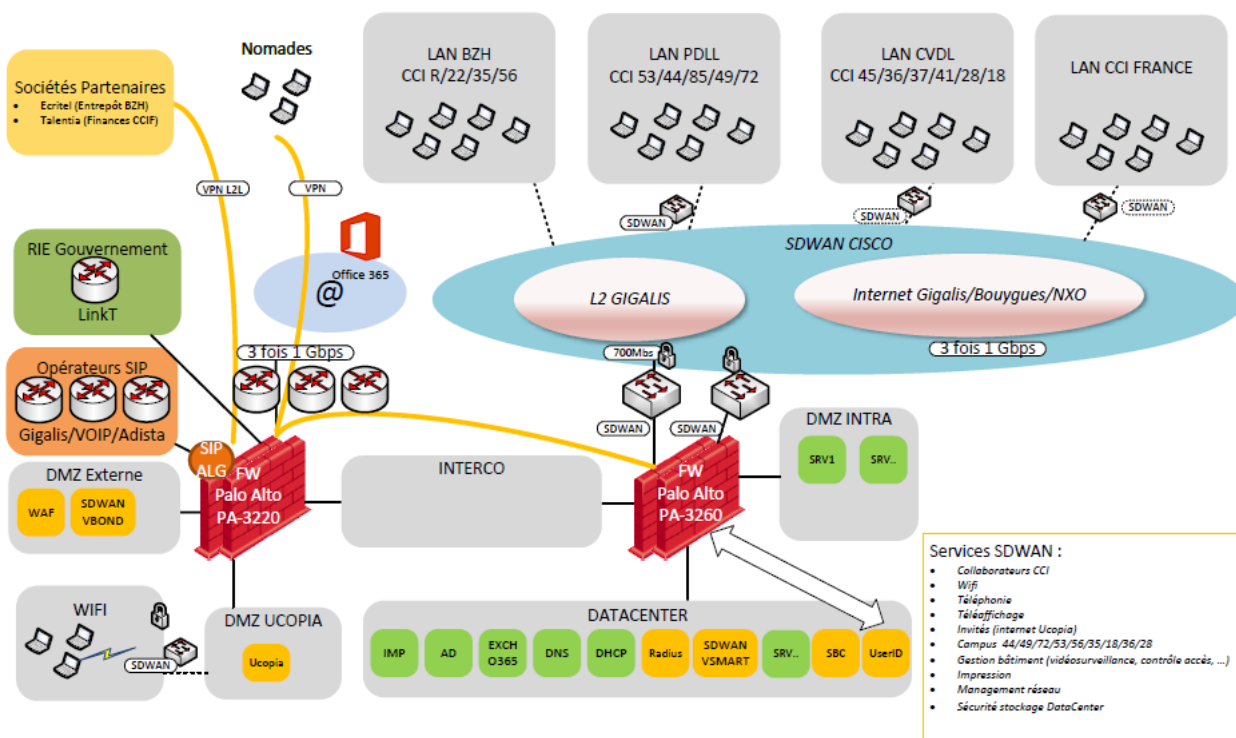
- 2 Palo Alto PA-3260 version 11.1.6-h10 Actif/Passif, routage au cœur du DataCenter (segmentation interne)

Licence	Expiration
Threat Prevention	28/01/2026
Pan-DB URL Filtering	28/01/2026
Wildfire	28/01/2026
Support	28/01/2026

- 1 VM Palo Alto panorama version 11.1.6-h10, fonctionnant sur VMware vSphere 8.0.3 : Management des 2 clusters et stockage des logs
- 2 VM Windows avec User-ID Agent, version 11.0.1-104 : correspondance utilisateurs et IP machine.
- Les 4 firewalls sont reliés à la télémétrie PaloAlto au travers de son Cloud avec 9 mois de rétention de Logs.

## 2.2 Schéma de l'architecture Internet

### Schéma du réseau CCI interrégional



## 2.3 Accès Internet

L'accès Internet client est géré par un cluster de deux Firewall 3220 connectés à 3 accès Internet différents qui sont utilisés simultanément suivant des stratégies précises.

Type population	Authentification	Politique d'accès	Accès Internet primaire	Accès Internet Secours
Hotspot	Ucopia	spg_hotspot	Internet NXO	Internet Bouygues
Virtlab	IP Virtlab	spg_virtlab	Internet NXO	Internet Bouygues
Apprennants	Ucopia	spg_apprenants	Internet Bouygues	Internet NXO
Apprennants	Active Directory (UserId)	spg_apprenants	Internet Gigalis	Internet Bouygues
CCI	Ucopia	spg_ccipdll	Internet Bouygues	Internet NXO
CCI	Active Directory (Global Protect + UserId)	spg_ccipdll	Internet Gigalis	Internet Bouygues
Serveurs	IP	spg_server	Internet Gigalis	Internet Bouygues

## 2.4 Firewall DataCenter

80% des règles du Firewall sont basées sur des groupes Active Directory récurifs (**nested group**) de sorte qu'un utilisateur puisse retrouver ses droits réseaux de n'importe où (Sites, VPN, Wifi, ...).

L'identification des utilisateurs par leur(s) adresse(s) IP repose sur le client Global Protect ou le serveur User-ID Agent qui scrute l'ensemble des domaines Active Directory de l'infrastructure :

- CCIPDLL.LOCAL : domaine collaborateurs CCI Pays de la Loire, CCI Centre Val de Loire, CCI Bretagne et CCI France
- CAMPUS72.LAN : domaine formation 72
- SERVICES.LAN : domaines de services spécifiques CCI
- CAMPUS53.LAN : domaine formation 53
- CAMPUS36.LAN : domaine formation 36
- CAMPUS49.LAN : domaine formation 49
- CAMPUS44.LAN : domaine formation 44
- CCIFDM.PRIV : domaine formation 35
- CAMPUS-18.LAN : domaine formation 18

L'ensemble de ces domaines sont **approuvés** par le domaine principal CCIPDLL.LOCAL.

## 2.5 Métriques de l'infrastructure et dimensionnement

Les solutions de supervision utilisées par les équipes DSI permettent de suivre en temps réel l'ensemble des métriques.

Voici les caractéristiques techniques principales de l'infrastructure. Le titulaire devra s'appuyer sur ces valeurs pour choisir une solution répondant à ces exigences en tenant compte de l'évolutivité des flux et des besoins futurs.



### 2.5.1 Firewall internet PA-3220

- Nombre de sessions TCP/UDP simultanées maximum : 126000 (12 %)
  - Nombre de groupes AD synchronisés sur le Firewall : 8700
  - Nombre de règles de NAT : 123
  - Nombre ACL ~ 100
  - Nombre de zones : 7
  - Nombre d'interfaces VLAN : 11
  - Taille de fichier de conf : 25 Mo
- 
- Data Throughput

#### Data Throughput - FW-44DC1-INT

Numéro de série: 016201013955 | Modèle: PA-3220 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.234

Dernière valeur mé...	Metric Name
62K	Data Throughput

##### DESCRIPTION MÉTRIQUE

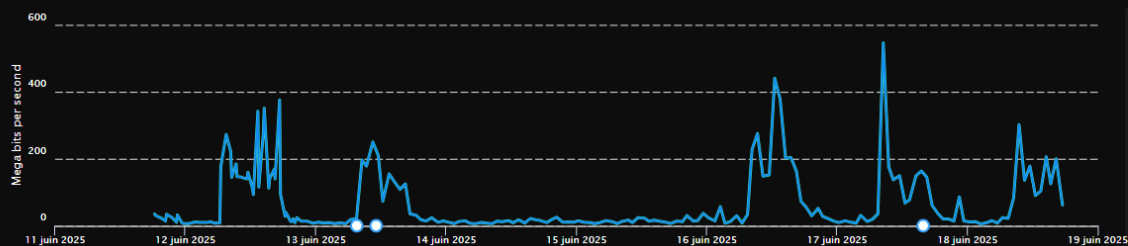
Identifies the amount of data moving through the device.

##### IMPACT

High data flows can result in packet drops at either the network interface level or at the packet buffer level. This can result in degraded network performance, or in increased hardware resource usage as the device attempts to keep up w

#### Data Throughput

Past 7 Days





- Dataplane Average CPU utilisation sur 1 semaine

### Dataplane Average CPU Utilization (s1dp0) - FW-44DC1-INT

Numéro de série: 016201013955 | Modèle: PA-3220 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.234

Dernière valeur mé... | Metric Name

15% | Dataplane Average CPU Utilization (s1dp0)

#### DESCRIPTION MÉTRIQUE

Identifies the dataplane CPU utilization, averaged across all cores available to the specific dataplane, and reports the average on the last period.

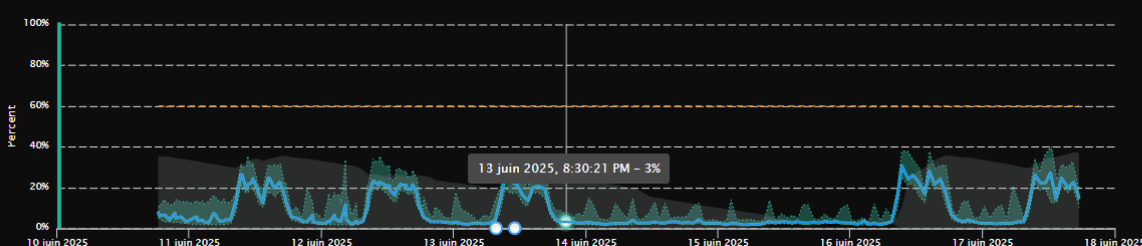
- Warning: 60% - 85% average CPU utilization.
- Critical: Greater than 85% average CPU utilization.

#### IMPACT

Dataplane CPU utilization increases as the device processes increasingly large amounts of traffic, and increasingly complex traffic. Every network protocol demands different processing requirements of the device. The nature of the n that the device decrypts, or a surge in volume for a particular protocol that matches a security profile, will increase the dataplane CPU utilization value. A high dataplane CPU utilization can degrade the device's ability to optimally per

#### Dataplane Average CPU Utilization (s1dp0)

Past 7 Days



- Packet descriptor Max On-chip sur 1 semaine

### Packet Descriptor Max(on-chip) (s1dp0) - FW-44DC1-INT

Numéro de série: 016201013955 | Modèle: PA-3220 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.234

Dernière valeur mé... | Metric Name

9% | Packet Descriptor Max(on-chip) (s1dp0)

#### DESCRIPTION MÉTRIQUE

Identifies the packet descriptor on-chip utilization. The device assigns every packet that it is processing an abstract indicator called a *descriptor*. The device uses these descriptors on-chip to access the packets that it is processing. Ev it can assign at any given time.

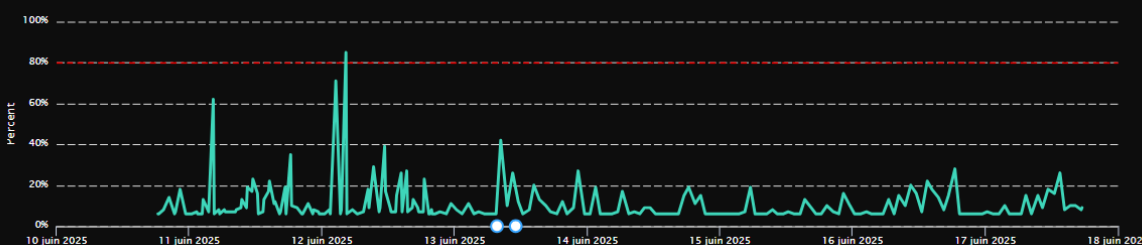
- Warning: 60% - 85% descriptor on-chip utilization.
- Critical: Greater than 85% descriptor utilization.

#### IMPACT

Network Throughput may be negatively impacted. Latency in traffic can be observed with increased usage on Packet Descriptors(on-chip).

#### Packet Descriptor Max(on-chip) (s1dp0)

Past 7 Days





- Traffic Log Generation Rate

### Traffic Log Generation Rate (s1dp0) - FW-44DC1-INT

Numéro de série: 016201013955 | Modèle: PA-3220 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.234

Dernière valeur mé...

Metric Name

806

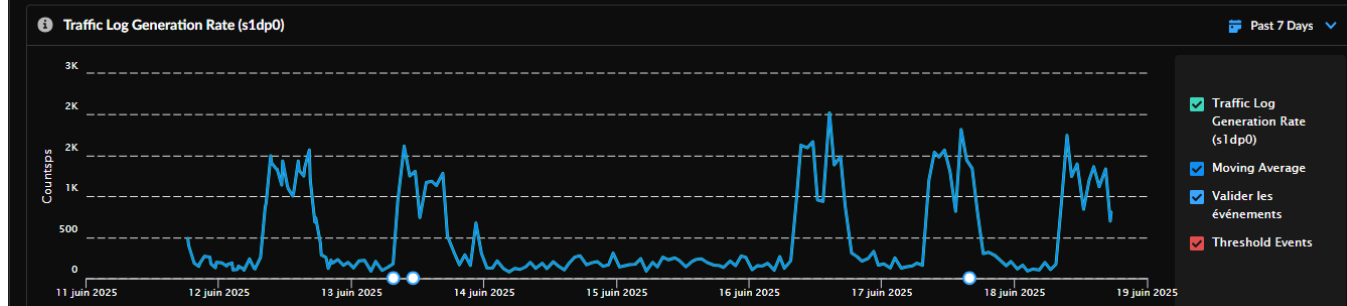
Traffic Log Generation Rate (s1dp0)

#### DESCRIPTION MÉTRIQUE

Identifies the rate at which the device is generating traffic logs.

#### IMPACT

If the traffic log generation rate is too high, traffic log records generated on the dataplane can not be written to disk, which results in their loss. Also, log forwarding to syslog servers or to Panorama can be adversely affected by a high your devices, and to debug any issues that might arise on your devices.



### 2.5.2 Firewall central PA-3260

- Nombre de sessions TCP/UDP simultanées maximum : 150000 (7 %)
  - Nombre de règles de NAT : 12
  - Nombre de groupes AD synchronisés sur le Firewall : 8700
  - Nombre d'utilisateurs connectés au VPN Global Protect : 500
  - Nombre ACL ~ 1100
  - Nombre de zones : 41
  - Nombre d'interfaces VLAN : 57
  - Taille de fichier de conf : 27 Mo
- Data Throughput

### Data Throughput - FW-44NEO-01

Numéro de série: 016401014372 | Modèle: PA-3260 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.231

Dernière valeur mé...

Metric Name

894K

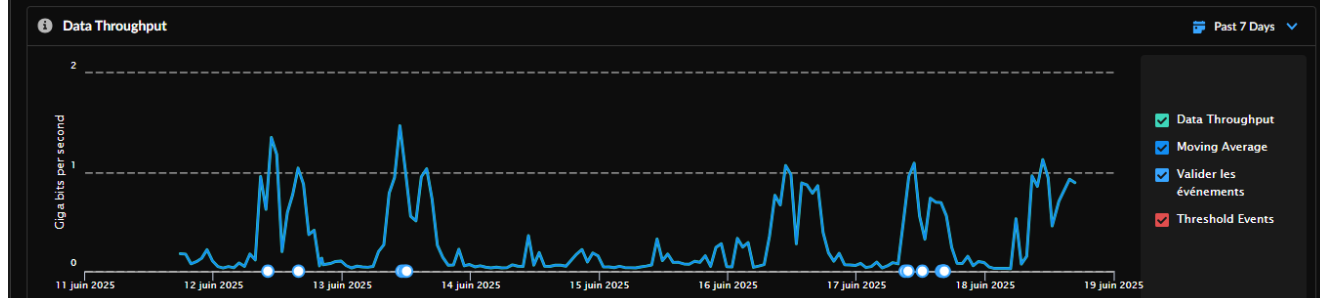
Data Throughput

#### DESCRIPTION MÉTRIQUE

Identifies the amount of data moving through the device.

#### IMPACT

High data flows can result in packet drops at either the network interface level or at the packet buffer level. This can result in degraded network performance, or in increased hardware resource usage as the device attempts to keep up v







- Dataplane Average CPU utilisation sur 1 semaine

### Dataplane Average CPU Utilization (s1dp0) - FW-44NEO-01

Numéro de série: 016401014372 | Modèle: PA-3260 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.231

Dernière valeur mé... | Metric Name

66% | Dataplane Average CPU Utilization (s1dp0)

#### DESCRIPTION MÉTRIQUE

Identifies the dataplane CPU utilization, averaged across all cores available to the specific dataplane, and reports the average on the last period.

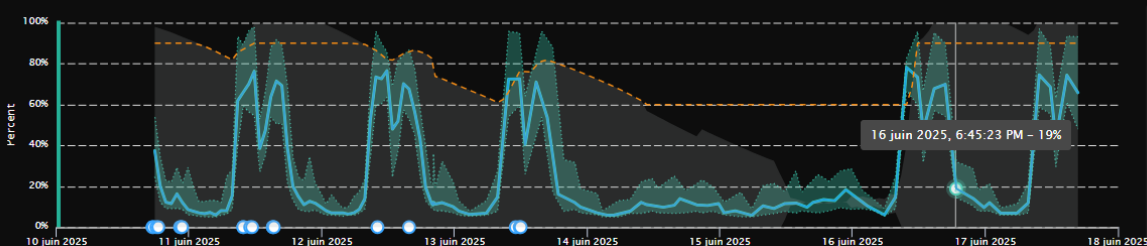
- Warning: 60% - 85% average CPU utilization.
- Critical: Greater than 85% average CPU utilization.

#### IMPACT

Dataplane CPU utilization increases as the device processes increasingly large amounts of traffic, and increasingly complex traffic. Every network protocol demands different processing requirements of the device. The nature of the traffic that the device decrypts, or a surge in volume for a particular protocol that matches a security profile, will increase the dataplane CPU utilization value. A high dataplane CPU utilization can degrade the device's ability to optimally process traffic.

#### Dataplane Average CPU Utilization (s1dp0)

Past 7 Days



- ☒ Dataplane Average CPU Utilization (s1dp0)
- ☒ Moving Average
- ☒ Valider les événements
- ☒ Threshold Events
- ☒ Min / Max range
- ☒ Normality Band

- Packet descriptor Max On-chip sur 1 semaine

### Packet Descriptor Max(on-chip) (s1dp0) - FW-44NEO-01

Numéro de série: 016401014372 | Modèle: PA-3260 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.231

Dernière valeur mé... | Metric Name

89% | Packet Descriptor Max(on-chip) (s1dp0)

#### DESCRIPTION MÉTRIQUE

Identifies the packet descriptor on-chip utilization. The device assigns every packet that it is processing an abstract indicator called a descriptor. The device uses these descriptors on-chip to access the packets that it is processing. Every packet that it can assign at any given time.

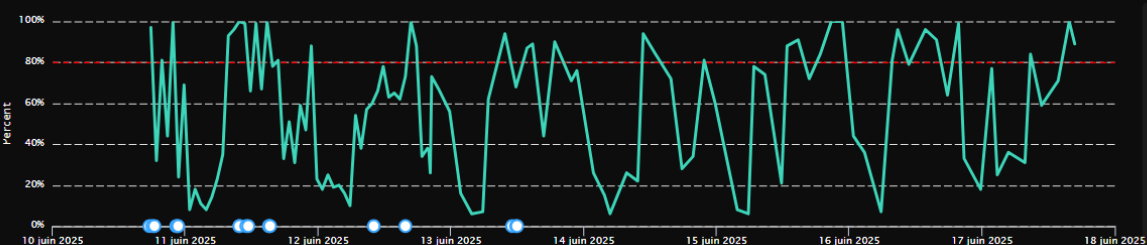
- Warning: 60% - 85% descriptor on-chip utilization.
- Critical: Greater than 85% descriptor utilization.

#### IMPACT

Network Throughput may be negatively impacted. Latency in traffic can be observed with increased usage on Packet Descriptors(on-chip).

#### Packet Descriptor Max(on-chip) (s1dp0)

Past 7 Days



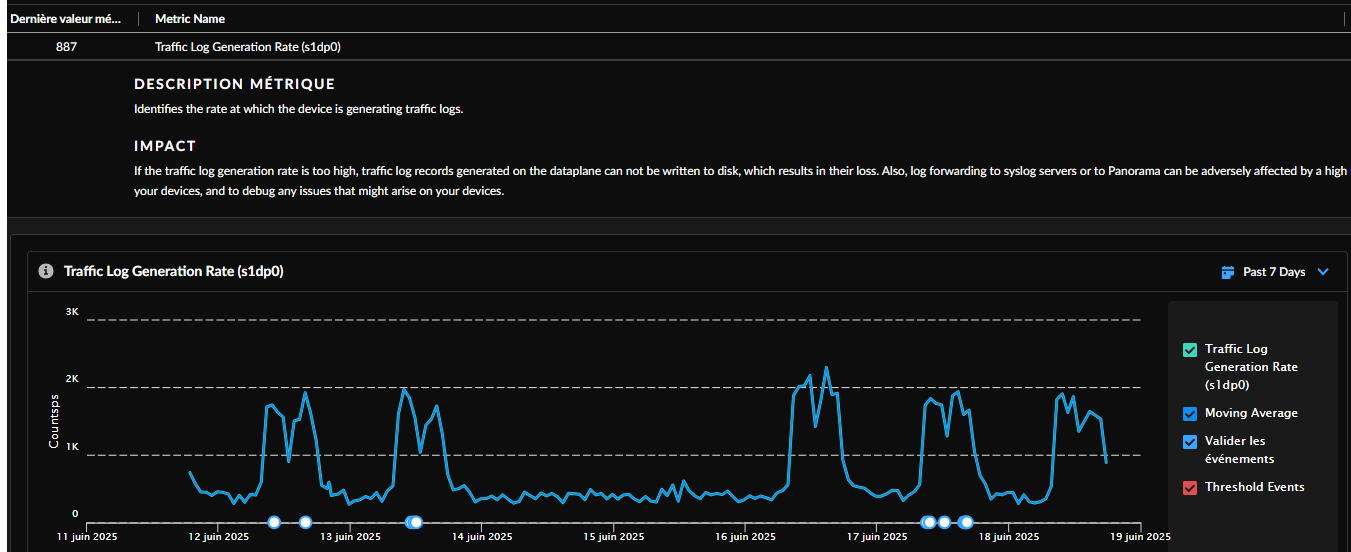
- ☒ Packet Descriptor Max(on-chip) (s1dp0)
- ☒ Valider les événements



- Traffic Log Generation Rate

## Traffic Log Generation Rate (s1dp0) - FW-44NEO-01

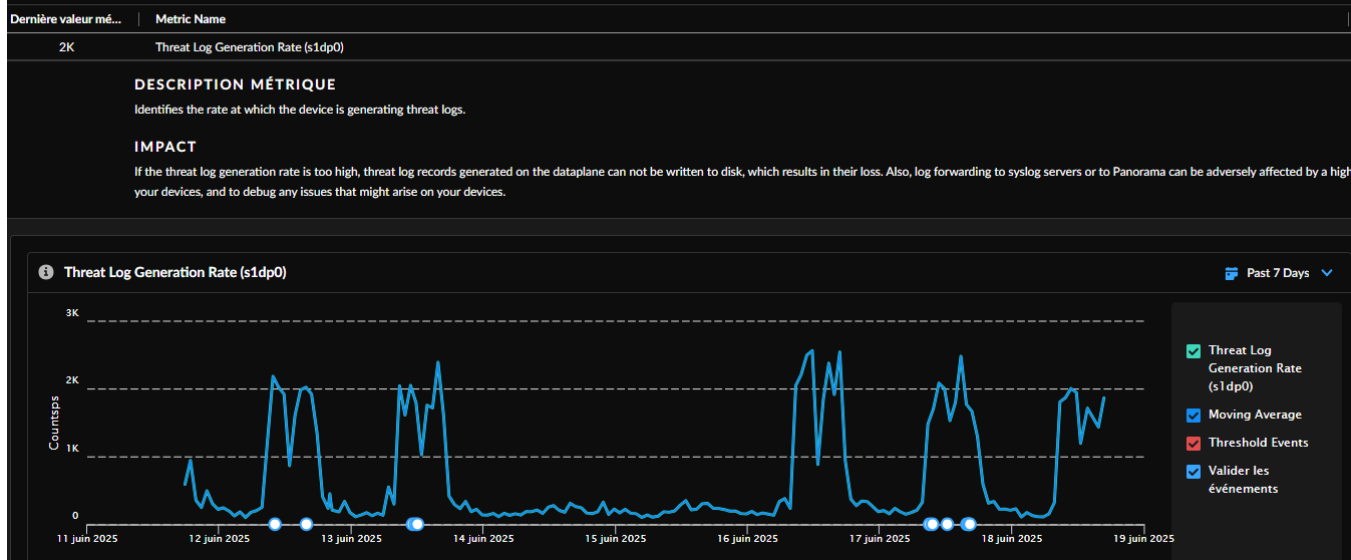
Numéro de série: 016401014372 | Modèle: PA-3260 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.231



- Threat log Generation rate

## Threat Log Generation Rate (s1dp0) - FW-44NEO-01

Numéro de série: 016401014372 | Modèle: PA-3260 | Version du logiciel: 11.1.6-h3 | Adresse IP: 192.168.220.231



### 2.5.3 User-ID Agent

Serveur UserID sur domaine CCIPDLL

- Nombre de contrôleurs de domaine connectés : 28
- Nombre moyen d'utilisateurs identifiés : 5000

Serveur UserID sur domaine FORMATION.LOCAL (CCI56)

- Nombre de contrôleurs de domaine connectés : 4
- Nombre moyen d'utilisateurs identifiés : 40

## 2.6 Caractéristiques techniques de l'architecture

### 2.6.1 Filtrage applicatif

Le filtrage Firewall est, dans la mesure du possible, basé sur des ACL de niveau 7, avec reconnaissance applicative. 70% des règles sont basées sur du niveau 7, sur environ 1100 access-list.

### 2.6.2 Routage

La solution route les flux entre les interfaces physiques ou virtuelles (VLAN) portées par l'équipement. A ce titre, la solution doit aussi permettre de configurer des routes statiques ou dynamiques (BGP, OSPF, RIP) pour créer des configurations de routage spécifiques.

Un routage de type OSPF est en place sur le Firewall central PA-3260 pour récupérer dynamiquement les routes vers les différentes interfaces de service sur les 2 routeurs SDWAN Cisco C8500L-8S4X.

Les Firewalls Internet et interne portent également des règles de routage suivant des sources IP ou des zones précises avec des liens principaux et des liens de secours.

### 2.6.3 Déchiffrement

Le déchiffrement est activé sur le Firewall central en utilisant l'autorité de certification du domaine Active Directory Central.

### 2.6.4 Qualité de service

Une politique de QOS est mise en place pour optimiser/prioriser les flux audio/vidéo TEAMS des utilisateurs CCI.

### 2.6.5 Identification

La solution identifie chaque utilisateur permettant de mettre en place des politiques de sécurité basées sur des groupes d'utilisateurs plutôt que sur des adresses IP.

La solution :

- Se base sur des groupes récurifs (users appartenant à des groupes de groupes).
- Est multi-domaines Active Directory
- Est compatible avec des domaines Microsoft de version minimum Windows 2016.

### 2.6.6 Système de détection des menaces connues

La solution permet les fonctionnalités suivantes :

- Détection et blocage de logiciels malveillants, sur la base d'une analyse par signature (antivirus) directement embarquée.
- Détection et blocage des exploitations de vulnérabilités (injections SQL, XSS, brute force, etc...) - Fonctionnalité IPS. La solution permet également d'intégrer des signatures de menaces personnalisées.
- Détection et blocage de certains types de fichiers (PDF, ZIP, documents office, exécutables, etc...).
- Détection et blocage des requêtes DNS vers des domaines malveillants. La solution permet de forger au niveau du firewall des réponses DNS pour renvoyer les clients vers une destinations choisie (plutôt que vers la destination malveillante).
- Détection et blocages des connexions vers ou depuis des adresses IP de réputation malveillante. La solution intègre nativement une base d'adresses malveillantes mais aussi de récupérer des bases d'adresses chez des fournisseurs tiers.

Il existe des politiques de sécurité différentes, pour les flux Internet (http/https), les flux SMTP et les flux SMB.

### 2.6.7 Filtrage URL

Les Firewalls gèrent le filtrage WEB en utilisant les caractéristiques suivantes :

- Catégories suivant des politiques différentes
- Autorisation, blocage ou avertissement de l'utilisateur en fonction de la catégorie qu'il tente d'accéder.
- Personnalisation des messages End-User avec logo CCI
- Personnalisation de catégories whitelist / blacklist pour chaque niveau d'accès.
- **Utilisation de catégories basées sur un fichier texte accessible à partir d'une URL**

La base d'URL fournie avec la solution ne doit pas se limiter strictement à une seule catégorie par URL car une même URL peut parfois être classée de plusieurs manières (par exemple un même site peut donner de l'information sportive et être également une plateforme de paris en ligne).

### 2.6.8 Rapports et analyse

La solution permet :

- Le Reporting et l'analyse de logs disponibles afin de permettre à un administrateur du firewall de disposer d'un maximum d'informations pour pouvoir résoudre un problème éventuel.
- D'analyser en temps réel ou en différé les flux qui ont transité sur le Firewall.
- De baser les recherches de connexion sur l'utilisateur, l'adresse IP source/destination, l'application, le port
- L'envoi automatisé de rapports d'usage de l'accès Internet.
- **D'analyser les logs sur une plate-forme Cloud sur une durée de 6 mois.**

### 2.6.9 Administration

La solution d'administration est basée sur un serveur Panorama qui permet :

- De s'authentifier sur sa console d'administration avec un login/mdp provenant de l'Active Directory.
- D'utiliser des rôles différents (Administration, Analyse des Logs, Gestion des Rapports).
- D'enregistrer ses propres requêtes de filtrage.
- De partager tous les objets de configuration (politiques, groupe d'hôtes, hôtes, configuration authentification, ...).

### 2.6.10 Failover

La solution intègre une architecture en FailOver Actif / Passif pour les deux niveaux de Firewall.  
En cas de panne d'un équipement, l'ensemble des connexions TCP/UDP et des connexions VPN doivent être reconduites automatiquement.

### 2.6.11 VPN

La solution :

- Permet la connexion VPN de 900 utilisateurs simultanés.
- Est basée sur une authentification Active Directory.
- Permet la connexion automatique de tous les postes nomades
- Est couplée avec la solution de reconnaissance automatique des utilisateurs (SSO)
- Permet la connexion via SSO à l'aide d'un client installé sur le poste utilisateur.
- Fournit un client packagé compatible avec la solution de distribution MECM.
- Utilise le certificat de domaine officiel \*.paysdelaloire.cci.fr

Le portail WEB VPN est désactivé. Seules les connexions via un client Global Protect sur un poste CCI sont autorisées.

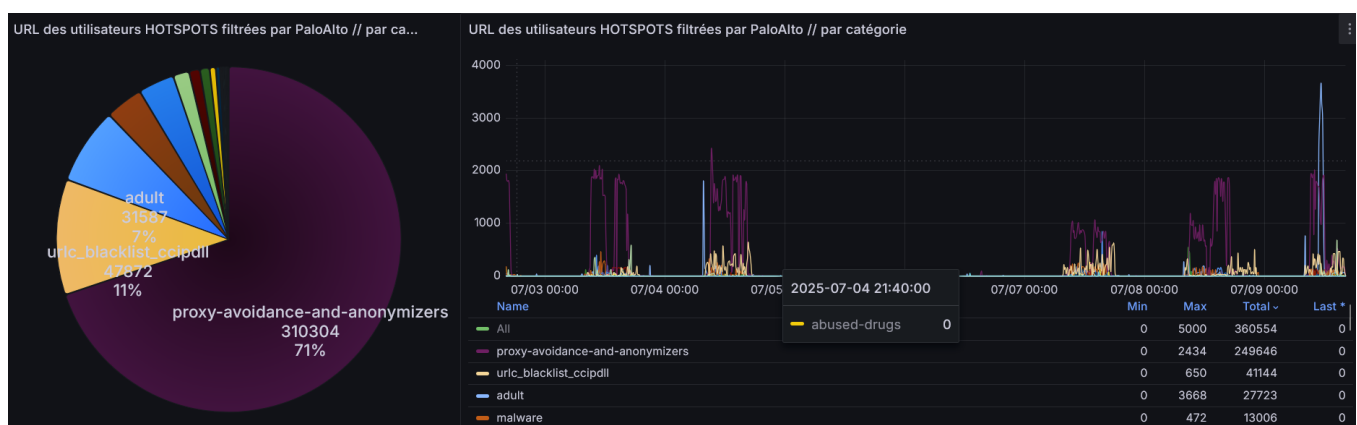
### 2.6.12 Plug-In VCENTER

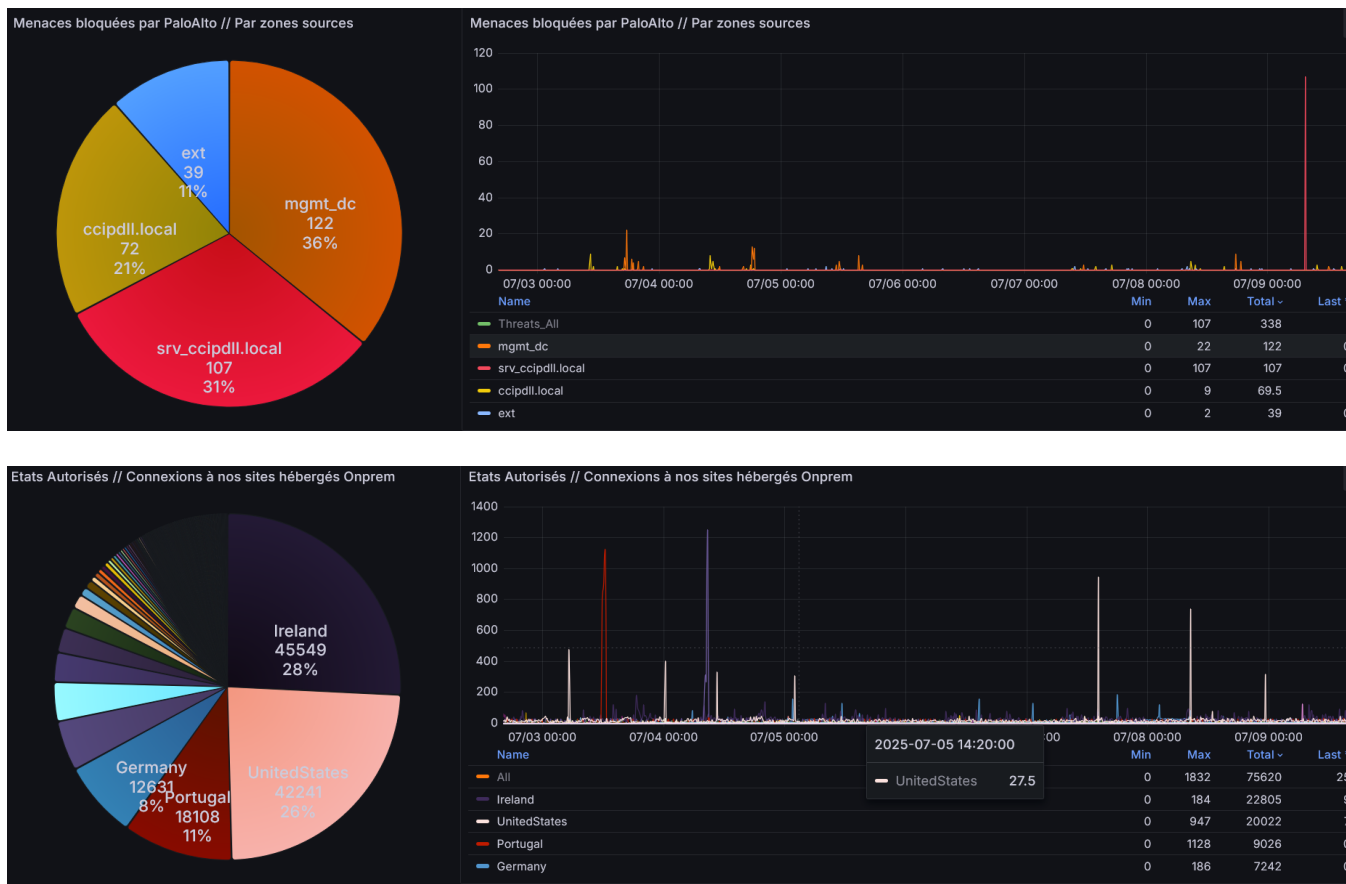
Le Panorama utilise un plug-in vCenter pour recenser dynamiquement les serveurs Linux hébergés sur l'infrastructure VMware et leur affecter une politique de sécurité particulière.

### 2.6.13 Supervision via API

Notre système de supervision utilise des connexions API en lecture seule sur les logs pour :

- Grapher des requêtes sur les logs monitoring
- Contrôler les connexions VPN
- ...





## 2.6.14 Assistance à l'analyse de configuration

Les deux Firewall sont connectés à la plate-forme AIOPS de PaloAlto permettant

- L'analyse de configuration
- L'aide à l'amélioration de la sécurité
- L'analyse des logs sur une durée de 6 mois
- L'état de santé des firewalls
- Différents dashboards permettant de suivre l'évolution de la consommation des ressources (cf métriques)

## 3 Projet de remplacement de l'infrastructure

### 3.1 Déplacement de fonctionnalités

Le remplacement des 2 niveaux de firewalls dans le même projet est une occasion pour optimiser l'architecture au niveau de la capacité des boitiers, de l'amélioration de la sécurité, et au niveau des couts de licences associés.

Les pistes identifiées (à confirmer/compléter par le titulaire) sont :

- Le déplacement du déchiffrement SSL et du filtrage sur le Firewall Internet (périmétrique)
- Le déplacement du VPN sur le Firewall Internet (périmétrique) avec changement de nom DNS  
vpn.paysdelaloire.cci.fr -> vpn.services.cci.fr (certificat fourni par la CCI)

**Le prestataire tiendra compte de ces optimisations pour le choix des boitiers proposés**, en s'assurant que le niveau de ressources des différents Firewalls soit suffisant pour porter les fonctionnalités qui lui seront affectées.

**Les métriques fournis ne tiennent donc pas compte de ces déplacements de fonctionnalités.**

### 3.2 Contraintes techniques de migration

- De par leurs positionnements et leurs rôles, les 2 niveaux de firewalls sont critiques pour l'activité de quelques milliers d'utilisateurs.  
**La migration devra donc être réalisée en HNO (après 18H00, ou durant le week-end).**
- Les services de la DSI modifient quotidiennement les configurations des firewalls pour améliorer le niveau de sécurité et pour permettre la mise en œuvre des autres projets métiers.  
Afin de ne pas retarder tous les projets, **le gel des configurations durant la phase de migration ne devra pas excéder 5 jours ouvrés.**
- **Modification de la configuration du VPN :**
  - Déplacement de la **fonctionnalité sur le Firewall périmétrique (internet).**
  - URL de connexion au VPN qui devra **évoluer en utilisant un autre nom DNS (autre domaine public : le certificat sera fourni par la CCI).**
  - Sécurisation de la connexion VPN par **vérification de certificat sur le poste de travail.**
- Une **validation du routage dynamique OSPF** entre le firewall central et les routeurs SDWAN Cisco devra être validé par le titulaire.

### 3.3 Connectiques de l'infrastructure proposée

Tout le matériel installé dans les baies est obligatoirement équipé d'une double adduction électrique. Les câbles électriques ont un embout de type C14 pour être compatible avec la baie informatique.

Côté réseau, chaque firewall a deux liens Etherchannel de 10Gb ou 25 Gb (suivant le modèle proposé) vers deux switches Cisco (un lien WAN, un lien LAN). Le titulaire proposera tout le matériel nécessaire pour mettre en œuvre sa solution de sorte que les 8 liens physiques soient au 10 ou 25 Gb compatibles Cisco.

La configuration de l'Etherchannel côté switch est à la charge des équipes CCI.

### 3.4 Contraintes de planning de migration

Le planning devra être défini **en tenant compte des dates d'expiration des licences pour éviter tout arrêt de service et toute diminution du niveau de sécurité.**

Le titulaire doit s'engager à pouvoir négocier auprès de l'éditeur Palo Alto la possibilité d'obtenir une période de grâce.

Les dates d'expiration des différentes licences sont indiquées au § 2.1

### 3.5 Contraintes budgétaires

- Le **budget global du projet est de 180 k€ HT maximum**, comprenant la fourniture du matériel, licences et maintenance pour 5 ans, prestation de mise en œuvre.
- Une **segmentation de la facturation sur les 2 années 2025 et 2026** sera toutefois nécessaire :  
Budget 2025 = 60 k€ HT,      Budget 2026 = 120 k€ HT
- De plus, comme indiqué au § 1.2, **la proposition financière est globale dans un premier temps, mais donnera lieu à un découpage de la facturation entre les CCI, selon une clé de répartition qui sera fournie après la notification du marché.**

### 3.6 Prestations

L'ensemble des étapes seront réalisées conjointement avec les équipes DSI internes de la CCIR : la gestion, la configuration et l'installation des équipements en place ont été réalisées entièrement par les équipes internes sans l'aide de prestations extérieures. Elles sont donc maîtrisées de bout en bout.

**Un intervenant technique unique** doit être proposé pour ce projet. Il devra être certifié par le constructeur de la proposition et suffisamment expérimenté (10 ans minimum d'expérience sur la technologie).

### 3.7 Maintenance

**La maintenance doit inclure obligatoirement la réassurance du constructeur. Le titulaire devra être certifié constructeur et avoir un support privilégié vers celui-ci.**

**La maintenance du matériel acquis devra être en GTI 8H 5 jours sur 7**

Le titulaire détaillera précisément le déroulé de la prise en charge, jusqu'au traitement d'un incident majeur dans le cadre de la GTI.

La sauvegarde de la configuration est à la charge de l'équipe informatique de la CCI.

Un responsable de compte servant d'interlocuteur unique pour toute demande ou d'escalade doit être proposé. Le titulaire précisera aussi si une reconnaissance automatique du client par numéro appelant ou appelé est possible.

### 3.8 Reprise de matériel

Dans son chiffrage global, le titulaire pourra proposer une offre de reprise des équipements suivants à l'issu de projet :

- 2 Firewalls PA-3220
- 2 Firewalls PA-3260

Ces reprises devront être notées dans [l'Onglet Reprise](#) du devis estimatif.



### 3.9 Délais de livraison

Les candidats remettront un délai de livraison en adéquation avec les échéances des licences indiquées dans le présent CCTP, soit le 8 décembre 2025.

Il peut être proposé un délai de grâce auprès de l'éditeur actuel PaloAlto.

### 3.10 Marché à bons de commande

Dans le marché à bons de commande, toutes les licences associées au produit devront être proposées dans le tableau, le calcul comparatif des offres se fera équitablement sur des durées d'abonnement comparable (1, 3 ou 5 ans).

Voici la description des équipements demandés :

- Cluster Firewall Central (Antivirus)
- Cluster Firewall Internet (URL Filtering, SSL decryption, VPN, Antivirus, DNS protection).
- Console de supervision centralisée **sous la forme d'appliance virtuelle VMware** (si équipements proposés incompatibles avec la solution en place Paloalto panorama) :
  - Permet une gestion centralisée des règles (filtrage, NAT, QoS, etc...), des objets (adresses, ports, etc...) et des configurations de base (interfaces, routage, services, mises à jour, comptes utilisateurs, etc...) de l'ensemble des firewalls du constructeur.
  - Consolide les logs de plusieurs équipements
  - Créé des rapports d'usage.

*Un détail des licences (par équipements gérés) devra être énuméré dans le document du marché à bons de commande.*

### 3.11 Remise constructeur / éditeur

Une remise sur une solution de protection de type XDR (détection et réponse) devra être proposée dans le DE. Nous ne pouvons pas fournir dans le document un estimatif, car il fait l'objet d'une multitude de budgets différents. Nous pouvons juste vous indiquer le potentiel du parc : **370 serveurs / 2900 postes de travail**, sachant que notre politique est de rationaliser et uniformiser les applicatifs.

Ce chiffrage ne fait pas l'objet d'un engagement de commande, pour autant la qualité de cette remise fera l'objet d'une attention particulière sur la qualité de votre offre.

### 3.12 Evolution technologique

En cas d'évolution technologique, le titulaire devra alerter de l'obsolescence et être en mesure de proposer des matériels similaires ou au moins équivalents dans les mêmes conditions du marché (prix identique, puissance technologique équivalente ou supérieure). Dans ce cas, le titulaire informera, par tout moyen, les achats et la DSI de l'évolution de sa gamme.