Zoom sur le Filtrage DNS

Guide d'expert

Olfeo
La sécurité positive

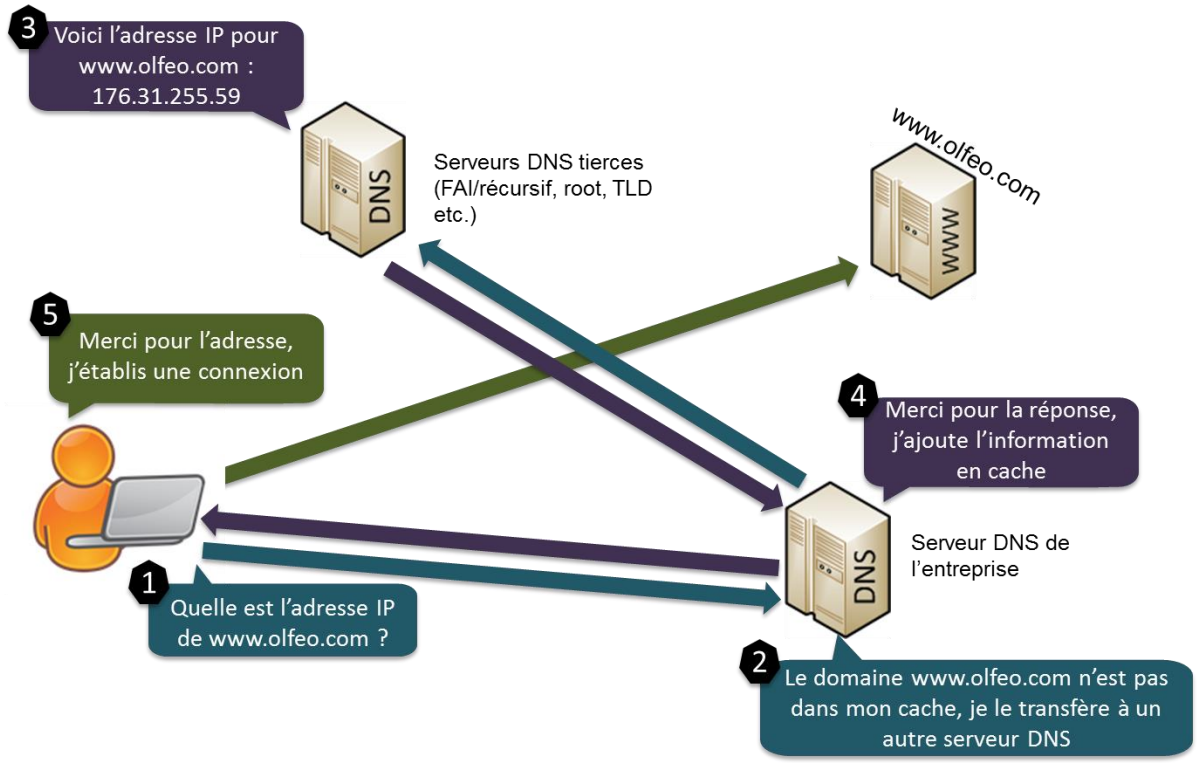
TABLE DES MATIERES

1 CONCEPTS DE BASE

1.1 LE MECANISME DNS

Le mécanisme DNS (Domain Name System) permet de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

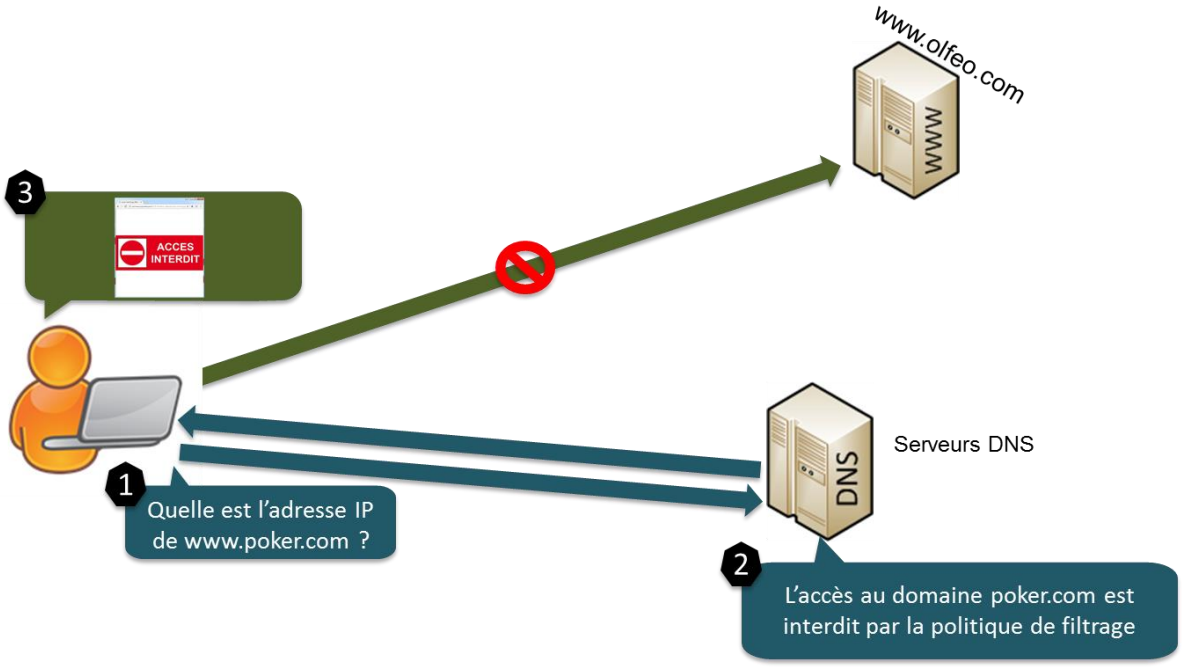
Lorsque l'utilisateur renseigne une URL dans son navigateur, celui-ci demande au serveur DNS, disponible à une adresse connue, de rechercher le nom de domaine indiqué dans l'URL et de fournir l'adresse IP correspondante.



Les entreprises disposent de serveurs DNS pour la résolution des requêtes de leurs zones internes, un transfert vers d'autres serveurs se produit pour les requêtes DNS ne concernant pas les zones internes.

1.2 PRINCIPE DE BASE DU FILTRAGE DNS

Lorsqu'un serveur DNS est configuré pour bloquer l'accès, il consulte une liste de domaines interdits. Lorsque le navigateur demande l'adresse IP de l'un de ces domaines, le serveur DNS retourne une fausse résolution. Un standard existe, il s'appelle RPZ. D'autres noms existent sur le marché, ex : DNS Firewall.



Lorsque le serveur DNS donne une mauvaise réponse ou aucune réponse, le poste client ne parvient pas à apprendre l'adresse IP correcte du service qu'il tente de joindre. Sans cette information, il ne peut pas poursuivre et un message d'erreur ou une page de blocage est affichée. Puisque le navigateur ne récupère pas l'adresse IP réelle du site web, il est incapable de le contacter pour obtenir la page web. Par conséquent tous les services et pages web servis sous ce nom de domaine sont inaccessibles. Dans ce contexte, le blocage délibéré peut être assimilé à un problème technique ou à un échec quelconque.

Dans certains environnements la mise en place d'un proxy web peut être une opération complexe et affecter les performances lors de la navigation. Les responsables de la sécurité informatique peuvent trouver des lacunes à ces solutions qui couvrent uniquement certains ports et protocoles.

Le DNS est un composant fondamental pour le fonctionnement d'Internet, il est utilisé par tous les périphériques : postes de travail, tablettes, smartphones, objets connectés (IOT). Par conséquent le DNS est un moyen efficace sur lequel les outils de filtrage DNS peuvent se reposer pour s'assurer de traiter tout le trafic et bloquer tous types de menaces ou accès inappropriés sur tous les ports et protocoles.

2 FILTRAGE DNS AVEC OLFEO

Ce nouveau mode d'intégration est disponible dans la solution Olfeo. Pour le moment il n'est disponible qu'en version 5. Il peut être déployé de 2 façons :

1. Mode on-premise : dans l'infrastructure de l'entreprise
2. Mode hébergé (SaaS) : dans une infrastructure tierce accessible via Internet

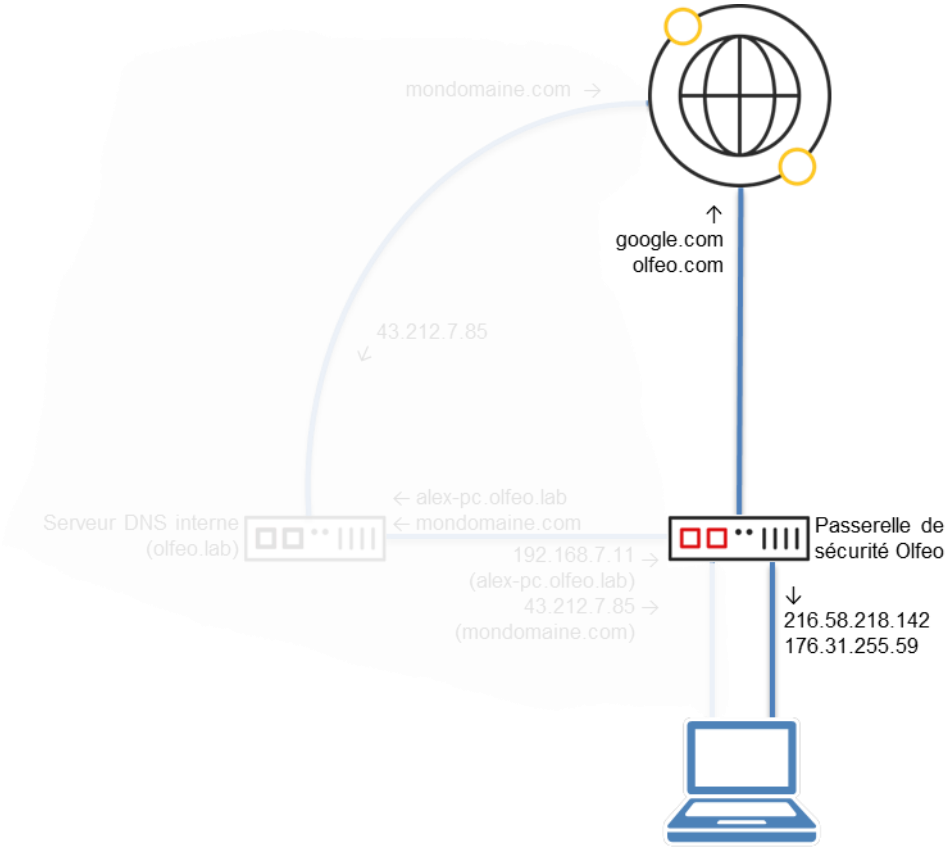
Ce mode d'intégration est compatible avec tous les modes d'installation disponibles pour la mise en place de la passerelle de sécurité Olfeo :

- Installation logicielle (sur machine physique ou virtuelle)
- Appliance virtuelle (compatible avec les hyperviseurs VMware vSphere, MS Hyper-V, Citrix XenServer, KVM, etc.)
- Appliance physique

2.1 MODE LOCAL/ON-PREMISE

Ce mode consiste à positionner le filtrage DNS Olfeo dans la chaine de résolution des clients. Soit en direct principal soit en redirecteur pour des serveurs de site.

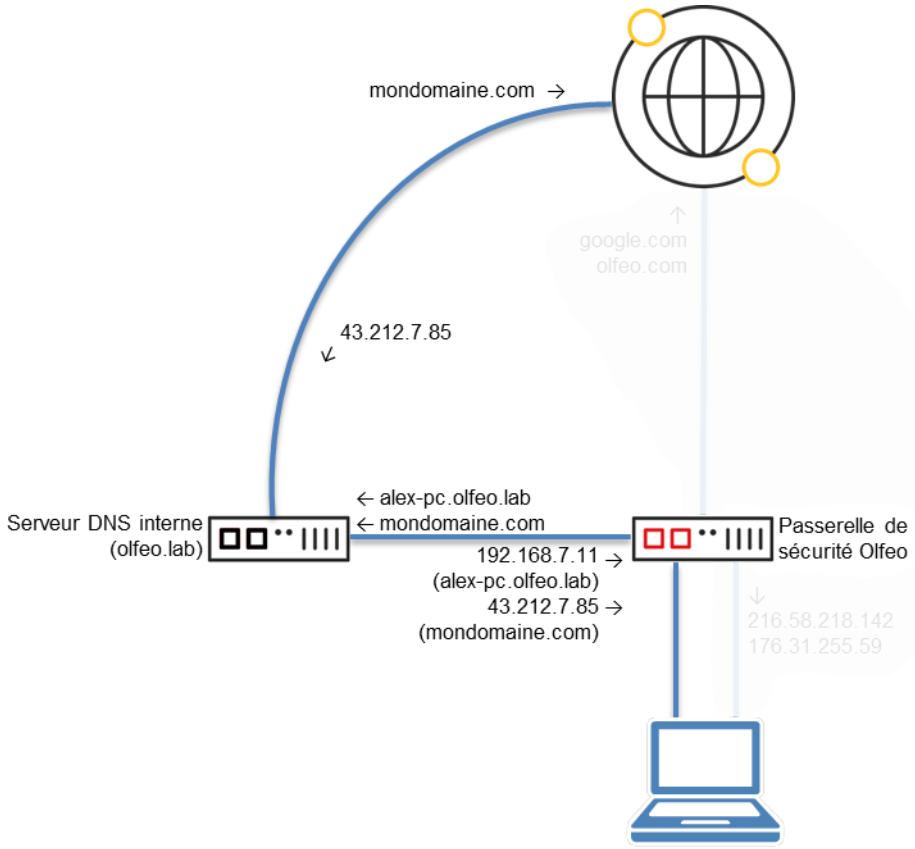
L'Olfeo est configuré pour transmettre les requêtes autorisées à un serveur DNS ayant accès aux ressources demandées (Internet, zones internes…)



Le client envoie une requête DNS à l'Olfeo, celui-ci évalue les règles et politiques concernant le domaine demandé dans la requête DNS et détermine le verdict : autorisé/bloqué :

- En cas de blocage, l'Olfeo envoie une réponse à la requête DNS en mentant : il envoie une adresse IP qui correspond à celle de l'Olfeo afin que le client affiche la page de blocage
- En cas d'accès autorisé, l'Olfeo transmet la requête à un autre serveur DNS externe (celui du fournisseur d'accès à Internet, de Google ou autre), ce serveur DNS envoie la réponse à l'Olfeo qui la transmet au client.

L'Olfeo est configuré pour transmettre les requêtes autorisées à un serveur DNS interne :



Le client envoie une requête DNS à l'Olfeo, celui-ci évalue les règles et politiques concernant le domaine demandé dans la requête DNS et détermine le verdict : autorisé/bloqué :

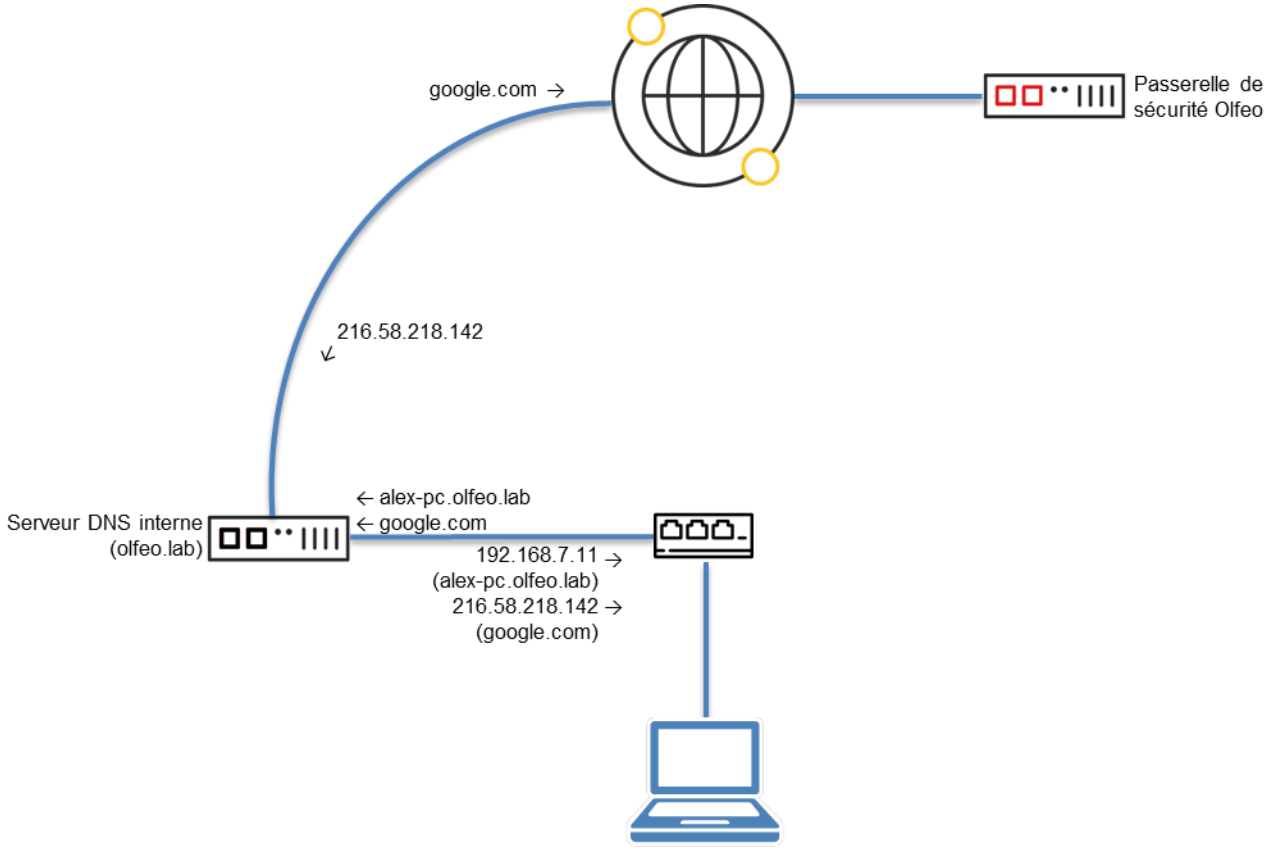
- En cas de blocage, l'Olfeo envoie une réponse à la requête DNS en mentant : il envoie une adresse IP qui correspond à celle de l'Olfeo afin que le client affiche la page de blocage
- En cas d'accès autorisé, l'Olfeo transmet la requête à un autre serveur DNS interne (celui de l'entreprise), ce serveur DNS envoie la réponse à l'Olfeo qui la transmet au client.

À noter que l'Olfeo peut être positionné après le serveur DNS interne, ce qui permet de bénéficier des éventuelles fonctions de cache et d'optimisation pour la résolution de noms internes.

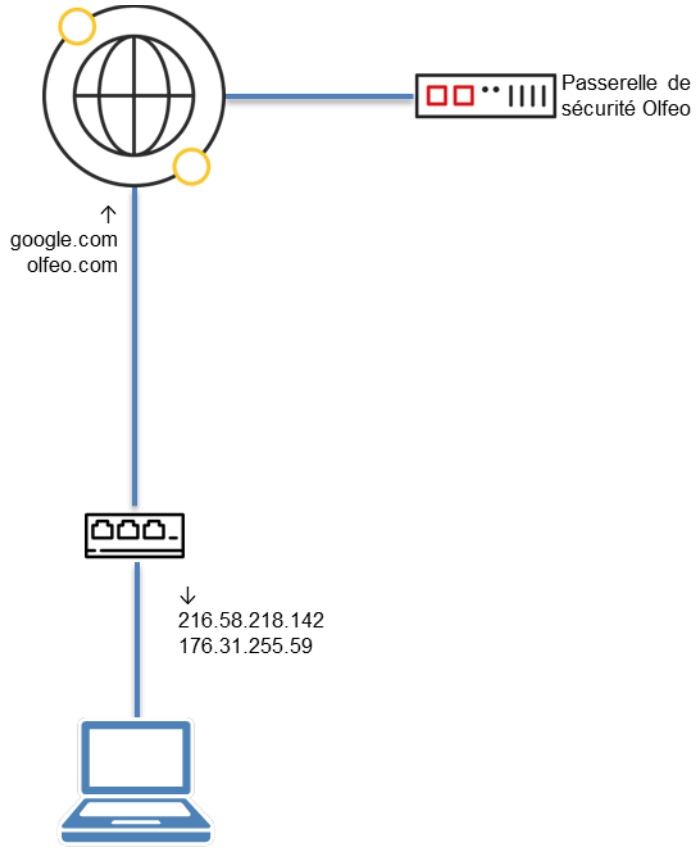
2.2 MODE HEBERGE (SAAS)

Ce mode consiste à positionner le filtrage DNS Olfeo dans le cloud et à le rendre accessible sur Internet via une adresse IP publique. Ce serveur sera utilisé pour la résolution des noms de domaine dans le réseau de l'entreprise.

L'adresse IP publique du filtrage DNS Olfeo est alors configurée en tant que redirecteur dans les paramètres du serveur DNS interne.



Pour les entreprises qui ne disposent pas de serveurs DNS internes et pour les nomades équipés d'ordinateurs portables qui se trouvent en dehors du réseau de l'entreprise, la passerelle de sécurité Olfeo peut être directement configurée en tant que serveur DNS sur les clients.



La publication du service de filtrage DNS Olfeo sur Internet nécessite de sécuriser l'accès à cette ressource contre les attaques et intrusions. Cette partie est à la charge du prestataire ou du client final.

2.3 FONCTIONNALITES DISPONIBLES

En mode d'intégration Filtrage DNS, les fonctionnalités suivantes sont disponibles :

Filtrage d'URL	Filtrage Protocolaire	Cache / QoS / Déchiffrement SSL	Antivirus	Portail Public
✓ HTTP HTTPS[1]	✗	✗	✗[1]	✓

[1] Le filtrage d'URL des flux HTTPS est effectué sur le nom de domaine uniquement, le déchiffrement SSL n'est pas nécessaire ni pertinent.
[2] Aucun fichier ne sera analysé. Cependant le filtrage d'URLs Olfeo, de par la catégorie risques de sécurités, pourra bloquer les sites malveillants.
Les autres fonctions peuvent être accessibles sur un mode d'intégration mixte, par exemple filtrage DNS + couplage ICAP (antivirus) ou filtrage DNS + proxy explicite (déchiffrement SSL).

2.4 AVANTAGES DU FILTRAGE DNS

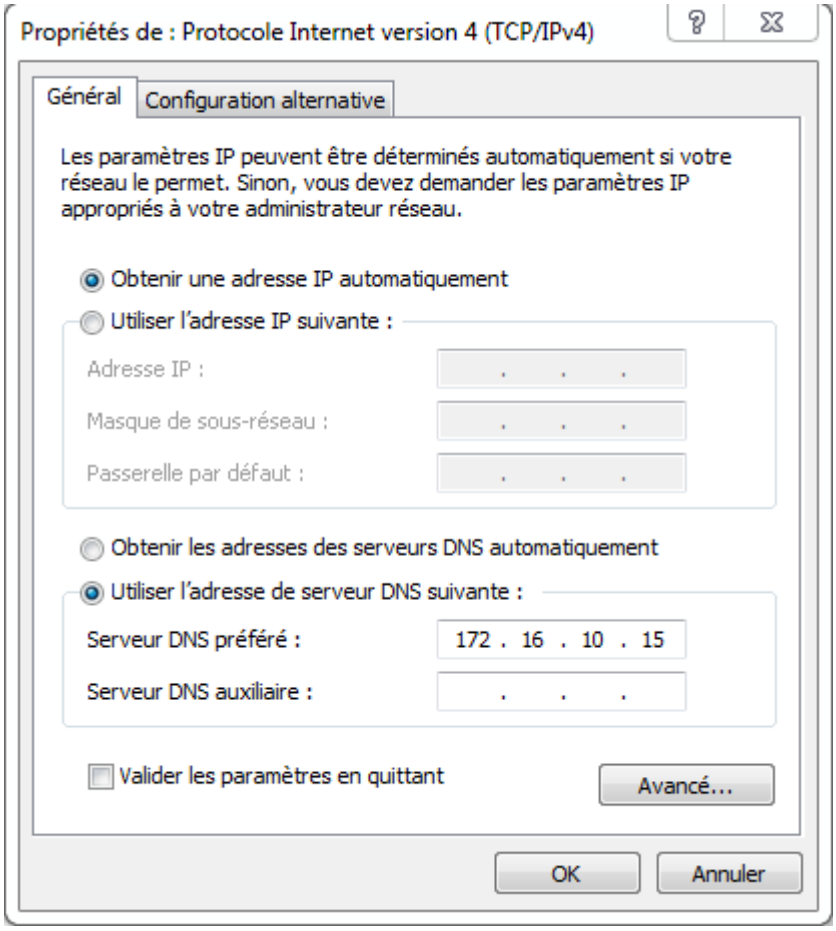
Le mode d'intégration Filtrage DNS présente de nombreux avantages, notamment au niveau de la simplicité de la mise en œuvre.

2.4.1 FACILITE DE DEPLOIEMENT

En mode d'intégration Proxy Explicite, mode le plus fréquemment utilisé, le déploiement des paramètres de proxy est souvent fastidieux : il faut prendre en compte les différents navigateurs et leurs particularités (Mozilla Firefox), les différents périphériques (PC portable/fixe, smartphone, tablette, etc) et les différents systèmes d'exploitation (MS Windows, Linux, Android, iOS, etc).

Le filtrage DNS se reposant uniquement sur la résolution des noms de domaine réalisés par le navigateur, il n'est pas nécessaire de paramétrer les options du proxy ou de déployer une configuration quelconque des navigateurs.

Il suffit de renseigner l'adresse IP de la machine Olfeo qui effectue le filtrage DNS dans les paramètres DNS du système d'exploitation de la machine cliente. Par exemple si la machine Olfeo dispose de l'adresse IP 172.16.10.15 (Mode local/on-premise), il faudra modifier les propriétés de la connexion réseau comme suit dans MS Windows :

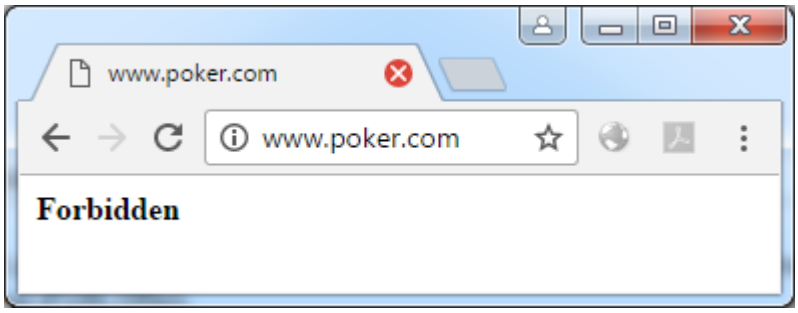


Ce paramétrage peut être diffusé automatiquement, par un routeur ou un pare-feu, via DHCP sur les différents équipements clients connectés.

2.4.2 FILTRAGE D'URL SIMPLIFIE

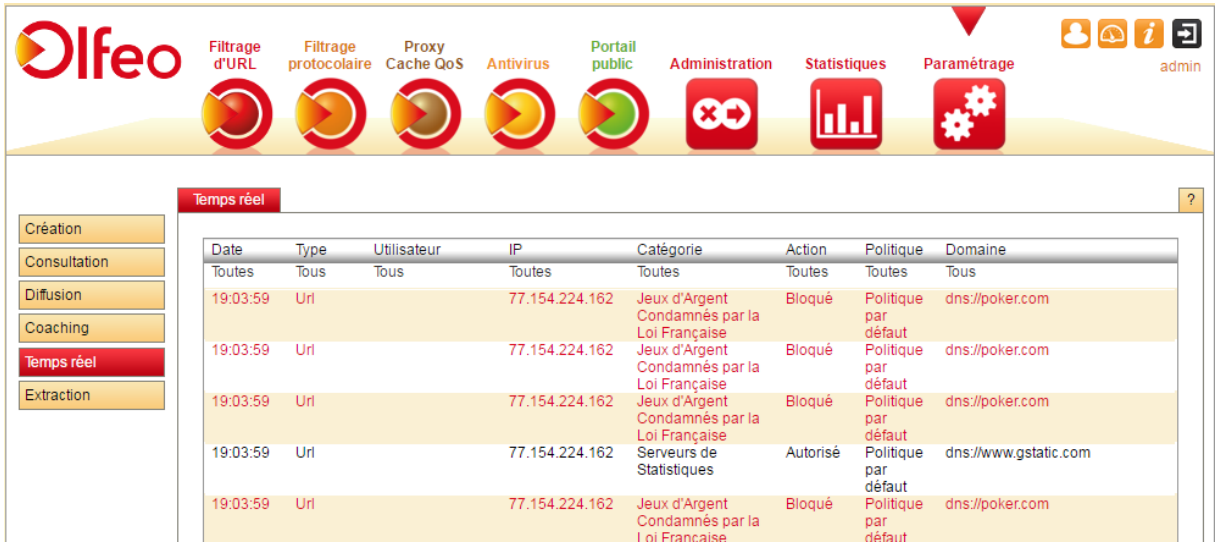
Le Filtrage DNS permet de bloquer l'accès à certaines catégories de sites Internet en profitant de la qualité de la base d'URL Olfeo.

La page de blocage renvoyée est simplifiée à l'extrême, le blocage est direct et efficace (flux HTTP) :



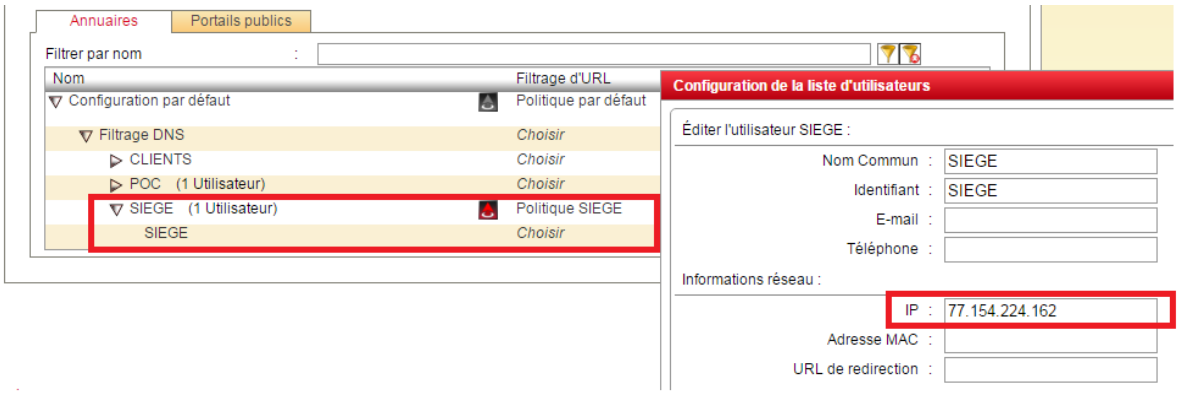
La page de blocage peut être personnalisée, différentes solutions nous permettent de le faire(ex : installation d'un service type Apache sur le système, redirection vers une page existante…)

L'administrateur de la solution Olfeo visualise les requêtes autorisées et bloquées en temps réel comme pour les autres modes d'intégration :

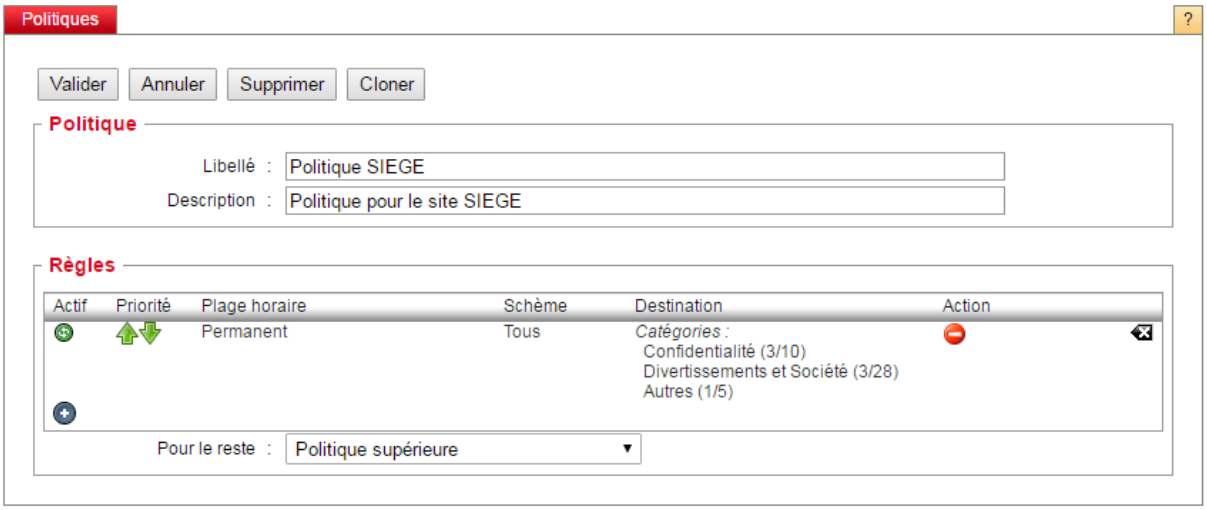


L'interface des statistiques, pour la création d'analyse, est également exploitable.

L'application de politiques de filtrage différenciées peut être réalisée via sur la base des groupes des utilisateurs synchronisés (authentification via portail captif avec ou sans NTLM) ou l'adresse IP privée source des machines (mode local/on-premise) ou via adresse IP publique de sortie de la connexion à Internet (mode SaaS).



Différentes règles d'accès (ACL) et politiques peuvent être appliquées à ces groupes (adresses IP), le principe de fonctionnement de l'application des politiques (pyramide inversée) s'applique également à ce mode :



2.4.3 PERFORMANCE

Le Filtrage DNS Olfeo se repose sur le protocole DNS, lui-même exploitant le protocole UDP avec tous les avantages qui lui appartiennent.
Le protocole UDP a été introduit pour transmettre des données rapidement et simplement.
Ainsi le volume de données échangé entre le poste client et le système de filtrage sera beaucoup plus faible dans le mode d'intégration Filtrage DNS.

2.4.4 FILTRAGE DES NOMADES

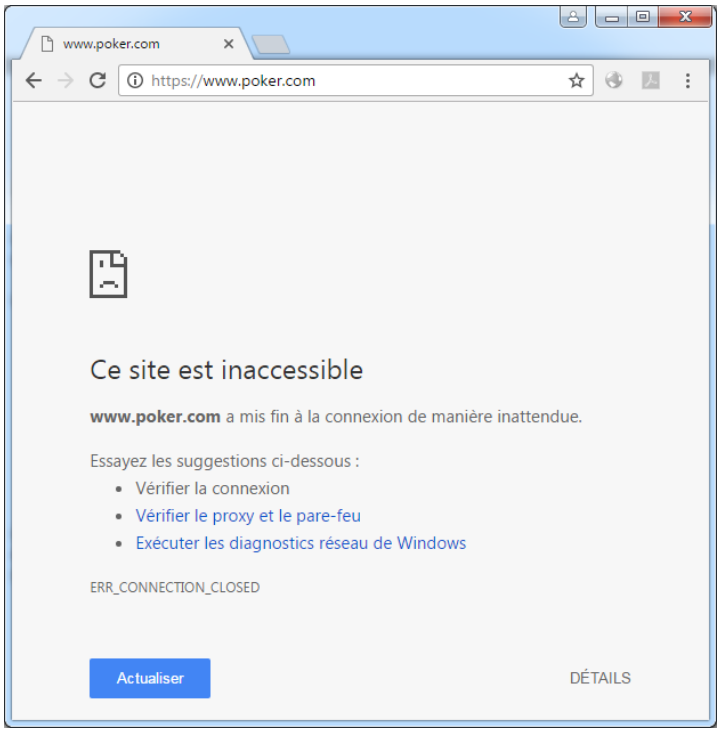
Lorsque Olfeo est intégrée en mode hébergé, le service de filtrage DNS est accessible en permanence à partir du moment où le client est connecté à Internet.

Cela permet d'avoir une continuité dans l'application des politiques de filtrage indépendamment de l'emplacement géographique du nomade. Afin de conserver la politique nous devrons pouvoir l'identifier. A défaut la politique minimale s'appliquera.

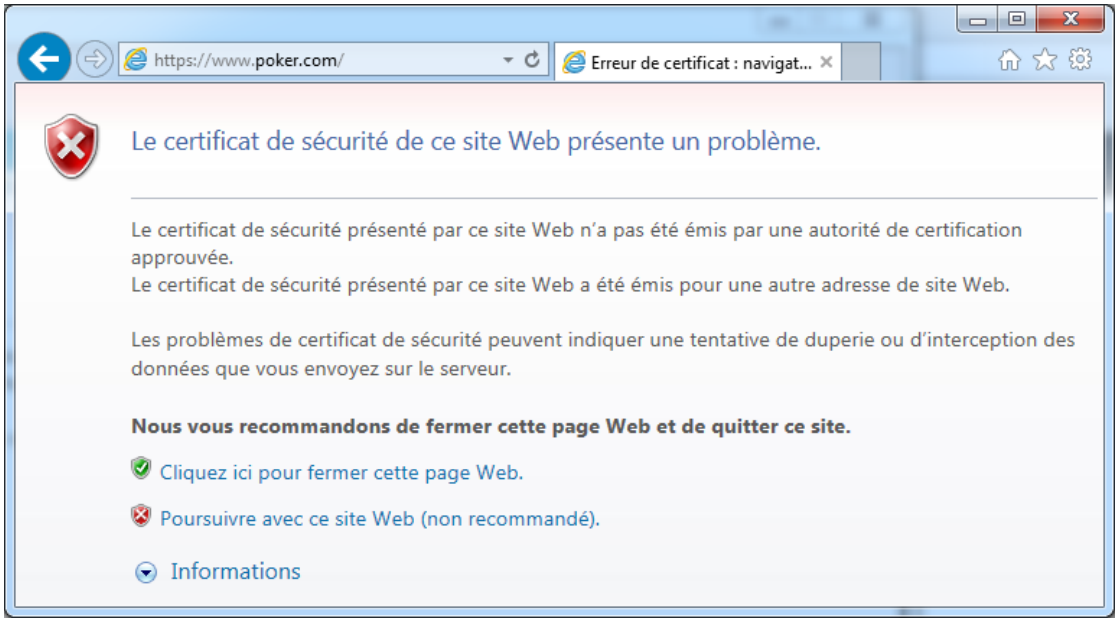
2.5 LIMITES DU FILTRAGE DNS

2.5.1 FILTRAGE HTTPS

Le blocage d'un site HTTPS se traduit par une erreur SSL si la configuration du proxy Olfeo n'est pas réalisée (filtrage basique) :



En cas d'utilisation du proxy Olfeo, il est possible d'afficher une page de blocage personnalisée lors de l'accès à un site HTTPS bloqué après validation de l'accès « Poursuivre avec ce site Web » :



Le déchiffrement SSL ne peut pas être implémenté dans ce mode d'intégration.

Olfeo est toutefois en mesure de traiter le nom de domaine dans les requêtes HTTPS, le taux de filtrage obtenu reste ainsi très élevé. Exemple d'une requête bloquée sur le site https://www.8changes.com :

3 LEXIQUE

DNS : Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.
Les ordinateurs connectés à un réseau IP, comme Internet, possèdent une adresse IP. Ces adresses sont numériques afin d'être plus facilement traitées par une machine. En IPv4, elles sont représentées sous la forme « xxx.xxx.xxx.xxx », où « xxx » est un nombre variant entre 0 et 255 (en système décimal). En IPv6, les IP sont sous forme « xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx », où « x » représente un chiffre de la base hexadécimale. Pour faciliter l'accès aux systèmes qui disposent de ces adresses, un mécanisme a été mis en place permettant d'associer à une adresse IP un nom, plus simple à retenir, appelé « nom de domaine ». Résoudre un nom de domaine consiste à trouver l'adresse IP qui lui est associée.

UDP : Le User Datagram Protocol (UDP, en français protocole de datagramme utilisateur) est un des principaux protocoles de télécommunication utilisés par Internet.
Le rôle de ce protocole est de permettre la transmission de données de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Contrairement au protocole TCP, il fonctionne sans négociation : il n'existe pas de procédure de connexion préalable à l'envoi des données (le handshaking). Donc UDP ne garantit pas la bonne livraison des datagrammes à destination, ni leur ordre d'arrivée. Il est également possible que des datagrammes soient reçus en plusieurs exemplaires.
La nature de UDP le rend utile pour transmettre rapidement de petites quantités de données, depuis un serveur vers de nombreux clients ou bien dans des cas où la perte d'un datagramme est moins gênante que l'attente de sa retransmission. Le DNS, la voix sur IP ou les jeux en ligne sont des utilisateurs typiques de ce protocole.

Client : ici, le terme client désigne tout équipement connecté à un réseau privé (entreprise, domicile de l'employé) ou public (réseau wifi invité) et disposant d'un accès à Internet. Cela couvre les postes de travail, les serveurs, les smartphones, les tablettes, les objets connectés : tout type d'appareil faisant appel au DNS pour l'accès à Internet.

Adresse IP publique : il s'agit d'adresses IP qui ne peuvent normalement pas être utilisées dans un réseau local mais uniquement sur Internet. Votre modem/routeur (Freebox, Bbox, box SFR, etc.) dispose d'une adresse IP publique côté Internet ce qui la rend visible sur Internet. Lorsque vous accédez à un site web vous utilisez l'adresse IP publique du serveur web (après résolution DNS). Les adresses IP publiques représentent toutes les adresses IP qui ne font pas partie des plages d'adresses privées (par exemple de 10.0.0.0 à 10.255.255.255 ou encore de 192.168.0.0 à 192.168.255.255).

A PROPOS D'OLFEO

Olfeo est éditeur de logiciel et expert de la sécurité web et du filtrage de contenus. Chez Olfeo, nous croyons que la sécurité positive est le meilleur moyen de vous protéger contre les nouvelles menaces du web tout en accompagnant les nouveaux usages chez vos collaborateurs.

Notre solution a aujourd'hui été adoptée par 2000 clients, représentant plus de 3 millions d'utilisateurs.

Il est dans notre ADN de considérer les projets de sécurité web au-delà des seuls aspects fonctionnels et techniques. Pour cela, nous proposons aux organisations exigeantes, la seule passerelle de sécurité Web basée sur une infrastructure proxy qui réunit à la fois l'expertise technologique, la conformité légale et culturelle ainsi que le facteur humain au service de la sécurité positive.

La sécurité positive doit être vue au sens large du terme. C'est l'approche novatrice d'Olfeo qui réunit ces trois enjeux fondamentaux de la sécurité Web dont deux d'entre eux sont trop souvent négligés dans beaucoup d'autres solutions. Olfeo est ainsi la seule solution qui peut réellement créer un environnement de confiance pour vos utilisateurs sur le Web.

Notre passerelle de sécurité web, basée sur une infrastructure Proxy inclut les modules suivants :

- Proxy Cache QoS et déchiffrement SSL
- Filtrage d'URL
- Filtrage DNS
- Filtrage Protocolaire
- Antivirus de flux
- Portail Public

Retrouvez des actualités juridiques, métier et produit sur nos réseaux sociaux :

www.linkedin.com/company/olfeo

https://twitter.com/olfeo

www.youtube.com/user/OlfeoTV

https://www.facebook.com/societeolfeo

LES GUIDES D'EXPERTS OLFEO

Notre équipe d'experts techniques rédige et diffuse régulièrement des guides d'experts destinés à répondre à des problématiques techniques d'actualité. Ces guides vous permettent d'optimiser l'utilisation de la passerelle de sécurité web Olfeo.

Nos guides d'experts Olfeo visent à aborder des thématiques d'actualité principalement sous l'angle de l'expertise technologique. Pour accéder à nos ressources sous l'angle de la conformité légale & culturelle ainsi que sur le facteur humain, rendez-vous sur : www.olfeo.com/societe/actualites/ressources

Olfeo
La sécurité positive

LA SECURITE POSITIVE POUR LES ORGANISATIONS EXIGEANTES

consulting@olfeo.com

+33 (0) 969 396 999

www.olfeo.com