DOSSIER DE SECURISATION DES WEB SERVICES

ANNEXE 2 : FILTRAGE IP

ABREVIATIONS

Abréviation	Signification
SOAP	Simple Object Access Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
IPX	Implémentation Novell de l'Internet Datagram Protocol (IDP)
ACK	Drapeau du protocole TCP
RST	Drapeau du protocole TCP
SYN	Drapeau du protocole TCP
SSL	Secure Socket Layer
CA	Autorité de Certification
ESB	Enterprise Service Bus

REFERENCES

Abréviation	Signification
[DOSSIERSECWS]	Dossier_Securisation_Web_Services_v1r0.pdf
[ANASEC]	Annexe1_Analyse_Sécurité_Préalable_v1r0.pdf
[FILTRAGE]	Annexe2_Etude_ Securistation_WS_FiltrageIP_v1r0.pdf
[SSL]	Annexe3_Etude_ Securistation_WS_TunnelSSL_v1r0.pdf
[SYNAPSE]	Annexe4_Etude_ Securistation_WS_Synapse_v1r0.pdf
[SPRING]	Annexe5_Etude_ Securistation_WS_SPRING-Security_v1r0.pdf
[PROTOTYPE]	Annexe6_Etude_ Securistation_WS_Prototype_v1r0.pdf

TABLE DES MATIERES

TABLE DES ILLUSTRATIONS

TABLE DES LISTINGS

1.AVANT PROPOS

Ce document constitue une annexe du « Dossier de sécurisation des Web Services » publié par l'AMUE. Il a pour objectif de présenter la mise en œuvre d'un filtrage IP dans un objectif de sécurisation des Web Services. Par conséquent, afin d'appréhender correctement le contexte et le contenu de ce document, il est conseillé de lire au préalable le dossier de sécurisation des Web Services [DOSSIERSECWS].

Ce document concernant le filtrage IP s'adresse à un public connaissant déjà ce domaine proche du monde des réseaux et du système.

2.IMPLEMENTATION DU FILTRAGE IP

2.1. PRINCIPES

Le transport des web-service se réalise par l'utilisation des protocoles de transport TCP ou UDP et du protocole de réseau IP. Chaque message SOAP est divisé en un ou plusieurs paquets TCP ou UDP, chacun divisé en un ou plusieurs paquets IP. Le réseau transfère ses *paquets*, appelés aussi *datagrammes*. Chaque paquet est routé indépendamment des autres, même s'ils ont la même source et la même destination.

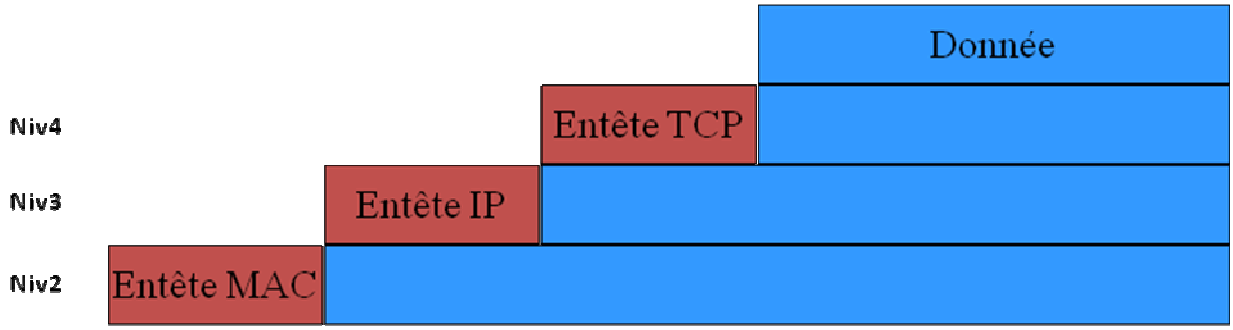

Figure 1 : Pile IP

Les paquets peuvent être filtrés en fonction de différentes caractéristiques :

- Filtrage de niveau 2 :
  - Adresse Mac
  - type de protocole (IP, IPX, ...)
- Filtrage de niveau 3
  - Adresse source, destination
  - Type de protocole supérieur (TCP, UDP,ICMP, , ...)
  - Options IP (source-routing, ...)
- Filtrage de niveau 4
  - Ports source et destination (identification de l'application)
  - Les bits ACK, RST, SYN

Dans le cadre de cette étude seul le filtrage de niveau 3 nous intéresse. En effet il permet de mettre en œuvre une identification sommaire de l'appelant. Le filtrage est basé sur les adresses IP qui permettent d'identifier l'appelant. Pour réaliser le filtrage, il faut mettre en place des règles permettant de déterminer si un paquet IP peut continuer sa route ou s'il doit être supprimé.

Le principe à mettre en œuvre est d'interdire tout sauf ce qui est autorisé. C'est-à-dire que toutes les adresses IP sont interdites sauf celles explicitement autorisées.

Les inconvénients de cette solution sont :

- la lourdeur de la gestion des règles en fonction du nombre d'adresses IP à autoriser.
- la facilité à détourner le filtrage (Il suffit de changer d'adresse IP)

Cependant ses avantages sont :

- Une solution techniquement facile à mettre en œuvre.
- Un coût faible.

Ce document va présenter deux exemples de mise en œuvre. Le nombre de firewall et d'applications permettant le filtrage étant conséquent, nous présentons ici 2 solutions open-source qui ont une grande probabilité d'être maîtrisées par les établissements.

2.2. FILTRAGE PAR FIREWALL : IPTABLE

Iptables est la commande qui permet de configurer Netfilter (module qui fournit à Linux les fonctions de pare-feu, de traduction d'adresse et d'historisation du trafic réseau.) Netfilter fonctionne en mode noyau. Il intercepte et manipule les paquets IP avant et après le routage.

Ce document ne va pas expliquer le fonctionnement d'IPTable. Il existe sur internet d'excellents tutoriaux (ex : http://linux-france.unixtech.be/prj/inetdoc/guides/iptables-tutorial/)

Pour autoriser tous ce qui vient de l'adresse IP 10.11.12.13 et 10.20.* il faut mettre en place ces règles

```
(1)      Iptable -A INPUT -i eth0 –s 10.11.12.13 ACCEPT
(2)      Iptable -A INPUT -i eth0 –s 10.20.0.0/16 ACCEPT
```

IPTables utilise des politiques (-P) afin de créer des règles par défaut. La règle suivante bloque tous les paquets entrants sur le firewall :

```
(3)      Iptables -P INPUT DROP
```

Avec ces 3 règles, toutes les demandes provenant d'autre adresse que 10.11.12.13 et 10.20.* seront « droppées ». Il est possible de raffiner la règle (1) par exemple en précisant le port et le protocole de transport utilisé :

```
(4)      Iptable -A INPUT -i eth0 -p tcp --dport 80 –s 10.11.12.13 ACCEPT
```

2.3. FILTRAGE APPLICATIF : APACHE

Il est possible de mettre en place un filtrage IP au niveau d'Apache. Pour cela il faut mettre en œuvre ces différentes lignes soit dans un ficher .htaccess, soit dans le fichier apache.conf

Pour rejeter tout ce qui ne vient pas de l'adresse IP 10.11.12.13 et 10.20.*

```
<code>
    Order allow,deny
    Deny from all
    Allow from 10.11.12.13 10.20
</code>
```

Listing 1 : Filtrage IP Apache

Dans le cas de l'utilisation de SSL (Décrit dans le document [SSL]), si une authentification mutuelle (client et serveur) est réalisée, il est aussi possible de faire du filtrage au niveau des certificats SSL. Pour n'autoriser que les appelants qui ont un certificat valide provenant de l' "AMUE" avec une Autorité de Certification (CA) "APOGEE":

```
<code>
    SSLVerifyClient require
    SSLVerifyDepth 5
    SSLCACertificateFile conf/ssl.crt/ca.crt
    SSLOptions +FakeBasicAuth
    SSLRequireSSL
    SSLRequire %{SSL_CLIENT_S_DN_O} eq "APOGEE"
               %{SSL_CLIENT_S_DN_OU} eq "AMUE"
</code>
```

Listing 2 : Filtrage SSL Apache

2.4. FILTRAGE APPLICATIF : SYNAPSE

2.4.1. LE FILTRAGE IP AVEC WSO2 ESB

WSO2 ESB qui est présenté en détail dans le document [SYNAPSE], permet également d'utiliser le filtrage IP lors du routage des requêtes vers un consommateur. Cela consiste à filtrer les adresses IP ou domaines définis dans le fichier de configuration de l'ESB : *synapse.xml*. Ainsi on peut spécifier les actions à mener sur des adresses IP simples ou même une plage d'adresses IP. Ces actions peuvent être de permettre l'accès à une ressource web service ou de l'en empêcher en lui renvoyant un message d'erreur.

Notons que des paramètres très fins peuvent être utilisés pour affiner d'avantage les échanges. Ainsi, il est possible de préciser le nombre de fois qu'une adresse IP, une plage d'adresses IP ou même un domaine serait autorisé durant un laps de temps imparti. A l'expiration de ce laps de temps ou à l'issue du nombre d'accès autorisé, une faute est alors renvoyée au consommateur. De plus, il est possible de spécifier le délai d'attente nécessaire avant que le nombre d'accès se renouvelle.

2.4.2. LE FICHIER DE CONFIGURATION

Le listing suivant montre la configuration nécessaire à WSO2 ESB afin d'opérer du filtrage IP. Il s'agit du fichier *synapse.xml* se trouvant dans le répertoire *\webapp\WEB-INF\classes\conf* à la racine du serveur WSO2 ESB. Ce fichier est chargé au démarrage du serveur. Il peut aussi être édité à travers l'interface graphique d'interfaçage de Synapse : WSO2.

```
<definitions xmlns="http://ws.apache.org/ns/synapse">
    <sequence name="main">
```

```
<!--Précise le traitement à appliquer à tout message entrant-->
<in>
    <!--property à ne faire que si on est derrière un reverse proxy comme Apache par exemple -->
    <property xmlns:ns1="http://org.apache.synapse/xsd"
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" name="REMOTE_ADDR"
           expression="get-property('transport','X-Forwarded-For')" scope="axis2"/>
     <throttle id="MyThrottle">
        <policy>
            <!--Définition des policies à appliquer-->
              <wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
                      xmlns:throttle="http://www.wso2.org/products/wso2commons/throttle">
                <throttle:ThrottleAssertion>
                    <wsp:All>
                            <!--Définition d'une règle pour toutes les autres adresses IP non définies
                            dans ce fichier. Le throttle peut être soit du type IP ou DOMAIN-->
                            <throttle:ID throttle:type="IP">Other</throttle:ID>
                            <wsp:ExactlyOne>
                            <!-- Cette assertion indique si l'adresse IP indiquée est autorisée ou non à
                            accéder à la ressource. -->
                            <throttle:IsAllow>false</throttle:IsAllow>
                            </wsp:ExactlyOne>
                    </wsp:All>
                    <wsp:All>
                            <!--Définition d'une politique pour une plage d'adresses-->
                            <throttle:ID throttle:type="IP">172.16.6.90-
                                   172.16.6.120</throttle:ID>
                            <wsp:ExactlyOne>
                            <!--Indication que l'accès à la ressource n'est pas autorisé-->
                            <throttle:IsAllow>false</throttle:IsAllow>
                            </wsp:ExactlyOne>
                    </wsp:All>
                    <wsp:All>
                        <throttle:ID throttle:type="IP">172.16.6.120-172.16.6.200</throttle:ID>
                        <wsp:ExactlyOne>
                            <wsp:All>
                            <!--Indique le nombre de fois que la plage d'adresses indiquée, peut
                            accéder à la ressource. -->
                            <throttle:MaximumCount>4</throttle:MaximumCount>
                            <!--Dans ce délai spécifié-->
                            <throttle:UnitTime>600000</throttle:UnitTime>
                            <!--Délai nécessaire pour accéder de nouveau à la ressource-->
                            <throttle:ProhibitTimePeriod wsp:Optional="true">5000
                            </throttle:ProhibitTimePeriod>
                            </wsp:All>
                            <!--On alloue l'accès à la ressource. Dans cette policy, ce sont les règles
                            définies avant celles-ci à savoir <throttle :MaximumCount>… qui sont
                            prioritaires-->
                            <throttle:IsAllow>true</throttle:IsAllow>
                        </wsp:ExactlyOne>
                    </wsp:All>
                </throttle:ThrottleAssertion>
            </wsp:Policy>
        </policy>
        <!--Dans le cas où l'accès à la ressource a été spécifié-->
        <onAccept>
            <!--Log-->
            <log level="custom">
                <property name="text" value="**Access Accept**"/>
            </log>
            <send>
                <!--Spécification du EndPoint-->
                <endpoint>
                    <!--L'adresse du service à consommer-->
                    <address uri="http://172.16.6.196:8082/apogee/services/GeographieMetier"/>
                </endpoint>
            </send>
        </onAccept>
        <!--Dans le cas où l'accès à la ressource a été réfusé-->
        <onReject>
            <!--Log-->
            <log level="custom">
```

```
                    <property name="text" value="**Access Denied**"/>
                </log>
                  <!--Génération d'une faute vers l'appelant en précisant la raison-->
                <makefault>
                    <code value="tns:Receiver"
                          xmlns:tns="http://www.w3.org/2003/05/soap-envelope"/>
                    <reason value="**Access Denied**"/>
                </makefault>
                <property name="RESPONSE" value="true"/>
                <header name="To" action="remove"/>
                <send/>
                <drop/>
            </onReject>
        </throttle>
    </in>
    <!-- Précise le traitement à appliquer à tout message sortant-->
    <out>
        <throttle id=" MyThrottle "/>
        <send/>
    </out>
  </sequence>
</definitions>
```

Listing 3 : Filtrage IP WSO2

2.4.3. LE FILTRAGE IP PAR LA PRATIQUE

Suite aux définitions dans le fichier de configuration précédent, le fonctionnement du filtrage IP est expérimenté par différents appels provenant de plusieurs machines.

Sur la figure suivante représentant l'écran des traces en sortie de l'ESB, nous avons effectué un appel depuis la machine 172.16.6.196 qui appartient à la plage d'adresses *172.16.6.120-172.16.6.200*. Les adresses IP de cette plage étant autorisées (voir le fichier *synapse.xml*), nous pouvons alors consommer le web service se trouvant à : *http://172.16.6.196:8082/apogee/services/GeographieMetier* : d'où la trace en sortie : **Access Accept**.

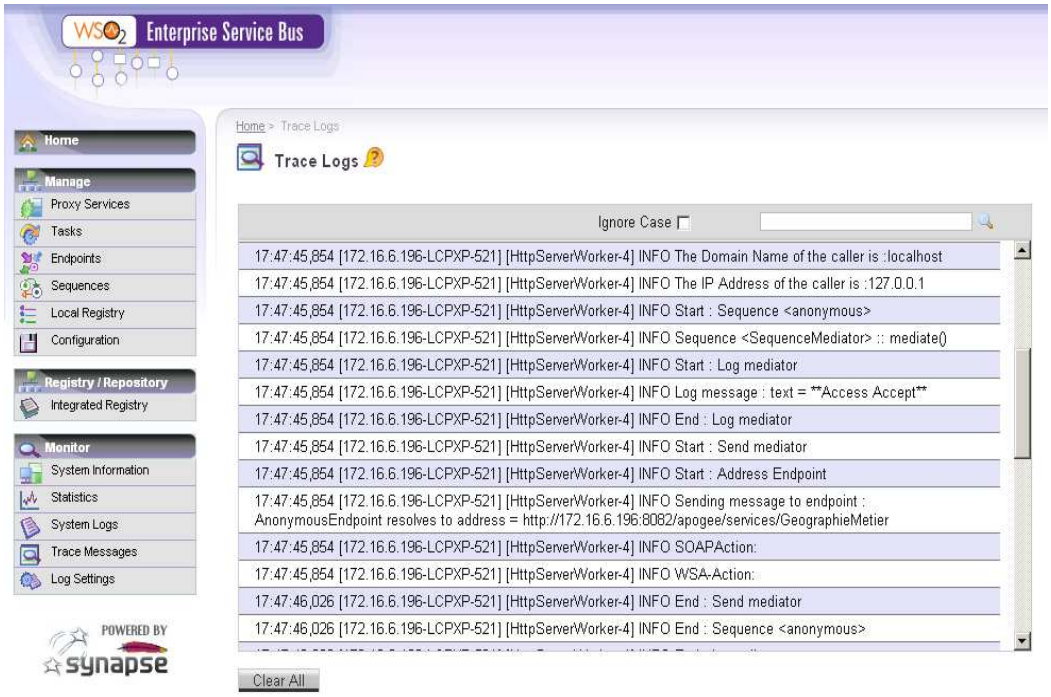

Figure 2 : Log de WSO2 "Access Accept"

Dans ce second cas, nous effectuons l'appel depuis la machine *172.16.6.101*. Cette adresse IP appartient à la plage d'adresses *172.16.6.90-172.16.6.120*. Il s 'agit des adresses non autorisées (voir le fichier *synapse.xml*). Nous nous en rendons compte sur la trace en sortie en voyant : **Access Denied** : signifiant que l'appel de cette machine a été rejeté. Une erreur lui a donc été renvoyée.

Figure 3 : Log de WSO2 "Access Denied"