**Projet «SECURITE CIVILE»**

**-**

**BTS SIO 2023 Option SISR**



**Epreuve E5**

**-**

**Situation professionnelle 2**

|  |  |  |  |
| --- | --- | --- | --- |
| **BTS Services informatiques aux organisations SESSION 2023**  **Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**  **ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)** | | | |
| **DESCRIPTION D’UNE RÉALISATION PROFESSIONNELLE** | | | **N° réalisation : 2** |
| **Nom, prénom :Felter Jules** | | **01949752930** | |
| **Épreuve ponctuelle** | **Contrôle en cours de formation** | **Date : 18** /04/2023 | |
| **Organisation support de la réalisation professionnelle**  Le projet est de permette aux Préfectures d’améliorer leur résilience informatique en cas de crise, d’optimiser son système d’information ainsi que l’accessibilité sécurisée de son système d’information à l’extérieur | | | |
| **Intitulé de la réalisation professionnelle**  Projet Sécurité Civile | | | |
| **Période de réalisation :** 02/01/2022 au 30/03/2022  **Lieu :** Strasbourg  **Modalité :  Seul****(e)  En équipe** | | | |
| **Compétences travaillées**  Concevoir une solution d’infrastructure réseau  Installer, tester et déployer une solution d’infrastructure réseau  Exploiter, dépanner et superviser une solution d’infrastructure réseau | | | |
| **Conditions de réalisation[[1]](#footnote-1) (ressources fournies, résultats attendus)**  **ressources fournies :** Cahier des charges « Sécurité Civile »  **résultats attendus :** mise en place d’une infra et d’une connexion à haute disponibilité et d’un accès distant. Mise en œuvre d’une solution de messagerie et de téléphonie ainsi que une solution de supervision et de monitoring. | | | |
| **Description des ressources documentaires, matérielles et logicielles utilisées[[2]](#footnote-2)**   * Mise en place de 2 routeur Pfsense * Mise en place de 2 serveurs Windows Active Directory (Principal et Secondaire) * Mise en place d’1 serveur de téléphonie Asterisk et déploiement d’un client softphone * Mise en place d’1 serveur de messagerie(Hmail) et déploiement d’un client de messagerie * Mise en place d’1 serveur Check MK pour la supervision et le monitoring * Mise en place d’une solution OpenVPN (Road Warrior) * Mise en place d’une DMZ pour accéder au Serveur WEB E-Brigade | | | |
| **Modalités d’accès aux productions[[3]](#footnote-3) et à leur documentation[[4]](#footnote-4)**  Disponible sur le portfolio : <https://julesfelter.fr> | | | |
| **BTS Services informatiques aux organisations SESSION 2023**  **Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**  **ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle**  **(verso, éventuellement pages suivantes)** | | | |

|  |
| --- |
| **Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs**  Table des matières  [Contexte 4](#_Toc100845269)  [Besoins et contraintes 4](#_Toc100845270)  [Solutions retenues et argumentations 4](#_Toc100845271)  [Schéma réseau 7](#_Toc100845272)  [Coût du projet 7](#_Toc100845273)  [Planning prévisionnel 8](#_Toc100845274)  [Planning réel 9](#_Toc100845275)  [Planning prévisionnel vs réel 9](#_Toc100845276)  [Conclusion 10](#_Toc100845277)  [Améliorations possibles 10](#_Toc100845278) |

# Contexte

Le projet est de permette aux Préfectures d’améliorer leur résilience informatique en cas de crise, d’optimiser son système d’information ainsi que l’accessibilité sécurisée de son système d’information à l’extérieur.

# Besoins et contraintes

**Besoin :**

Le projet est de permette aux Préfectures d’améliorer leur résilience informatique en cas de crise, d’optimiser son système d’information ainsi que l’accessibilité sécurisée de son système d’information à l’extérieur. Pour cela, les objectifs suivants devront être atteints :

* Mise en œuvre d’une haute disponibilité de routeurs et liaison Internet redondée (2    
  routeurs / 2 accès Internet)
* Mise en œuvre de 2 serveurs Active Directory (Principal et Secondaire)
* Mise en œuvre d’1 serveur de téléphonie IpBX et déploiement d’un client softphone
* Mise en œuvre d’1 serveur de messagerie et déploiement d’un client de messagerie -> Utilisation des comptes de l’Active Directory
* Mise en œuvre d’1 serveur de supervision et de monitoring
* Supervision de la disponibilité des routeurs et serveurs
* Monitoring et historique des indisponibilités des routeurs et serveurs
* Alerte par mail aux administrateurs en cas de panne
* Mise en œuvre d’une solution de VPN RW (Road Warrior)-> Utilisation des comptes de l’Active Directory (accès aux ressources disponible si la connexion VPN est établi)
* Mise en œuvre d’une DMZ pour accéder au Serveur WEB E-Brigade

**Contraintes :**

* -Respecter la date de début (06Janvier2023) et de fin de projet (25 Avril 2023)
* -La solution doit être à moindre coût,
  + -Proposer un devis complet qui tiendra compte de tous les éléments indispensables au projet (matériels, licences, main d’œuvre...)
* -Rendre les livrables aux dates prévues

# 

# Solutions retenues et argumentations

**Messagerie**

|  |  |  |
| --- | --- | --- |
|  | **Avantages** | **Inconvénients** |
| Zimbra | - Prise en charge de diverses fonctionnalités  - Open source   - Interface complète   - Haute disponibilité   - Fiable   - Gestion centralisé utilisateurs | - Installation et configuration complexe   - Pas très personnalisable   - Communauté limitée   - Fonctionnalité de sécurité limité |
| Postfix | Solution complète qui prend en charge de nombreux protocole   - Possède un bon nombre de fonctionnalité   - Grosse communauté   - Beaucoup de documentation - Permet une configuration avancée en terme de routage d’appel   - Utilisation intuitive   - Est assez facile à prendre en mains   - Open source | - Moins performant que Freeswitch   - Peu surcharger   - Compatibilité limitée   - Peu personnalisable |
| HMail | - Gratuit et open source, sans coût de licence   - Compatible avec Windows et facile à installer   - Gère plusieurs domaines et adresses e-mail  - Fonctionnalités avancées, telles que la mise en quarantaine et la recherche de courrier électronique   - Possibilité de créer des listes de diffusion | - Documentation limitée et communauté plus petite   - Les mises à jour peuvent parfois causer des problèmes   - L'interface utilisateur est assez basique et peu intuitive   - Peut-être plus lent que les solutions commerciales plus avancées   - Pas de support téléphonique ou de chat en direct |

Nous avons choisi la solution Hmail pour sa compatibilité Windows ainsi que le cout de License gratuit.

**VOIP**

|  |  |  |
| --- | --- | --- |
|  | **Avantages** | **Inconvénients** |
| Freeswitch | - Solution complète qui prend en charge de nombreux protocole  - Possède un bon nombre de fonctionnalité   - Est une solution sécurisée qui permet une détection des attaques et une protection contre les attaques DDOS   - Permet une configuration avancée en terme de routage d’appel   - Personnalisable   - Open source | - Difficile à prendre en mains   - Documentation limitée par rapport à l’autre solution  - Interface peu intuitive   - Configuration complexe |
| Asterisk | - Solution complète qui prend en charge de nombreux protocole   - Possède un bon nombre de fonctionnalité   - Grosse communauté  - Beaucoup de documentation - Permet une configuration avancée en termes de routage d’appel   - Utilisation intuitive   - Est assez facile à prendre en mains   - Open source | - Moins performant que Freeswitch   - Peu surcharger   - Compatibilité limitée   - Peu personnalisable |

Nous avons choisi dans le cadre du projet la solution d’Asterisk du au grand nombres de documentation sur le sujet et à sa prise en mains facile.

**Supervision**

|  |  |  |
| --- | --- | --- |
|  | **CheckMK** | **Zabbix** |
| **Prix** | Il existe une version CheckMK raw qui est gratuite et opensource, et qui convient aux PME.La version payante propose des fonctionnalités avancées ainsi qu’un support. | Zabbix est sous licence GNU GPL, et est donc gratuite et open source. La version payante propose des fonctionnalités avancées ainsi qu’un support. |
| **Equipements supervisés** | Serveurs, commutateurs, routeurs, pare-feu, ordinateurs (physique ou virtuelle) | Serveurs, commutateurs, routeurs, pare-feu, ordinateurs (physique ou virtuelle) |
| **Alertes** | Par mail, SMS | Par Mail, SMS |
| **Fonctionnement** | Agent installé sur un équipement / serveur | Agent installé sur un équipement / serveur |
| **Compatibilité de l’agent** | Linux, Unix, Windows, Mac, Esxi, FreeBSD | Linux, Unix, Windows, Mac, Esxi |
| **Prise en charge de SNMP** | Oui | Oui |
| **Documentation** | Oui, seulement en anglais | Oui |
| **Surveillance automatique** | Oui, grâce à des règles de découverte automatique | Oui, grâce à une découverte sur le réseau basé sur : - plage IP- services externes (SSH, FTP, IMAP, TCP, …)- agent Zabbixagent SNMP |

Nous remarquons que au vu de nos besoins, les 2 solutions remplissent les mêmes critères.

Nous utiliserons CheckMK car c’est un outil qui a déjà été testé par le groupe, et qu’il possède une installation, une prise en main ainsi qu’une interface facile.

# Schéma réseau

Le schéma nous montre l’infra qui à été mise en place pour ce projet, nous avons donc le réseau LAN dans le carré vers et la DMZ dans le carré rouge avec le serveur Web à l’intérieur. Au dessus

Nous avons les deux routeurs qui permettent la liaison VPN, l’IP virtuelle, la redondance des routeurs et qui ont le rôles de Firewall.Une image contenant diagramme

Description générée automatiquement

# Coût du projet

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Quantité** | **Prix unité** | **Prix** |
| Licence Windows Serveur 2019 Standard | 2 | 1946 € | 3892 € |
| CAL Utilisateurs | 10 | 50 € | 500 € |
| Licence OpenVPN pour 10 utilisateurs | 1 | 595 € | 595 € |
| Serveurs de virtualisation :Smart Selection PowerEdge  R7515 Rack Server | 2 | 3351,80 € | 6703,60 € |
| Mains d’oeuvre | 48h | 50 € | 2400 € |
| **Total HT** |  |  | **14 090, 60 €** |
| TVA |  |  | 2 818,12 € |
| **TOTAL TTC** |  |  | **16 908,72 €** |

# Planning prévisionnel

**Routeurs**

* Installation & configuration système et réseau
* Redondance des 2 routeurs
* Règles de pare-feu

**Active Directory**

* Installation & configuration des serveurs
* Installation de l’AD et création d’un domaine
* Mettre à jour règles de pare-feu pour les flux AD

**ERP**

* Installation & configuration d’un serveur Web
* Création de la DMZ (règles de pare-feu)
* Configuration de eBrigade

**Supervision**

* Installation & configuration d’un serveur Ubuntu
* Installation & configuration de CheckMK
* Installation de l’agent sur tous les équipements de l’infrastructure
* Création des alertes sur CheckMK

**Messagerie**

* Configuration et installation de Hmail
* Configuration du service de messageire au sein de l’infra

**Voip**

* Installation et configuration d’un serveur Ubuntu
* Installation et configuration de Asterisk
* Configuration de Asterisk avec l’infra

Une image contenant table

Description générée automatiquement

# Planning réel

Une image contenant graphique, table

Description générée automatiquement

# Planning prévisionnel vs réel

Voici le planning prévisionnel :

Une image contenant table

Description générée automatiquement

Voici le planning réel :

Nous pouvoir que les taches ont au final été fais sur une période plus courte et on été fais plus rapidement que prévue.

Une image contenant graphique, table

Description générée automatiquement

La

# Conclusion

Le projet a été mené à bien. Tous les résultats attendus ont été atteint. Ce projet a permis à chacun des membres d’apprendre beaucoup de chose tant sur le plan technique (solutions mises en place) que sur le plan organisationnel du projet (communication/gestion du temps/ …)

# Améliorations possibles

Une amélioration possible est de sécuriser le flux de messagerie et de VOIP.

Concernant la messagerie, on pourrait chiffrer les flux entrants et sortants, qui ne sont pas chiffrés actuellement :    
Une image contenant texte

Description générée automatiquement

Concernant la VOIP, on pourrait utiliser le protocole SIP via e port 5061 et non plus via le 5060. Le port 5061 est sa version sécurisée (SIP-TLS).

Afin d’accroitre la sécurité de l’architecture, on pourrait ajouter un IDS/IPS dans l’infrastructure. Cela peut être intéressant car notre firewall pfSense analyse seulement les entêtes des trames. Le contenu des paquets n’est pas analysé, et un hacker pourrait « camoufler » son attaque. L’IDS / IPS analysent les comportements suspects, et permet donc de compléter la sécurité du pare-feu.

1. En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO. [↑](#footnote-ref-1)
2. Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l’annexe II.E du référentiel du BTS SIO. [↑](#footnote-ref-2)
3. Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l’épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d’organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l’épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d’un espace de stockage et de la présentation de l’organisation du stockage. [↑](#footnote-ref-3)
4. Lien vers la documentation complète, précisant et décrivant, si cela n’a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services. [↑](#footnote-ref-4)