Reverse http proxy op CentOS7

Een reverse http proxy met apache voor zowel gewoon verkeer als SSL verkeer.

Het is belangrijk dat de interne servernamen aan de interne ip adressen gekoppeld zijn of door opname in de hosts file op de proxy server of op de interne DNS.

vervolgens moet in de firewall de poorten waarvoor ge-proxied wordt een NAT regel worden doorgezet naar de proxyserver in de DMZ en die poorten opengezet van de proxy in de DMZ naar de webserver in de veilige zone.

Begin met een Clone van de CentOS7 minimal

SSL Certificaten

Om het dataverkeer te beveiligen met SSL moeten we een certificaat en een key plaatsen. breng de keys en certificaten van de te proxyen webservers over naar de directory `/etc/ssl/cert`

Let op dat de SELinux context goed staat, fix dit eventueel door:

```
restorecon -R -v /etc/ssl/certs/sslservernaam.auriel.nl.key
restorecon -R -v /etc/ssl/certs/sslservernaam.auriel.nl.crt

yum install openssl
```

Apache

installeer apache en de ssl module voor apache:
`yum install httpd`
`yum install mod_ssl`

Vervolgens maken we virtual host files aan:

één voor gewoon web verkeer over poort 80 `/etc/httpd/conf.d/default.conf` zet hierin:

```
Listen 80
NameVirtualHost 192.168.X.X:80

<VirtualHost 192.168.X.X:80>
    ServerName server-naam.auriel.nl
    ProxyRequests off
    <Proxy *>
        Order deny,allow
        Allow from all
    </Proxy>
    ProxyPass / http://server-naam.auriel.nl/
    ProxyPassReverse / http://server-naam.auriel.nl/
```

```
</VirtualHost>

<VirtualHost 192.168.X.X:80>
    # dit is een redirect naar de SSL versie van de website
    ServerAdmin webmaster@auriel.nl
    ServerName otherserver.auriel.nl
    Redirect / https://otherserver.auriel.nl
</VirtualHost>
```

en één voor het SSL verkeer, bijvoorbeeld voor de calendar server `vi /etc/httpd/conf.d/ssl.conf` zet hier in:

```
Listen 443
#Listen 8443
NameVirtualHost 192.168.X.X:443

<VirtualHost 192.168.X.X:443>
    SSLEngine On
    SSLProxyEngine On

    ServerName otherserver.auriel.nl
    SSLCertificateFile /etc/ssl/certs/otherserver.auriel.nl.crt
    SSLCertificateKeyFile /etc/ssl/certs/otherserver.auriel.nl.key
    SSLProtocol All -SSLv2 -SSLv3
    BrowserMatch "MSIE [2-5]" \
             nokeepalive ssl-unclean-shutdown \
             downgrade-1.0 force-response-1.0
    ProxyRequests off

    <Proxy *>
        Order deny,allow
        Allow from all
    </Proxy>

    ProxyPass / https://otherserver.auriel.nl/
    ProxyPassReverse / https://otherserver.auriel.nl/
</VirtualHost>


<VirtualHost 192.168.X.X:443>
    SSLEngine on
    SSLProxyEngine On
    ServerName sslserver-two.auriel.nl
    SSLCertificateFile /etc/ssl/certs/sslserver-two.auriel.nl.crt
    SSLCertificateKeyFile /etc/ssl/certs/sslserver-two.auriel.nl.key
    SSLProtocol All -SSLv2 -SSLv3
    BrowserMatch "MSIE [2-5]" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
```

```
    ProxyRequests off

    <Proxy *>
        Order deny,allow
        Allow from all
    </Proxy>
    ProxyPass / https://sslserver-two.auriel.nl/
    ProxyPassReverse / https://sslserver-two.auriel.nl/
</VirtualHost>
```

harden de httpd install door de volgende entries toe te voegen aan: `vi /etc/httpd/conf.d/options.conf`

```
TraceEnable off

## Disable Signature
ServerSignature Off

## Disable Banner
ServerTokens Prod
```

en zorg dat de server start:

```
systemctl enable httpd.service
systemctl restart httpd.service
```

Firewall

Zet de nodige poorten in de firewall van de proxyserver zelf open zodat er van buitenaf verbinding kan worden gemaakt:

```
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```