



EDIAO

Politique de sécurité

HISTORIQUE DES VERSIONS

Edition	Date	Etat	Rédacteur	Description de l'évolution
A	07/09/2005	Approuvé	Michel DURANTE	Edition initiale
2.0	15/06/2006	Approuvé	Thibaud BENOIST	Mise à jour

APPROBATIONS

Approbateur(s)		
Société	Nom / Fonction	Date/Visa
EDISYS	/ Directeur Général	



Sommaire

CHAPITRE I : LA SECURISATION DES ECHANGES.....	5
1- PUBLICATION DU DCE.....	5
2- RETRAIT DES DCE.....	5
3- PREPARATION DES OFFRES.....	5
4- DEPOT DES OFFRES.....	6
5- RETRAIT DES PLIS.....	7
6- OUVERTURE DES PLIS.....	7
CHAPITRE II : SECURITE DE L'HEBERGEMENT.....	9
1- SECURITE DE LA PLATEFORME WEB.....	9
1.1- Capacité en bande passante.....	9
1.2- Une architecture sécurisée.....	12
1.3- Tolérance de pannes & Répartition de charges.....	13
1.4- Connectivité et emplacement.....	14
2- SECURITE DES INFRASTRUCTURES.....	14
2.1- Sécurité structurelle.....	15
2.2- Sécurité logique.....	16
3- MAINTENANCE DES EQUIPEMENTS.....	17
3.1- Supervision des systèmes et des applications : Sitescope.....	17
3.2- Surveillance.....	17
3.3- Sécurité.....	17
3.4- Disponibilité – Load balancing.....	18
3.5- Sauvegarde.....	18

Avant propos

La sécurisation des échanges dans le cadre de la dématérialisation des marchés publics est avant tout liée à la décomposition des processus lié à la passation des marchés publics. Afin d'installer la confiance entre les différents intervenants (collectivité et entreprises) il est nécessaire d'établir le maximum de transparence et d'interopérabilité dans la chaîne de sécurisation des échanges.

EDISYS a conçu une sécurisation des échanges en 4 points :

- **Hébergement professionnel** de ses applications en partenariat avec INTERNET FR
- **Signature électronique** des documents à base de la signature XML incorporée dans les outils EDI-AAPC, EDI-TENDER et EDI-CAO
- **Interface des gestions des droits** permettant de gérer les habilitations des personnels de la collectivité dans la gestion des appels d'offres
- **Coffre fort de séquestre et d'archivage** des soumissions des entreprises

Chapitre I : LA SECURISATION DES ECHANGES

1- PUBLICATION DU DCE

La publication d'un DCE n'est possible que quand l'annonce correspondante existe sur notre serveur et que l'ensemble des fichiers constitutifs du DCE est signé numériquement avec un certificat valide.

Il est également possible d'importer des signatures (format PKSC7) au cas où des fichiers seraient signés par des personnes extérieures aux services de la collectivité (Architecte, Maître d'œuvre ...)

L'outil permet la vérification des signatures, la vérification des certificats et la co-signature.

Avant l'envoi le fichier DCE.xml est signé par la personne qui va mettre en ligne le DCE et qui doit se connecter au serveur EDI-AO avec un certificat ayant les droits de diffusion.

Lors de la validation du fichier sur le site Internet sont

Le DCE validé fait l'objet d'une signature XML à l'aide du certificat de la personne émettrice et sera conservé en local, puis transmis à notre serveur par une connexion sécurisée (SSL). La validation sur notre serveur entraîne l'intégration des clés publiques qui vont servir au cryptage des 1ères et 2èmes enveloppes et qui auront été définies par l'administrateur dans l'interface de gestion des droits, la création d'un jeton d'horodatage par un tiers horodateur et la contre signature XML complète du fichier horodaté par notre certificat serveur permettant d'avoir une date certaine de mise en ligne.

Les fichiers constitutifs du DCE sont téléchargés automatiquement par notre serveur sur le poste client via une connexion sécurisée.

2- RETRAIT DES DCE

Les entreprises désirant retirer un DCE électronique doivent fournir des renseignements obligatoires et fournir une adresse email valide.

Le téléchargement ne s'effectue pas directement sur le site mais via un mail permettant de valider l'adresse email et faisant office d'accusé de réception.

Le DCE disponible au téléchargement est créé spécifiquement pour le candidat ce qui permet d'éviter de récupérer des lots inutiles, de personnaliser l'interface de téléchargement par candidat, de garantir l'intégrité du téléchargement par candidat et de tracer les différents événements.

Un fichier AO.XML est transmis aux candidats intégrant l'intégralité de l'AAPC, l'intégralité du contenu du DCE et des signatures des fichiers ainsi que les clés publiques nécessaires au cryptage des enveloppes.

La connexion au serveur pendant le téléchargement est sécurisée par le certificat serveur du site mais ne nécessite pas de certificat électronique de la part du candidat.

3- PREPARATION DES OFFRES

Le logiciel EDI-TENDER est téléchargeable gratuitement sur le site Internet et permet d'accompagner les candidats dans la préparation de leurs offres.

Il permet notamment :

- la vérification que le DCE est transmis par EDISYS et qu'il est intègre ;
- la vérification que les fichiers informatiques livrés par la collectivité sont intègres ;
- la signature électronique au format XMLDsig des fichiers constituant les enveloppes ;
- la contre signature des fichiers du DCE qui ne sont pas à joindre dans les enveloppes ;
- la vérification des certificats de la personne publique et éventuellement des cotraitants ;
- le cryptage des enveloppes avec les clés publiques livrées par la personne publique.

L'outil permet également l'import et l'export des signatures au format PKCS7 ce qui permet en cas de co-traitance d'échanger les signatures des fichiers par mail.

Une horloge basée sur le serveur de temps de référence de la plateforme Internet permet aux candidats de se caler précisément sur les horaires limite de dépôt des offres.

Les enveloppes sont cryptées avec les clés publiques de la collectivité garantissant la plus parfaite confidentialité par rapport au serveur Internet d'EDISYS. Lors de la génération de l'enveloppe une vérification de toutes les signatures est effectuée évitant que des fichiers possédant des signatures non valides soient transmis lors de la remise des plis.

4- DEPOT DES OFFRES

Une fois les enveloppes créées et cryptées il est nécessaire de se munir d'un certificat valide pour déposer les plis sur notre plateforme Internet.

Des fichiers de trace sont créés sur le poste client enregistrant l'ensemble de la structure de l'offre, les coordonnées de l'entreprise et de la personne déposante, l'ensemble des signatures des fichiers informatiques constituant l'offre, l'ensemble des contre signatures des documents du DCE original non présents dans les 2 enveloppes (RC, CCAP, CCTP, PLANS... tel que défini par la collectivité lors de la mise en ligne du DCE : notion d'enveloppe 0)

Ces fichiers sont signés sur le poste client avec le certificat du déposant et transmis par connexion sécurisée sur notre site qui procède à l'analyse des certificats ayant servi au dépôt et à la signature des fichiers. Il analyse la validité du certificat (dates), la nature de l'autorité de certification (AC) et la non présence sur les listes de révocation du numéro de certificat.

Si la date de validité du certificat est dépassée, l'autorité de certification non validée ou le certificat révoqué, l'interface de validation de dépôt avertit le soumissionnaire.

Celui-ci peut néanmoins poursuivre de dépôt de ses plis mais sans garantie de validité de son offre par la commission d'appels d'offres.

Une fois la validation effective le serveur demande un jeton d'horodatage pour le début du dépôt et l'enregistre dans le fichier SOUM.XML. Il passe ensuite au téléchargement des 2 enveloppes en enregistrant les heures de début et de fin de dépôt. L'ensemble des traces est enregistrée dans le fichier SOUM.XML et à la fin du dépôt de la 2^{ème} enveloppe un 2^{ème} jeton d'horodatage est inséré ainsi que la contre signature du certificat serveur.

Un accusé de réception décrivant l'ensemble des plis transmis, les éventuelles non-conformités concernant les certificats, les données d'horodatage et le n° unique de déposant est affiché sur le poste client et un mail d'accusé de réception est envoyé simultanément aux adresses email spécifiées.

Les données d'horodatage et le n° unique de déposant sont enregistrés sur le fichier SOUM.XML du poste local permettant ainsi la gestion des modifications de dépôt.

Le serveur de dépôt des offres permet aux candidats de modifier leur offres jusqu'à la date limite de remise des plis ainsi que l'annulation de leur offre grâce à l'identifiant unique des déposants. Afin de garder une traçabilité de l'ensemble des dépôts le serveur gère les versions des dépôts et conserve l'ensemble des fichiers transmis.

De même le serveur gère la procédure de double envoi permettant de transmettre l'enveloppe de signature séparément de l'enveloppe de candidature et des offres.

5- RETRAIT DES PLIS

Pour pouvoir retirer les plis des candidats il est nécessaire de prononcer la clôture des dépôts dans l'interface de gestion des droits du site Internet. Le profil associé à la clôture du dépôt est généralement celui de la PRM mais peut être celui du secrétaire de la CAO et une fois la clôture des dépôts prononcée aucun candidat ne pourra plus remettre une offre.

Un fichier trace ENV.XML est créé reprenant l'ensemble des dépôts effectués par les candidats et servant à générer automatiquement le registre des dépôts. Ce fichier est signé et horodaté par le certificat serveur en incluant le certificat de la personne ayant effectué le retrait des plis ce qui garantit l'intégrité des données permettant d'effectuer la séance d'ouverture des plis.

EDISYS propose en option le sur-cryptage des enveloppes des soumissionnaires avec la clé publique du logiciel EDI-CAO garantissant l'ouverture des plis à l'aide de ce logiciel et suivant les contraintes imposées en Séance d'Ouverture des Plis par le code des Marchés Publics.

Le téléchargement sécurisé s'effectue Offre par Offre sur le poste de la personne ayant effectué les retraits et un mail d'accusé de réception est envoyé automatiquement à la PRM ainsi qu'au président de la CAO les avertissant de la clôture des dépôts et du retrait des offres.

A l'aide du logiciel EDI-CAO la personne ayant retiré les plis peut effectuer la création du registre des dépôts en décryptant avec la clé logicielle le fichier trace ENV.XML et les enveloppes SOUM.XML de chaque candidat. Il peut ainsi vérifier la validité des certificats ayant servis au dépôt des offres et à la signature des fichiers constitutifs des enveloppes.

Il peut ajouter les offres papiers mais ne peut en aucun cas accéder aux enveloppes intérieures qui nécessitent la clé privée du président de la CAO ou de la PRM.

6- OUVERTURE DES PLIS

Le logiciel EDI-CAO permet de garantir un déroulement phasé de la séance d'ouverture des plis puisque chaque action doit être terminée et validée avant de passer à la suivante. Suivant les contraintes inhérentes à chaque collectivité locale il est possible de le paramétrer en fonction des typologies de procédures ou des besoins propres à chaque administration.

L'ouverture des plis ne peut se faire que lorsque le registre des dépôts est validé par le président de la CAO ou la PRM et les offres parvenues hors délais rejetées. Celle-ci sont alors cryptées (ou détruites suivant l'option retenue par la collectivité) avec une clé logicielle spécifique (EDISYS conserve la clé privée correspondante) empêchant toute ouverture ultérieure de ces plis.

Le registre des dépôts est horodaté et contre signé par la clé logicielle EDI-CAO garantissant ainsi son intégrité.

Une fois le registre des dépôts validé le président de la CAO peut passer à l'ouverture des candidatures. Il doit se munir de son certificat pour décrypter le contenu de la 1^{ère} enveloppe des candidats. Le logiciel vérifie l'intégrité des signatures apposées sur les documents et affiche les certificats correspondants. La signature logicielle EDI-CAO est appliquée systématiquement à chaque fichier joint permettant de garantir la non manipulation ultérieure de fichier.

L'ouverture des 1^{ères} enveloppes s'effectue dans l'ordre d'arrivée des plis et on ne peut pas ouvrir le pli suivant tant que l'on n'a pas statué sur le pli en cours car le décryptage logiciel empêche l'ouverture du pli suivant (sauf en cas de procédures restreintes ou toutes les enveloppes peuvent être ouvertes afin de sélectionner les entreprises retenues). Si la candidature est rejetée la 2^{ème} enveloppe est cryptée avec la clé logicielle spécifique empêchant toute ouverture ultérieure de l'offre.

Une fois le procès verbal d'ouverture des 1^{ères} enveloppes rédigé, celui-ci est horodaté et contre signé par la clé logicielle EDI-CAO garantissant ainsi son intégrité.

L'ouverture des 2^{èmes} enveloppes est globale afin de pouvoir comparer les offres. . Le logiciel vérifie l'intégrité des signatures apposées sur les documents et affiche les certificats correspondants. La signature logicielle EDI-CAO est appliquée systématiquement à chaque fichier joint permettant de garantir la non manipulation ultérieure de fichier.

Une fois le procès verbal d'ouverture des 2^{èmes} enveloppes rédigé, celui-ci est horodaté et contre signé par la clé logicielle EDI-CAO garantissant ainsi son intégrité.

L'ensemble des traces relatives à la séance d'ouverture des plis peut être déposés sur notre site à des fins de conservation

Chapitre II : SECURITE DE L'HEBERGEMENT

1- SECURITE DE LA PLATEFORME WEB

Depuis 1999 EDISYS a confié l'hébergement de ses plates-formes Internet à la société Internet-Fr. Véritable expert dans ce domaine, Internet-Fr propose des services d'hébergement d'applications complexes, des structures d'hébergement dédié et des formules d'hébergement mutualisé.

Depuis 1999, Internet-Fr s'est notamment engagé dans une démarche de qualité qui l'a conduit à obtenir la norme ISO 9001 en 2000, preuve de la mise en œuvre d'une organisation interne rigoureuse au service de ses clients.

En outre, depuis 2000, Internet-Fr a développé des solutions d'hébergement résolument haut de gamme pour l'hébergement d'applications critiques. Pour cela Internet-Fr s'appuie sur des investissements importants, sur des technologies de pointe (commutateurs Foundry server Iron, serveurs NAS NetApp) et des équipes d'experts techniques.

Avec plus de 15 000 sites Web hébergés toutes plates-formes confondues, Internet-Fr figure parmi les leaders français avec plus de 10% du marché de l'hébergement professionnel français.

Internet FR est présent en Italie au travers de sa filiale Level IP et prévoit de s'implanter en Espagne courant 2003.

1.1- Capacité en bande passante

Depuis 1995, Internet-Fr construit et administre un réseau indépendant et dynamique. D'une gestion fine et rationnelle de la topologie de son infrastructure IP résulte une capacité à fournir à ses clients les garanties de disponibilité indispensables au développement d'une activité en ligne pérenne.

Les data centers d'Internet-Fr sont connectés au réseau mondial Internet par fibre optique à haute capacité, par 3 grands opérateurs de niveau 1 :

- France Telecom;
- Colt Telecom;
- Nets-Tiscali.

En complément, Internet-Fr achète du transit IP à d'autres opérateurs (OpenTransit, Colt, Tiscali).

Le data center principal de Massy est interconnecté au data center de la filiale italienne Level IP par une dorsale Londres-Paris-Milan en double STM1, ce qui permet d'acheminer d'importants flux d'informations en des temps minimaux et de bâtir de vraies architectures d'hébergement distribuées.

1.1.1- Indépendance et réseau multi-opérateurs

La présence d'Internet-Fr sur les nœuds de peering français de première importance, avec un total de plus de 200 peerings internationaux, renforce la capacité de ses data centers à délivrer l'information à la demande, et quelle qu'en soit la destination.

Les sites et les applications des clients hébergés sont ainsi visibles de manière privilégiée depuis n'importe quel point d'Europe ou du Globe.

1.1.2- La redondance au service de la disponibilité

En choisissant l'indépendance vis-à-vis des opérateurs, Internet-Fr est à même de bâtir et de proposer un réseau IP ayant une tolérance élevée aux éventuelles pannes.

En cas d'altération des performances ou de rupture d'un lien IP, le trafic est automatiquement basculé sur un lien sain par le protocole BGP, de manière totalement transparente pour l'utilisateur final.

Enfin, tous les équipements localisés en tête de data center sont redondants, mettant les clients hébergés à l'abri des pannes matérielles.

1.1.3- Une capacité en bande passante modulaire

La plateforme EDIAO bénéficie d'une capacité modulaire en bande passante allouée par Internet-FR.

Cette souplesse est un véritable avantage pour les clients consommant une bande passante importante de manière ponctuelle ou permanente.

1.1.4- Disponibilités du réseau

Le temps de disponibilité de l'accès au réseau Internet par la plate forme client est garanti à :

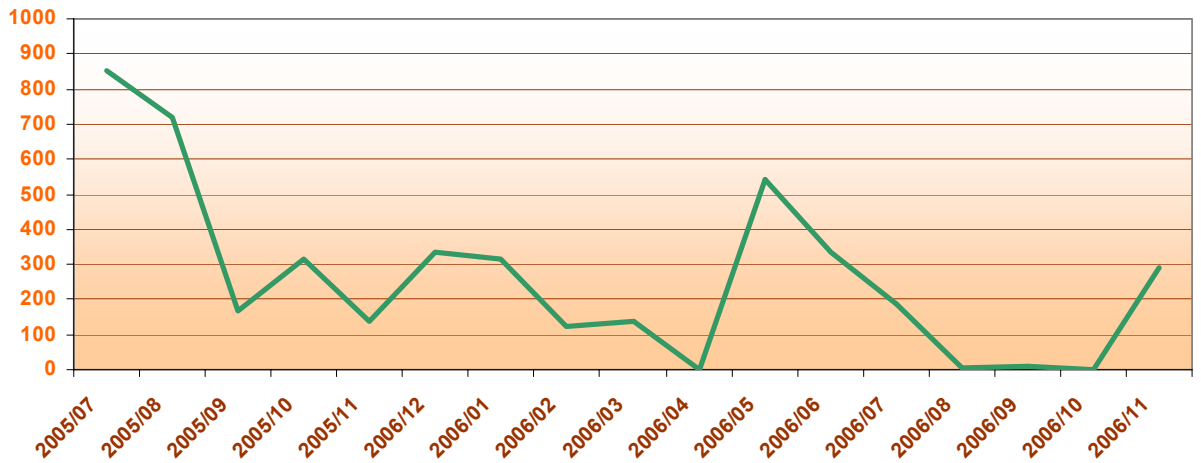
Taux de disponibilité mensuel	Temps d'interruption annuel en équivalent horaire	Pénalités (en % des frais mensuels de bande passante)
99,95% > TD ≥ 99,8%	Entre 22 et 88 minutes	10%
99,8% > TD ≥ 99,7%	Entre 88 et 132 minutes	20%
TD < 99,7%	Au-delà de 132 minutes	30%

1.1.5- Monitoring de l'activité

Les moyens internes sont mis en œuvre au niveau de l'hébergement des serveurs et permettent de mesurer l'accessibilité des différents serveurs.

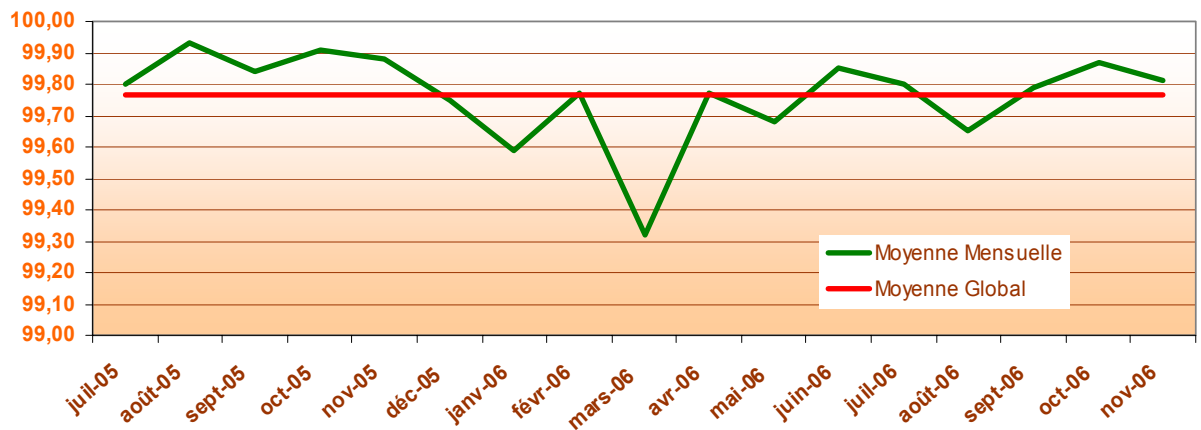
Le système est basé sur l'interrogation régulière et permanente d'un page du site edi-tender.com. Cette page effectue des opérations blanches sur des données afin d'être au plus près des conditions réelles d'utilisation. L'intervalle entre 2 mesures se situe en moyenne à 600 milli seconde. On trouvera ci-dessous un graphique représentant les temps moyens d'accès au site données par ces mesures.

Temps Moyen d'accès au site EDI-TENDER.COM en milliseconde

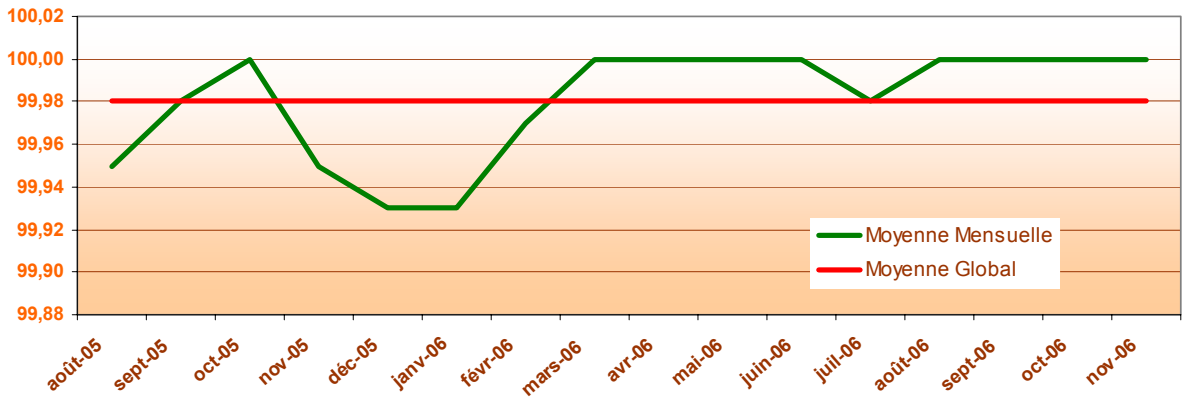


Les incidents ou tentatives non aboutis sont enregistrés et transmis pour exploitation à la direction informatique d'EDISYS. Ces alertes datées permettent d'établir des graphiques temps réels de disponibilité des différents serveurs. Ci-dessous 2 graphiques affichant la disponibilité du site des editender.com ainsi que du serveur de base de données.

Taux de disponibilité EDI-TENDER.COM



Taux de disponibilité Base de Donnée EDI-TENDER.COM



Nous effectuons également des mesures de la bande passante utilisée. Cette surveillance permanente est effectuée directement sur notre Pare-feu et produit des alertes en cas de dépassement des seuils fixés.

Vous trouverez ci-dessous les mesures d'utilisation de la bande passante sur un an.

En rouge le bande passante utilisée par les téléchargements effectués depuis le site et en bleu la bande passante utilisé par les dépôts effectués sur le site.

1.2- Une architecture sécurisée

L'architecture est protégée en entrée de réseau par un firewall de la gamme Cisco.

Le serveur web est directement relie au serveur de bases de données qui a pour fonction de stocker les datas et de faciliter les échanges de fichiers en cas de basculement du service vers le serveur web de secours.

Le matériel fourni est neuf et fait l'objet d'une garantie. Au titre de cette garantie, Internet-Fr s'engage à intervenir sous 2 heures suite à une alerte et à réparer le matériel incriminé dans les meilleurs délais.

La réparation peut soit conduire aux changements de certaines pièces (disque dur, alimentation, carte réseau...) soit à la mise à disposition d'une machine de remplacement de niveau équivalent ou supérieur.

- Equipements mutualisés Internet-Fr

	Désignation	Caractéristiques du matériel	Versions OS / logiciels
Système de sauvegarde	Bibliothèque LTO	LTO Dell Powervault 136T	VERITAS DataCenter Net Backup 3.4
Répartition de charge	Foundry ServerIron	24x10/100 Mb/s et 2x1Gb/s	Propriétaire Foundry

- Equipements dédiés à plate forme Edisys :
 - Equipements de sécurité et d'interconnexion :

	Désignation	Caractéristiques du matériel	Versions OS / logiciels
Firewall de tête de réseau web	Cisco Pix 506 E	32 Mo de RAM Processeur 433 MHz 2 interfaces 10/100 Mb/s VPN (25 simul)	IOS version : 6.3.3
Switch	1 Cisco Catalyst 2950	Processeur Risc 32 Bits 8 Mo mémoire Flash 12 ports	IOS version : 6.3.3

- Equipements de type serveur :

	Désignation	Caractéristiques du matériel	Versions des OS
Serveurs web	2 Serveurs DELL PE 1750	Xeon 2,4 Ghz/512 Ko cache L2 1 Go de Ram, 2X36 Go SCSI 10 Ktpm sur double carte réseau 10/100 bicanal, alim redondantes, Rack 1U	Windows 2000 ASP
Serveur BDD	Serveur DELL PE 2650	Xeon 2,4 Ghz/512 Ko cache L2, 1 Go de Ram, 4X73 Go SCSI 10 Ktpm sur double carte réseau 10/100 bicanal, alim redondantes, Rack 2U	Windows 2000 SQL server 2000

1.3- Tolérance de pannes & Répartition de charges

Internet-Fr dispose d'une réelle expertise dans le domaine de la répartition de charge. Internet-Fr a choisi les load balancer Foundry ServerIron car ils permettent de :

- faire du load balancing en mode transparent : pas de connexion physique directe nécessaire ce qui permet de faciliter la redondance des matériels ;
- capacité à faire du load balancing de niveau 7 (tests sur la réponse des applications) ;
- capacité de faire du fail over entre plusieurs load balancer et éventuellement de faire du global load balancing entre des sites distants.

Afin de mettre en place une bonne politique de load balancing un certain nombre de paramétrages devront être faits et en particulier :

- création de pages spécifiques à superviser pour savoir si la machine peut recevoir une nouvelle session ;
- mise en place d'un cookie applicatif afin de maintenir chaque session sur le serveur initial.

En effet, en cas de perturbation ou de panne du serveur Web 1 , le serveur restant peut continuer à fournir le service en attendant la remise en place rapide du serveur défaillant.

1.4- Connectivité et emplacement

Les serveurs sont installés dans le data center de Massy au sein d'une baie, fermée à clé, ventilée et ondulée, de 800X600.

Les serveurs disposent d'une double alimentation électrique et de deux prises RJ45 (une pour le réseau primaire et une pour le réseau data).

La plate forme bénéficie d'une bande passante dédiée de 512 kb/s avec un burst de 100%.

La bande passante utilisée par un serveur est mesurée sur le firewall se trouvant entre ce serveur et les commutateurs de tête, et immédiatement après ce serveur (généralement un switch).

Nous utilisons pour ce faire des fonctions intégrées de l'IOS Cisco. Les valeurs mesurées sont ensuite récupérées par protocole SNMP, puis stockées dans une base de données.

2- SECURITE DES INFRASTRUCTURES

Implantés au cœur d'un réseau IP paneuropéen en constante évolution et directement connectés aux plus grands backbones IP mondiaux, les centres serveur d'Internet-Fr sont construits selon un cahier des charges précis et extrêmement rigoureux.

Dotés de dispositifs de contrôle et de régulation redondants, ces centres serveurs constituent un environnement hautement sécurisé idéal pour l'hébergement d'applications web à mission critique dont le fonctionnement requiert un niveau de QoS élevé. L'interconnexion de nos Data Centers par fibre optique SDH permet le déploiement de solutions globales de «Crash & Disaster Recovery».

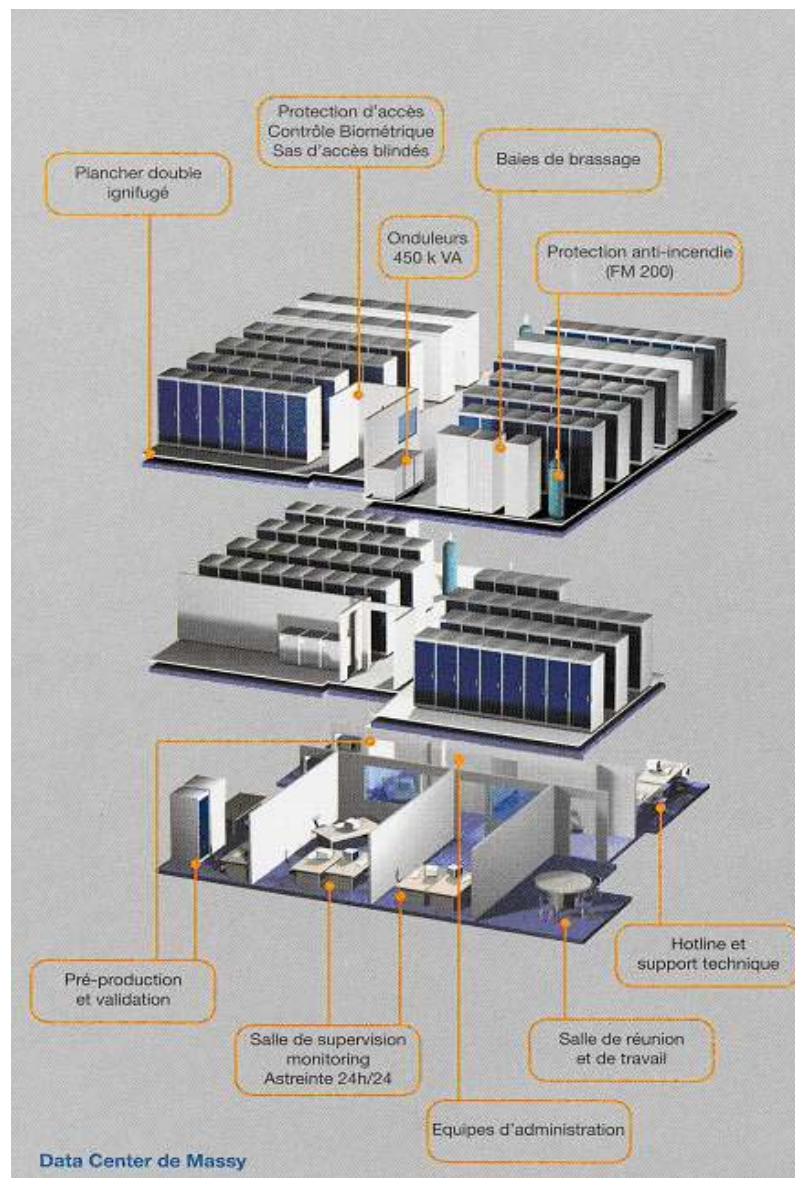


Figure 1 – Sécurité des infrastructures d'hébergement

2.1- Sécurité structurelle

2.1.1- Sécurité anti-incendie

- Multiples niveaux de portes coupe-feu.
- Système d'extinction d'incendie ultra-rapide par gaz FM200.
- Notification aux sapeurs-pompiers automatique.

2.1.2- Sécurité électrique

- Alimentation électrique générale redondante.
- Groupement d'onduleurs d'une capacité individuelle de 275 kVA.
- Groupe électrogène d'une capacité de 450 kVA et d'une autonomie de 9 jours minimum.

2.1.3- Sécurité des infrastructures

- Accès soumis à un contrôle d'identité rigoureux. Sas d'accès et contrôle biométrique.
- Surveillance par vidéosurveillance.
- Surveillance par une société tierce de télésurveillance et intervention immédiate.
- Contrôle environnemental.
- Contrôle permanent et régulation automatisée de l'hygrométrie.
- Contrôle actif et régulation automatisée de la température.

2.2- Sécurité logique

2.2.1- Topologie réseau

Le réseau dédié à l'hébergement des plates-formes clientes est un réseau « ouvert ».

Par défaut, les serveurs communiquent à l'aide de protocoles sans restriction depuis l'Internet. Par défaut les serveurs sont configurés en IP publiques donc consultables depuis l'extérieur sur les principaux ports (port 80 pour http, port 25 pour smtp, port 21 pour FTP...).

L'une des premières solutions employée par Internet-Fr pour déjouer les premières attaques industrielles fut d'appliquer des filtres (Access Cisco List) directement sur les routeurs.

2.2.2- Protections logiques

Plan d'adressage privé : Procédé consistant à translater une IP privée (IP physique du serveur) en une IP publique destinée à communiquer avec l'extérieur du réseau.

Ce mécanisme appelé NAT (Network Address Translation), évite que l'on puisse remonter à l'équipement par son adresse.

Filtrage : Limitation des flux de données des ressources d'un système uniquement vers les personnes, programmes, processus autorisés ou vers d'autres systèmes du réseau.

Appliquer des listes de contrôle d'accès (A.C.L.) directement sur les routeurs, ou sur les commutateurs permet de prévenir les attaques industrielles classiques (IP Spoofing, SMURF, Spamming, rooling...).

Dispositif matériel de firewall : Ces équipements autonomes sont spécialisés dans le filtrage d'adresse, la translation des services et des ports P.A.T. (Port Adress Translation). Les équipements pare-feu Cisco choisis par Internet-Fr, sont dotés de fonctions d'authentification et de cryptage V.P.N. (Virtual Private Network). Ils utilisent leur propre système d'exploitation sécurisé afin de se rendre plus stables et moins vulnérables aux attaques.

Sonde d'intrusion : Surveillance et analyse des flux de paquets de données du réseau à la recherche de toute activité non autorisée. En cas de comportement suspect remonté par la sonde, le système enregistre les traces, avertit l'administrateur et peut ordonner automatiquement à d'autres équipements d'intervenir en stoppant les sessions non autorisées.

Audit de failles de sécurité : technique préventive d'exploration du réseau et des systèmes d'information. La recherche de vulnérabilité permet de mesurer la sécurité, et de remédier aux éventuelles faiblesses.

Ce procédé collecte l'information, la compare avec une liste de faiblesses répertoriées entre autres en fonctions des systèmes d'exploitation, des services activés et lance une série d'attaques pertinentes compatibles avec les éléments détectés. Il classe et répertorie les failles et présente la méthode corrective.

Ce procédé permet de valider la continuité de la politique de sécurité.

3- MAINTENANCE DES EQUIPEMENTS

La maintenance inclut la supervision, l'administration système et applicative quotidienne, et le support technique de la plate-forme.

3.1- Supervision des systèmes et des applications : Sitescope

SiteScope surveille le statut et l'exécution des composants critiques des serveurs hébergés.

Principales fonctionnalités :

- Surveiller la disponibilité d'une URL en HTTP ou HTTPS et tester le fonctionnement approprié des séquences.
- Vérifier la disponibilité des connexions critiques.
- Surveiller le niveau disponible d'espace disque et d'utilisation CPU, RAM.
- Exécuter automatiquement des procédures correctives (scripts).
- Informer automatiquement par email, pager et téléphone lorsqu'un processus est en état critique ou hors service.
- Produire des états de gestion sur la disponibilité.

3.2- Surveillance

Internet-Fr assure une surveillance de l'ensemble des matériels de la plate-forme client. Ceci inclut les matériels appartenant à Internet Fr utilisés dans l'infrastructure du client.

Liste des processus à surveiller :

Matériel	Processus	Test	Fréquence	Alerte	Notification
Frontal 1	Disque dur	Espace	3 s	Si espace libre < 2 Go après 3 tests	Email + pager IFR + astreinte + client
SGBD 1	CPU	Taux d'utilisation	3 s	Si taux d'utilisation >90 % sur 3 tests consécutifs	Email + pager IFR + astreinte + client
www.edi-tender.com	Validation fonctionnement de l'application	Match content	3 s	Si la page testée ne retourne pas le contenu prévu 3 fois de suite	Email + pager IFR + astreinte + client

3.3- Sécurité

Internet-Fr administre les équipements de sécurité de l'infrastructure client. Cette administration couvre différents domaines :

- Suivi des équipements de sécurité : Internet-Fr s'engage à mettre à jour l'OS des équipements dans un délai maximum de 2 jours ouvrés.
- Tests de failles de sécurité : Internet-Fr procède régulièrement à des tests de faille de sécurité dont il communique les résultats au client. Internet-Fr propose des plans d'actions afin de corriger ces failles.
- Sonde d'intrusion : Internet-Fr met en place une sonde d'intrusion afin d'analyser les attaques et remonter des alertes en temps réel.

- Reporting : Internet-Fr produit un reporting mensuel de sécurité reprenant les diverses informations ci-dessus. Ce reporting est inclus dans le dossier mensuel d'exploitation.

3.4- Disponibilité – Load balancing

Internet-Fr administre les équipements de disponibilité de l'infrastructure client. Cette administration couvre différents domaines.

Suivi des équipements de disponibilité : Internet-Fr s'engage à mettre à jour les équipements dans un délai maximum de 2 jours ouvrés.

3.5- Sauvegarde

Internet-Fr assure la sauvegarde de la plate forme du client. Les données qui doivent être sauvegardées ainsi que la police de sauvegarde sont détaillées dans le dossier d'installation et d'exploitation.

Internet-Fr utilise Veritas global data manager pour la sauvegarde des plates-formes clients.

La librairie de sauvegarde est surveillée continuellement. De même, Internet-Fr analyse quotidiennement les journaux de logs afin de vérifier que les sauvegardes ont été correctement effectuées.