xmpp.chapril.org - Demande #5614

Rendre le service XMPP joignable sur le port 443

06/10/2021 20:41 - pitchum .

Statut:	Nouveau	**Début:**	06/10/2021
Priorité:	Normale	**Echéance:**	
Assigné à:	pitchum .	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Backlog		
Difficulté:	3 Moyen		

Description

Ça permettrait de rendre le service utilisable depuis certains campus universitaires par exemple, où la connectivité vers internet est très limitée.
Ça impliquerait de publier des méta-données sur https://chapril.org/.well-known/host-meta et d'activer un module nginx stream_ssl_preread sur bastion.

Historique

#1 - 20/02/2024 18:53 - pitchum .

Expérimenté sur mon serveur perso, ça nécessite de modifier tous les vhosts nginx pour qu'ils écoutent sur un port différent du port 443.

Ajouter ce bloc *stream* dans /etc/nginx/nginx.conf :

```
diff --git a/nginx/nginx.conf b/nginx/nginx.conf
index f52668a..c1dd930 100644
--- a/nginx/nginx.conf
+++ b/nginx/nginx.conf
@@ -81,3 +81,48 @@ http {
 #               proxy      on;
 #       }
 #}
+
+stream {
+
+    upstream httpserver {
+        server 127.0.0.1:442;
+    }
+
+    upstream xmppserver {
+        server 127.0.0.1:5223;
+    }
+
+    map $ssl_preread_alpn_protocols $upstream {
+        default httpserver;
+        "xmpp-client" xmppserver;
+    }
+    server {
+        listen 443;
+
+        ssl_preread on;
+        proxy_pass $upstream;
+        proxy_protocol on;
+    }
+}
```

Puis patcher **tous** les vhosts ainsi :

```
sed -i 's/listen (.*)443/listen \1442/g' /etc/nginx/sites-available/*
# puis
sed -i 's/listen (.*) default_server/listen \1 proxy_protocol/g' /etc/nginx/sites-available/*
```

Pour continuer d'avoir les IPs dans les logs (pour fail2ban notamment), créer le fichier /etc/nginx/conf.d/real_ip.conf contenant ceci :

```
set_real_ip_from 127.0.0.1;
set_real_ip_from ::1/128;
```

```
real_ip_header proxy_protocol;
```

Ajouter au bloc listen: du fichier /etc/ejabberd/ejabberd.yml :

```
  -
    port: 5225
    use_proxy_protocol: true
    ip: "::"
    module: ejabberd_c2s
    tls: true
    max_stanza_size: 65536
    shaper: c2s_shaper
    access: c2s
```

Adapter les enregistrements DNS :

```
_xmpps-client._tcp.chapril.org.         86400   IN      SRV  5 10 5223  xmpp.chapril.org.
_xmpps-client._tcp.chapril.org.         86400   IN      SRV 10 10  443  xmpp.chapril.org.
```