tetaneutral.net - Evolution #156

Reverse proxy

28/02/2012 17:00 - davy rangom

Statut:	Fermé	**Début:**	01/02/2012
Priorité:	Normal	**Echéance:**	
Assigné à:	davy rangom	**% réalisé:**	70%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:			

Description

J'ai fait n'importe quoi en voulant mettre à jour le suivi de projet et j'ai supprimé le projet parmi les tickets.
Mais je me suis empressé de le refaire afin de les laisser des traces et de vous tenir au courant de mon avancée.
Pour rappel, voici la machine mis à ma disposition:
- testlg2.tetaneutral.net

Donc voilà, aujourd'hui j'ai finis la mise en production du reverse proxy avec une interface Web protégé par https et mot de passe.
Il y a des modifications à réaliser sur le dns aussi mais j'ai pu tester facilement en renseignent mon fichier /etc/hosts.
Pour le fun, j'ai aussi rajouté une interface nagios configuré de manière basique pour alimenter le portail. J'ai pensé que ce serait utile et ce instance de nagios peut évoluer par la suite avec les besoins.
Je n'ose pas vous fournir les login et mot de passes à travers ce portail.
Je vous les enverrai par mail.
Il faudra que je fournisse une documentation technique afin de pouvoir utiliser et mettre à jour le portail et le reverse proxy.

Historique

#1 - 28/02/2012 17:19 - Laurent GUERBY

Historique du #151 via courriel :

Mettre en place un reverse proxy avec authentification pour acceder aux interfaces du subnet radio 172.31.31.x (et tout autre subnet RFC1918 utile).

Alors, j'ai effectivement commencé la-dessus grâce à une petite maquette virtuelle avec un switch virtuelle. Mes premiers tests sont concluants car j'ai réussi à mettre en place un reverse proxy d'apache.Il y a un détail que j'avais omis mais que j'ai résolu, c'est que j'ai besoin de rajouter des noms symboliques au domaine tetaneutral.net; ce qui implique quelques modifications sur votre serveur DNS, c'est indispensable. Est ce que tu as pu me créer la machine virtuelle? J'ai besoin d'un machine qui a la même configuration que h2 d'un point de vue "Réseau"; c'est à dire qui une ip publique et accès au réseau privé. En ce moment je suis en train de réfléchir à l'apparence de l'interface, puis je m'occuperai un peu de la partie sécurité.

J'ai ajouté ta clé :

ssh -p 2222 root@testlg2.tetaneutral.net

La machine virtuelle a une IP 172.31.31 sur eth0 en plus de son IP publique donc elle est comme h2

Si ta clé ne marche pas directement, logue toi sur h1 en root puis la meme commande que ci dessus. Sinon je mettrai un password

#2 - 29/02/2012 14:28 - Philippe Latu

Suite à la réunion de ce matin, voici quelques éléments.

. Exemple de règle iptables du type port forwarding
Dans la chaîne PREROUTING de la table nat, on peut utiliser une syntaxe du type suivant

```
-A PREROUTING -i eth0 -d <@ip publique> -p tcp --dport 50154 -j DNAT --to-destination <@ip privée>:22
```

. Ce type de règle peut être invoquée par portknocking
Le paquet knockd devrait convenir pour cette fonction

. La limitation de durée utilise le module time d'iptables
Les heures de début et de fin sont données via la paramètres timestart et timestop qui peuvent être alimentés à l'aide de la commande date

heure de début :

```
$ date "+%H:%M"
14:22
```

heure de fin :

```
$ date "+%H:%M" -d "1 hour"
15:23
```

exemple :

```
# iptables -A INPUT -i eth0 -p udp --dport 8888 -m time --timestart `date "+%H:%M"` --timestop `date "+%H:%M"
-d "1 hour"` -j ACCEPT

# iptables -vL INPUT | grep -i time
0     0 ACCEPT     udp  --  eth0   any     anywhere     anywhere      udp dpt:8888 TIME from 14:25:00 to 15:25
:00 UTC
```

#3 - 29/02/2012 15:07 - Philippe Latu

Toujours suite à la réunion de ce matin, voici quelques éléments sur la configuration du module proxy d'apache2

Il faut bien sûr que le module soit actif ...

```
# a2enmod «nom du module»

# find /etc/apache2/mods-enabled/ -name \*proxy\*
/etc/apache2/mods-enabled/proxy_http.load
/etc/apache2/mods-enabled/proxy.load
/etc/apache2/mods-enabled/proxy.conf
/etc/apache2/mods-enabled/proxy_connect.load
```

Exemple de fichier de config pour un équipement dans le répertoire /etc/apache2/sites-available

```
<VirtualHost «@ip-proxy»:80>
ServerAdmin webmaster@proxy.mondomaine.fr

ServerName www.equipement.mondomaine.fr
ErrorLog /var/log/apache2/equipement-error.log
TransferLog /var/log/apache2/equipement-access.log

ProxyPass / http://«@ip-equipement»:80/
ProxyPassReverse / http://«@ip-equipement»:80/
ProxyVia on
</VirtualHost>
```

Autrement, pour utiliser un domaine unique avec /equipement, on utilise la directive Location

```
<Location /equipement>
  ProxyPass http://«@ip_equipement»/
  ProxyPassReverse http://@ip_equipement»/
</Location>
```

#4 - 01/03/2012 11:53 - davy rangom

Monsieur Latu,
Suite à ce qui avait été dit et la piste que vous m'avez donné concernant la directive <Location> pour le reverse proxy ,j'ai mis en application ce qui a été dit.
J'avais bien activé auparavant tous les modules nécessaires mais j'utilisais les virtual hosts pour le proxy inverse. J'ai donc réalisé un premier test avec la directive <Location> sur mon réseau virtualisé en local et le test était positif, j'était satisfait; je n'avais plus besoin de renseigner mon fichier /etc/hosts.
Puis j'ai réalisé les tests sur la machine qu'on m'a prété à tetaneutral, j'ai obtenu un comportement très bizarre du serveur proxy.
En tapant https://testlg2.tetaneutral.net/equipement6 , j'ai obtenu une erreur 404.
En analysant le problème, je me suis aperçu que dans un premier temps le proxy inverse faisait bien la requête vers le la machine 172.31.31.6.
Mais par la suite il doit chargé un fichier login.cgi ; c'est à ce moment que le serveur ne se comporte pas comme je l'aurait voulu.
En effet j'ai remarqué que l'url avait changé. Au lieu d'avoir https://testlg2.tetaneutral.net/equipement6, elle a changé en https://testlg2.tetaneutral.net/login.cgi?uri=/ or normalement j'aurais du avoir https://testlg2.tetaneutral.net/equipement6/login.cgi?uri=/. Cela veut dire que le proxy essaie de renvoyer le fichier login.cgi qui est en fait sur l'équipement wifi et ce n'est pas normal.
Je vous avoue que je ne comprend vraiment pas le problème puisqu'avec les virtual host je n'ai pas de ce genre comportement et sur ma machine personnelle non plus.
Je vous demande si vous savez à quoi cela peut être du ?
Voici le contenu du fichier /etc/apache2/sites-available/tsfeq6 par exemple:
<Location /equipement6>
ProxyPass http://172.31.31.6/
ProxyPassReverse http://172.31.31.6/
</Location>
Je continue à essayer d'identifier le problème et je passe aussi à l'autre aspect évoqué en attendant.

#5 - 01/03/2012 14:24 - Mehdi Abaakouk

Bonjour,

On ne peut changer la racine d'une application avec le "mod_proxy", uniquement si l'application est prévu pour.
c'est à dire:
- que l'on puisse spécifier la racine du site, pour que celle-ci construise toutes les urls de l'application en y ajoutant cette racine
- soit l'application à était complément conçus avec des urls relative.

Dans le cas, de l'interface des web NS, la page "/" contient (j'imagine j'ai pas vérifier) un redirect vers "/login.cgi?uri=/" (une url en absolue malheureusement), voila pourquoi ce ne doit pas fonctionner.

Pour les applications de ce genre, il reste une solution pas très sexy, le module apache "mod_proxy_html", qui peut réécrire les urls dans les pages, ça marche bien dans des applis par trop complexe.

http://httpd.apache.org/docs/2.4/mod/mod_proxy_html.html

Voir surtout la directive "ProxyHTMLURLMap"

#6 - 01/03/2012 15:08 - Laurent GUERBY

On peut faire comme on a prévu pour le ssh avec une redirection de port de testlg2:650IP vers 172.31.31.IP:80 si c'est trop compliqué avec les outils apache.

D'un autre coté le ProxyHTMLURLMap permettrai d'avoir les liens entre les antennes (section "Stations" de Main) qui marchent tout seul.

#7 - 01/03/2012 22:20 - davy rangom

Merci Mehdi!
Il s'agit effectivement d'une URL absolue, j'ai vérifié dans les logs du serveur.Je vais me pencher actuellement sur le proxy_html. Je n'avais pas entendu parler de ce module.
Bonne soirée

#8 - 06/03/2012 18:29 - davy rangom

Bonsoir à tous,

J'ai mis en application le module proxy_html et je crois que cela fonctionne mais pas comme nous l'aurions désiré.
Le module n'est nativement pas disponible dans /etc/apache2/mods-available/ cependant il est disponible dans les sources debian -> résolu.
Je pense que comme l'a dit Mehdi, l'application présente sur l'interface web des équipements radio est un peu complexe.

1. Je crois qu'il ne charge pas tous les fichiers car l'affichage n'est pas le même.
2. Même si l'affichage n'est pas le même, je me suis dis que ce n'étais pas trop grave et je me suis connecté sur l'une des interfaces et j'ai eu l'impression que quelques fonctionnalité ne fonctionnaient plus aussi bien .
3. Pour le moment, j'ai laissé les liens sur le portail de type "https://testlg2.tetaneutral.net/equipement43" pour que vous jugiez par vous-même.Il suffit de cliquer dessus.
4. Voici quand même le contenu d'un fichier de type site au cas où le problème vous semblerait évident :

```
ProxyRequests off
ProxyPass /equipement7/ http://172.31.31.7/
ProxyHTMLURLMap http://http://172.31.31.7/ /equipement7/

<Location /equipement7/>
ProxyPassReverse /
SetOutputFilter  proxy-html
ProxyHTMLURLMap  /      /equipement7/
ProxyHTMLURLMap  /equipement7/  /equipement7/
RequestHeader    unset  Accept-Encoding
</Location>
```

Voici ce que je pense :
Même si la première solution proposée avec les différents noms de domaine ne vous convenait pas elle est cependant la plus efficace et aussi fonctionnelle que le système de tunnel SSh que vous utilisez classiquement.

- L'avantage est que l'on peut cliquer sur le lien et on est dirigé vers l'interface désirée.
- L'inconvénient qui aurait du être palier par le module proxy_html et les directive de type "Location" et qu'il faille utiliser un service de noms ou renseigner sont fichier /etc/hosts.
  Cependant, j'avoue que l'idéal serait la solution utilisant la directive "Location" mais le rendu désiré n'est pas au rdv à 100% .

Voici ce que j'avais à dire par rapport à l'avancement du projet. Faites un tour sur le portail et posez moi des questions si le besoin s'en ressent.
Maintenant, je passe à la fonctionnalité manquante qui est très intéressante.

#9 - 21/03/2012 08:50 - davy rangom

Bonjour à tous,

Toutes les fonctionnalités ont été incluses au portail. On a maintenant le déclenchement du port-knocking à travers un formulaire, ça fonctionne plutôt bien.
Je dois juste remettre l'authentification par mot de passe au site, mais je ne peux pas le faire d'où je suis actuellement.
J'ai également changé ma politique de nommage pour les URL des différents hôtes. Maintenant, on a des URL de ce type: https://<equipement>.testlg2.tetaneutral.net.
J'ai effectué ce changement car nous avions parlé de délégation du domaine testlg2.tetaneutral.net.
Même si le TER est fini dans le cadre scolaire, je veux bien m'occuper du DNS testlg2.tetaneutral.net pour que le portail soit complètement fonctionnel.

Passez une bonne journée.

#10 - 21/03/2012 16:47 - Mehdi Abaakouk

Bonjour davy,

Je t'ai créé un sous-domaine tsf.tetaneutral.net que j'ai délégué à la machine ns.tsf.tetaneutral.net (qui est la même machine que testlg2.tetaneutral.net)

J'ai volontairement pas mis testlg2 comme nom car ce nom d'hôte devrait disparaitre quand on mettra ton outil en prod.

Extrait de la conf bind du DNS de ttn

```
# Actuallement c'est la vm testlg2
$ORIGIN tsf.tetaneutral.net.
@                       IN NS   ns.tsf.tetaneutral.net.
ns                      IN  A      91.224.149.122
ns                      IN  AAAA   2a01:6600:8081:7A00::1
```

A toi de jouer, j'ai hâte d'essayé ton travail :)

Mehdi

#11 - 23/03/2012 00:57 - davy rangom

Cool merci Mehdi,

Dès que c'est OK je vous fait signe ;-)

#12 - 10/08/2018 08:50 - Matthieu Herrb

- Statut changé de En cours à Fermé

fermeture de tous les vieux tickets non suivis depuis plusieurs années