

MedicArgile

livrable individuel

BLOC 1 : MODELISER L'INFRASTRUCTURE SYSTEME ET RESEAU
ETUDIANT : BERNOIS DAMIEN
DATE FINALE DE REMISE : 29/01/2025 (AVANT MINUIT)
DATE DE SOUTENANCE INDIVIDUEL : 30/01/2025 DE 11H50 A 12H30



Table des matières

1. Note de cadrage	3
1.1. Base du projet.....	3
1.2. Objectifs du projet	3
1.3. Amplitudes du projet.....	3
2. Analyse de l'infrastructure existante	4
2.1. Cartographie de l'infrastructure existante	4
2.2. Besoins techniques	4
2.3. Révision, risques et contraintes de l'infrastructure existante.....	5
3. Solutions d'améliorations proposées	6
3.1. Solution d'amélioration du routeur Cisco d'accès aux FAI (SFR et Orange).....	6
3.1.1. Ses avantages	6
3.1.2. Les risques et contraintes de la mise en place de cette solution.....	6
3.2. Solution d'amélioration du pare-feu Stormshield	7
3.2.1. Ses avantages	7
3.2.2. Les risques et contraintes de la mise en place de cette solution.....	8
3.3. Solution d'amélioration des commutateurs Cisco.....	8
3.3.1. Ses avantages	8
3.3.2. Les risques et contraintes de la mise en place de cette solution.....	9
3.4. Cartographie de la solution d'amélioration.....	9
4. Organisation du projet	10
4.1. Planning organisationnel (3 mois et 6 jours)	10
4.2. Ressources du projet	12
4.2.1. Ressources matérielles.....	12
4.2.2. Ressources Humaines et parties prenantes	12
4.2.3. Ressources budgétaires et budget prévisionnel	13
4.2.4. Ressources immatérielles et critères d'évaluation pour les prestataires externes	14
4.3. Triangle qualité, coût, délai	14
4.4. Livrables, évaluation du prestation et indicateurs de pilotage	14



1. Note de cadrage

1.1. Base du projet

Afin de mettre à niveau son système d'information et d'assurer la fiabilité et la sécurité de ce dernier, l'entreprise fait appel à mes services de prestation afin d'analyser leur infrastructure systèmes et réseaux et de leur proposer une solution technique d'amélioration de cette dernière.

1.2. Objectifs du projet

Ce projet a pour objectif de proposer une mise à niveau de l'infrastructure systèmes et réseaux de l'entreprise MedicArgile en adéquation avec leurs multiples besoins, ainsi que l'étude et l'organisation de la mise en place de ce projet.

Il faudra mettre un accent sur le respect des coutumes et des habitudes du personnel informatique de l'entreprise MedicArgile, comprenant l'environnement des logiciels et des équipements informatiques.

1.3. Amplitudes du projet

La mise en place de la solution d'amélioration de ce projet (comprenant l'organisation du projet, la prise de contact avec les fournisseurs et les prestataires, les achats et livraisons des équipements et des licences, ainsi que le déploiement de la solution d'amélioration) s'effectuera sur une durée totale et maximale de 3 mois et 6 jours.

De plus, un support technique et de maintenance sera garanti à l'entreprise pour une durée de 1 an (renouvelable) à compter de la réception des équipements informatiques grâce aux licences associées.



2. Analyse de l'infrastructure existante

2.1. Cartographie de l'infrastructure existante

Vous trouverez en pièces jointes à ce livrable dans le dossier « Annexes > Cartographies > Cartographie de l'infrastructure existante », la cartographie complète de l'infrastructure réseau existante de l'entreprise MédicArgile.

De plus, vous trouverez aussi en pièces jointes à ce livrable dans le dossier « Annexes > Synthèse des équipements existants », un tableau complet faisant guise de synthèse de tous les équipements Informatiques MédicArgile existants.

2.2. Besoins techniques

MédicArgile étant une entreprise pharmaceutique, elle contient des données importantes qui nécessitent une haute disponibilité et une haute sécurité. Pour cela, la solution proposée devra remplir ces 3 besoins, tels que :

➤ Un besoin continuité :

La solution actuelle mise en œuvre ne garantit pas à l'entreprise une continuité des équipements concernés du système d'information.

En cas de panne ou de défaillance d'un équipement tels que les deux routeurs Cisco, ou bien le pare-feu Stormshield, l'accès à internet et la fonctionnalité de certains services des serveurs nécessitant ce dernier ne pourront pas être maintenus.

➤ Un besoin de modernité :

La solution actuelle mise en œuvre ne garantit pas à l'entreprise une modernité des équipements concernés du système d'information.

En cas de panne ou de défaillance d'un équipement, due à l'ancienneté de leur version, un support technique permettant de remettre en service ces équipements ne pourra peut-être pas être garanti.

➤ Un besoin de sécurité :

La solution actuelle mise en œuvre ne garantit pas à l'entreprise une sécurité des équipements concernés du système d'information.

En cas de panne ou de défaillance d'un équipement, due à l'ancienneté de leur version, le manque ou l'arrêt des mises à jour de leur système et/ou du support technique peut entraîner des failles de sécurité et donc un risque majeur pour les données et la sécurité du réseau.



2.3. Révision, risques et contraintes de l'infrastructure existante

Après analyse de l'infrastructure systèmes et réseaux de MédicArgile, plusieurs points à améliorer m'ont été pertinents, parmi eux :

- L'obsolescence et le manque de modernité des deux routeurs Cisco R800 Series donnant accès aux deux FAI (ADSL SFR et FTTH Orange), ainsi que leur manque de redondance.

En cas de panne d'au minimum l'un des deux routeurs, cela peut entraîner :

- La coupure de l'accès aux FAI et donc à Internet ou à la téléphonie.
- L'isolation du réseau LAN de MédicArgile d'Internet.
- La coupure des systèmes nécessitant Internet.
- L'arrêt de la production et des travailleurs sur l'ensemble du site MédicArgile.

- L'obsolescence et le manque de modernité du pare-feu Stormshield SN210 assurant la sécurité du réseau, ainsi que son manque de redondance.

En cas de panne du pare-feu, cela peut entraîner :

- La coupure de l'accès aux routeurs FAI et donc à Internet ou à la téléphonie.
- L'isolation du réseau LAN de MédicArgile d'Internet.
- La coupure des systèmes nécessitant Internet.
- Le manque de sécurité du réseau LAN MedicArgile.
- L'arrêt de la production et des travailleurs sur l'ensemble du site MédicArgile.

- L'obsolescence et le manque de modernité des multiples commutateurs Cisco Catalyst 3560, Cisco Catalyst 2960 et Cisco Catalyst 2950, assurant le flux et la répartition de la communication au sein du réseau.

En cas de panne de l'un ou de plusieurs de ces commutateurs, cela peut entraîner :

- La coupure de l'accès aux services des serveurs en isolant la salle serveur du reste du réseau.
- La coupure de l'accès à Internet en isolant le réseau du pare-feu et des routeurs qui donnent quant à eux l'accès aux FAI.
- L'isolation de chacun des bâtiments avec le reste du réseau.
- L'arrêt de la production et des travailleurs sur l'ensemble du site MédicArgile.



3. Solutions d'améliorations proposées

Afin de répondre aux différents besoins de l'entreprise soulignés précédemment et résoudre les problèmes de redondance des équipements informatiques de l'infrastructure, la solution de mettre à niveau les équipements, ainsi que de créer des clusters de redondance, me semble la plus adéquate quant à l'importance de la haute disponibilité du réseau MedicArgile. Cette solution d'amélioration vous est précisée ci-dessous.

3.1. Solution d'amélioration du routeur Cisco d'accès aux FAI (SFR et Orange)

Mise en place d'une solution d'amélioration des routeurs d'accès aux FAI avec :

- Un cluster de redondance de deux routeurs Cisco C891F-K9 (qui centralisera l'interconnexion avec les deux FAI et le reste du réseau, dans la salle serveurs du bâtiment B).

3.1.1. Ses avantages

- La redondance du routeur qui fournit l'interconnexion entre les FAI et le reste du réseau :
 - Si le routeur principal du cluster tombe en panne ou est défaillant, le deuxième routeur (backup) prendra la main sur le service instantanément par la redondance fournie grâce à la configuration du protocole VRRP (Virtual Router Reduncancy Protocol) mise en place sur chaque cluster.
 - Les deux routeurs se partagent la même interface à travers une IP virtuelle (VIP) qui est l'interface renseignée sur le reste du réseau, la bascule d'un routeur à l'autre sera invisible pour les utilisateurs et l'extérieur du réseau.
- La spécificité du modèle :
 - Il possède 8 ports RJ45 (dont 4 compatibles PoE) avec un débit allant jusqu'à 1Gb/s, 2 ports WAN pour la connexion à des sites distants.
 - La fiabilité et la modernité du routeur (il bénéficie de mises à jour de sécurité régulières corrigeant les failles de sécurité grâce à la modernité du logiciel).
 - La possibilité de mettre en place une redondance de l'alimentation.
- La possibilité d'évoluer le réseau dans le futur :
 - Il supporte jusqu'à 50 tunnels IPSec (pour une future mise en place de VPN pour une solution de télétravail).
 - Normé 802.1Q (pour une future mise en place de VLAN afin de segmenter le réseau).

3.1.2. Les risques et contraintes de la mise en place de cette solution

- Les contraintes du prix de la mise en place de la solution d'amélioration, ainsi que sa maintenance :
 - Prix de l'achat du matériel (achat de 2 routeurs Cisco C891F-K9, achat de câbles réseau RJ45, 2 alimentations de rechange).



- Prix de l'achat de la licence (ici la licence « SMARTnet » assure l'accès à un support technique 24h/24, 7j/7 et l'accès aux mises à jour logiciels, la licence est applicable sur tous les périphériques Cisco du réseau).
- Les risques de la mise en place de la solution :
 - L'installation et complexification de l'infrastructure (ajout d'un routeur en plus sur l'infrastructure à maintenir physiquement et logiquement).
 - Nécessite une copie minutieuse des configurations des anciens équipements vers les nouveaux équipements (une possibilité d'oublier des configurations).
 - Nécessite une sauvegarde minutieuse des nouvelles configurations en cas de perte.
 - Nécessite une synchronisation automatique de la configuration du premier au deuxième routeur de secours.
 - Coupure du réseau lors de la bascule (à faire lors de périodes de vide de production, lorsque cela n'aura aucun risque sur la production du site).
 - Basculement des deux liens des deux FAI vers un seul et même routeur.

3.2. Solution d'amélioration du pare-feu Stormshield

Mise en place d'une solution d'amélioration du pare-feu Stormshield avec :

- Un cluster de redondance de deux pare-feu Stormshield SN-S-Series 320 (dans la salle serveurs du bâtiment B).

3.2.1. Ses avantages

- La redondance du pare-feu :
 - Si le pare-feu principal du cluster tombe en panne ou est défaillant, le deuxième pare-feu (backup) prendra la main sur le service instantanément par la redondance fournie grâce à la configuration du mode actif/passif (possible grâce à la mise en place de la haute disponibilité des 2 pare-feu).
 - La synchronisation des configurations du pare-feu actif vers le pare-feu passif se fait instantanément grâce à la mise en place du protocole K2K (Kernel to Kernel, port 44242/UDP).
- La spécificité du modèle :
 - Il possède 8 ports RJ45 avec un débit allant jusqu'à 2Gb/s, l'accès à la console se fait à partir du port RJ45 ou USB-C.
 - Il peut supporter jusqu'à 300 000 connexions en simultanées.
 - La fiabilité et la modernité du pare-feu (il possède une fiabilité MTBF de 36,5 ans et bénéficie de mises à jour de sécurité régulières corrigeant les failles de sécurité grâce à la modernité du logiciel).
 - La possibilité de mettre en place une redondance de l'alimentation.
- La possibilité d'évoluer le réseau dans le futur :
 - Il supporte jusqu'à 100 tunnels IPsec (pour une future mise en place de VPN pour une solution de télétravail).



3.2.2. Les risques et contraintes de la mise en place de cette solution

- Les contraintes du prix de la mise en place de la solution d'amélioration, ainsi que sa maintenance :
 - Prix de l'achat du matériel (achat de 2 pare-feu Stormshield SN-S-Series 320, achat de câbles réseau RJ45, 2 alimentations de rechange).
 - Prix de l'achat de la licence (ici la licence « support et maintenance avancée » assure l'accès à un support technique 24h/24, 7j/7 et l'accès aux mises à jour logiciel).
- Les risques de la mise en place de la solution :
 - L'installation et complexification de l'infrastructure (ajout d'un pare-feu en plus sur l'infrastructure à maintenir physiquement et logiquement sur l'infrastructure).
 - Nécessite une copie minutieuse des configurations des anciens équipements vers les nouveaux équipements (une possibilité d'oublier des configurations).
 - Nécessite une sauvegarde minutieuse des nouvelles configurations en cas de perte.
 - Nécessite une synchronisation automatique de la configuration du premier pare-feu vers le deuxième de secours.
 - Coupure du réseau lors de la bascule (à faire lors de périodes de vide de production, lorsque cela n'aura aucun risque sur la production du site).

3.3. Solution d'amélioration des commutateurs Cisco

Mise en place d'une solution d'amélioration des commutateurs Cisco avec :

- Trois clusters de redondance de deux commutateurs Cisco Catalyst C9200-48P-E (dans la salle serveurs du bâtiment B et dans les deux unités de productions).
- Un cluster de redondance de deux commutateurs Cisco Catalyst C9200L-24P-4X-E (dans le bâtiment A).
- Un cluster de redondance de deux commutateurs Cisco Catalyst C9200CX-8P-2X2G-E (dans le laboratoire de production).

3.3.1. Ses avantages

- La redondance des commutateurs :
 - Si le commutateur principal du cluster tombe en panne ou est défaillant, le deuxième commutateur prendra la main sur le service instantanément par la redondance fournie.
 - La répartition et l'équilibrage des charges au sein du cluster, permettant de ne pas surcharger la bande passante sur un unique commutateur, fluidifiant le réseau.
 - La synchronisation des configurations entre les commutateurs dit « en pile » se fait instantanément grâce à la mise en place du protocole TFTP (Trivial File Transfer Protocol, port 69/UDP).
 - Les commutateurs disposent de ports SFP+, permettant de faire des sauvegardes des différentes configurations et aussi le transfert de ces dernières.
- La spécificité du modèle :
 - Chacun des modèles ci-dessus a respectivement 8, 24 ou 48 ports, en adéquation avec le besoin de chacun des bâtiments.



- La fiabilité et la modernité des commutateurs (ils bénéficient de mises à jour régulières corrigeant les failles grâce à la modernité du logiciel).
- La possibilité de mettre en place une redondance de l'alimentation.
- La possibilité d'évoluer le réseau dans le futur :
 - Normé 802.1Q (pour une future mise en place de VLAN afin de segmenter le réseau).

3.3.2. Les risques et contraintes de la mise en place de cette solution

- Les contraintes du prix de la mise en place de la solution d'amélioration, ainsi que sa maintenance :
 - Prix de l'achat du matériel (achat de 6 commutateurs Cisco Catalyst C9200-48P-E, achat de 2 commutateurs Cisco Catalyst C9200L-24P-4X-E, achat de 2 commutateurs Cisco Catalyst C9200CX-8P-2X2G-E, achat de câbles réseau RJ45, 10 alimentations de rechange).
 - Prix de l'achat de la licence (ici la licence « SMARTnet » assure l'accès à un support technique 24h/24, 7j/7 et l'accès aux mises à jour logiciels, la licence est applicable sur tous les périphériques Cisco du réseau).
- Les risques de la mise en place de la solution :
 - L'installation et complexification de l'infrastructure (ajout d'un commutateur en plus sur chacun des commutateurs existants, à maintenir physiquement et logiquement sur l'infrastructure).
 - Nécessite une copie minutieuse des configurations des anciens équipements vers les nouveaux équipements (une possibilité d'oublier des configurations).
 - Nécessite une sauvegarde minutieuse des nouvelles configurations en cas de perte.
 - Nécessite une synchronisation automatique de la configuration du premier vers le deuxième commutateur de la même « pile ».
 - Coupure du réseau lors de la bascule (à faire lors de périodes de vide de production, lorsque cela n'aura aucun risque sur la production du site).

3.4. Cartographie de la solution d'amélioration

Vous trouverez en pièces jointes à ce livrable dans le dossier « [Annexes > Cartographies > Cartographie de la solution d'amélioration](#) », la cartographie complète de l'infrastructure réseau existante de l'entreprise MédicArgile.



4. Organisation du projet

4.1. Planning organisationnel (3 mois et 6 jours)

La durée de ce projet est estimée à 3 mois et 6 jours, du 9 Décembre 2024 au 16 Mars 2025. De plus, 2 journées seront dédiées au basculement de l'ancienne solution vers la nouvelle.

Le basculement doit impérativement être fait le samedi et le dimanche, sur des jours de creux, afin de ne pas ralentir ou mettre à l'arrêt la production et le travail du personnel MédicArgile.

- Organisation du projet (3 semaines).
- Contact avec les fournisseurs et les prestataires (2 semaines).
- Achats et livraisons des équipements et des licences (4 semaines).
- Déploiement de la solution d'amélioration (1 mois et 6 jours).

Pour le déploiement de la solution, le/les prestataire(s) devront suivre et assurer ces différentes étapes lors de la mise en place :

- Câblage de deux clusters de deux routeurs Cisco.
- Câblage d'un cluster de deux pare-feu Stormshield.
- Copie des configurations des anciens routeurs Cisco vers les nouveaux routeurs primaires des clusters de routeurs Cisco.
- Copie des configurations de l'ancien pare-feu Stormshield vers le nouveau pare-feu primaire du cluster de pare-feu Stormshield.
- Vérification et test de la fonctionnalité des configurations des nouveaux routeurs Cisco.
- Vérification et test de la fonctionnalité des configurations du nouveau pare-feu Stormshield.
- Mise en place du processus de la redondance par le protocole VRRP sur les 2 clusters de routeurs Cisco.
- Mise en place du processus de la redondance par le mode active-passif sur l'interface Web du cluster de pare-feu Stormshield.
- Mise en place du processus de la redondance d'alimentation des pare-feu Stormshield.
- Vérification et test du processus de la redondance de deux clusters de routeurs Cisco.
- Vérification et test du processus de la redondance du cluster de pare-feu Stormshield.
- Vérification et test du fonctionnement de l'interconnexion entre les 2 clusters des routeurs Cisco et le cluster des pare-feu Stormshield.
- Vérification et test du fonctionnement de la redondance des routeurs Cisco.
- Vérification et test du fonctionnement de la redondance du pare-feu Stormshield.
- Vérification et test du fonctionnement de la redondance d'alimentation des pare-feu Stormshield.



- Basculement du réseau actuel (via le switch Cisco Catalyst 3560) de la salle des serveurs vers le nouveau pare-feu primaire du cluster.
 - Basculement des 2 liens FAI vers les nouveaux routeurs primaires des clusters de routeurs.
 - Vérification et test du fonctionnement du réseau avec les 2 nouveaux clusters de routeurs Cisco.
 - Vérification et test du fonctionnement du réseau avec le nouveau cluster de pare-feu Stormshield.
- Accès au support technique, maintenance et mise à jour logicielle des routeurs et commutateurs Cisco et pare-feu Stormshield grâce aux licences (1 an, renouvelable annuellement).

Tâches

Nom	Date de début	Date de fin
Organisation du projet	09/12/2024	27/12/2024
Réunion de la validation des spécifications	09/12/2024	09/12/2024
Appel d'offre à la prestation	10/12/2024	20/12/2024
Rédaction du cahier des charges	10/12/2024	20/12/2024
Entretien pour le choix du/des prestataire(s)	23/12/2024	27/12/2024
Contact avec les fournisseurs	30/12/2024	10/01/2025
Contact avec le fournisseur Cisco	30/12/2024	10/01/2025
Contact avec le fournisseur Stormshield	30/12/2024	10/01/2025
Contact avec les prestataires	30/12/2024	10/01/2025
Achats et livraisons des équipements et licences	13/01/2025	07/02/2025
Achat et livraison des équipements Cisco (routeurs, commutateurs, alimentations, licence)	13/01/2025	07/02/2025
Achat et livraison des équipements Stormshield (pare-feux, alimentations, licences)	13/01/2025	07/02/2025
Achat et livraison d'un lot de 50 câbles RJ45 de 1m et de 2m	13/01/2025	24/01/2025
Achat et livraison de 9 cables d'alimentation basiques	13/01/2025	24/01/2025
Déploiement de la solution d'amélioration	10/02/2025	16/03/2025
Mise en place et recette de tests du cluster de routeurs Cisco	10/02/2025	14/02/2025
Mise en place et recette de tests des clusters de commutateurs Cisco	17/02/2025	28/02/2025
Mise en place et recette de tests du cluster de pare-feux Stormshield	03/03/2025	07/03/2025
Tests de fonctionnalité du déploiement avec le reste du réseau	10/03/2025	14/03/2025
Basculement de l'ancienne solution vers la nouvelle	15/03/2025	16/03/2025
Maintenance du matériels / renouvellement des licences	10/02/2025	06/02/2026
Support technique et maintenance des 2 pare-feux Stormshield	10/02/2025	06/02/2026
Support technique et maintenance des 4 routeurs Cisco	10/02/2025	06/02/2026

Vous trouverez en pièces jointes à ce livrable dans le dossier « Annexes > Planning prévisionnel », le planning prévisionnel complet pour la mise en place de ce projet.



4.2. Ressources du projet

4.2.1. Ressources matérielles

- Synthèse des équipements à acheter pour la mise en place du projet d'amélioration de l'infrastructure :

Référence	Quantité
Cisco C891F-K9	2
Cisco C9200-48P-E	6
Cisco C9200-24P-4X-E	2
Cisco C9200CX-8P-2X2G-E (PoE+)	
Licence Cisco SMARTnet accéléré (applicable sur plusieurs équipements)	1
Stormshield SN-S-Series 320	2
Licence support et maintenance avancée	
NA-SN-S-PWR-EXT (alimentation redondance pare-feu Stormshield)	2
LITEON Power AC adapter 4-PIN	
PA-2121-1-LF 341-0502-01 (alimentation redondance routeur Cisco)	
PWR-C6-1KWAC (alimentation redondance commutateur 48 ports Cisco)	
PWR-C5-600WAC (alimentation redondance commutateur 24 ports Cisco)	
Cable d'alimentation basique pour commutateur, 230V, 2m	10
Prix cables Ethernet, 1m	25
Prix cables Ethernet, 2m	

4.2.2. Ressources Humaines et parties prenantes

- Parties prenantes Internes :
 - Le personnel MedicArgile (chefs d'équipe, ouvriers, etc) : le projet est mis en place afin d'assurer l'accès aux outils nécessaires à leur mission au sein de l'entreprise et afin de protéger leurs données.
 - Directeur général : il autorise les décisions prises à l'égard du projet.
 - Responsable des achats et directrice commerciale et comptables : ils s'occupent de prévoir, d'autoriser et d'effectuer les achats des équipements nécessaires au projet.
 - Community Manager juridique et CM administratif : Ils s'occupent de l'administration, l'autorisation et les droits juridiques qu'entraîne le projet.
- Parties prenantes Externes :
 - Les prestataires externes qui vont nous fournir leurs compétences et leur main d'œuvre afin de mettre en place et d'assurer le projet.
 - Les fournisseurs des équipements nécessaires au projet.
 - Les fournisseurs d'accès à Internet qui nous fournissent leur service d'accès.

4.2.3. Ressources budgétaires et budget prévisionnel

➤ Le budget prévisionnel complet du projet d'amélioration de l'infrastructure :

Référence	Prix (sans)	Prix (avec marge)	Quantité	Durée	Prix avec somme (sans marge)	Prix avec somme (avec marge)	Prix total (sans)	Prix total (avec marge)		
Routeurs FAI et licence										
Cisco C891F-K9	925 €	1 017.5 €	2		1 850 €	2 035 €	27 718.71 €	30 894.581 € *		
Cisco C9200-48P-E	1 155 €	1 270.5 €	6		6 930 €	7 623 €				
Cisco C9200-24P-4X-E	1 035 €	1 138.5 €	2		2 070 €	2 277 €				
Cisco C9200CX-8P-2X2G-E (PoE+)	1 094 €	1 203.4 €			2 188 €	2 406.8 €				
Licence Cisco SMARTnet accéléré (applicable sur plusieurs équipements)	3 018.51 €	3 320.361 €	1	1 an, renouvelable	3 018.51 €	3 320.361 €				
Pare-feu et licence										
Stormshield SN-S-Series 320	2 036.4 €	2 240.04 €	2	1 an, renouvelable	4 072.8 €	4 480.08 €				
Licence support et maintenance avancée	750 €	825 €			1 500 €	1 650 €				
Equipements complémentaires										
NA-SN-S-PWR-EXT (alimentation redondance pare-feu Stormshield)	69,00 €	75.9 €	2		138,00 €	151.8 €				
LITEON Power AC adapter 4-PIN PA-2121-1-LF 341-0502-01 (alimentation redondance routeur Cisco)	26.58 €	29.238 €			53.16 €	58.476 €				
PWR-C6-1KWAC (alimentation redondance commutateur 48 ports)	455 €	500.5 €			910 €	1 001 €				
PWR-C5-600WAC (alimentation redondance commutateur 24 ports)	341.62 €	375.782 €			683.24 €	751.564 €				
Cable d'alimentation basique pour commutateur, 230V, 2m	9 €	9.9€			10	90	99 €			
Prix cables Ethernet, 1m	3 €	3.3 €			25	75 €	82.5 €			
Prix cables Ethernet, 2m	4 €	4.4 €				100 €	110 €			
Prestation et déplacements										
Prestation externe pour la mise en place d'un cluster de routeurs Cisco	750 €	900 €	1	1 semaine maximum	750 €	900 €				
Prestation externe pour la mise en place d'un cluster de commutateurs Cisco	400 €	480 €	5	2 semaines maximum (au total)	2 000 €	2 400 €				
Coût des déplacements de la prestation de l'expert Cisco (sur X semaines)	200 € par semaine	240 € par semaine	1	3 semaines maximum (au total)	600 €	720 €				
Prestation externe pour la mise en place d'un cluster de pare-feux Stormshield	490 €	588 €		1 semaine maximum	490 €	588 €				
Coût des déplacements de la prestation des de l'expert Stormshield (sur X semaines)	200 € par semaine	240 € par semaine		200 €	240 €					
<p>* +10% du prix de base (estimation de la variance du prix du marché des matières premières) * +20% du prix de base (estimation de la variance du prix du marché de la prestation)</p>										

- Prévision budgétaire couvrant les achats matériels TTC et le coût de la prestation et des déplacements :
- Prix total (sans marge) : 27 718.71 € dont 4 518.51 € à renouveler annuellement.
 - Prix total à prévoir (avec marge) : 30 894.581 € dont 4 970.361 € à renouveler annuellement.

Le budget prévisionnel présenté à MedicArgile pour la mise en place de projet, en prenant en charge les marges d'imprévu, est d'un total de 30 894.581€. De plus, l'entreprise devra renouveler annuellement le montant de 4 970.361 € afin de s'assurer le support technique des routeurs et des commutateurs Cisco, ainsi que des pare-feu Stormshield.

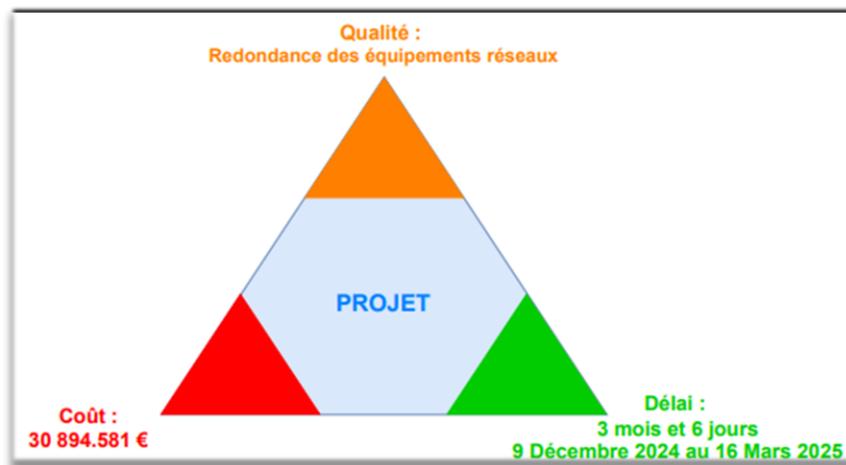


4.2.4. Ressources immatérielles et critères d'évaluation pour les prestataires externes

- La connaissance et les compétences en infrastructure et sécurité réseau.
- La connaissance et les compétences de l'environnement et des interfaces Cisco.
- La connaissance et les compétences de l'environnement et des interfaces Stormshield.

4.3. Triangle qualité, coût, délai

Le triangle qualité/coût/délai est un outil essentiel pour les chefs de projet afin d'assurer la gestion de ce dernier. Il permet de représenter simplement l'état d'un projet en fonction de ces trois éléments clés.



4.4. Livrables, évaluation du prestation et indicateurs de pilotage

- Les prestataires externes devront compléter un livrable sur l'évolution du projet à destination du chef de projet (qui lui, le remontera au directeur général) afin d'assurer l'avancement du projet.
Ce livrable devra s'appuyer sur le planning organisationnel du déploiement des équipements et des logiciels afin de comparer les résultats réels aux résultats préétablis à l'aide de recettes de tests et de documentations.
Les prestataires devront utiliser le support de livrable imposé par l'entreprise, assurer la confidentialité des données et de fournir le ou les livrable(s) à jour hebdomadairement au chef de projet.
Ces derniers devront signer un contrat de confidentialité afin d'assurer la non-divulgence des données de l'entreprise MedicArgile.
- Le chef de projet, quant à lui, veillera à assurer le respect de ces consignes, mais aussi d'assurer le pilotage du projet à l'aide des indicateurs de pilotage suivants :
 - L'écart des coûts de la mise en place de la solution d'amélioration, durant la phase des achats, des livraisons et de la prestation (coûts estimés – coûts réels).
 - L'écart des durées de chacune des étapes du projet, et ce tout au long du projet (durées estimées – durées réelles).

- Les risques et niveaux de priorités de chacune des tâches du projet (utilisation d'une matrice des risques).
 - Les résultats et bons fonctionnements de la mise en place de la solution d'amélioration (% des résultats prédits par rapport au % des résultats obtenus).
 - La satisfaction du client MédicArgile par rapport à ses attentes et à la validation des spécifications (% de la satisfaction prédite par rapport au % de satisfaction obtenue).
- Le prestataire à retenir lors de l'évaluation devra remplir différents points afin d'assurer la bonne mise en place de la solution ainsi que son suivi de progression :
- Au minimum un diplôme de niveau RNCP 5 ou plus (BAC+2 minimum).
 - Les connaissances et compétences en infrastructure et sécurité réseau (particulièrement en routage et sécurité du réseau).
 - Les connaissances et compétences de l'environnement, des commandes et des interfaces Cisco.
 - Les connaissances et compétences de l'environnement, des commandes et des interfaces Stormshield.

