

DATA PROTECT

Security is our **commitment**

*Projet de fin d'étude,
pour l'obtention du titre*

**Ingénieur d'état en
Réseaux et Télécommunications**

Mise en place d'une solution **forcepoint pour la sécurité web à l'aide d'un proxy**

Réalisé par :

RHAZZOUL Hamza

Soutenue le : 26 juin 2019

devant le jury composé de :

Mr. Bentajer Ahmed

Encadrant ENSA

Encadrant

Mr. Choukri Ali

Enseignant chercheur au sein de l'ENSA

Examinateur

Mme. Semlali Hayat

Enseignante chercheuse au sein de l'ENSA

Examinatrice

Mme. Boulahia Chaimaa

Consultante en sécurité informatique à DATA PROTECT

Encadrante

Dédicace

À mes chers parents, Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitte jamais assez. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive. **A ma très chère sœur Marwa,** En témoignage de l'attachement, de l'amour et de l'affection que j'ai pour vous. Je vous dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite.

À toute ma famille, Pour votre véritable et sincère amour. Je vous souhaite une vie pleine de succès avec beaucoup de bonheur et de joie.

À mes chers amis, ceux qui ont partagé mes peines et mes joies, et dans mes instants de faiblesse et de désespoir, et qui n'ont jamais manqué de croire en moi. Merci à tous, car sans vous ce travail n'aurait peut-être pas vu le jour

Rhazzoul Hamza

Remerciement

Dans un projet qui nécessite plusieurs mois de travail, on rencontre des personnes qui nous aident de près ou de loin, nous accompagnent et nous supportent.

Il est donc normal de commencer par remercier toutes les personnes qui ont compté en début de ce projet.

*Mes remerciements vont également vers **Mme. Boulahia Chaimaa**, consultante en sécurité informatique à DATA~~PROTECT~~, qui m'a accueilli en stage. Elle a pleinement contribué à mon intégration rapide et efficace et m'a permis d'évoluer tout au long de mon stage. Son expertise a apporté une grande valeur ajoutée à mon stage et me servira grandement tout au long de ma vie professionnelle.*

*Je remercie également Monsieur **Ali El Azzouzi**, Directeur général de DATA~~PROTECT~~ et Monsieur **Rabii Amzerin** le directeur technique pour leur Accueil et leur confiance".*

Je tiens à exprimer mes remerciements aux membres du jury consacrant leurs efforts et temps pour juger ce travail, ainsi tous ceux et celles qui ont contribué de près ou de loin à l'aboutissement de ce projet.

Mes dernières pensées iront vers mes parents qui m'ont permis de poursuivre mes études jusqu'à aujourd'hui.

Résumé

Abstract

Table des matières

Dédicace	I
Remerciement	II
Résumé.....	III
Abstract.....	IV
Table des matières.....	V
Tables des figures	VIII
Liste des tableaux	X
Tables des acronymes.....	XI
Introduction générale.....	XII
Chapitre 1.....	1
Contexte général du projet	1
1. Présentation de l'organisme d'accueil DATAPROTECT	2
1.1. Présentation de l'entreprise	2
1.2. La mission de l'entreprise	4
1.3. Les activités et projets de DATAPROTECT	4
1.4. Organigramme.....	7
2. Contexte de projet	7
2.1. Contexte générale	Erreur ! Signet non défini.
2.2. Objectif du projet	7
2.2. Planification de la mission.....	8
2.4. Processus de développement	9
3. Conclusion.....	9
Chapitre 2	10
1. Rappel sur les proxys	11
1.1. Définition d'un proxy.....	11
2. Les fonctionnalités de forcepoint.....	11
2.1. Présentation de forcepoint.....	11
2.2. Les principaux rôles de proxy forcepoint.	12
3. Conclusion.....	12
Chapitre 3	13
Définir, Mesurer et Analyser	13
I- Définir	14

1.	Mission du projet	14
2.	Acteur de projet.....	14
3.	Cadrage de la problématique	14
4.	Processus de déroulement de la mission	16
5.	Analyse des risques de la mission	16
II-	Mesurer.....	18
1.	Les différents composants de la solution.....	18
2.	Le fonctionnement de chaque composant de la sécurité web.....	21
2.1.	Networking	21
2.1.1.	Content Gateway :	22
2.1.2.	Network agent :	23
2.2.	Filtering.....	24
2.2.1.	Filtering service :	25
2.2.2.	Policy broker :.....	25
2.2.3.	Policy server :.....	26
2.3.	Authentication	27
2.3.1.	User service	28
2.3.2.	Transparent identification agent.....	28
2.4.	Gestion de la configuration	28
2.5.	Reporting alerting	29
2.5.1.	Log server	29
III-	Analyser	31
1.	Les différents modes de déploiement de proxy.....	31
2.	Analyser la différence entre le proxy explicite et proxy transparent.....	31
2.1.	Déploiement du proxy explicite	31
2.2.	Déploiement du proxy transparent.....	32
IV-	Conclusion	33
	Chapitre 4	34
	Innover	34
1.	Création du LAB pour la mise en place de la solution	35
1.1.	Installation de forcepoint security manager	35
1.2.	Installation de forcepoint web security	39
1.3.	L'active directory.....	40
1.3.1.	Définition de l'active directory	40
1.3.2.	Installation de l'active directory	41
2.	La configuration de forcepoint security manager	43
2.1.	L'ajoute d'un nouvel administrateur réseau	43
2.2.	La création d'un nouveau rôle (engineering delegated)	43
2.3.	Création d'une nouvelle politique.....	45
2.4.	Les types de filtrage	46
2.4.1.	Filtrages par catégorie	46

• Différents types de malwares :	47
2.4.2. Filtrage de protocoles	50
2.4.3. Filtrage d'application cloud.....	51
2.5. Le choix du mode de déploiement de notre proxy.....	52
3. Implémentations et résultats	53
3.1. Définir une politique de sécurité	53
Chapitre 5	57
Contrôler.....	57

Tables des figures

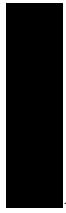
Figure 1 : Principaux pôles d'activités de l'entreprise.....	2
Figure 2 : Les différentes emplacements de DATAPROTECT	3
Figure 3 : Les prestations couvertes par le pôle conseil	4
Figure 4 : les prestations couvertes par le pôle intégration	5
Figure 5 : l'approche de DATAPROTECT	6
Figure 6 : Organigramme de DATAPROTECT	7
Figure 7 : Diagramme de GANTT	8
Figure 8 : Méthodologie de la mission	9
Figure 9 : Cartographie de processus du stage	16
Figure 10 : Déploiement des principaux composants de la protection Web.....	18
Figure 11 : Composants politiques fondamentaux.....	19
Figure 12 : Composants de gestion de base.....	19
Figure 13 : Composants de base du reporting	20
Figure 14 : les composants de la sécurité web.....	20
Figure 15 : les composants de la partie networking.....	21
Figure 16 : les composants de la partie filtering.....	24
Figure 17 : détermination de la politique.	26
Figure 18 : les composants de la partie authentification.....	28
Figure 19 : les composants de la partie management de configuration.....	29
Figure 20 : les composants de la partie reporting.	30
Figure 21 : Forcepoint LAB.	35
Figure 22 : lancement de l'exécutable.	35
Figure 23 : Installation de SQL server.	36
Figure 24 : Installation de Policy server.....	36
Figure 25 : création du compte administrateur.	37
Figure 26 : résumé de l'installation.	37
Figure 27 : Installation des éléments sur la machine FP-SEC-SVR.	38
Figure 28 : la licence de forcepoint security manager.....	38
Figure 29 : le choix du mode sécurité pour cette machine	39
Figure 30 : La configuration de l'adresse IP de l'appliance management.	39
Figure 31 : l'ajoute de l'adresse IP du Policy broker	39
Figure 32 : Vérification de la configuration.	40
Figure 33 : L'installation de l'appliance management.	40
Figure 34 : Installation de l'active directory.....	41
Figure 35 : les utilisateurs de l'active directory.....	41
Figure 36 : l'ajoute de l'actif directory sur forcepoint security manager.....	42
Figure 37 : Création d'un nouvel administrateur réseau.	43
Figure 38 : Création d'un nouveau rôle 'engineering delegated'.	43
Figure 39 : l'attribution de l'administrateur au nouveau rôle.....	44
Figure 40 : l'accès avec le nouvel administrateur	44
Figure 41 : Création d'une nouvelle politique	45
Figure 42 : Application de la politique aux utilisateurs.	45
Figure 43 : Filtrage par catégorie	46
Figure 44 : Filtrage des malwares	47
Figure 45 : Filtrage par Protocol.....	50
Figure 46 : Filtrage par application cloud.....	51

Figure 47 : configuration du proxy explicite.....	52
Figure 48 : Création de la politique pour le test	53
Figure 49 : blocage du réseau social Facebook.....	53
Figure 50 : blocage de YouTube	54
Figure 51 : blocage de monster.fr	54
Figure 52 : blocage des différents malwares	55
Figure 53 : blocage d'un lien de site web malveillant	55



Liste des tableaux

Tableau 1 : Fiche technique de DATAPROTECT	3
Tableau 2 : QQQOCP de la problématique	15
Tableau 3 : Echelle de cotation des risques	17



Tables des acronymes

Introduction générale

Chapitre 1

Contexte général du projet

Dans ce chapitre nous présenterons le contexte général dans lequel s'est déroulé notre projet de fin d'étude. La première partie sera consacrée à un bref aperçu sur la société DATA~~PROTECT~~ et bien que dans la deuxième partie nous présentons le contexte de projet.

1. Présentation de l'organisme d'accueil DATAPROTECT

1.1. Présentation de l'entreprise

DATAPROTECT est une entreprise spécialisée en sécurité de l'information. Fondée par Ali EL AZZOUZI, un expert en sécurité de l'information ayant mené plusieurs projets de conseil et d'intégration de solutions de sécurité au Maroc et à l'étranger,

DATAPROTECT appuie son offre sur une vision unifiée de la sécurité de l'information. DATAPROTECT est dotée d'un réservoir de compétences pointues certifiées en sécurité lui permettant d'assurer une expertise unique sur le marché marocain. DATAPROTECT est organisée autour de 5 pôles d'activités :

- Le conseil : Activité de conseil et d'assistance à maîtrise d'œuvre dans la mise en œuvre de solutions de sécurité.
- L'intégration : Activité de maîtrise d'œuvre complète et d'ingénierie de solutions de sécurité.
- L'infogérance : Activité de supervision et d'administration des équipements de sécurité.
- La recherche et le développement : Activité de veille, de recherche et de développement de nouvelles solutions de sécurité.
- La formation : Activité de transfert de compétences sur des thèmes pointus de la sécurité



Figure 1 : Principaux pôles d'activités de l'entreprise

Voici un petit descriptif sur la société DATA~~PROTECT~~ :

Siège social	Casablanca Nearshore Park - Shore 4, boulevard Al Qods, Sidi Maârouf, 20270 Casablanca - Maroc
Activité	Sécurité informatique
Capital	
Chiffre d'affaire	66 MDH de chiffre d'affaires en 2016
Forme juridique	Société Anonyme
Date de création	2009
Effectif	
Implantation	Pays

Tableau 1 : Fiche technique de DATA~~PROTECT~~

DATA~~PROTECT~~ est partout dans l'Afrique et aussi en France le figure ci-dessous montre les différents emplacements de DATA~~PROTECT~~ :

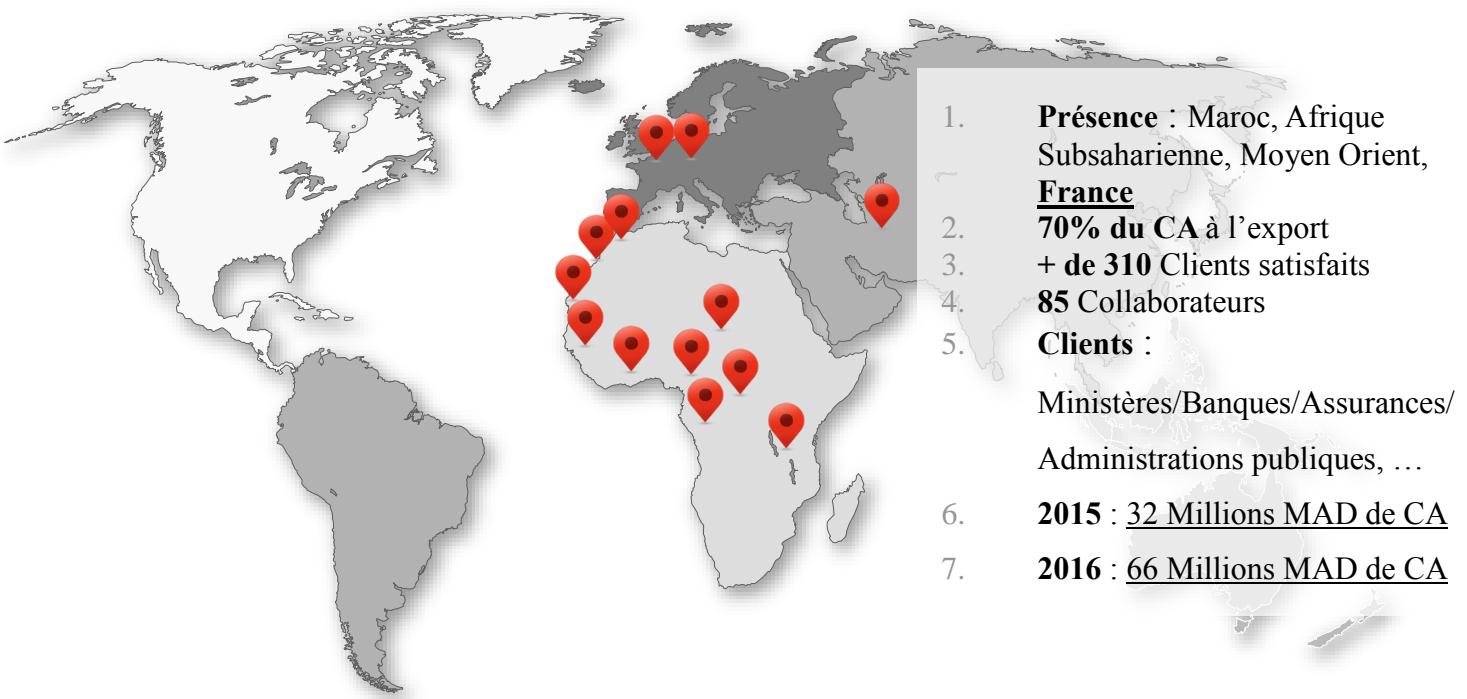


Figure 2 : Les différentes emplacements de DATA~~PROTECT~~

1.2.La mission de l'entreprise

DATAPROTECT a pour mission de faire bénéficier ses clients du retour d'expérience à forte valeur ajoutée de ses équipes. Pour y parvenir, DATAPROTECT s'est lancée, depuis sa création, dans la constitution des équipes composées des ressources certifiées ayant conduit de nombreux projets liés à la sécurité de l'information aussi bien au Maroc qu'à l'étranger. En combinant son expertise pointue au niveau technologique et sa compréhension complète et singulière de la chaîne des menaces informationnelles, DATAPROTECT se donne comme mission de ne fournir que des prestations spécialisées et concentrées uniquement autour de la sécurité de l'information.

1.3.Les activités et projets de DATAPROTECT

- **Le conseil :**

Ayant mené une centaine de missions d'audit de sécurité et de certification des systèmes d'informations pour le compte d'organisations exerçants dans divers domaines d'activités, DATAPROTECT dispose d'un retour d'expérience très riche et varié en la matière. Unique prestataire Marocain autorisé par le consortium PCI SSC à mener des missions de certification PCI DSS, et doté de compétences certifiées en audit de sécurité (CISA, CEH, OSCP, CISSP, Lead Implémenter & Lead Auditor ISO 27001, Risk Manager ISO 27005, PA QSA, PCI QSA, etc...), l'activité conseil de DATAPROTECT couvre les prestations ci-après.



Figure 3 : Les prestations couvertes par le pôle conseil

- **L'intégration :**

De la sécurité périphérique jusqu'à la corrélation des logs de sécurité en passant par la sécurité des postes de travail et des accès distants, divers outils existent sur le marché pour assurer diverses fonctions de sécurité. Fort de son retour d'expérience dans la mise en place de solutions de sécurité, DATA~~PROTECT~~ dispose des ressources qualifiées en intégration de solutions de sécurité des systèmes d'informations, certifiées sur les différentes technologies et solutions : (KASPERSKY, SAFENET, CYBEROAM, BEEWARE, TRIPXIRE, RUCKUS, WEBSENSE, QUALYS, PGP, McAfee, SPLUNK, GALLEON, SYMANTEC, ...)

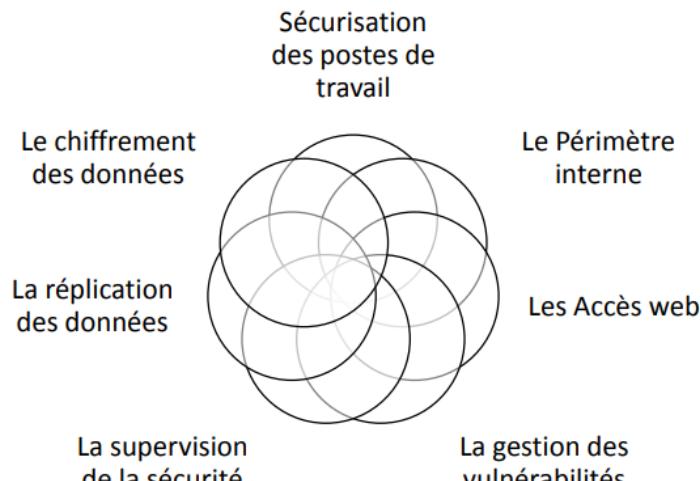


Figure 4 : les prestations couvertes par le pôle intégration

- **L'infogérance**

- Infogérance des solutions de sécurité (Firewall, UTM, IPS/IDS, Gestion des logs, etc.)
- Offre Mars : Maintenance, Administration, Reporting, Supervision.
- Security Operations Center (SOC).
- Management des vulnérabilités.
- Recherche et Développement
 - Développement de solutions sécurisées.
 - Recherches et veille de vulnérabilités.
 - Développement sécurisé des applications souveraines.
 - Recette de sécurité des applications critiques.

● La formation

Destinée aux dirigeants d'entreprises et aux collaborateurs souhaitant appréhender les nouvelles approches en matière de sécurité, les formations proposées par DATAPROTECT sont particulièrement adaptées aux besoins du marché. Leader dans son domaine d'activité, DATAPROTECT dispose de salles parfaitement équipées et d'une équipe de formateurs hautement qualifiés dont la plupart ont acquis une expérience à l'international et sont dotés de certificats reconnus à l'échelle internationale dans le domaine de la sécurité. L'approche de DATAPROTECT est la suivante :

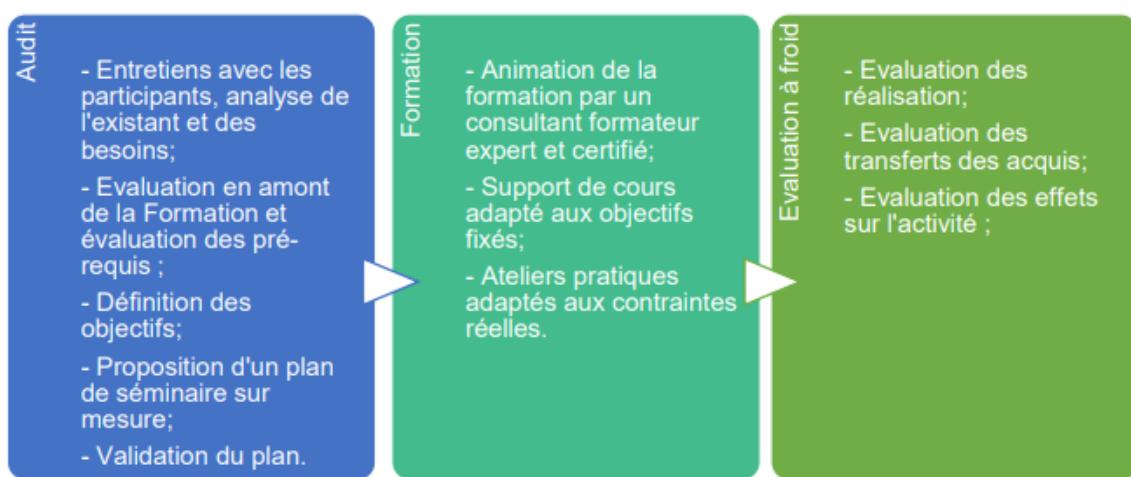


Figure 5 : l'approche de DATAPROTECT

1.4. Organigramme

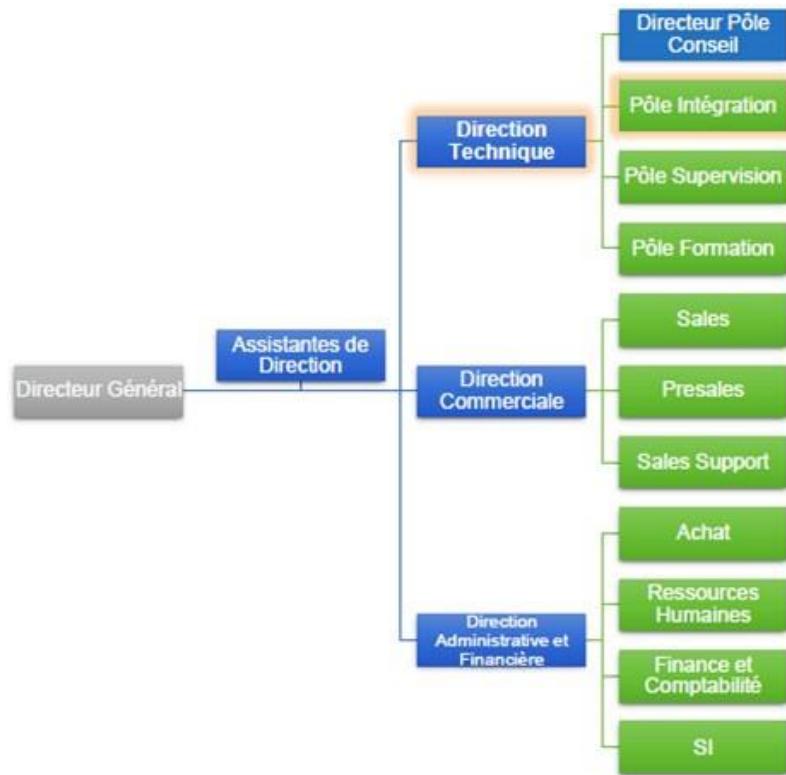


Figure 6 : Organigramme de DATA PROTECT

2. Contexte de projet

2.1. Contexte général

Il existe plusieurs solutions défensives au but d'arrêter les activités des attaquants extérieurs et intérieurs et de protéger la navigation internet des utilisateurs à partir de l'utilisation de web et email en utilisant nombreux solutions défensives, Forcepoint représente l'une des solutions les plus célèbre dans le marché de la sécurité informatique.

2.2. Objectif du projet

Ce projet a pour but d'implémenter une solution de la sécurité web afin de se protéger contre les malwares et tester la performance et l'efficacité de la solution forcepoint, également faire un audit de configuration de la plateforme interne afin de chercher des vulnérabilités.

2.2. Planification de la mission

Un planning avec jalons a été mis en place ci-dessous afin de séquencer les missions principales au cours du déroulement du stage. Ce planning a été soumis pour validation au tuteur et a subi des ajustements au cours de l'avancement du stage. Le planning sous forme de diagramme GANTT, a permis de prévoir les différentes missions définies initialement ainsi que les missions quotidiennes qui sont venues compléter nos missions principales.

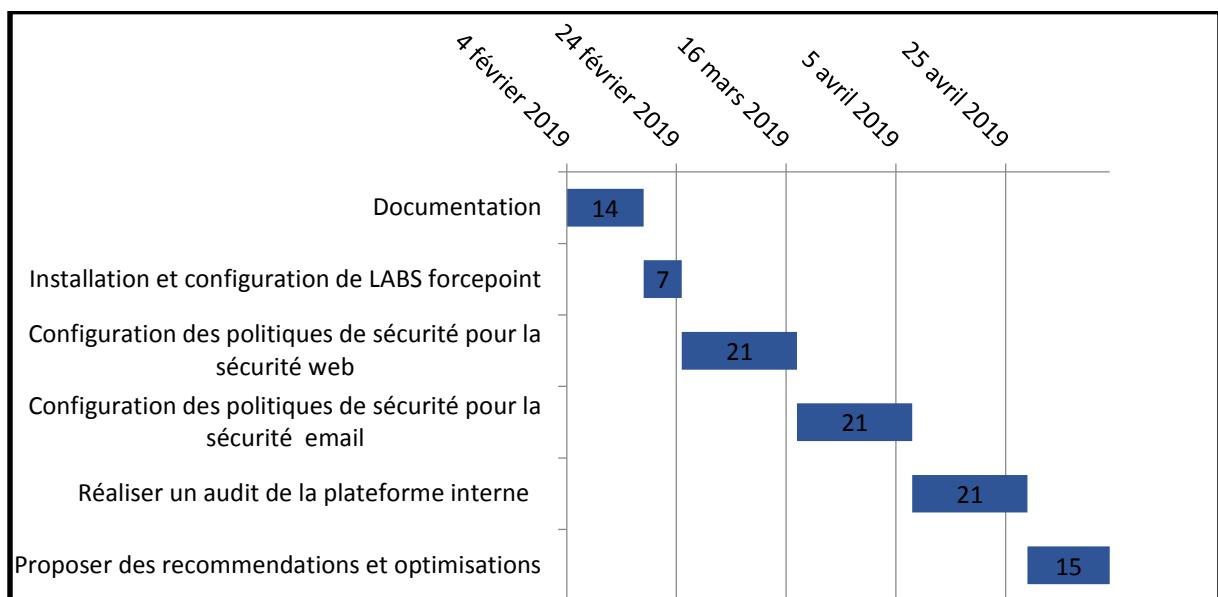


Figure 7 : Diagramme de GANTT

2.4. Processus de développement

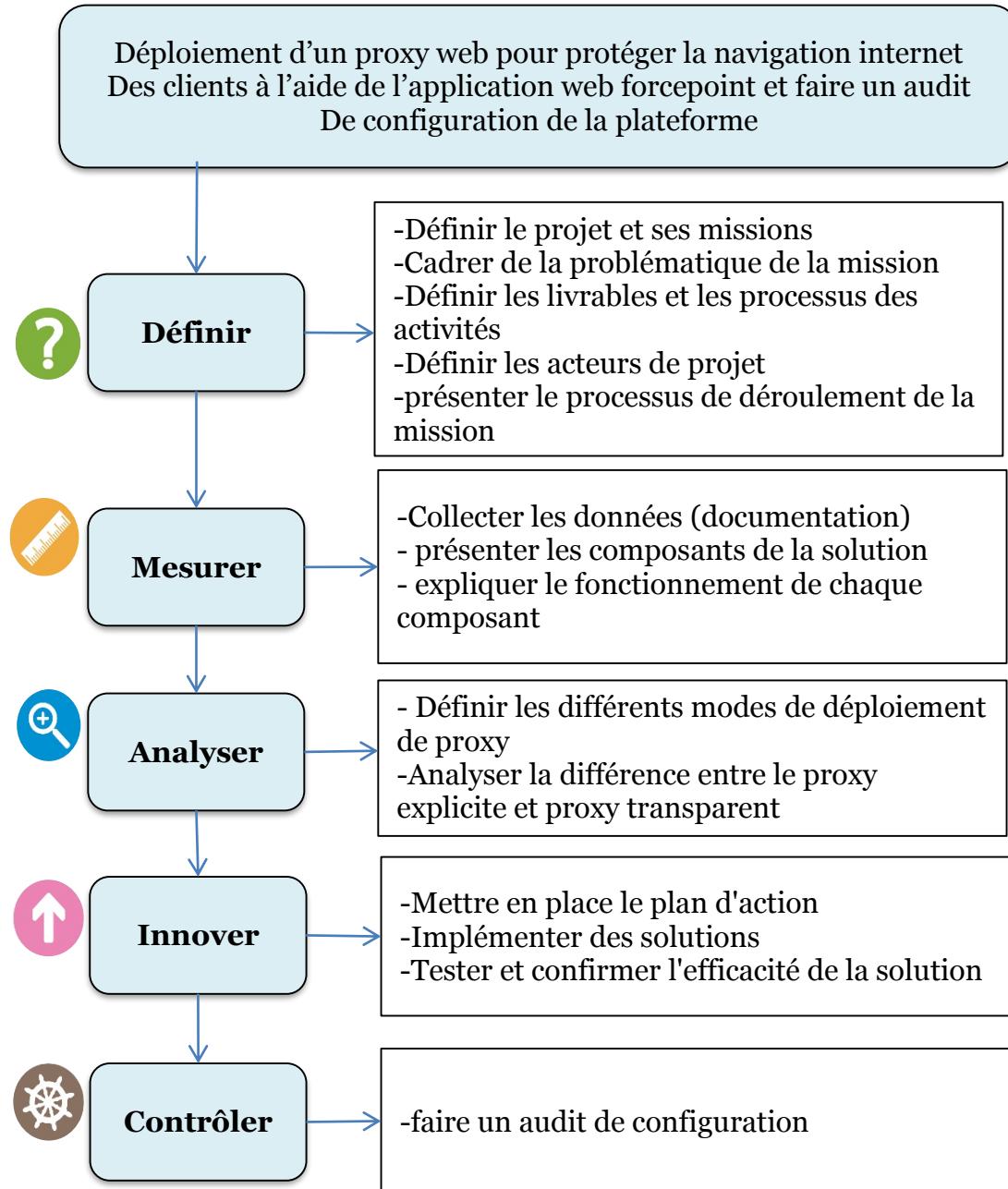


Figure 8 : Méthodologie de la mission

3. Conclusion

Après avoir présenté l'environnement et le contexte du projet et décrit la méthodologie suivie pour atteindre les objectifs suivant le planning qu'on a tracé, Nous allons mettre le point dans les prochains chapitres sur chaque étape de la démarche.

Chapitre 2

Introduction

Dans ce chapitre nous présenterons, une définition de proxy et ses principaux rôles
Et une définition de la société américaine forcepoint et ses produits de sécurité des
systèmes d'information aussi les principaux rôles de proxy forcepoint.

1. Rappel sur les proxys

1.1. Définition d'un proxy

Dans les réseaux informatiques, un serveur proxy est un serveur (un système informatique ou une application) qui sert d'intermédiaire pour les demandes des clients qui recherchent des ressources auprès d'autres serveurs. Un client se connecte au serveur proxy en demandant un service, tel qu'un fichier, une connexion, une page Web ou une autre ressource disponible sur un serveur différent, et le serveur proxy évalue la demande comme un moyen de simplifier et de contrôler sa complexité. Les mandataires ont été inventés pour ajouter une structure et une encapsulation aux systèmes distribués.

1.2. Le rôle d'un proxy

- **La protection :** il vous autorise à vous connecter à l'extérieur et interdire les ordinateurs d'Internet de se connecter sur le vôtre. Cette fonction de protection du proxy est souvent incluse dans les pare-feu des ordinateurs programmés pour filtrer les communications entre les réseaux.
- **L'anonymisation :** lors de votre navigation sur internet, tous les sites Web peuvent connaître de quel site vous venez, depuis quel navigateur vous venez de se connecter, quel est votre système d'exploitation, votre adresse IP... Certains proxys masquent ces informations. Ces proxys sont dits proxys anonymes.
- **La mémorisation des pages web :** lorsque vous demandez plusieurs fois la page <http://www.facebook.com>, donc automatiquement le proxy vous la donnera la page sans aller la chercher. Cela peut accélérer les choses. Il s'appelle alors *proxy-cache*.

2. Les fonctionnalités de forcepoint

2.1. Présentation de forcepoint

Forcepoint est une société fondée en 1994, Il développe et commercialise des logiciels de cybersécurité pour empêcher les employés de visualiser des contenus inappropriés ou malveillants, ou de divulguer des données confidentielles. Elle vend également des produits de pare-feu, d'accès au cloud et de sécurité informatique inter-domaines.

2.2. Les principaux rôles de proxy forcepoint.

Les produits de la société sont utilisés pour bloquer certains sites Web, ou seulement certaines parties d'un site Web [inspecter](#) le trafic réseau, filtrer les e-mails. Et contrôle où les fichiers sensibles sont accessibles. Les produits Forcepoint peuvent également être utilisés pour empêcher les employés d'accéder à des sites Web jugés inappropriés pour être visualisés sur leur lieu de travail par leur employeur. Par exemple, les employeurs peuvent empêcher les employés d'afficher du contenu pornographique au travail ou des informations relatives à l'éducation sexuelle, à la religion, aux rencontres ou à la politique.

Lors de l'utilisation des produits Forcepoint, les navigateurs Internet des employés sont généralement modifiés pour diriger tout le trafic vers un serveur proxy. Ce serveur héberge des copies locales des sites Web fréquemment visités, afin d'accroître la vitesse de téléchargement. Le logiciel vérifie également chaque adresse URL visitée par l'employé par rapport aux bases de données de sites Web identifiés comme des logiciels malveillants ou un objet interdit. L'historique des URL d'employé peut être analysé pour identifier les comportements à risque.

3. Conclusion

Chapitre 3

Définir, Mesurer et Analyser

Ce chapitre est dédié à définir les éléments en rapport avec la problématique en faisant appel aux différents outils, suivie par l'étape mesurer qui consiste à collecter les informations et diagnostiquer l'état actuel puis analyser les résultats trouvés.

I- Définir

1. Mission du projet

Selon le cahier de charge les missions du stage sont :

-Déploiement d'un proxy web pour protéger la navigation internet des clients à l'aide de l'application web forcepoint

-Installation du LAB

-Mise en place de la solution forcepoint

-Configuration avancée de la solution forcepoint

-Tester les performances de la solution

-Faire un audit de configuration de la plateforme

2. Acteur de projet

-Pilotes projet : RHAZZOUL Hamza

-L'encadrante de stage : BOULAHIA Chaimaa

-L'encadrant pédagogique : Mr. BENTAJER Ahmed

-Le Team support

3. Cadrage de la problématique

Après avoir clarifié le projet, il a fallu déterminer au mieux le problème qui se posait. Pour ce faire, L'outil QQOCP, présenté dans le tableau 3, nous a été utile dans cette démarche.

Qui ? Qui est concerné ?	- Demandeur : DATA <color>PROTECT</color> .
Quoi ? Quel est le problème ?	-Nouvelles activités avec des déficits : Traiter la problématique des proxy web afin de protéger la navigation internet des utilisateurs à l'aide de l'application web forcepoint et faire un audit de la plateforme.
Où ? Où apparaît ce problème ?	Activités : Intégration et support.
Quand ? Quand a lieu le projet ?	Durant la période de stage (du 04 Février au 04 aout 2019)
Comment ? Comment réaliser le projet ?	A partir : <ul style="list-style-type: none"> - Des informations requises pendant les formations. - Recensement, compréhension, et l'analyse de la documentation des activités. -L'assistance aux tâches quotidiennes des consultants. -Mise en place de la solution. -le suivi et accompagnement les consultants dans leur application des plans d'actions.
Pourquoi ? Quels enjeux poussent à réaliser ce projet ?	-Protection de la navigation internet des clients contre les menaces potentielles et les contenus malveillants

Tableau 2 : QQOCP de la problématique

4. Processus de déroulement de la mission

Afin d'avoir une lecture synthétique, la méthodologie de la mission est représentée par une cartographie du processus applicable au projet de stage.

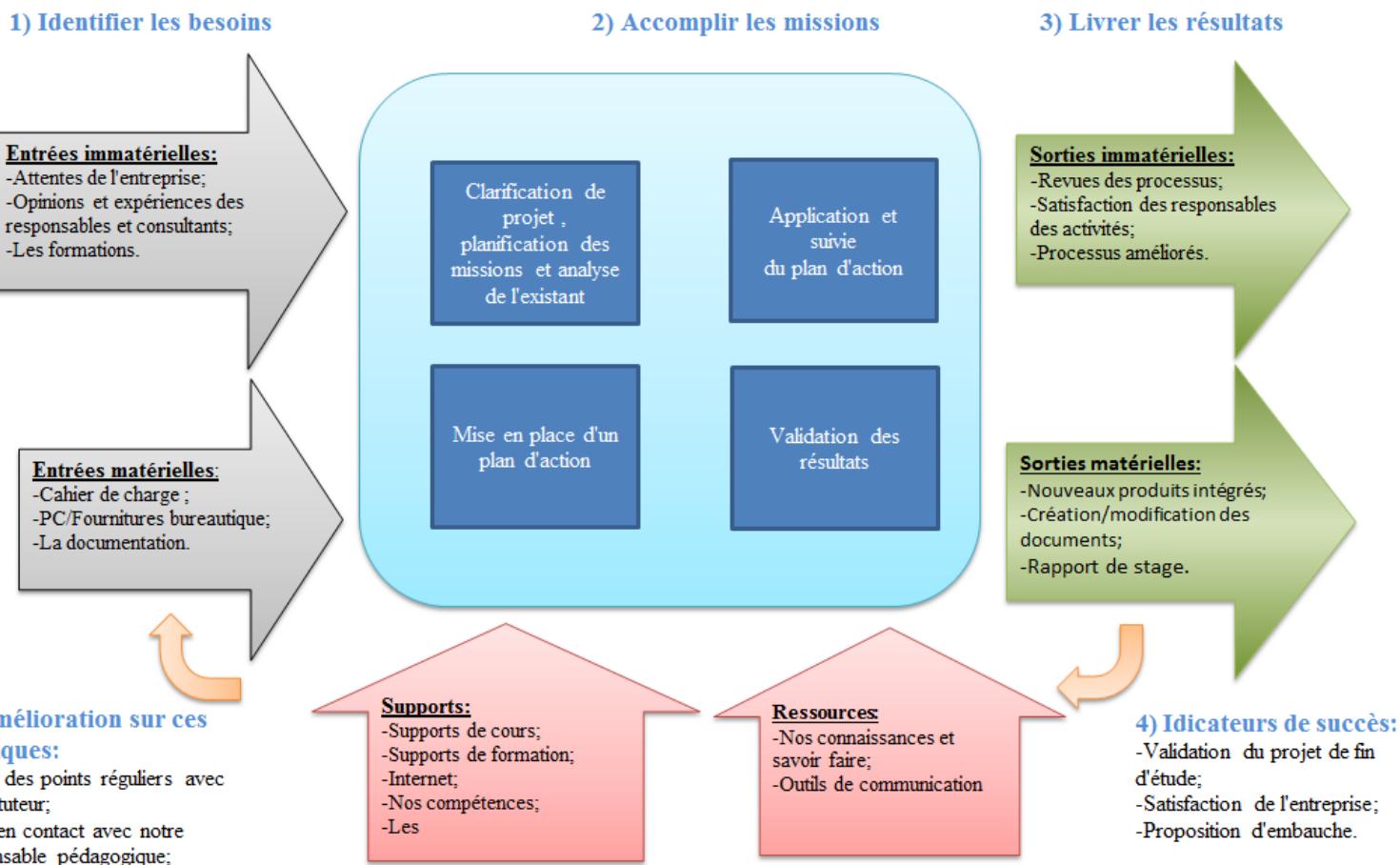


Figure 9 : Cartographie de processus du stage

5. Analyse des risques de la mission

Pour faire face aux risques qui pourraient entraver le bon déroulement du projet, une analyse de risque est nécessaire pour mener des actions préventives de sorte à mieux se préparer ou à réduire les chances qu'ils se produisent.

Pour rendre l'étude homogène, la criticité des problèmes de tous les éléments du projet sera évaluée suivant une même échelle de cotation, à partir de deux critères indépendants (Probabilité, Gravité) auxquels nous associons des échelles de cotation définies selon quatre niveaux :

		Probabilité			
		TRES IMPROBABLE	IMPROBABLE	PROBABLE	TRES PROBABLE
Gravité	MAJEUR	4	8	12	16
	IMPORTANTE	3	6	9	12
	MODEREE	2	4	6	8
	MINEURE	1	2	3	4
Risque	3	Risque inacceptable (Prioritaire)			
	2	Risque moyennement acceptable (à diminuer)			
	1	Risque acceptable (à surveiller)			

Tableau 3 : Echelle de cotation des risques

La mise en application de cette démarche est présentée dans le tableau dans l'annexe I.1. Les différents risques identifiés et priorisés permettent de réfléchir à des plans d'action à mettre en place pour réduire l'impact associé. Ainsi, on a mis en place des plans d'action pour contrôler les risques du projet. Et durant notre période de stage on était face à plusieurs problèmes dont on a pu remédier grâce à cette analyse.

II- Mesurer

1. Les différents composants de la solution

Les solutions de protection Web sur site incluent les composants principaux de stratégie, de gestion et de création de rapports illustrés dans le diagramme ci-dessous :

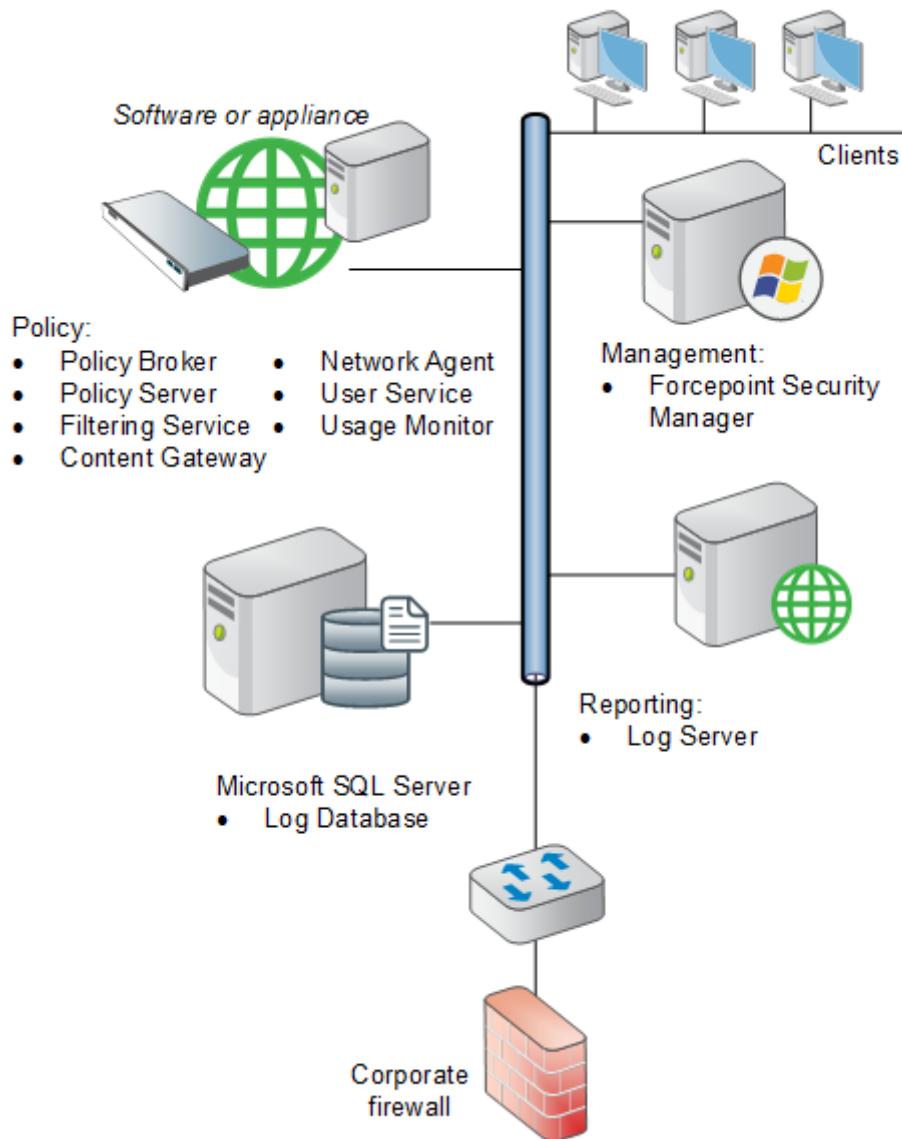


Figure 10 : Déploiement des principaux composants de la protection Web.

Le diagramme ci-dessus se compose de 3 grandes parties :

- Composants politiques fondamentaux.
- Composants de gestion de base.
- Composants de base du reporting

Qui à leur tour se composent de :

- Composants politiques fondamentaux :



Core policy components:

- Policy Broker
- Policy Server
- Filtering Service
- Content Gateway
- Network Agent
- User Service
- Usage Monitor

Figure 11 : Composants politiques fondamentaux.

- Composants de gestion de base :



Core management components:

- Forcepoint Security Manager
- Web module

Figure 12 : Composants de gestion de base.

- Composants de base du reporting



Reporting:
• Log Server



Microsoft SQL Server
• Log Database

Figure 13 : Composants de base du reporting

On va bien définir et expliquer les rôles des différents composants avec une architecture bien simplifié.

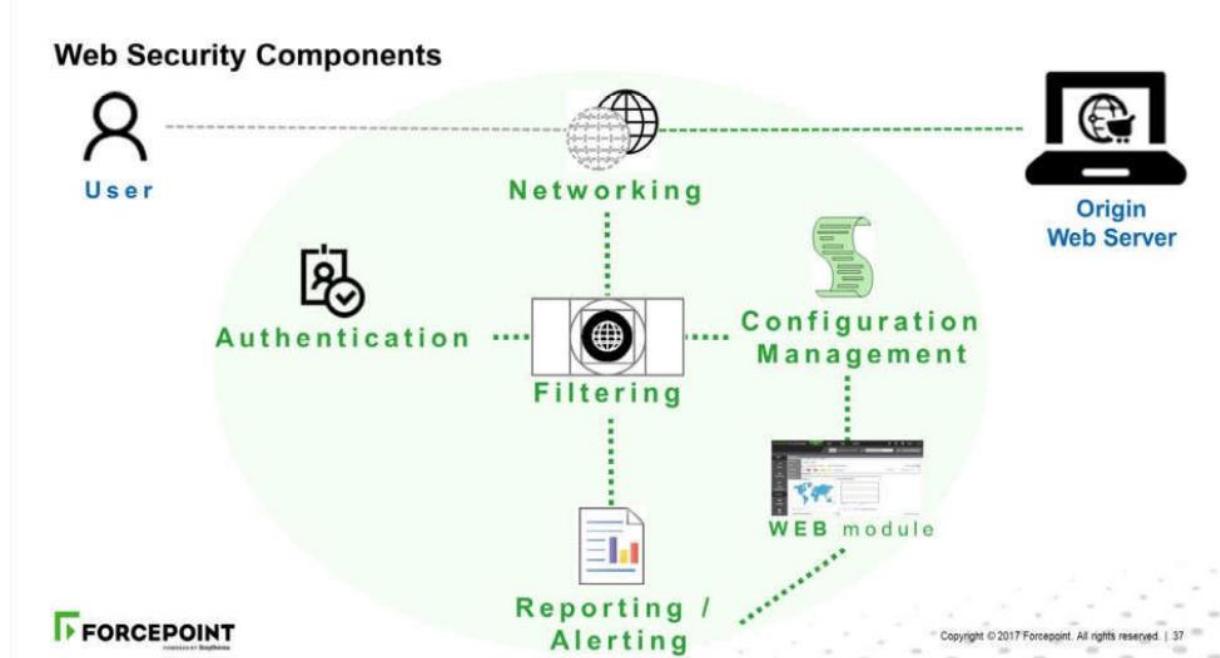


Figure 14 : les composants de la sécurité web.

Notre architecture de la sécurité web se compose de 5 composants :

- Networking
- Filtering
- Authentication
- Reporting alerting
- Configuration management

2. Le fonctionnement de chaque composant de la sécurité web.

On utilise la sécurité web pour développer la politique de sécurité afin de protéger notre réseau, une série de composants de forcepoint assure la sécurité des transaction web, le management, l'identification de l'utilisateur, les alertes et les rapports, donc on va définir chaque composant et de quoi il se compose :

2.1. Networking

Représente un facteur important et joue un rôle essentiel dans le fonctionnement de notre architecture, il transmet le trafic web à l'utilisateur final et au serveur d'origine pour appliquer les décisions de sécurité et de stratégie à l'aide d'un filtre, et effectue un décryptage SSL.

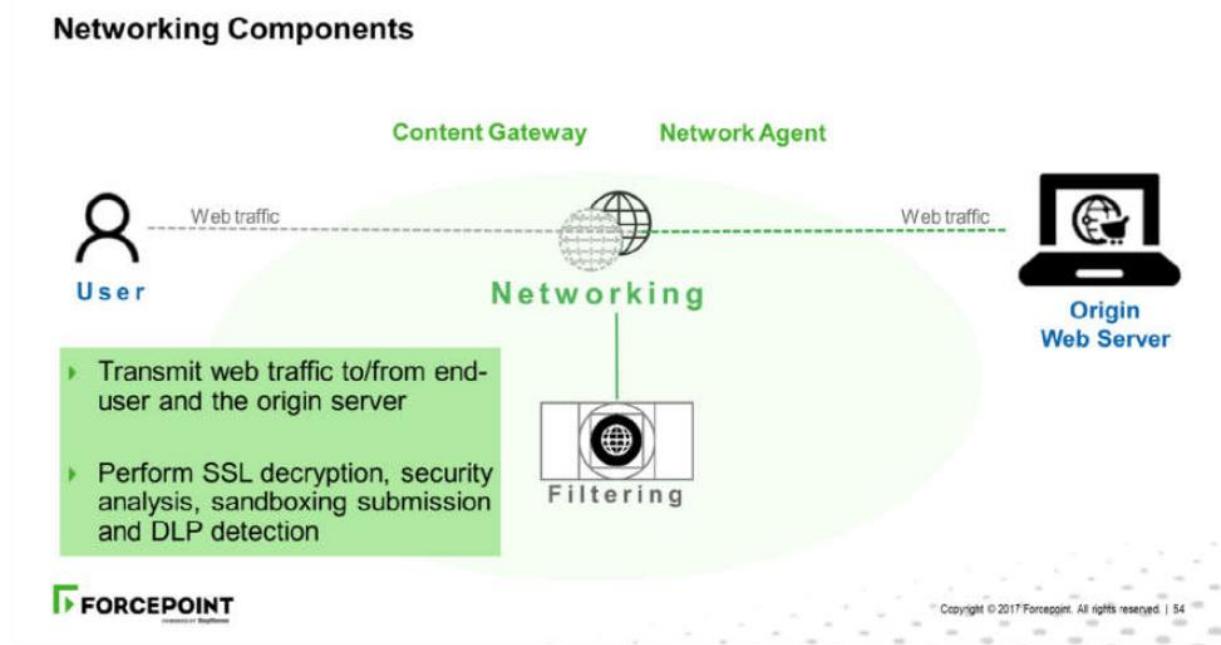


Figure 15 : les composants de la partie networking.

Content Gateway est un composant obligatoire de la sécurité Web Forcepoint. Network agent, d'autre part, est largement utilisé dans le produit de filtrage Web hérité, qui exclut les fonctionnalités de proxy

Networking se compose de 2 parties :

2.1.1. Content Gateway :

- Un proxy par lequel les clients se connectent au contenu Web. Content Gateway Forcepoint s'intègre à la sécurité Web Forcepoint afin d'accroître encore le niveau de sécurité du Web. Content Gateway forcepoint offre une visibilité sur le trafic Web crypté SSL, afin d'empêcher tout contenu malveillant de pénétrer sur le réseau. Il permet également de catégoriser en temps réel le contenu dynamique du Web 2.0 et d'identifier les sites précédemment non consultés susceptibles de n'exister que pendant une très courte période, tels que ceux utilisés pour les attaques de phishing et les sites Web d'évitement de proxy.
- Avant la sortie de Forcepoint Web Security Gateway, le produit de sécurité Web intégré aux mandataires produits par d'autres fournisseurs (par exemple le serveur ISA de Microsoft). Ces intégrations sont toujours prises en charge, mais forcepoint recommande l'utilisation de la suite de produits complète, car les autres mandataires ne fournissent pas l'analyse en temps réel offerte par content Gateway de forcepoint.
- Content Gateway est un proxy direct qui effectue une analyse de contenu avancée au fur et à mesure que le contenu passe par le proxy. Il s'agit de l'homme de milieu pour les textes clairs et le trafic chiffré. Content Gateway intercepte et analyse le trafic Web avant de le transmettre aux clients demandeurs ou aux serveurs d'origine qui répondent. Avec la sécurité Web, Content Gateway fournit :
 - L'analyse des requêtes proxy http, https et ftp.
 - L'analyse des demandes et des réponses en temps réel pour détecter les menaces potentielles.
 - La détection des protocoles entrants et sortants tunnels sur http et https et application de la mise en application de stratégies basées sur des protocoles
 - L'utilisation des signatures.

- L'analyse de fichier avancée pour détecter et bloquer le téléchargement de fichiers infectés ou malveillants.

2.1.2. Network agent :

- Network agent agit comme un renifleur de paquets, en utilisant la méthode promiscue pour capturer et analyser les paquets. Bien qu'il ne s'agisse pas d'un composant obligatoire, il offre une sécurité considérablement améliorée
- Surveille le réseau pour identifier le trafic de protocole non Web. Une fois identifié, cela peut être filtré par la sécurité Web Forcepoint.
- Les considérations suivantes concernent le déploiement du network agent :
 - Doit être déployé de manière à voir tout le trafic Internet interne des machines qu'il doit surveiller.
 - Peut être installé sur une machine dédiée pour augmenter le débit global.
 - Doit avoir une visibilité bidirectionnelle sur le trafic Internet pour permettre le blocage des demandes.
- Plusieurs instances du network agent peuvent être nécessaires dans des réseaux plus grands ou distribués. Chaque network agent doit être affecté à une plage d'adresses IP ou à un segment de réseau spécifique. L'utilisation de plusieurs network agent permet de surveiller facilement tout le trafic réseau et de répartir la charge sur plusieurs hôtes. L'utilisation de plusieurs network agent garantit la surveillance de tout le trafic réseau et évite la surcharge du serveur.
- Le nombre requis du network agent dépend de la taille du réseau et du volume des demandes Internet.
- Network agent peut généralement surveiller 50 Mbits de trafic par seconde, soit environ 800 requêtes par seconde. Le nombre d'utilisateurs que network agent peut surveiller dépend du volume de demandes Internet de chaque utilisateur, de la configuration du réseau et de l'emplacement du network agent par rapport aux ordinateurs qu'il est chargé de surveiller. Network agent fonctionne mieux lorsqu'il est proche de ces ordinateurs.
- Jusqu'à quatre network agent peuvent être déployés par filtering service. Filtering service peut gérer plus de quatre network agent, en fonction du nombre de demandes Internet.

- En mode intégré, sa fonction est de couvrir les protocoles non http et les protocoles tunnalisés. Network agent étend l'analyse aux protocoles qui ne peuvent pas être proxy. Network agent est capable de visualiser et d'analyser le contenu du protocole, il ne s'agit donc pas uniquement de réagir au port utilisé comme un pare-feu.
- Network agent peut être déployé avec les composants de filtrage ou sur un ordinateur séparé.
- Network agent ne doit pas être déployé sur le même ordinateur que les composants critiques

2.2. Filtering

Les composants de filtrage encapsulent tous les processus décisionnels de la sécurité Web. Ils prennent la stratégie Web de l'entreprise configurée par un administrateur de Forcepoint et l'appliquent à chaque transaction Web. Ils communiquent la décision avec les composants réseau pour appliquer la décision de politique.

Filtering service interagit avec les composants d'authentification pour garantir l'application des stratégies basées sur l'utilisateur

Les composants de filtrage fonctionnent avec les composants de rapport pour enregistrer toutes les activités Web

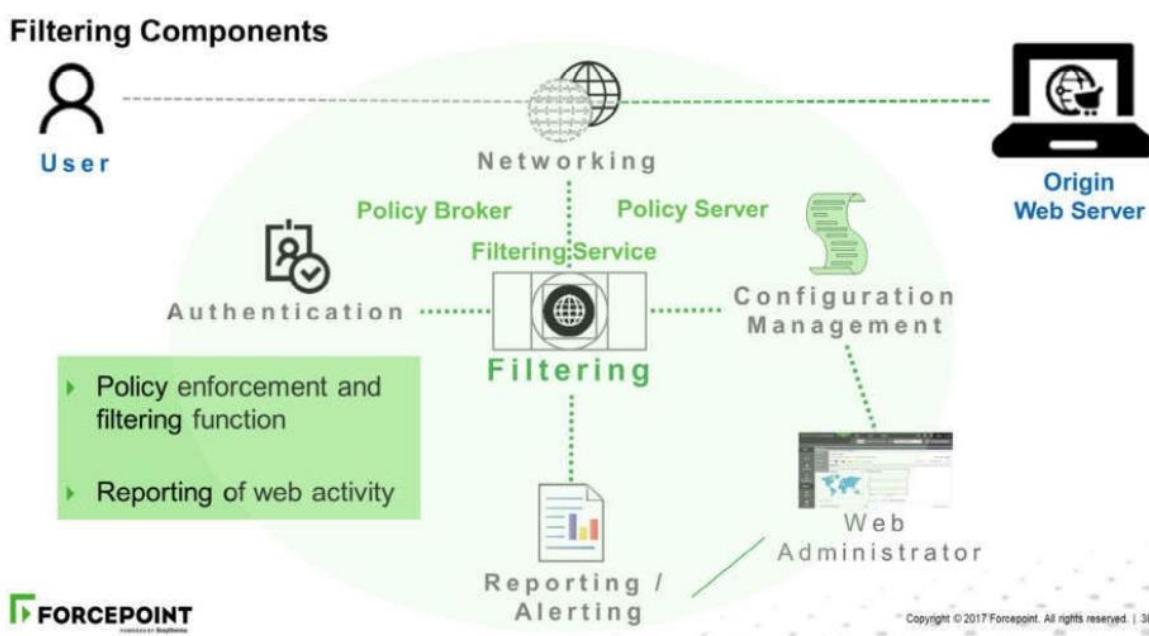


Figure 16 : les composants de la partie filtering.

La partie filtering se compose de 3 grandes parties :

2.2.1. Filtering service :

- Fournit l'application de la politique dans votre réseau
- Lorsqu'un utilisateur demande un site, filtering service est responsable de recevoir la demande et de déterminer la stratégie applicable. Le service de filtrage doit être en cours d'exécution pour que les demandes Internet soient filtrées et journalisées.
- Filtering service est le composant qui fonctionne avec content Gateway, network agent ou un produit d'intégration à des tiers, pour assurer l'application des règles. Lorsqu'un utilisateur demande un site, filtering service reçoit la demande, détermine la politique à appliquer et utilise la politique applicable pour déterminer si le site est autorisé ou bloqué
- Chaque instance de filtering service télécharge sa propre copie de la base de données maître Forcepoint à utiliser pour déterminer comment gérer les demandes Internet
- Filtering service envoie également des informations sur l'activité Internet au serveur de journalisation afin qu'il puisse être un enregistreur et utilisé pour les rapports.
- Filtering service assure la mise en application des stratégies sur votre réseau. Ce service fonctionne conjointement avec un agent de réseau ou un produit d'intégration pour fournir un filtrage Internet. Lorsqu'un utilisateur demande un site, filtering service est responsable de recevoir la demande et de déterminer la stratégie applicable. Filtering service doit être en cours d'exécution pour que les demandes Internet soient filtrées et journalisées.

2.2.2. Policy broker :

- Chaque déploiement de protection Web Forcepoint doit inclure une Policy source. Il s'agit d'une appliance ou d'un autre serveur qui héberge au moins deux composants : Forcepoint policy broker et Forcepoint policy database (policy server doit également être présent ; des composants supplémentaires sont souvent installés). Tous les autres appareils Forcepoint ou autres serveurs pointent vers cette machine et en reçoivent des mises à jour régulières.

- Policy Broker est le composant qui contrôle l'accès aux informations de configuration globale et aux données de stratégie utilisées par d'autres composants. Policy Broker peut être déployé dans une configuration autonome ou dans une configuration répliquée. Policy broker gère les demandes des composants de forcepoint pour la politique et les informations de configuration générales.

2.2.3. Policy server :

- Policy Server est responsable de l'identification des autres composants de sécurité Web et du suivi de leur statut.
- De nombreux environnements ne requièrent qu'un seul policy server. Un seul policy server peut communiquer avec plusieurs instances de filtering server et d'instance de network agent pour l'équilibrage de la charge. Dans les très grandes organisations (plus de 10 000 utilisateurs), il peut toutefois s'avérer utile d'installer plusieurs instances de policy server. Si vous installez des policy server supplémentaires, ajoutez chaque instance au module Web.
- Les règles et la plupart des paramètres de configuration sont partagés entre les policy server partageant une policy database.

Le diagramme illustre comment la détermination de la politique est réalisée grâce à l'interaction entre le filtering service et d'autres composants de forcepoint :

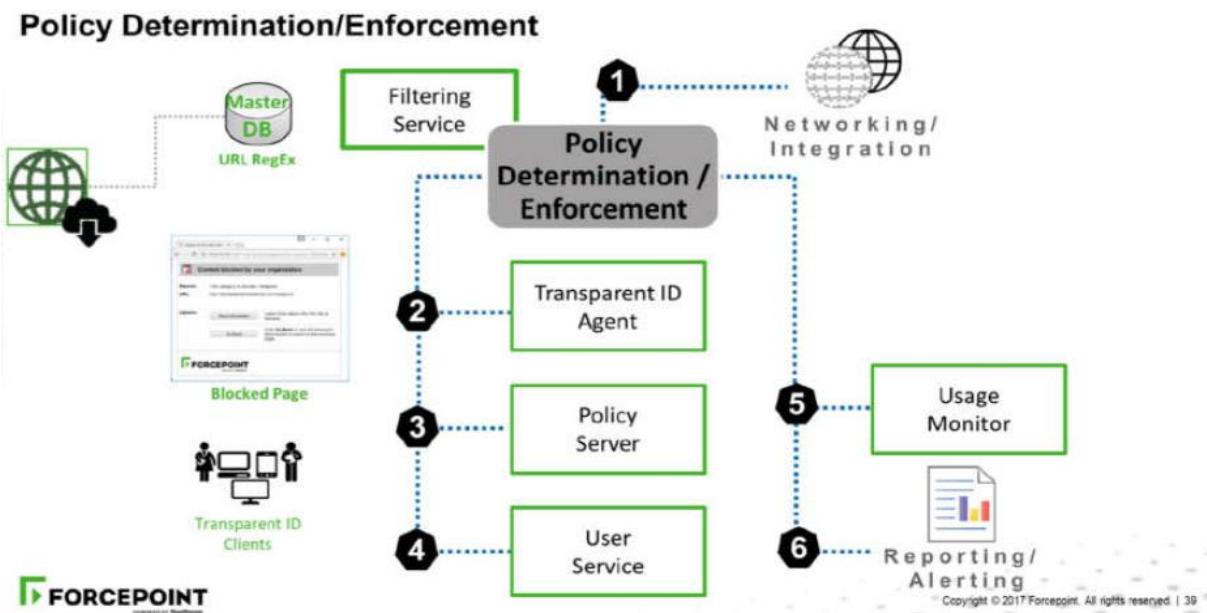


Figure 17 : détermination de la politique.

- 1- les composants d'intégration / réseau capturent une demande d'accès Web
- 2- l'agent d'identification transparent (s'il est utilisé) fournit à l'utilisateur le mappage d'adresse IP, ce qui permet d'appliquer des stratégies basées sur l'utilisateur et le groupe
- 3- Policy server / policy database contient les paramètres de filtre et de stratégie - ceux-ci sont mis en cache par le filtering service et mis à jour si des paramètres sont modifiés et validés (à l'aide du bouton Enregistrer tout)
- 4- le filtering service communique avec le service utilisateur pour déterminer (et mettre en cache) les appartенноances à un groupe
- 5- le filtering service partage les informations avec le moniteur d'utilisation pour les alertes d'utilisation de catégorie, de protocole ou d'application, puis fournit des informations aux composants de création de rapports / d'alerte applicables.
- 6- le filtering service fournit des informations au service de serveur de journalisation

2.3. Authentication

Les composants d'authentification garantissent l'application effective des stratégies basées sur l'utilisateur. Son principal rôle est d'authentifier les utilisateurs et les mapper vers la structure organisationnelle. Deux modules remarquables effectuant des fonctionnalités d'authentification sont user service et transparent identification agent (ou agents XID)

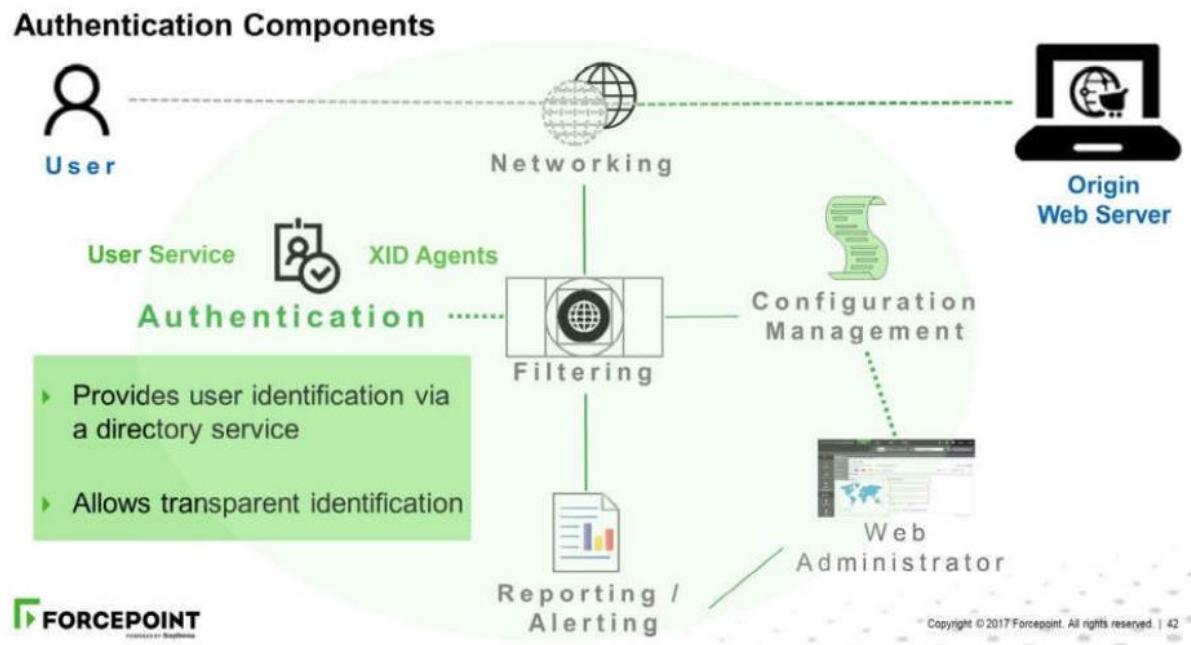


Figure 18 : les composants de la partie authentification.

2.3.1. User service

Fournit l'identification de l'utilisateur sur votre réseau. Ce service communique avec le service d'annuaire de l'organisation pour transmettre des informations relatives à l'utilisateur au policy broker et au filtering service, afin de les utiliser dans l'application de stratégies de filtrage. Ces informations utilisateur incluent les relations utilisateur à groupe et utilisateur à domaine.

2.3.2. Transparent identification agent

Fournit une option permettant d'obtenir de manière transparente et de fournir une adresse IP client en résolution de nom d'utilisateur indépendante des autres mécanismes d'authentification. Les agents XID fournissent un mappage des adresses IP des clients aux entrées de nom d'utilisateur afin de filtrer le service en vue de l'application des stratégies basées sur les utilisateurs et les groupes.

2.4. Gestion de la configuration

Ces composants fournissent à l'administrateurs du produit forcepoint un moyen de configurer le produit qui comprend les stratégies, les paramètres auxiliaires et les options associées, ces composants fournissent également le mécanisme de répartition de la configuration vers la partie mise en réseau et filtrage.

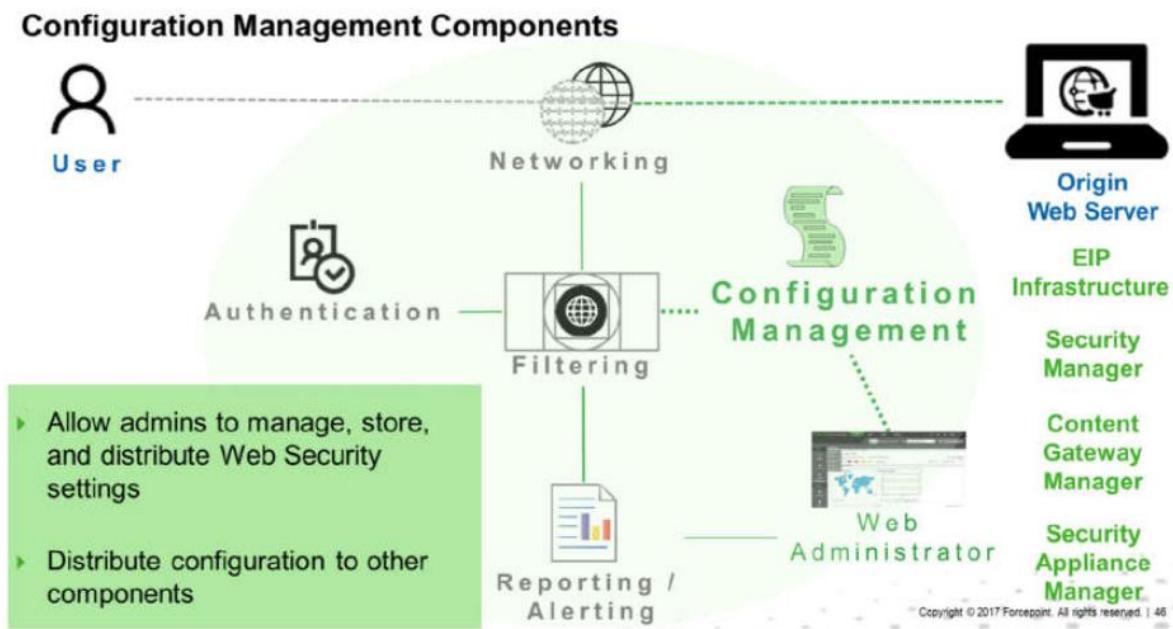


Figure 19 : les composants de la partie management de configuration.

Les composants de management de configuration fournissent les fonctionnalités suivantes :

- Permettre à plusieurs composants de sécurité Web déployés sur différents hôtes de partager un seul référentiel de données de stratégie et de configuration
- Séparer les données de configuration de politique et de déploiement logiquement et physiquement
- Prendre en charge les appels simultanés pour les données, maintenir le contrôle d'accès et l'intégration référentielle, et éviter la corruption des données
- Soutenir l'administration déléguée

2.5. Reporting alerting

Ces composants autorisent et permettent aux administrateurs d'analyser les activités web de leur utilisateur final, cela comprend les tableaux de bord, les rapports et le moniteur en temps réel.

2.5.1. Log server

- Le log server de journalisation est un composant Windows uniquement requis pour activer les fonctionnalités de création de rapports de Security Manager (y compris les graphiques, les rapports de présentation et les rapports d'enquête).
- Avant de pouvoir installer ce composant, Microsoft SQL Server ou Microsoft SQL Server Express doit être installé.
- Le serveur de journalisation offre les fonctionnalités suivantes :

- Reçoit les journaux du service de filtrage
- Crée des fichiers de cache pour les insérer plus tard dans le SQL
- Interagit avec SQL
- Envoie des enregistrements d'activité Internet à la base de données de journal, y compris les noms de catégorie, le nom de protocole et les noms de classe de risque de la base de données principale à la base de données de journal

Reporting / Alerting Components

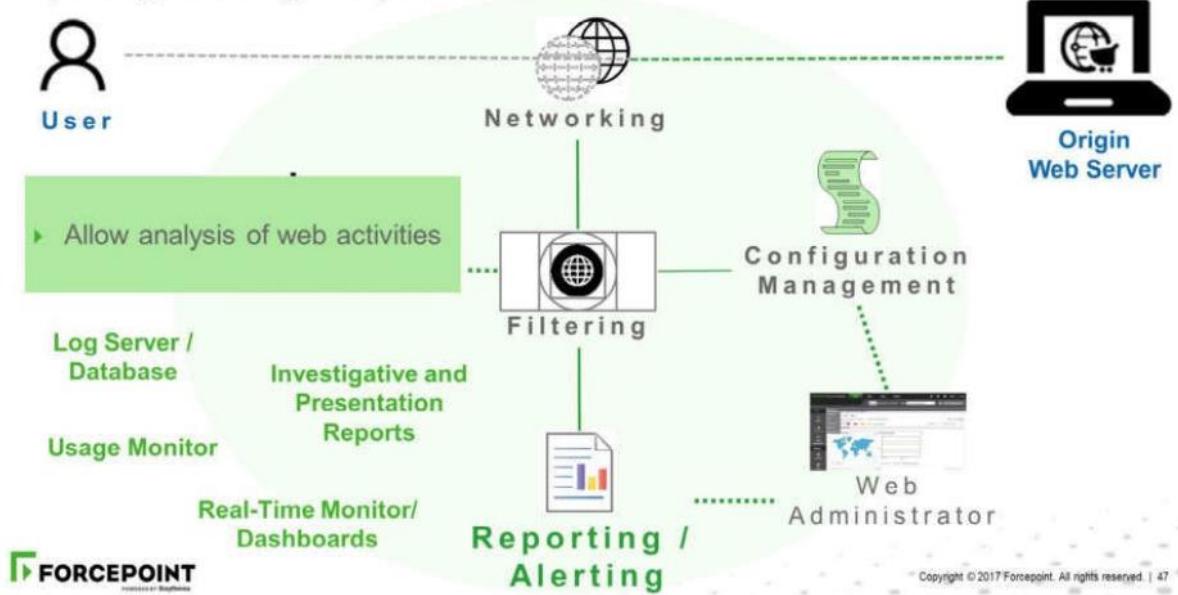


Figure 20 : les composants de la partie reporting.

III- Analyser

1. Les différents modes de déploiement de proxy

Le proxy fournit les options de déploiement suivantes :

Déploiement de proxy explicite, où le logiciel client de l'utilisateur est configuré pour envoyer des demandes directement à Content Gateway

Déploiement transparent du proxy, où les demandes des utilisateurs sont automatiquement redirigées vers un proxy Content Gateway, généralement par un commutateur ou un routeur, en route pour leur destination finale.

2. Analyser la différence entre le proxy explicite et proxy transparent

2.1. Déploiement du proxy explicite

L'utilisation de Content Gateway dans un déploiement de proxy explicite constitue un moyen simple de gérer les demandes Web des utilisateurs. Ce type de déploiement est recommandé pour les réseaux simples avec un petit nombre d'utilisateurs. Le proxy explicite est également utilisé efficacement lorsque les paramètres de proxy peuvent être appliqués par la stratégie de groupe. Cela nécessite une configuration réseau minimale, ce qui peut être un avantage lors du dépannage.

Pour un déploiement de proxy explicite, les navigateurs client individuels peuvent être configurés manuellement pour envoyer des requêtes HTTP et, en option, HTTPS et FTP, directement au proxy.

Pour configurer un navigateur afin qu'il envoie des demandes à Content Gateway, les clients doivent fournir les informations suivantes pour chaque protocole qu'ils souhaitent que le proxy serve dans leurs navigateurs :

- Le nom d'hôte ou l'adresse IP du proxy.
- Le port du serveur proxy. Le port du serveur proxy par défaut de Content Gateway est 8080.

De plus, les clients peuvent spécifier de ne pas utiliser le proxy pour certains sites. Les demandes adressées aux sites répertoriés vont directement au serveur d'origine.

Pour Microsoft Internet Explorer, les paramètres de configuration du proxy se trouvent dans **Outils > Options Internet > Connexions > Paramètres réseau**. Par défaut, Microsoft Internet Explorer définit tous les protocoles sur le même serveur proxy. Pour configurer chaque protocole séparément, cliquez sur **Avancé** dans la section **Paramètres réseau**. Consultez la documentation du navigateur pour obtenir des instructions complètes sur la configuration du proxy.

2.2. Déploiement du proxy transparent

Dans un déploiement de proxy transparent, le logiciel client de l'utilisateur (généralement un navigateur) ne sait pas qu'il communique avec un proxy. Les utilisateurs demandent le contenu Internet comme d'habitude, sans configuration client particulière, et le proxy traite leurs demandes. Le composant ARM (Adaptive Redirection Module) de Content Gateway intercepte les paquets entrants et les redirige vers le proxy. Le proxy établit une connexion avec le serveur d'origine et renvoie le contenu demandé au client. Les redirections ARM ont renvoyé le contenu comme s'il provenait directement du serveur d'origine.

Notez que dans un déploiement de proxy transparent, tout le trafic Internet d'un client passe par le proxy (pas uniquement le trafic des navigateurs Web), notamment :

- Trafic tunnelisé via HTTP et HTTPS par des applications de bureau à distance.
- Clients de messagerie instantanée.
- Mise à jour de logiciels pour Windows et les applications antivirus.
- Applications internes personnalisées.

Ce type de déploiement nécessite la mise en œuvre d'au moins un autre périphérique réseau qui n'est pas requis dans le déploiement de proxy explicite. Les équipements ajoutés posent des problèmes de compatibilité, car tous les périphériques réseau doivent fonctionner ensemble de manière fluide et efficace. Le système global est souvent plus complexe et nécessite généralement davantage d'expertise réseau pour la construction et la maintenance.

L'utilisation d'un commutateur de couche 4 ou d'un routeur compatible pour rediriger le trafic dans un déploiement de proxy transparent peut fournir des fonctionnalités de redondance et de distribution de charge pour le réseau. Ces périphériques non seulement acheminent le trafic de manière intelligente entre tous les serveurs disponibles, mais peuvent également détecter si un proxy est non fonctionnel. Dans ce cas, le trafic est redirigé vers d'autres serveurs proxy disponibles.

IV- Conclusion

Ce chapitre nous a permis de définir les missions de projet et les pilotes ainsi, les différents composants de la solution et le fonctionnement de chaque composant
Par suite, on a défini la différence entre les modes de déploiement des proxys.

Chapitre 4

Innover

Ce chapitre est dédié à la mise en place de la solution de sécurité forcepoint proposées dans l'étape de l'analyse. Ainsi, la configuration des politiques de sécurité et la gestion des utilisateurs à l'aide de l'active directory.

1. Création du LAB pour la mise en place de la solution

On va créer 3 machines virtuelle afin de créer un LAB forcepoint, 2 machines à la base de Windows server 2012 et la 3ème à la base de CentOS linux :



Figure 21 : Forcepoint LAB.

1.1. Installation de forcepoint security manager

On va créer une machine virtuelle sur l'ESXI à base de Windows server 2012 sous le nom “FP-SEC-SVR”, après l'installation de la machine virtuelle on doit lancer l'exécutable en cliquant sur run as administrator

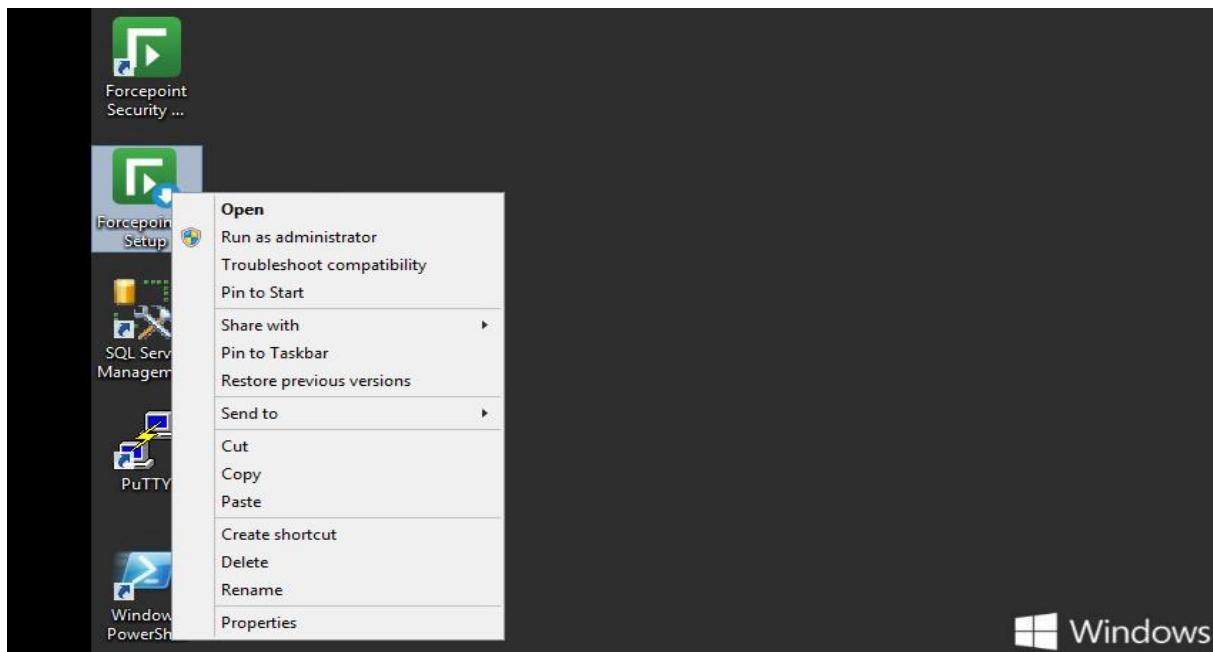


Figure 22 : lancement de l'exécutable.

Après l'extraction du fichier exécutable, on va lancer l'installation de forcepoint management infrastructure, la première étape est de configurer SQL server avec user Name et le mot de passe :



Figure 23 : Installation de SQL server.

Après l'installation de SQL server on va installer le Policy server en lui donnant une adresse IP et créer l'administrateur de forcepoint et le mot de passe :



Figure 24 : Installation de Policy server.

Donc après l'installation du Policy server, on doit configurer le compte administrateurs comme ci-dessous :



Figure 25 : création du compte administrateur.

L'installation se termine avec suivant (Next) :

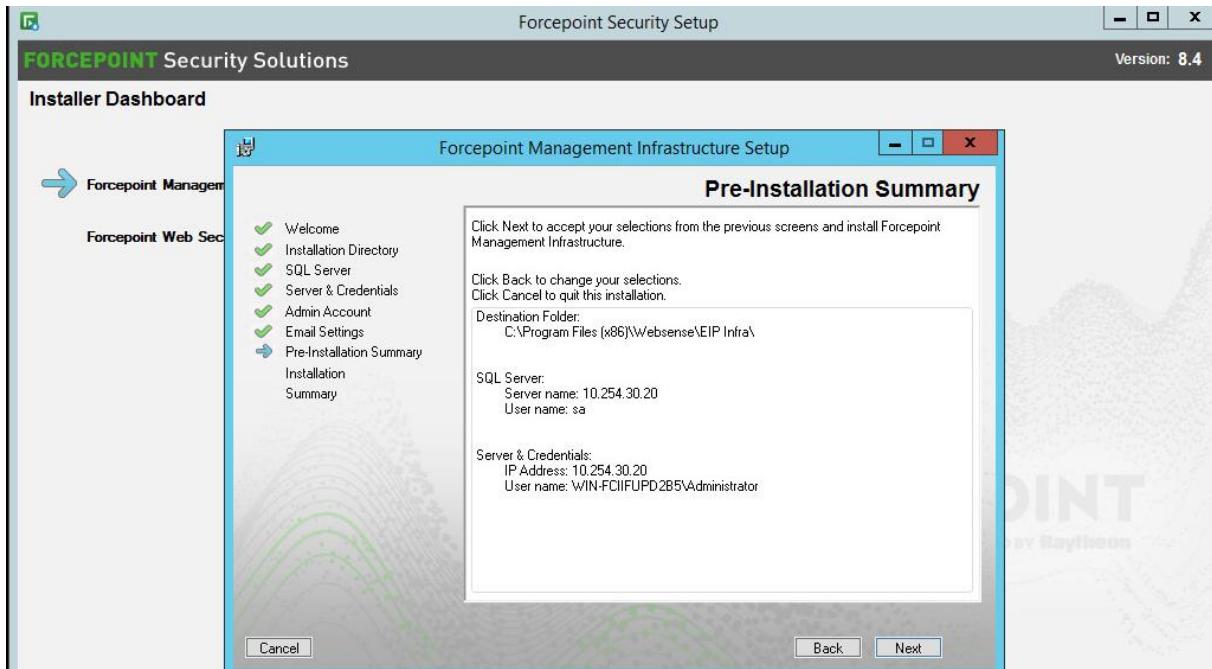


Figure 26 : résumé de l'installation.

Après l'installation de forcepoint management infrastructure, on va passer à la deuxième étape qui représente l'installation de forcepoint web Security afin de choisir les éléments à installer sur cette machine (Policy broker, Policy server, Log server, real time monitor et forcepoint manager security) :

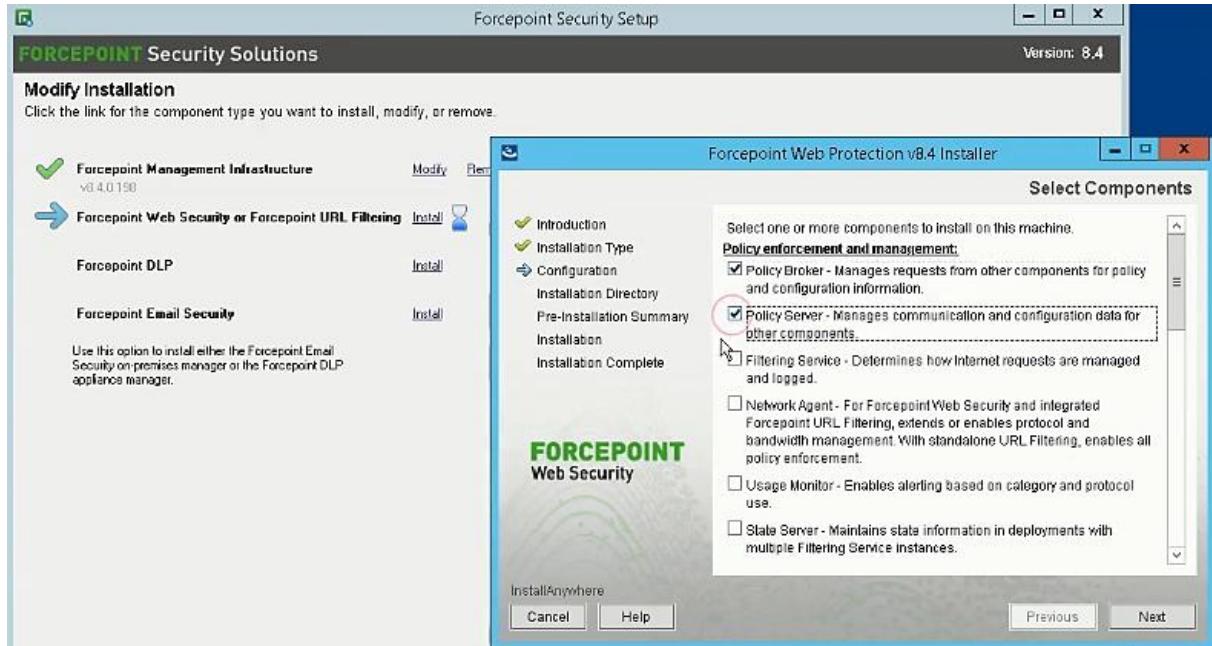


Figure 27 : Installation des éléments sur la machine FP-SEC-SVR.

Finalement on a terminé l'installation de forcepoint security manager, donc on doit entrer la licence :

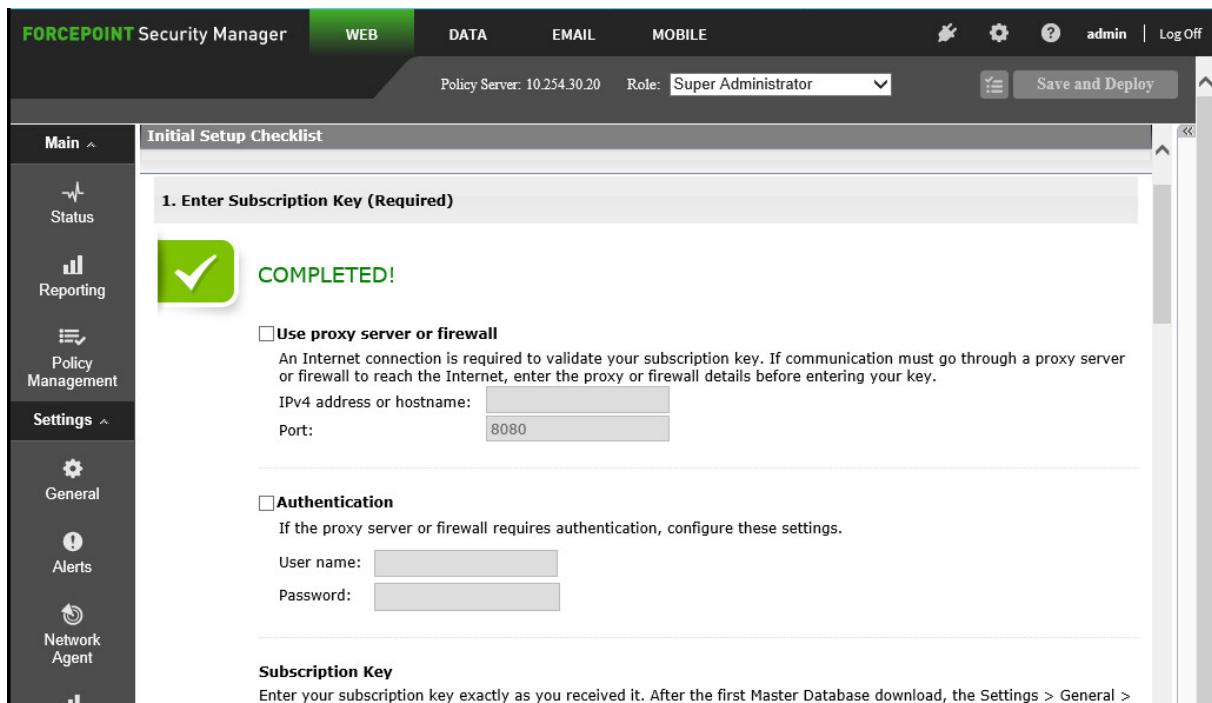


Figure 28 : la licence de forcepoint security manager.

1.2. Installation de forcepoint web security

Donc on a terminé l'installation de la première machine et on va passer à la deuxième machine à base de CentOS linux



Figure 29 : le choix du mode sécurité pour cette machine

Après le choix d'installer forcepoint web security on va choisir une adresse IP pour cette appliance management comme vous voyez ci-dessous :

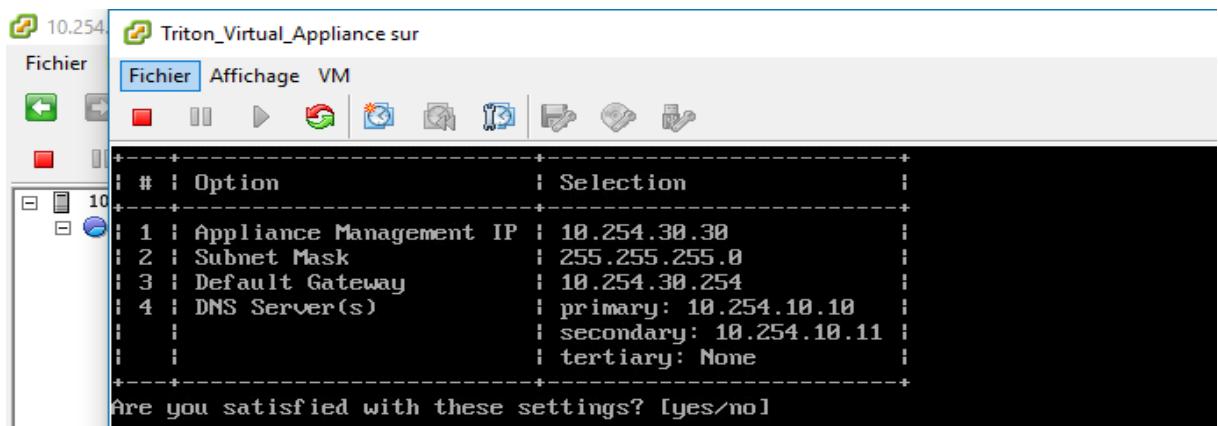


Figure 30 : La configuration de l'adresse IP de l'appliance management.

L'étape suivante représente la configuration du Policy broker qui est déjà installé sur la première machine, il faut entrer son adresse IP sur l'installation de la deuxième machine pour la cohérence de l'installation de la solution forcepoint.

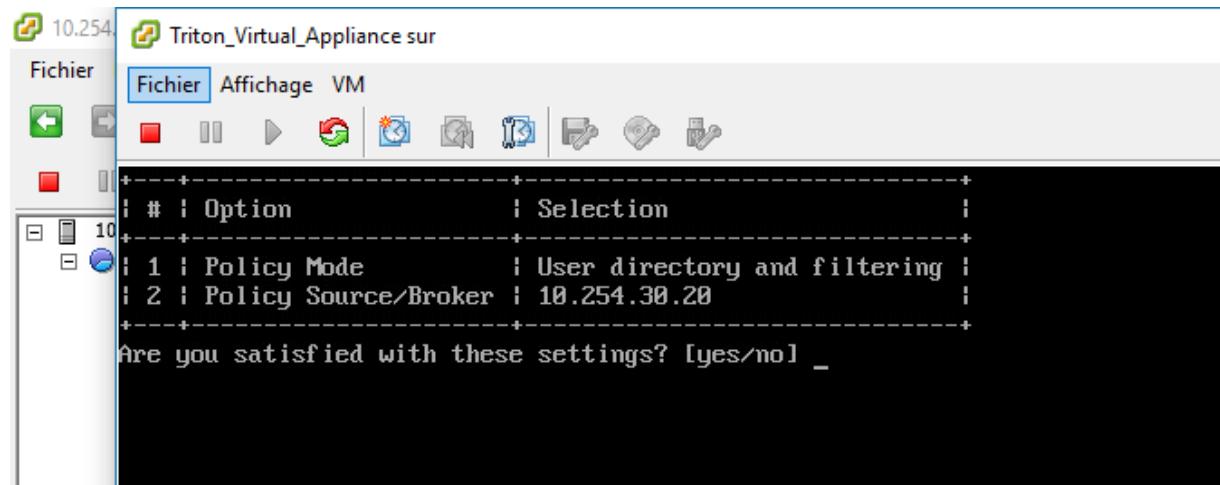


Figure 31 : l'ajoute de l'adresse IP du Policy broker

Finalement on va vérifier la configuration de notre appliance management :

#	Section	Configuration
1	Appliance Base	Option Selection Security Mode Forcepoint Web Security Hostname frpt.test.local NTP Disabled Date 2019/03/11 Time 15:06:50 Timezone Asia/Taipei Password **** Communication with Forcepoint LLC False
2	Appliance Network	Option Selection Appliance Management IP 10.254.30.30 Subnet Mask 255.255.255.0 Default Gateway 10.254.30.254 DNS Server(s) primary: 10.254.10.10 secondary: 10.254.10.11 tertiary: None
3	Forcepoint Web Security	Option Selection Policy Mode User directory and filtering Policy Source/Broker 10.254.30.20

Figure 32 : Vérification de la configuration.

Après avoir terminé la configuration, l'installation commence comme ci-dessous

Configuring Appliance Base Pre Installation requirements.....	Done
Configuring Appliance Network Pre Installation requirements.....	Done
Configuring Forcepoint Web Security Pre Installation requirements.....	Done
Installing Appliance Base requirements.....	DoneC6~
Installing Appliance Network requirements.....	Done
Configuring Forcepoint Web Security Pre Software Installation requirements.....	Done
Installing Forcepoint Web Security requirements.....	!_

Figure 33 : L'installation de l'appliance management.

1.3. L'active directory

1.3.1. Définition de l'active directory

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi

facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

1.3.2. Installation de l'active directory

Après avoir terminé l'installation de la deuxième machine de l'appliance management, on doit installer une troisième machine virtuelle à base Windows server 2012 au but d'installer l'active directory sur cette machine qui fournit des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

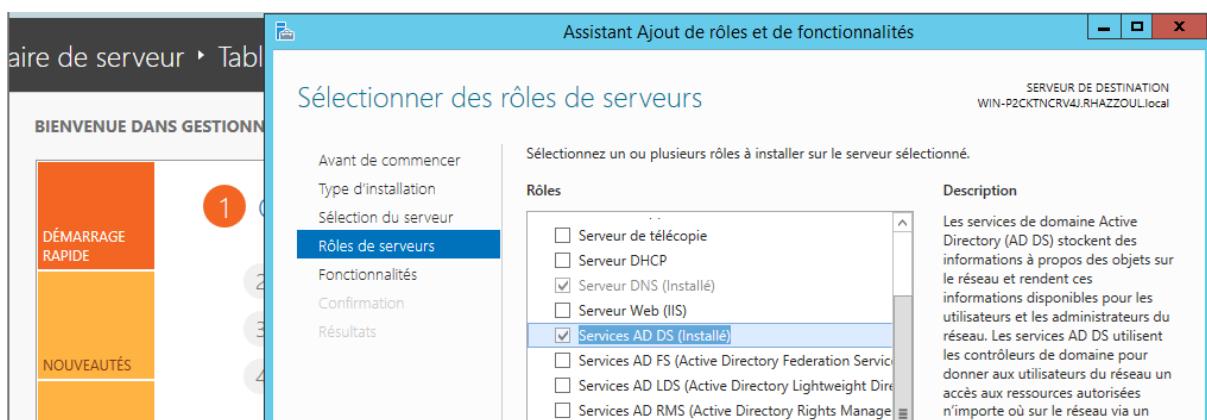


Figure 34 : Installation de l'active directory

Après l'installation de l'active directory, on va créer les utilisateurs de notre réseau

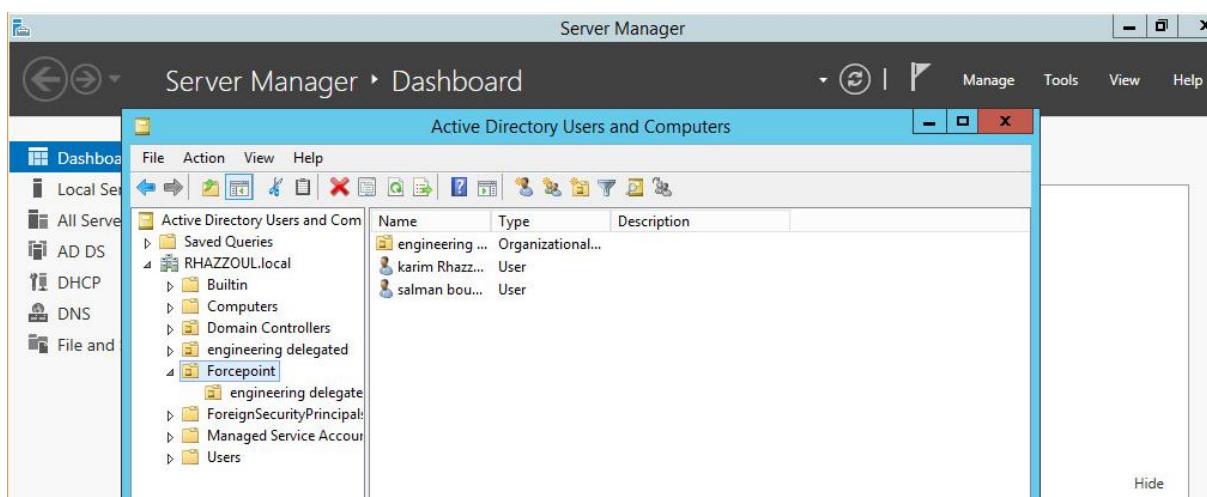


Figure 35 : les utilisateurs de l'active directory.

Après l'installation de l'active directory sur la troisième machine, on doit joindre le serveur de l'actif directory sous l'adresse IP 10.254.30.40 sur la première machine (forcepoint Security manager) :

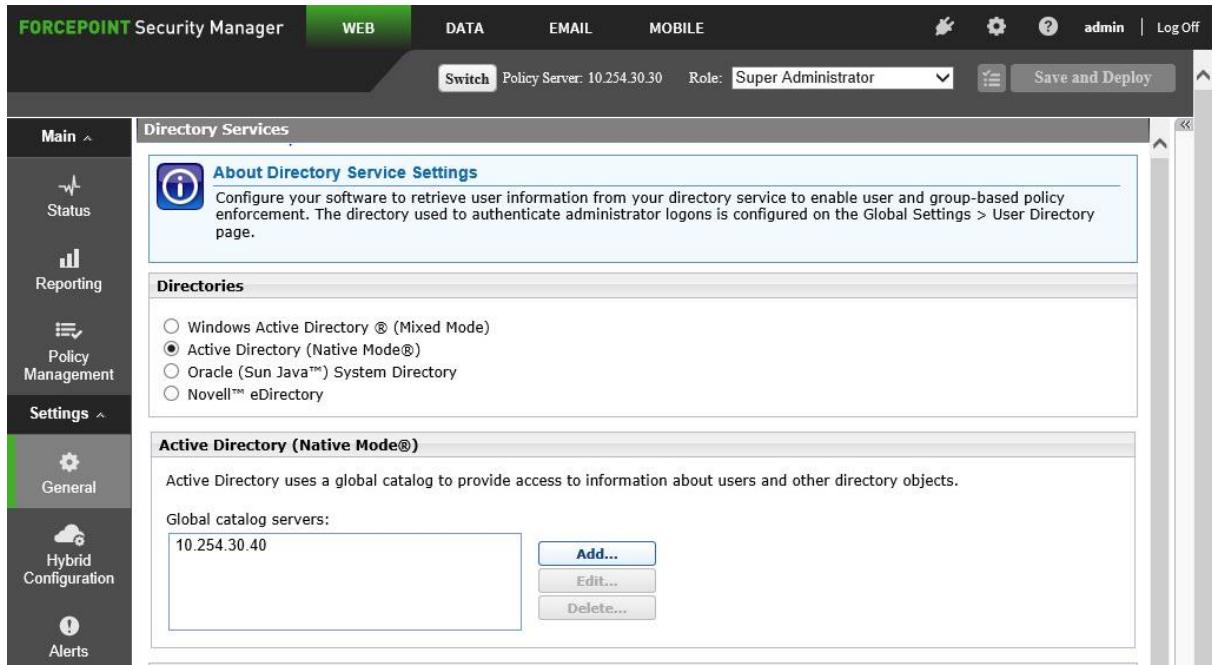


Figure 36 : l'ajoute de l'actif directory sur forcepoint security manager

Finalement on a terminé l'installation et la configuration de notre LAB, dans le chapitre suivant on va passer à la manipulation, on va créer des nouveaux administrateurs réseaux et de nouveau clients et des règles, et on va tester la performance de la solution de sécurité de forcepoint de la façon d'appliquer des règles sur des utilisateurs du réseau et on va remarquer l'efficacité de la solution forcepoint.

2. La configuration de forcepoint security manager

2.1. L'ajoute d'un nouvel administrateur réseau

On va ajouter un nouveau administrateurs réseau depuis l'active directory qui va être responsable d'un groupe qui va être créer après, la figure ci-dessous présente la création du nouvel administrateur réseau :

The screenshot shows the 'Administrators' page in the Forcepoint Security Manager. The left sidebar has 'Global Settings' selected under 'General'. The main area displays a success message: 'One or more administrator accounts were successfully added or updated.' Below this, a table lists two administrators: 'admin' (Local, hamza.rhazzoul@gmail.com, Global Security Administrator) and 'karim.rhazzoul' (Network, karim.rhazzoul@rhazzoul.com, Web (access only)).

User Name	Type	Email Address	Role
admin	Local	hamza.rhazzoul@gmail.com	Global Security Administrator
karim.rhazzoul	Network	karim.rhazzoul@rhazzoul.com	Web (access only)

Figure 37 : Crédit d'un nouvel administrateur réseau.

2.2. La création d'un nouveau rôle (engineering delegated)

On va créer un nouveau rôle sous le nom de 'engineering delegated' sur le quelle on va ajouter des utilisateur, l'administrateur responsable de ce rôle est Mr. Rhazzoul Karim

The screenshot shows the 'Delegated Administration' page in the Forcepoint Security Manager. The left sidebar has 'Policy Management' selected under 'Main'. The main area displays a table with two roles: 'Super Administrator' (Policy and reporting, Super Administrator) and 'engineering delegated' (Policy and reporting). At the bottom right, there are 'Add' and 'Delete' buttons.

Role	Type	Description
Super Administrator	Policy and reporting	Super Administrator
engineering delegated	Policy and reporting	

Figure 38 : Crédit d'un nouveau rôle 'engineering delegated'.

Après on va attribuer l'administrateur réseau déjà créer l'étape précédente à ce rôle afin de gérer la politique des utilisateurs qui vont être créer dans les étapes suivantes :

User Name	Account Type	Policy Management	Reporting	Real-Time Monitor
karim Rhazzoul	Network	Full policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 39 : l'attribution de l'administrateur au nouveau rôle.

On va se déconnecter du compte admin et on va se connecter avec la session du nouvel administrateur réseau qui est responsable sur le nouveau rôle ‘engineering delegated’

Policy	Override	Quota
eng policy	None	Default

Figure 40 : l'accès avec le nouvel administrateur

2.3. Crédation d'une nouvelle politique

On va créer une nouvelle politique sous le nom de ‘engineering Policy’ et après l’administrateurs réseau va appliquer cette politique sur des utilisateurs.

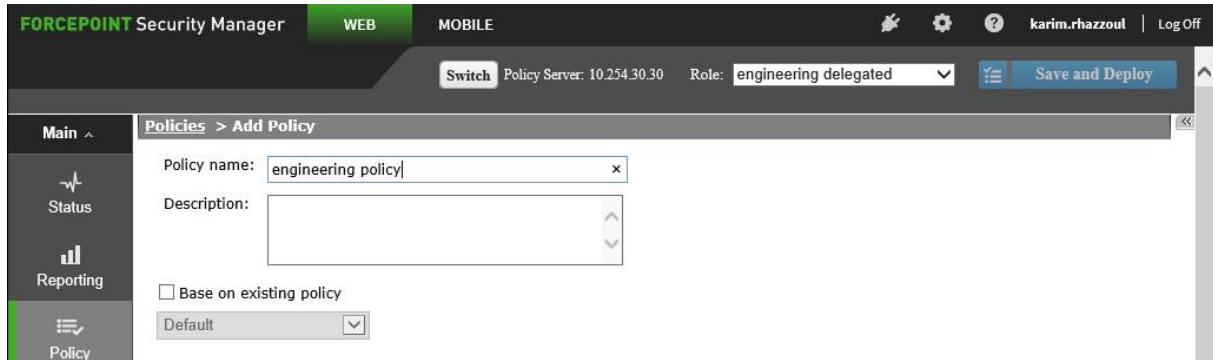


Figure 41 : Crédation d'une nouvelle politique

Après la création de la nouvelle politique ‘engineering Policy’, l’administrateur réseau va appliquer cette politique sur des utilisateurs comme ci-dessous :

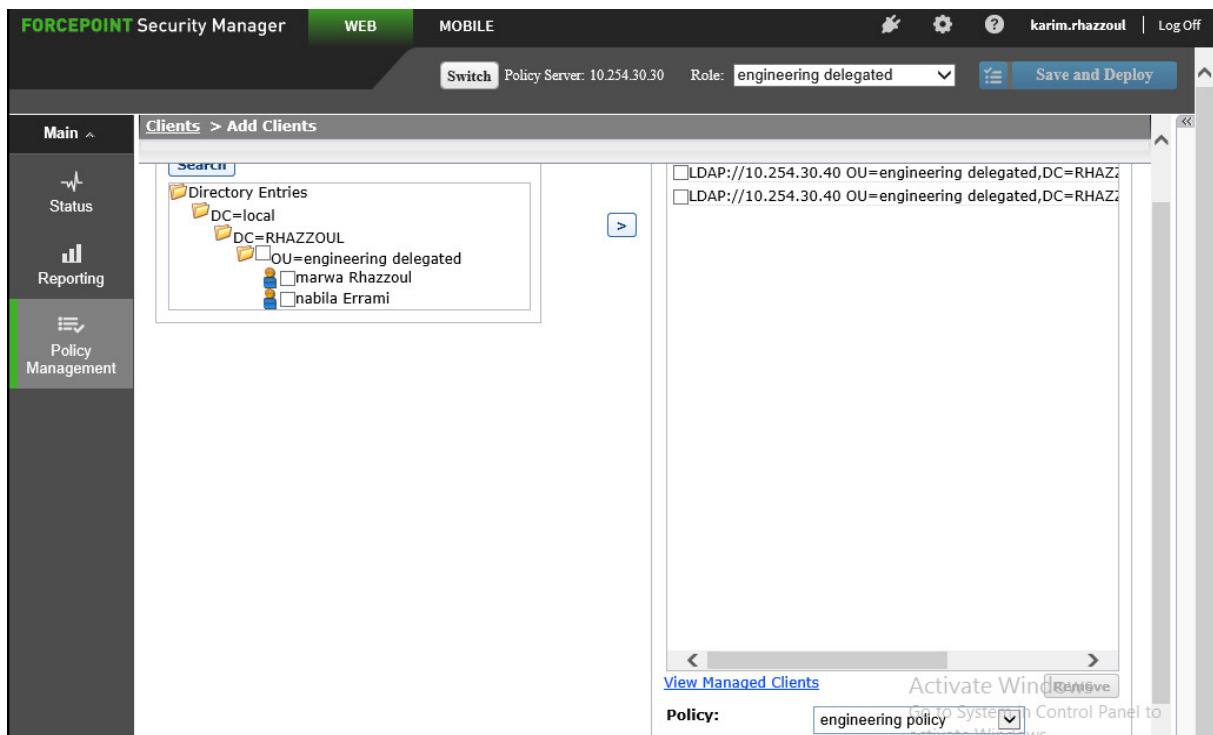


Figure 42 : Application de la politique aux utilisateurs.

2.4. Les types de filtrage

2.4.1. Filtrages par catégorie

Définir les catégories de sites http et https à appliquer aux actions de filtrage, les possibilités de filtrage possibles sont les suivants :

- **Bloquer** : bloquer les sites appartenant aux catégories
- **Autoriser** : autoriser les sites appartenant aux catégories
- **Optimiseur de bande passante** : lorsque cette action est activée et que l'utilisation de la bande passante atteint un seuil spécifié, les demandes Internet pour une catégorie spécifique sont bloquées
- **Confirmer** : les utilisateurs reçoivent une page de blocage leur demandant de confirmer que le site est utilisé à des fins commerciales. Si un utilisateur clique sur continuer, il peut consulter le site
- **Quota** : les utilisateurs reçoivent une page de blocage, leur demandant s'ils doivent utiliser une heure de quota pour afficher le site.
- **Bloquer les mots clés** : bloquer les demandes adressées à un site dont l'URL contient un mot clé bloqué

Ce type de filtrage présente un filtrage par catégorie, ce type de filtrage dépend sur le filtrage des sites web par catégorie par exemple (sécurité web, entraînement, réseau sociaux, drogue...).

Donc quel que soit un site web qui peut contenir par exemple une source de drogue on peut le bloquer sur une société ou un établissement.

The screenshot shows the Forcepoint Security Manager web interface. The top navigation bar has 'FORCEPOINT Security Manager' on the left, 'WEB' in the center, and 'MOBILE' on the right. On the far right of the top bar are icons for user 'karim.rhazzoul', 'Log Off', and a gear icon. Below the top bar is a toolbar with buttons for 'Switch', 'Policy Server: 10.254.30.30', 'Role: engineering delegated', and 'Save and Deploy'. The main content area is titled 'Policies > Edit Policy' and shows a configuration for an 'Apply to Clients' policy. It includes fields for 'Start' (00:00), 'End' (24:00), 'Days' (Mon Tue Wed Thu Fri), 'Category / Limited Access Filter' (set to 'Default'), 'Protocol Filter' (set to 'Default'), and 'Cloud App Filter' (set to 'Monitor Only'). Below these fields are buttons for 'Add' and 'Delete'. Underneath the main configuration, there are tabs for 'Category/Limited Access Filter', 'Protocol Filter', and 'Cloud App Filter'. A 'Filter description:' section explains the purpose of the filter. At the bottom of the main panel is a 'Category Filter: Default' section with a 'Find category:' input field and a list of categories. The categories listed include: Business and Economy, Drugs, Education, Entertainment, Extended Protection (Unpurchased), Gambling, Games, Government, Health, Illegal or Questionable, Information Technology, Internet Communication, Job Search, and Militancy and Extremist. The sidebar on the left has sections for 'Status', 'Reporting', and 'Policy Management' (which is currently selected). A status message at the bottom right says 'Activate Windows' and 'Go to System in Control Panel to activate Windows'.

Figure 43 : Filtrage par catégorie

Le filtrage par catégorie son rôle essentiel est de bloquer les sites web qui contient des malwares donc ce filtrage aide à bloquer les sites malveillants :

Figure 44 : Filtrage des malwares

- **Différents types de malwares :**
 - Advanced malware command and control :

Les serveurs C & C servent également de siège pour les machines compromises dans un botnet. Il peut être utilisé pour diffuser des commandes pouvant voler des données, propager des logiciels malveillants, perturber des services Web.

Outre la possibilité pour les attaquants de voler des données, la présence de logiciels de commande et de contrôle sur un serveur peut également perturber les applications légitimes et entraîner la mauvaise utilisation des ressources futures.

Les serveurs C & C peuvent être utilisés pour créer de puissants réseaux de périphériques infectés capables de mener des attaques par déni de service (DDoS), de voler des données, de les supprimer ou de les chiffrer, afin de mettre en œuvre un stratagème d'extorsion.

- Advanced malware Payloads :

Sont souvent conçus pour la furtivité ou la persistance et sont capables d'éviter la détection par les solutions antivirus traditionnelles. Au cours des dernières années, les attaques impliquant des logiciels malveillants avancés ont augmenté, mettant les entreprises en danger en raison des capacités d'attaque sophistiquées des logiciels malveillants et de la vitesse à laquelle elles évoluent pour rester en avance sur la détection,

Les attaques de logiciels malveillants avancés suivent généralement une séquence d'attaque commune :

- **Planification** : cette étape consiste à sélectionner une cible et à rechercher son infrastructure afin de déterminer la manière dont le logiciel malveillant sera introduit, les méthodes de communication utilisées pendant l'attaque, et comment et où les données seront extraites.
 - **Introduction des logiciels malveillants** : à cette étape, les logiciels malveillants sont transmis à la ou aux cibles pour une infection initiale.
 - **Commande et contrôle** : les logiciels malveillants avancés doivent communiquer avec les attaquants pour envoyer les informations découvertes et recevoir des instructions supplémentaires. Il enverra des informations sur les utilisateurs et le réseau.
 - **Extension** : les pirates vont explorer le réseau et propager latéralement des malwares cherchant à infecter des ordinateurs ou des systèmes ayant accès aux données ciblées.
 - **Identification de la cible** : À ce stade, le logiciel malveillant se propage pour infecter des machines ou des systèmes contenant ou ayant accès aux données ciblées.
 - **Événement d'attaque / Exfiltration** : il s'agit de la phase de compilation des données ciblées et de leur transfert vers un emplacement contrôlé par l'attaquant.
 - **Retrait** : une fois l'attaque de malware avancée terminée, le malware s'efface et se cache dans un réseau informatique ou se détruit lui-même.
- Bot networks :

C'est un Scareware malveillant qui, une fois installé, fournit une passerelle dans votre système aux développeurs de logiciels malveillants pour installer des éléments tels que les rootkits et les botnets. Logiciel d'activation.

Le logiciel bot net configure efficacement votre ordinateur pour recevoir des instructions d'un terminal de contrôle maître contrôlé par le propriétaire du botnet, qui est généralement un pirate informatique ou un autre cybercriminel qui a acheté l'utilisation de votre ordinateur à la personne qui l'a infecté.

Non seulement votre ordinateur est infecté, mais les gens gagnent de l'argent en vendant le droit d'utiliser votre ordinateur (à votre insu) pour mener des attaques sur d'autres ordinateurs. La puissance de calcul et les ressources réseau de tous les ordinateurs du réseau pour attaquer une seule cible. Ces attaques sont appelées attaques par déni de

service (DDoS).

- Keyloggers :

Représente un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.

Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur.

- Malicious Embedded iframe :

Représente un code malveillant qui infecte des pages Web sur des sites Web. Ceux-ci sont considérés comme une forme de malware. La plupart d'entre eux utilisent du code HTML iframe, causant des dommages en injectant des balises iframe dans le site Web. Le code peut être injecté dans des fichiers sources HTML, PHP, ASP ou tpl. Le virus peut faire connaître sa présence en recherchant des fichiers de page d'accueil tels que index. PHP, index.html ou default.html et en y injectant le code iframe. Le code iframe se trouve généralement au début de la page Web.

- Mobile malware :

Sont des logiciels malveillants qui ciblent spécifiquement les systèmes d'exploitation des téléphones mobiles. Les Différents types de programmes malveillants mobiles :

- Logiciels espions et logiciels malveillants.
- Téléchargements au passage.
- Virus et chevaux de Troie.
- Phishing mobile

- Phishing :

Est une approche détournée qu'utilisent les cyber-escrocs pour vous pousser à révéler des informations personnelles, comme des mots de passe ou des numéros de carte de crédit, de sécurité sociale ou de compte bancaire. Ils le font en vous envoyant des e-mails contrefaits ou en vous dirigeant sur un site web contrefait.

Les messages d'hameçonnage semblent provenir d'organisations légitimes comme PayPal, UPS, une administration ou votre banque ; cependant, il s'agit en fait d'habiles

escroqueries. Les messages demandent poliment l'actualisation, la validation ou la confirmation d'informations sur un compte, en suggérant fréquemment qu'un problème est survenu. Vous êtes alors redirigé vers un faux site où l'on vous pousse à entrer des informations sur le compte. Il peut en résulter un vol d'identité.

- Spyware :

Est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

2.4.2. Filtrage de protocoles

Une des actions suivantes peut être assignée à chaque filtre de protocole lorsqu'un utilisateur tente d'accéder à un protocole dans la catégorie.

Bloquer : utilisateur ne peut pas utiliser le Protocol

Autoriser : utilisateur ne peut pas utiliser le Protocol

Optimiseur de bande passante : lorsque cette action est activée et que l'utilisation de la bande passante atteint un seuil spécifié, les demandes de protocole supplémentaires sont bloquées

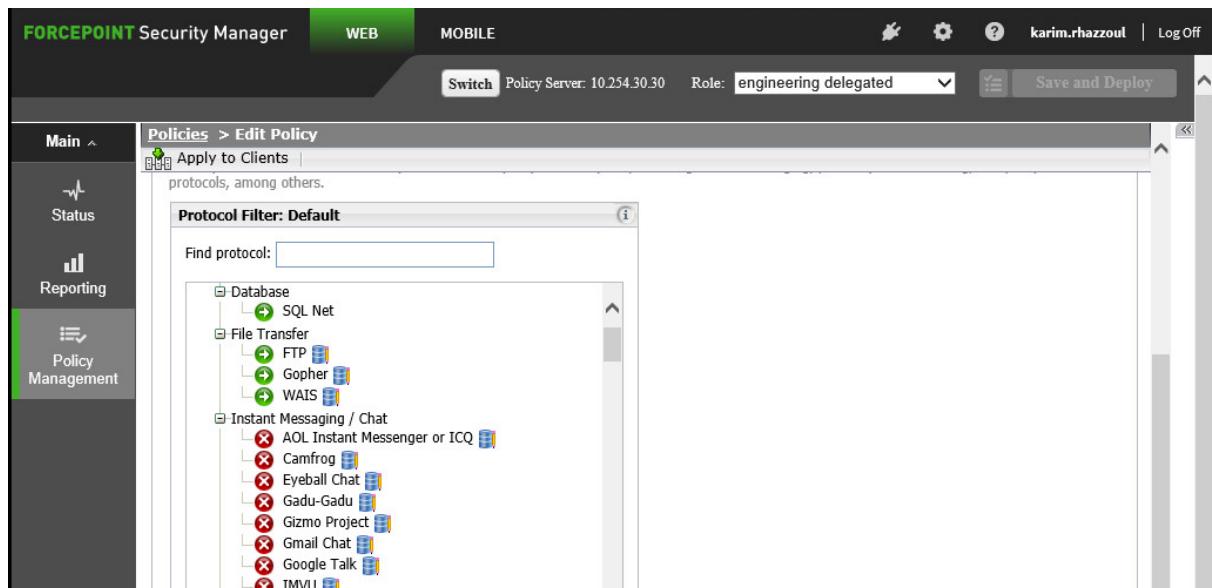


Figure 45 : Filtrage par Protocole

2.4.3. Filtrage d'application cloud

Définir les applications cloud à bloquer et à autoriser

Bloquer : les applications cloud de la liste des applications bloquées sont toujours bloquées, quel que soit leur niveau de risque

Permit : les applications cloud dans la liste des applications autorisées sont toujours autorisées

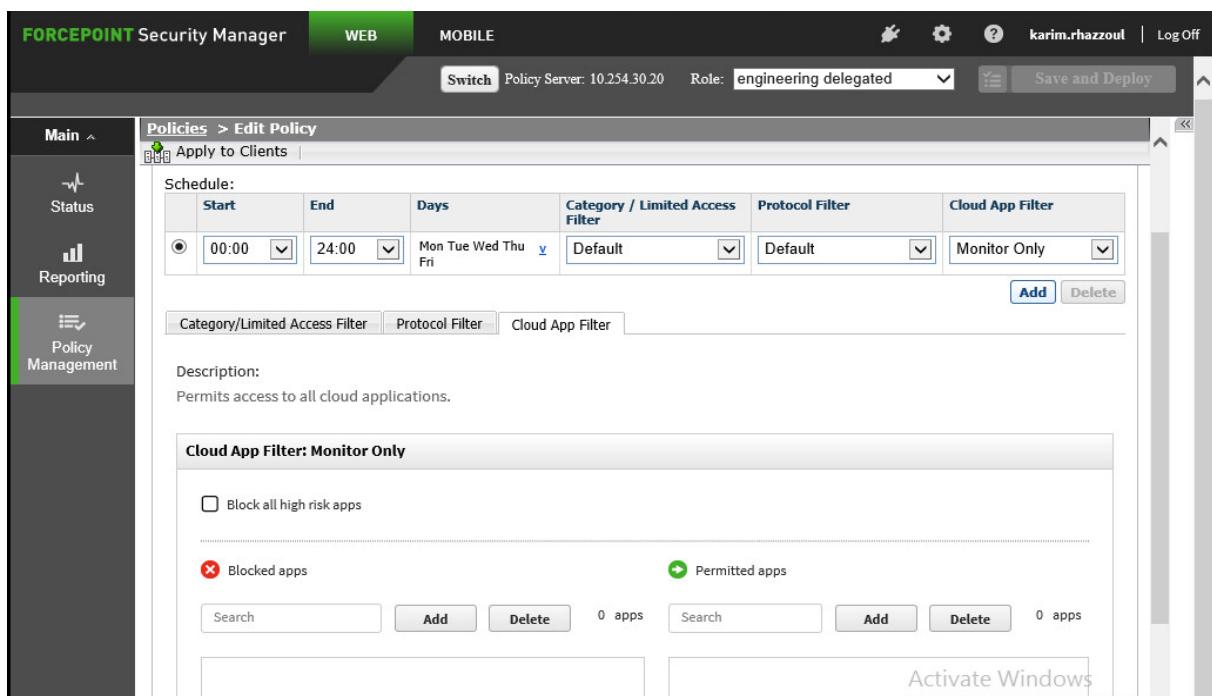


Figure 46 : Filtrage par application cloud.

2.5. Le choix du mode de déploiement de notre proxy

Puisqu'on a une simple architecture de réseau avec un petit nombre d'utilisateurs, on va utiliser le mode explicite donc on doit configurer chaque client de façons manuellement pour envoyer des requêtes HTTP et, en option, HTTPS et FTP, directement au proxy

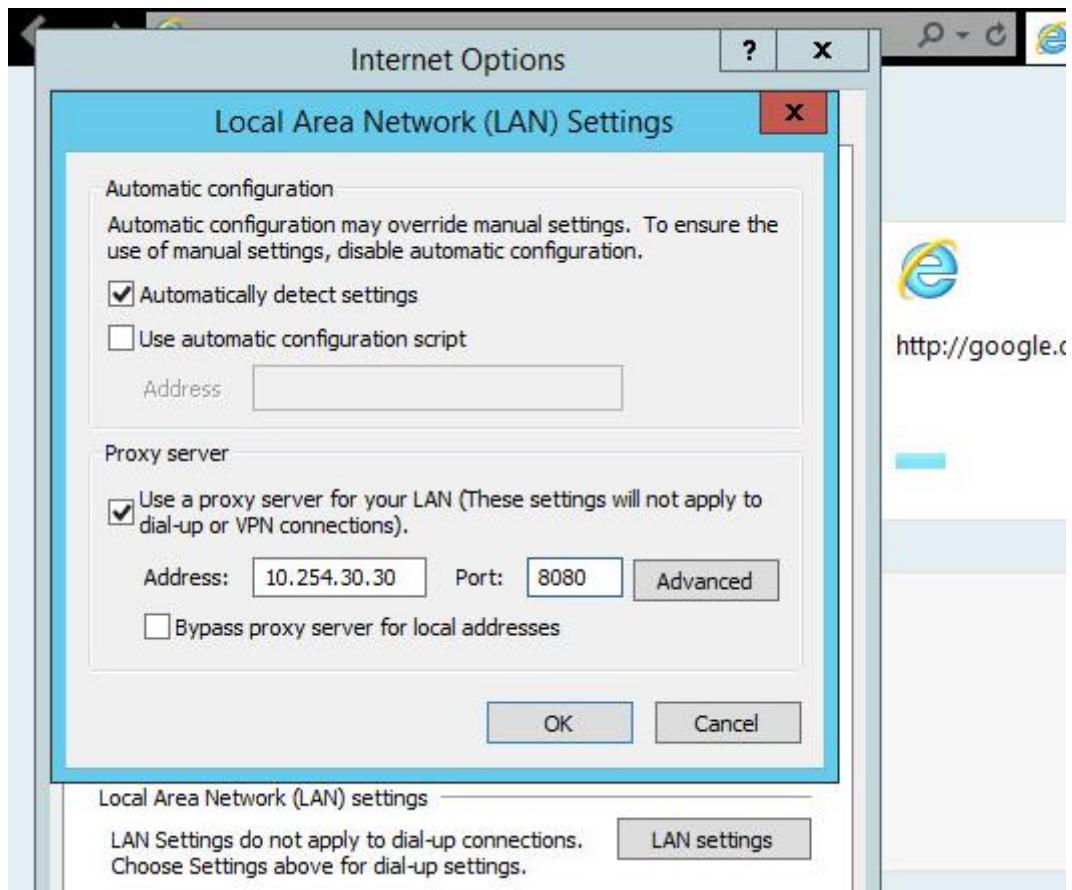


Figure 47 : configuration du proxy explicite

3. Implémentations et résultats

3.1. Définir une politique de sécurité

Pour la nouvelle politique que je vais appliquer sur mes clients je vais définir une politique et je vais tester l'efficacité de la solution forcepoint.

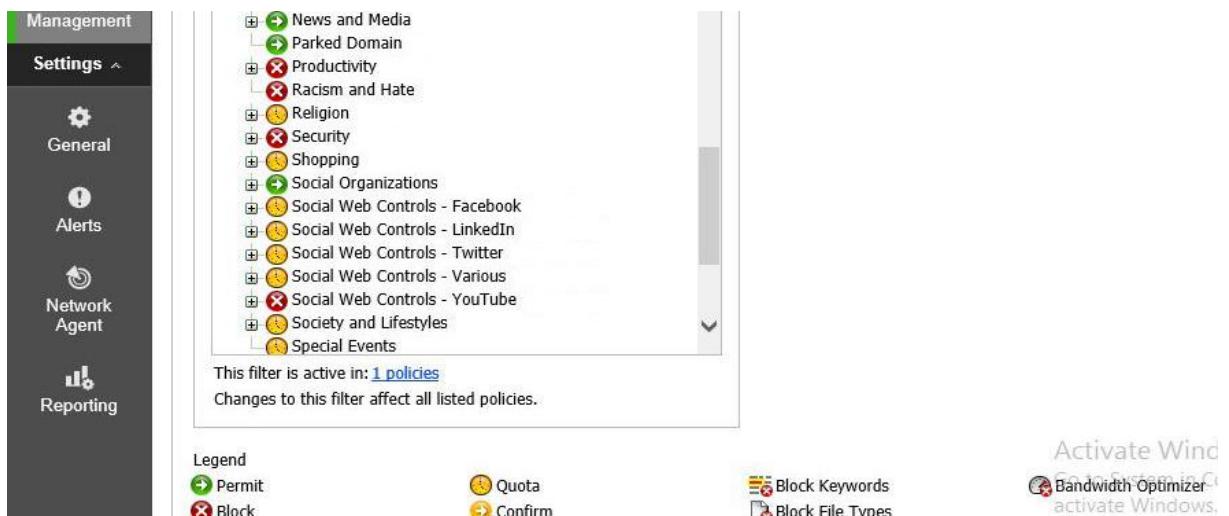


Figure 48 : Crédit de la politique pour le test

La politique que j'ai utilisé pour tester concerne en premier temps de limiter l'accès aux réseaux sociaux en configurant le temps d'accéder à un réseau social par exemple (Facebook, LinkedIn et twitter...), lorsque le client veut accéder à un réseau social le proxy forcepoint informe le client de la façon suivante, si le client clique sur 'use quota time' il peut bénéficier d'une 15 minutes en premier temps et en général d'une heure par jour.



Figure 49 : blocage du réseau social Facebook.

En deuxième temps, on a configuré un blocage total des clients à YouTube, lorsque le client ou bien l'utilisateur veut accéder à youtube.com le proxy forcepoint informe son blocage du site web de la façon suivante comme ci-dessous :

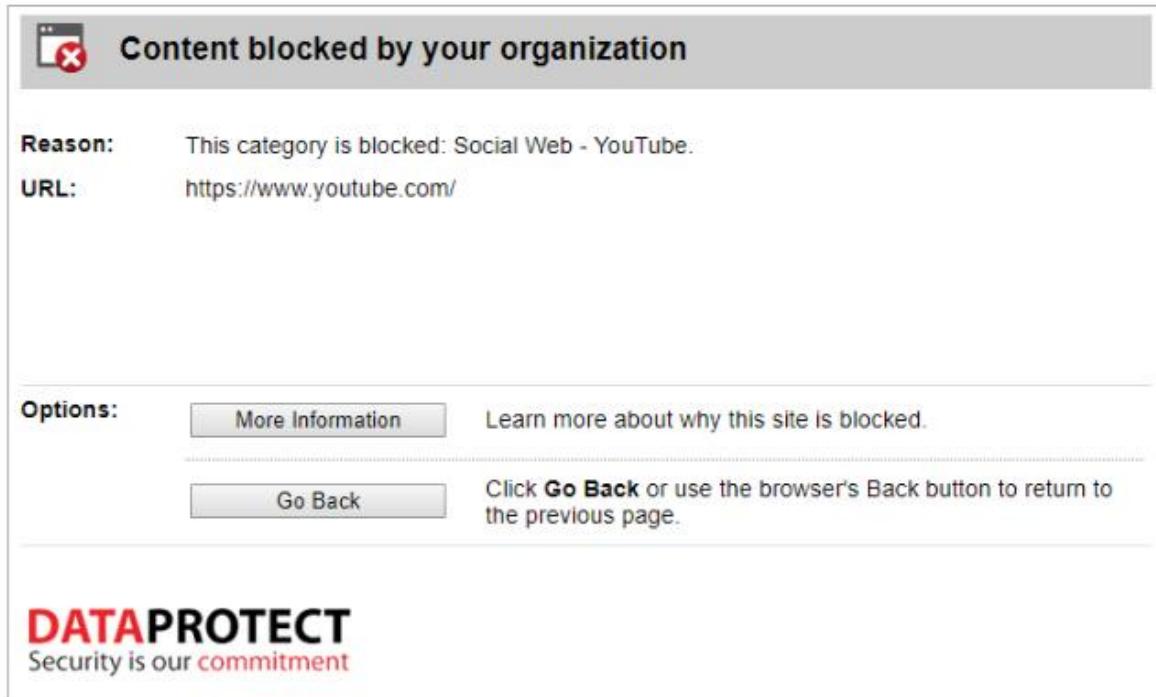


Figure 50 : blocage de YouTube

En troisième temps, on a configuré des politiques sur des sites web qui vous avertissent avant d'accéder à des sites web :

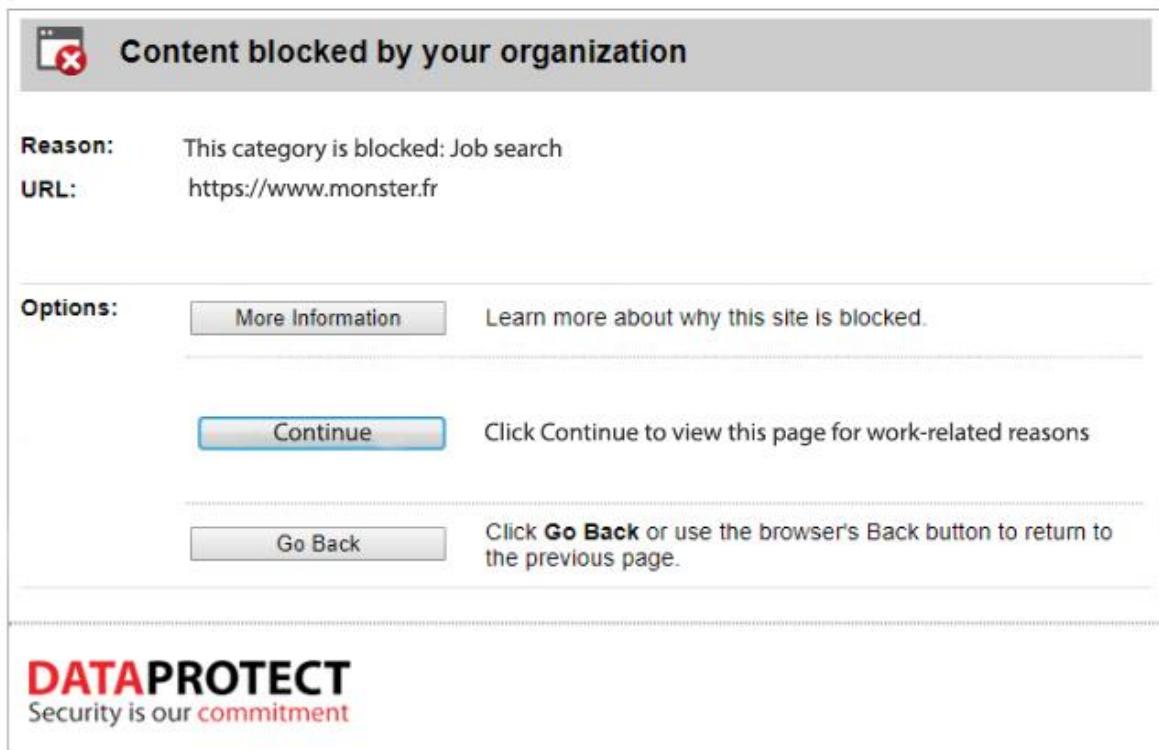


Figure 51 : blocage de monster.fr

En quatrième temps, on va configurer une politique contre les malware qui bloque tous les malware et les virus provenant de l'internet créés par des hackers au but d'endommager votre système soit pour voler des informations sensibles ou pour exploiter les ressources de vos équipements.

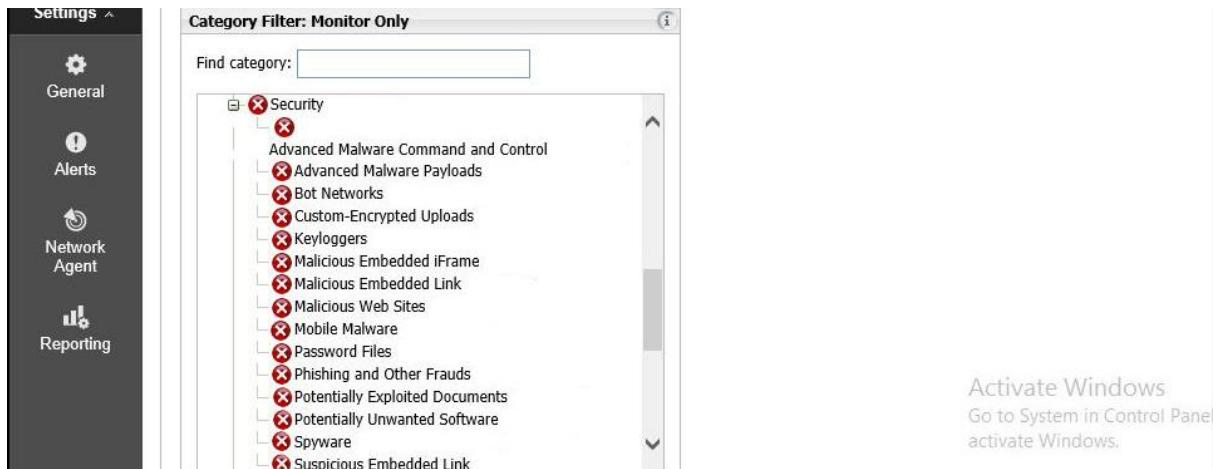


Figure 52 : blocage des différents malwares

La solution forcepoint détecte tous les différents types des malwares comme nous avons déjà vu, une fois un malware est détecté par la solution le résultat sera le message suivant :

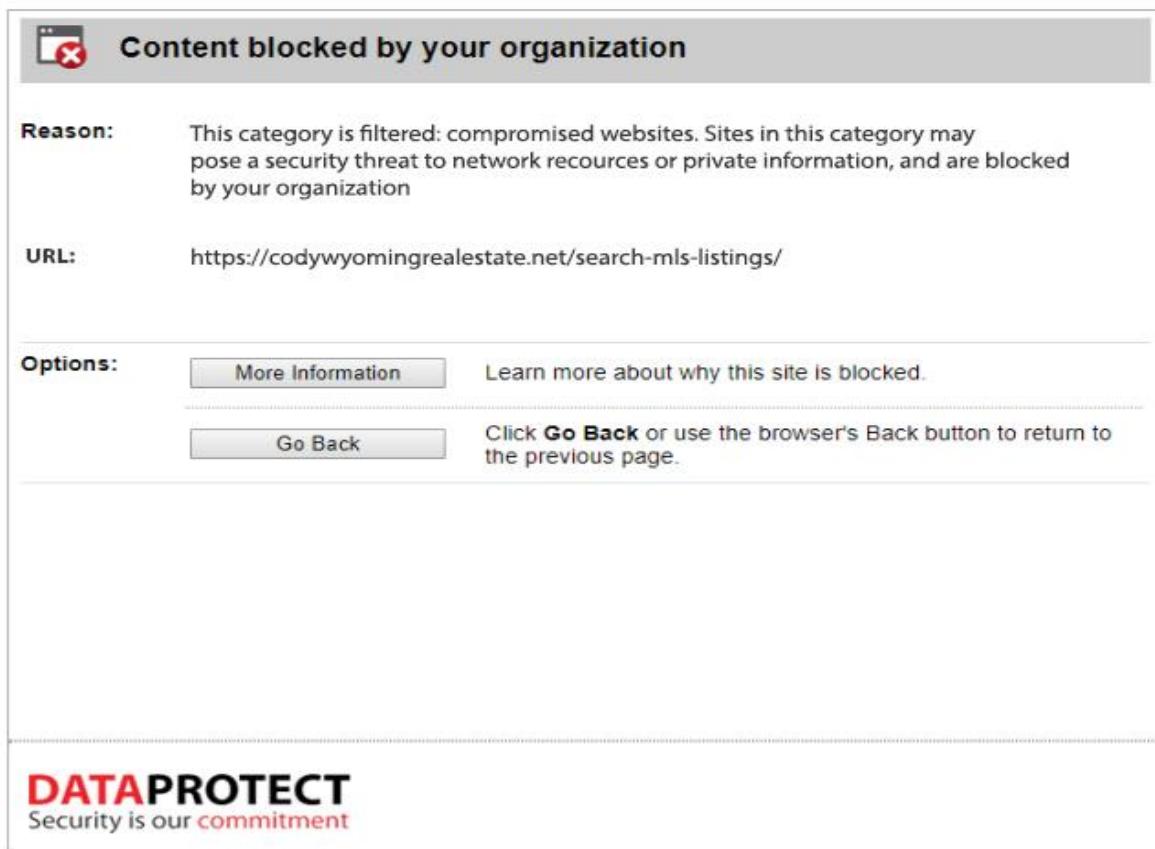


Figure 53 : blocage d'un lien de site web malveillant

Conclusion :

Chapitre 5

Contrôler

Après l'implémentation et la configuration du dispositif vient la partie du hardening qui s'agit de fortifier et rendre plus efficace notre équipement proxy donc on va faire un audit de configuration au but de chercher les vulnérabilités au niveau de la configuration.