Table des matières

Présentation du contexte

Le port de Cherbourg est un port en eau profonde (13 mètres minimum d'eau). Bien protégé des vents, il possède la plus grande rade artificielle du monde. Il est accessible à toute heure, tous les jours de l'année, avec un passage direct sans écluse aux différents quais commerciaux.

Ses activités sont diverses :

- accueil de ferries (pour les liaisons transmanche),
- déchargement de fret (de marchandises),
- croisières
- réparation navale.

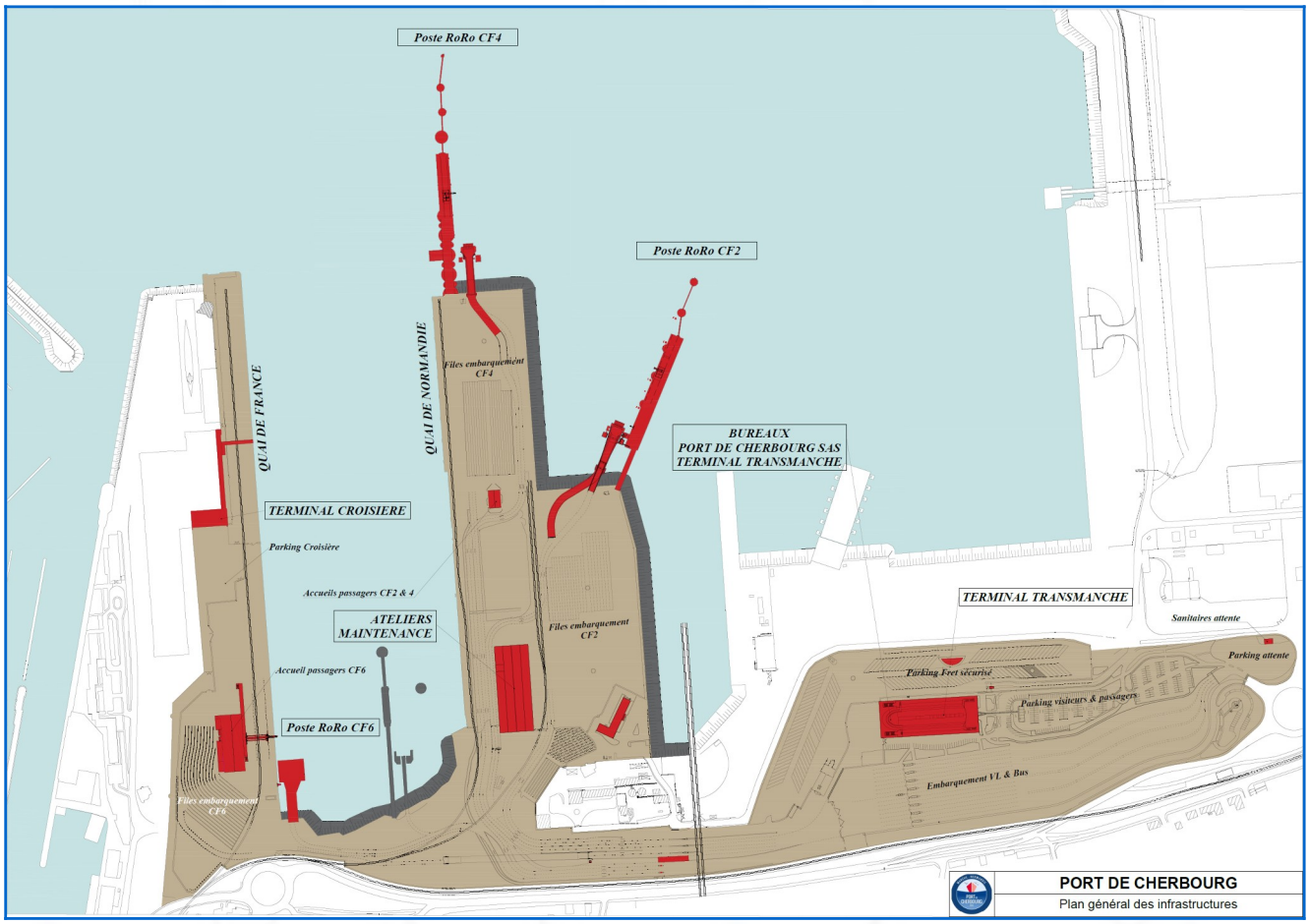
De par sa situation géographique et sa culture largement tournée vers le maritime, Cherbourg joue un rôle essentiel sur les marchés de la construction et de la réparation navale.

Ce secteur d'activité représente en effet environ 3 500 emplois dans la communauté urbaine.

Monsieur DUNARD est le gestionnaire du port de Cherbourg au travers d'une société d'économie mixte locale.

Le système d'information est sous la responsabilité de son DSI (Directeur des Systèmes d'Information), M. Richard. Il est chargé, entre autres, avec l'aide de ses assistants, de la maintenance des solutions techniques d'accès (postes de travail, tablettes, smartphones), des serveurs et du réseau local.

Plan du port de Cherbourg



Note : une version plus lisible est disponible en page 17 (Annexe : Plan de situation du port)

Système informatique du port

Réseau

Le réseau du port de Cherbourg comporte relie l'ensemble des espaces commerciaux entre eux (terminal de croisière, terminal transmanche, zone de frêt) ainsi que les espaces des fonctions de support de l'activité (Ateliers de maintenance, bureaux). Il est qualifié de réseau d'infrastructure. Ce réseau est utilisé dans trois cas :

- afin de permettre l'accès des espaces commerciaux aux réseaux externes (internet notamment)
- afin de permettre la communication entre les espaces commerciaux et les espaces des fonctions support (par exemple : postes du terminal de croisière nécessitant un accès au réseau de maintenance)
- afin de connecter des équipements dans les parties communes (utile pour l'extension ponctuelle du réseau)

- Dans chaque bâtiment, des boucles locales étaient censée permettre l'interconnexion de réseaux indépendants, mais ce travail n'a jamais été réalisé.

Plan d'adressage

- une adresse de classe B est utilisée (128.0.0.0/16)

Volumétrie des débits

Les débits sont exprimés en kilo-bits par seconde, par client d'accès.

Le trafic local correspond aux échanges réseaux au sein du réseau du port (filaire et wifi).

Le trafic externe correspond aux échanges réseaux exploitant les lignes internet.

Gescale :

- Trafic local : 100 kb/s
- Traffc externe : 100 kb/s

Client mobile pour Gescale :

- Trafic local : 70 kb/s
- Trafic externe : 70 kb/s

Gentrepot

- Trafic local : 250 kb/s
- Trafic externe : 250 kb/s

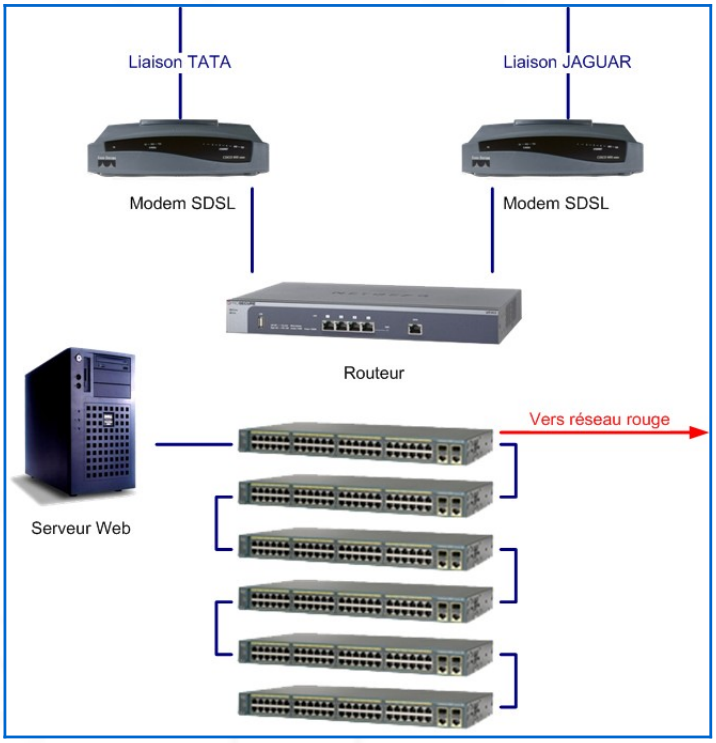
Portail internet

- Trafic local : 90 kb/s
- Trafic externe : 50 kb/s

Note : le nombre d'usager simultané du portail internet est de 100 personnes

Matériel

- Un serveur (serveur web) hébergeant le portail internet du port :
  - les visiteurs peuvent consulter les informations du portail
  - les loueurs des espaces commerciaux (compagnies maritimes) peuvent modifier le contenu du site associé à leur espace commercial (c'est-à-dire leur boutique web).
- Deux modems Cisco 888 G.SHDSL
- Un parefeu Netgear RG204
- Un routeur CISCO série 2900, avec un module supplémentaire d'agrégation de lien SDSL
- 6 commutateurs CISCO Catalyst 2960 cascadés
- Deux liaisons louées SDSL 3,2 Gb (chez TATA communications et Jaguar)
- Le câblage est réalisé en cuivre SFTP catégorie 5E compatible Ethernet Gb



Matériel de production

Le résumé résultant de l'inventaire du matériel de production est le suivant :

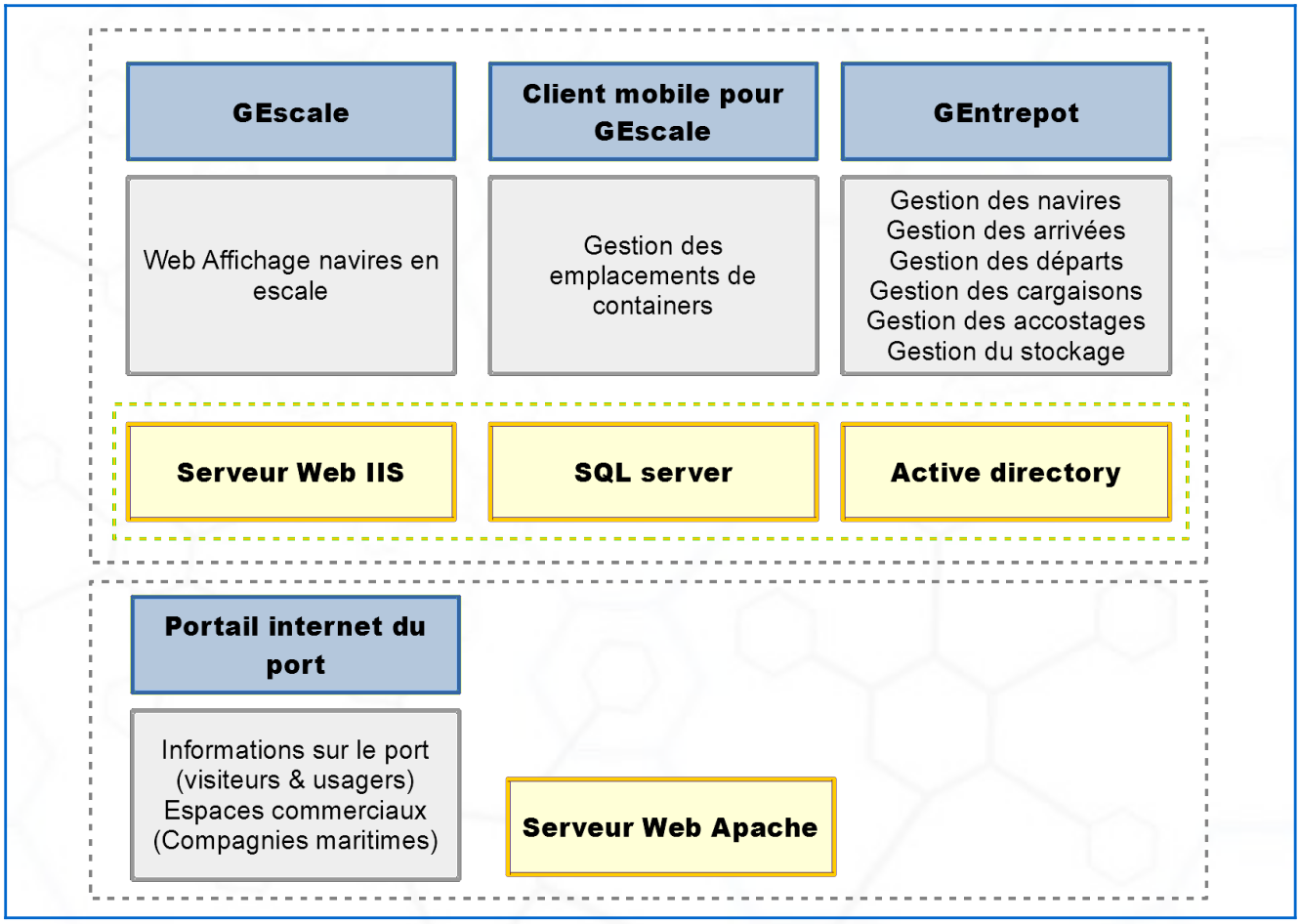
- 1 x Serveur Dell R510 hébergeant les applications de gestion (usage 100%)
- 1 x Serveur Dell R510 hébergeant le portail internet du port (usage 10%)
- 2 x modems Cisco 888 G.SHDSL
- 1 x parefeu Netgear RG204
- 1 x routeur CISCO série 2900, avec un module supplémentaire d'agrégation de lien SDSL
- 6 x commutateurs coeurs de réseau CISCO Catalyst 2960
- 2 x commutateurs secondaires CISCO Catalyst 2940
- 8 x répéteurs ethernet PERLE eR-S1110
- 15 x points d'accès sans fil CISCO AP321

Matériel d'exploitation

Le résumé résultant de l'inventaire du matériel d'exploitation est le suivant :

Quai 1 (Appelé quai de France)	
Salle d'embarquement croisière 1A	1 x poste « superviseur port » 8 x postes « Compagnies maritimes »
Salle d'embarquement ferry1B	1 x poste « superviseur port » 8 x postes « Compagnies maritimes »
Files embarquement ferry 1B	1 x poste « superviseur port »
Tour d'assistance à la navigation	1 x postes « superviseur port »
Quai 2 (Appelé quai de Normandie)	
Salle d'embarquement ferry2A	1 x poste « superviseur port » 4 x postes « Compagnies maritimes »
Files embarquement ferry 2A	1 x poste « superviseur port »
Salle d'embarquement ferry 2B	1 x poste « superviseur port » 4 x postes « Compagnies maritimes »
Files embarquement ferry 2B	1 x poste « superviseur port »
Accueil passager 2A et 2B	2 x postes « superviseur port » 4 x postes « Compagnies maritimes »
Atelier de maintenance (maintenance des navires et grues)	1 x poste « superviseur port » 6 x postes « atelier »
Bâtiment technique annexe (maintenance du site)	1 x postes « atelier » 1 x poste « superviseur port » 1 x poste «administratif »
Quai transmanche	
Bureaux (Premier et second étage du bâtiment)	4 x postes « superviseur port » 20 x postes «administratif »
Espaces commerciaux (Rez de chaussée des bureaux)	8 x postes « Compagnies maritimes »
Zone de fret sécurisé	2 x postes « superviseur port »
File d'embarquement général	1 x postes « superviseur port »

Architecture logicielle



Les logiciels sont utilisés par les catégories d'utilisateurs suivants :

Gescale : « superviseur port », « compagnies maritimes », « atelier », «administratif », « usager »

Client mobile pour Gescale : « superviseur port », « compagnies maritimes », «administratif »

Note : le nombre de clients mobiles est identique au nombre de postes de travail.

Gentrepot : « superviseur port », « compagnies maritimes », « atelier », «administratif »

Portail internet : «administratif », « usager »

Sécurité

- La sécurité y est minimale
  - Tous les accès internes sont autorisés. Tous les types d'application sont autorisés
  - Les accès externes ne sont autorisés qu'à destination du serveur web et ceci uniquement pour le protocole HTTP.

Insuffisances du système actuel et perspectives d'évolution

Un récent audit de l'existant a laissé apparaître un certain nombre de défauts liés à la sécurité.

L'administration du pare-feu actuel est complexe malgré une simplicité apparente des règles de filtrage. De plus le matériel pare-feu vieillissant rend obligatoire son remplacement, bien sûr par un système plus performant.

De la même manière, même si l'accès externe par le public au serveur web est nécessaire, il constitue néanmoins une faille de sécurité puisque le serveur web se trouve sur le réseau de production.

Il est actuellement impossible de distinguer les tentatives d'intrusion sur le réseau des locale.

Il faut suivre avec précision le matériel installé dans les différents espaces afin de connaître l'état des fonctionnement.

Compte-tenu de ces perspectives d'évolution, et du volume d'information à gérer, le DSI souhaite la mise en place d'un véritable outil de gestion du parc informatique, accessible en temps réel.

D'autre part, les gestionnaires du port aimeraient que ce dernier se d'un service supplémentaire permettant d'afficher des vidéos sur affichages multimédia répartis dans différents points stratégiques du port.

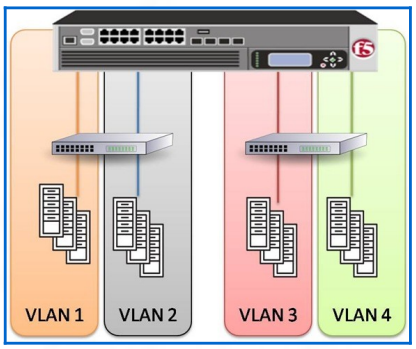
A l'issue de l'audit et des demandes des gestionnaires, le DSI a décidé de mettre en œuvre plusieurs solutions techniques.

Il a été prévu de mettre en œuvre une zone démilitarisée, permettant de créer plusieurs zones de sécurité. Cette solution doit permettre de limiter les intrusions, en définissant des règles d'accès différentes en fonction des zones. Cette solution repose sur l'utilisation d'un pare-feu, ce qui sera l'occasion de remplacer l'actuel pare-feu vieillissant.

Parallèlement à cela, il a été décidé de surveiller les accès de deux manières différentes :

- d'un point de vue logiciel, en implémentant un système de détection d'intrusion, devant permettre d'identifier rapidement les tentatives d'intrusions sur les différentes zones réseaux.
- d'un point de vue physique, en installant un réseau de surveillance par webcam, afin de surveiller les parties communes du port.

Pour la mise en œuvre, du réseau d'affichage multimédia, une solution économique basée sur du matériel embarqué à faible coût a été préconisé.



Enfin, dans un but de facilité d'administration et d'optimisation, il a été convenu de séparer les flux de communication des différents réseaux mis en œuvre : réseaux des espaces commerciaux, réseaux des fonctions de support, réseaux wifi accessibles au public... Cette solution emploiera les réseaux locaux virtuels (VLAN)

Cahier des charges à respecter

Répondre au obligation légales de surveillance

Répondre aux obligations légales de surveillance

Le système retenu devrait permettre aux responsables de répondre aux exigences des politiques d'accès et d'utilisation des réseaux de consultation Internet. En France, ces exigences consistent à authentifier les usagers du réseau de consultation lorsqu'ils décident de se connecter à Internet et à produire, pour chacun d'eux, une trace précise de toutes les activités réalisées (consultation, téléchargement, écoute multimédia, courrier, discussion, blog, etc.). Le but est de produire ces traces sous forme de fichiers pouvant être aisément archivés sur supports externes afin d'être exploitées dans le cadre d'une enquête judiciaire.

Sécuriser le réseau wifi

Le portail captif doit intégrer des protections vis-à-vis d'une attaque interne (anticontournement)

Le portail doit, en outre, mettre en œuvre un dispositif de filtrage permettant de bloquer l'accès aux sites dont le contenu est jugé répréhensible ou non-conforme. Celui-ci doit être entièrement paramétrable (activation, désactivation, ajout ou retrait de site, etc.). La possibilité d'utilisation de liste blanche et/ou noire serait un plus.

Enfin le portail doit être capable de bloquer tout trafic autre que le trafic WEB et de n'activer que les services réseaux désirés (https, flux multimédia...).

Comportements attendus

L'usager doit pouvoir utiliser n'importe quel équipement connecté sur le réseau de consultation.

Au lancement d'un navigateur WEB, une page d'authentification lui est présentée dans la langue configurée dans ses préférences. Cette page contient une information l'informant des fonctions principales du portail. Elle lui permet aussi de modifier son mot de passe.

Une fois l'authentification effectuée, le navigateur affiche la première page de consultation ainsi qu'une fenêtre supplémentaire permettant à l'usager de se déconnecter. En fonction de la configuration du filtrage, un ensemble de protocoles réseau sont alors disponibles pour les usagers authentifiés (web, courrier électronique, discussion, radio Internet...).

Pour se déconnecter, l'usager peut utiliser la fenêtre de déconnexion dédiée ou l'un des raccourcis intégrés dans le marque-page de son navigateur ('logout' dans l'URL par exemple).

Les administrateurs doivent pouvoir accéder de manière authentifiée et chiffrée à l'interface graphique du centre de gestion du portail

Ce centre de gestion doit donner accès à :

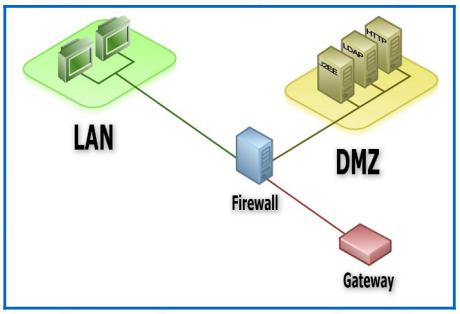
- la gestion des équipements de consultation
- la gestion des usagers : création et suppression d'usagers ou de groupe d'usagers, modification de leurs caractéristiques (par exemple : date d'expiration, périodes de connexions hebdomadaires autorisées, durées limites de connexion par session, par journée et par mois, limites de bande passante...)
- la consultation de statistiques d'exploitation du réseau de consultation et de la bande passante

DMZ

Zones

Au minimum, trois zones de sécurités doivent être établies :

- zone extérieure : correspondant au réseau en dehors du port
- zone web : correspondant au réseau hébergeant le serveur web
- zone intérieure : correspondant au réseau interne du port



Accès aux zones

	...vers la zone extérieure.	...vers la zone web.	...vers la zone intérieure.
De la zone extérieure...		Autorisée	Refusée
De la zone web...	Autorisée		Refusée
De la zone intérieure...	Toujours autorisée pour les réseaux des espaces commerciaux Autorisée après authentification via le portail captif	Toujours autorisée pour les réseaux des espaces commerciaux Autorisée après authentification via le portail captif	

Séparation des flux de communication des différents réseaux

Les flux de communication des différents réseaux logiques doivent être isolés les uns des autres par l'utilisation de VLAN.

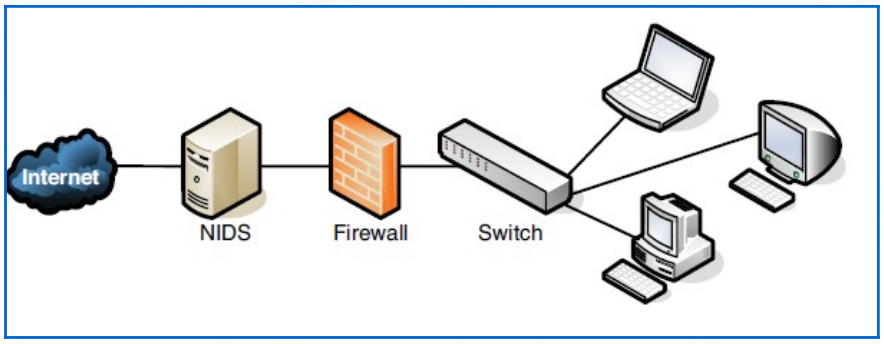
Les réseaux concernés

- réseaux des espaces commerciaux
- réseaux de surveillance par webcam
- réseaux d'affichage publicitaires
- réseaux wifi accessibles au public

La configuration des VLAN sera établie sur les commutateurs CISCO

IDS

- Le système doit être capable de détecter une intrusion ou tentative d'intrusion
- Le système doit être capable d'identifier le type d'attaque
- Il doit être capable de déclencher des alertes administratives
  - la forme de l'alerte est libre (email, sms, syslog...)
- Les statistiques de détection des intrusions doivent être consultables à distance.



- Le matériel associé à l'IDS doit être supervisé et inclus dans l'inventaire du parc informatique

Réseau de surveillance

- Le réseau de surveillance doit être constitué de caméra de surveillance IP ou Webcam
- Le contrôle des webcam doit pouvoir s'opérer à distance (consultation, orientation...)
- Certaines webcam doivent enregistrer les images en permanence, d'autre sous détection de mouvement uniquement (dans ce cas, une alerte administrative doit être envoyée)
- Les images issues des webcam de surveillance doivent être enregistré pendant une certaine période (une semaine par exemple)

Gestion du parc informatique

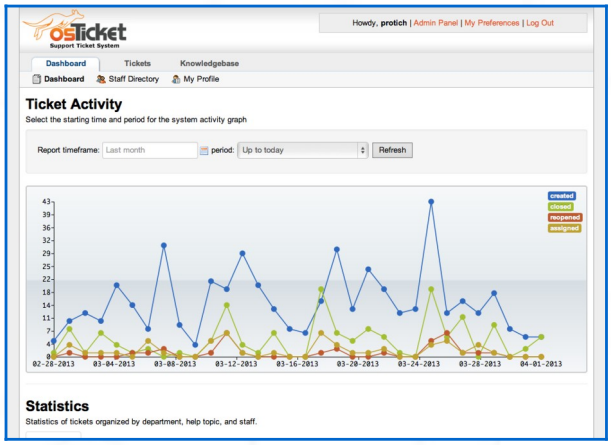
- Le système doit être capable de déployer des OS et des logiciels sur les plate-formes matérielles au niveau des espaces commerciaux.
- Le système doit permettre l'inventaire du parc informatique, ainsi que sa gestion.
- Le système doit surveiller également le fonctionnement correct des actifs informatiques du port.
- Il est demandé que ce système soit disponible dans un temps proche de 100 % du temps (les techniques de haute-disponibilité, de répartition de charge et/ou continuité de service... sont préconisées)

La gestion des incidents (tickets)

Vous devez mettre en œuvre un logiciel de gestion des incidents permettant aux utilisateurs et aux membres de la société de communiquer ensemble lors de la gestion d'un incident.

Les fonctionnalités obligatoires attendues pour un logiciel de ce type sont :

- l'ouverture d'un ticket (demande d'intervention par un utilisateur)
- la communication lors de la résolution (informations successives sur le traitement de la demande par les administrateurs)
- l'obtention de statistiques détaillées sur les incidents et leur résolution. Ces informations sont largement utilisées par les administrateurs afin d'améliorer les temps de reprise sur panne ou de justifier les demandes d'évolution de l'infrastructure.



L'assistance téléphonique

Les utilisateurs se plaignent de la lourdeur des communications avec l'entreprise.

Effectivement, tout appel d'un utilisateur par téléphone auprès d'un service particulier est effectué sans aiguillage préalable du destinataire.

Dans l'organisation actuelle, le premier membre du service concerné qui décroche prend l'appel, identifie le bon interlocuteur et fait venir physiquement la personne près du téléphone afin de répondre à la demande.

Ce mode de fonctionnement fait apparaître plusieurs points noirs :

- la solution manque de professionnalisme
- les délais de réponses sont longs,
  - à cause des déplacements physiques des personnes
  - parfois l'utilisateur est invité à rappeler son interlocuteur parce que la personne responsable du service concerné n'est pas disponible
  - l'identification du service concerné est mauvaise, et le client n'obtient pas le bon interlocuteur

- certains membres du port ne répondent jamais au téléphone, prétextant que la plupart du temps l'appel ne leur est pas destiné.

Il a été décidé de mettre en place une plate forme de téléphonie IP. Cette plate forme qui va remplacer la téléphonie classique actuelle devra permettre les fonctionnalités suivantes :

- L'accueil téléphonique automatique, invitant l'utilisateur a faire des choix en fonction de sa demande. L'objectif est de mettre en relation le membre de l'équipe concerné avec le client, sans passer par un intermédiaire.
- Une solution du type suivant est attendue :
  - message d'accueil
  - choix du client sur son combiné (service à joindre – si l'appel correspond à des heures d'ouverture)
  - redirection automatique vers le ou les postes des membres de l'équipe choisie
  - mise en attente éventuelle de l'utilisateur.

(Facultatif) En cas d'indisponibilité d'un interlocuteur sur les horaires de travail, un rappel automatique de l'utilisateur serait souhaitable.

Pour les accès extérieurs, les comptes SIP du fournisseur d'accès internet seront utilisés (non gérés puisque hors du périmètre d'administration), l'infrastructure ToIp du port doit par contre être gérée en interne.

Stockage et accès aux données

Les fichiers des clients sont stockés directement sur le serveur Active Directory de la société.

Chaque service dispose d'un dossier partagé dans lequel les membres du service stockent leurs données.

Bien entendu, un utilisateur d'un service ne peut accéder aux données d'un utilisateur d'un autre service.

Les droits d'accès sont gérés au niveau du système de fichier du système d'exploitation.

Aucune redondance n'est prévue.

Il vous est demandé de mettre en œuvre une solution permettant de garantir :

- le stockage sécurisé des données
- la résilience de l'accès aux données
- la disponibilité des liaisons réseau est aussi concernée par ce point.

Sauvegarde des données

Une récente coupure de services subie par le port de Cherbourg a fait prend conscience que même si tous des éléments de redondances étaient prévus, une perte de données était toujours possible. Fort de cet expérience, il vous est demandé de bâtir un plan de sauvegarde complet, prenant en compte :

- pour les utilisateurs
  - les données des différents services
- pour l'entreprise
  - les données du portail internet du port
  - les configurations des différents matériels d'infrastructure
  - les éventuelles machines virtuelles utilisées en production
  - toute donnée nécessaire au fonctionnement de l'entreprise (y compris les bases de données)

Votre plan devra être mis en œuvre et testé pour validation avant généralisation.

Amélioration serveur web

Le serveur web correspondant au portail du port de Cherbourg est utilisé pour la mise en ligne du site vitrine du port, ainsi que pour les différentes parties correspondant aux espaces commerciaux des compagnies maritimes.

Le serveur web est actuellement hébergé sur une machine de bureau utilisée en tant que serveur. Il exploite Apache 2.

Aucune liaison SSL n'est utilisable pour l'instant.

Vous devez proposer une solution permettant :

- de garantir la continuité du service HTTP
- de garantir la qualité de service du serveur Web
- de chiffrer les connexions du serveur Web

Annexe : Plan de situation du port