Sécurisation d'accès Internet par

Squid/SquidGuard

sur pfsense

Ershad Ramezani

Table des matières

Introduction 2
La demande 2
La solution proposée 2
Le serveur proxy 2
Comment fonctionne-t-il ? 2
Squid et SquidGuard 2
Première partie de la demande : LAN 2
Deuxième partie de la demande : Portail captif (GUEST-LAN) 3
Schéma 3
Installation de pfsense 3
Installation du serveur Windows SRVAD 6
La machine Windows pour le réseau invité 6
Configuration de base de routeur 6
Configuration de base de serveur portail captif : 7
Configuration Routage 7
Tester le bon fonctionnement du réseaux par ping 8
création des utilisateurs et des groupes sur l'AD 8
Installer et configurer le proxy Squid pour le réseau LAN 8
Configuration générale de squid 8
Création d'un autorité de certificat sur pfsense 9
Des ACLs 10
Configuration de Firefox pour le proxy 10
Test du site http 10
Test du site https 10
La solution pour les site https 11
Authentication LDAP sur Squid 12
Method LDAPS sur le port 636 12
Pourquoi j'utilise LDAPS : 12
Comment le mettre en place : 12
Installation SquidGuard 13
Configuration Common ACL 14
Configuration groups ACL 15
Portail Captif 17
Configuration d'un portail captif 18
Tester le portail captif 19
Squid : Proxy transparent pour le portail captif 20
La demande pour le réseau invité : 21

Introduction

La demande

Le centre de formation ADRAR-FROM demande de sécuriser les accès Internet sur son site qui reçoit, en plus du personnel et des stagiaires, de nombreux visiteurs.

La gestion des droits d'accès à certains sites se fera en fonction du groupe LDAP auquel appartient l'utilisateur pour le personnel du centre de formation et des stagiaires.

En plus de la gestion des droits, il nous faut mettre en place une solution conservation des accès Internet comme le prévoit la loi pour tout organisme fournissant un accès Internet public.

Les utilisateurs seront répartis dans 3 groupes :

- Administration : pour le personnel administratif
- Formation : pour les stagiaires en formation
- Invité : pour des postes en libre-service et pour des visiteurs occasionnels

- Le personnel administratif aura accès à tous les sites internet, sauf ceux inclus dans la blacklist « Shopping » de UT1.
- Les stagiaires n'auront pas accès aux sites : réseaux sociaux + shopping de la blacklist UT1.
- Les visiteurs devront passer par un portail captif en se connectant à un navigateur Web, et n'auront accès qu'à un nombre de sites limités.

La solution proposée

Le serveur proxy

Ma solution pour ce cahier des charges est un serveur proxy. Mais qu'est-ce qu'un serveur proxy ? Un serveur proxy agit comme une passerelle entre l'utilisateur et Internet. Il s'agit d'un serveur intermédiaire séparant les utilisateurs finaux des sites Web où ils naviguent. Les serveurs proxy offrent différents niveaux de fonctionnalité, de sécurité et de confidentialité.

Comment fonctionne-t-il ?

Lorsque vous envoyez une requête Web, votre requête est d'abord transmise au serveur proxy. Le serveur proxy effectue ensuite votre demande Web en votre nom, recueille la réponse du serveur Web et vous transmet les données de la page Web afin que vous puissiez voir la page dans votre navigateur.

Un serveur proxy peut modifier l'adresse IP dans la requête, de sorte que le serveur Web ne sache pas quelle est l'adresse IP de l'utilisateur d'origine. Il peut mettre en cache les données afin que lorsque vous essayez d'accéder à un site Web, le serveur proxy vérifie s'il possède la copie la plus récente du site, puis vous envoie la copie enregistrée au lieu de la télécharger à partir du serveur Web sur Internet. Et enfin, un serveur proxy peut bloquer l'accès à certaines pages Web, en fonction de l'adresse IP ou le nom du domaine de site web, etc.

Squid et SquidGuard

Squid est un proxy. Je le propose car il prend en charge HTTP, HTTPS, FTP, etc. Squid dispose de contrôles d'accès aux sites web. Il fonctionne sur la plupart des systèmes d'exploitation disponibles, y compris Windows et linux et il est gratuit.

SquidGuard est un logiciel de redirection d'URL, qui peut être utilisé pour le contrôle avancé du contenu des sites Web auxquels les utilisateurs peuvent accéder. Il est écrit comme un plug-in pour Squid et utilise des Blacklists pour définir les sites pour lesquels l'accès est redirigé.

Première partie de la demande : LAN

Pour réaliser la première partie de ce projet, c'est-à-dire la gestion des droits d'accès à certains sites pour des personnels et des stagiaires, j'installe le Squid et SquidGuard sur un routeur pfsense et ensuite je configure la connexion entre le Squid et SquidGuard avec le serveur AD afin de mettre en place des règles des filtrage selon les différents groupes d'utilisateurs que j'ajouterai dans le serveur AD.

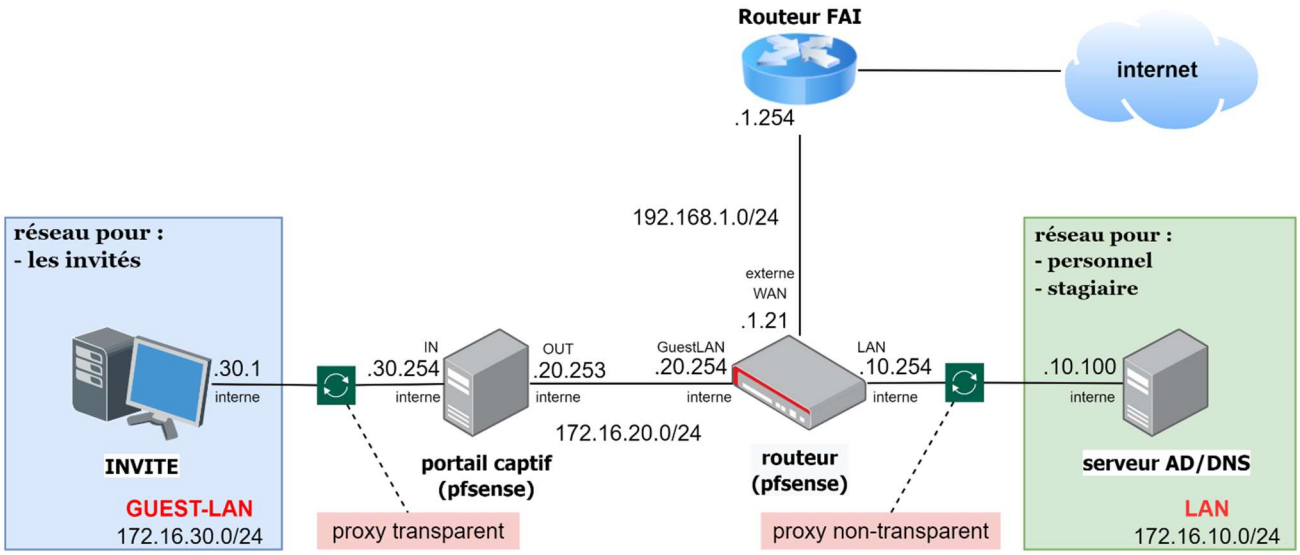
Deuxième partie de la demande : Portail captif (GUEST-LAN)

Seconde partie consiste à créer un portail captif pour les invités. A cause des limites techniques qu'on a avec le squid sur un routeur pfsense, je vais ajouter une deuxième machine pfsense pour utiliser la fonctionnalité portail captif avec un squid dédié pour les invités qui se connectent à travers ce portail captif. Cela me permet de créer les utilisateurs invités au fur et à mesure et localement sur ce serveur pfsense. Ce pfsense peux être aussi un point d'accès wifi pour faciliter la connexion au réseau pour les invités.

C'est quoi la limite :

Mon but est d'ajouter un squid transparent derrière le portail captif ce qui n'est pas possible à la fois avec proxy non-transparent sur le même squid. En plus, je vais configurer l'authentification LDAP pour les utilisateurs LAN mais authentification locale pour les invités car je ne veux pas polluer mon AD avec les utilisateurs invités qui sont temporaires.

Schéma



Installation de pfsense

Pour ce projet j'aurai besoin de deux machines pfsense. Accéder au lien suivant pour faire une simple installation de pfsense sur une machine virtuelle. J'ai installé mes deux machines sur le Hyper-V. pendant l'installation des deux machines, ajoutez une interface type **externe** et deux autre interface type **interne** sur le routeur et seulement deux interfaces internes sur le serveur portail captif. Configurer les adresses IP par l'option 2 et selon le schéma au-dessus. Ensuite on utilisera l'interface de la configuration de chaque machine pour la suite des configurations. Je commence par la configuration du routeur. J'ai utilisé ma machine SRVAD (l'installation est expliquée dans la prochaine partie) pour accéder à l'interface de la configuration de mon routeur. L'adresse IP qu'on utilise pour accéder à cette interface web doit être forcément sur l'interface LAN où il y a le SRVAD (dû à la configuration par défaut du pare-feu sur pfsense qui ne nous autorise que la connexion par cette interface).

La version complète est disponible aussi mais protéger par un mot de passe.

Merci de me contacter par email :

Ershad.ra@gmail.com