Καράμπελας Γεώργιος, 3180072

1. Έχουν γίνει αλλαγές στα path του πιστοποιητικού και του κλειδιού του στο αρχείο /etc/httpd/conf.d/ssl.conf:

   SSLCertificateFile /etc/pki/tls/certs/web-server.crt

   SSLCertificateKeyFile /etc/pki/tls/private/web-server.key

   Επίσης έχει προστεθεί και VirtualHost για να κάνει το Redirection από http σε https στο αρχείο /etc/httpd/conf/httpd.conf

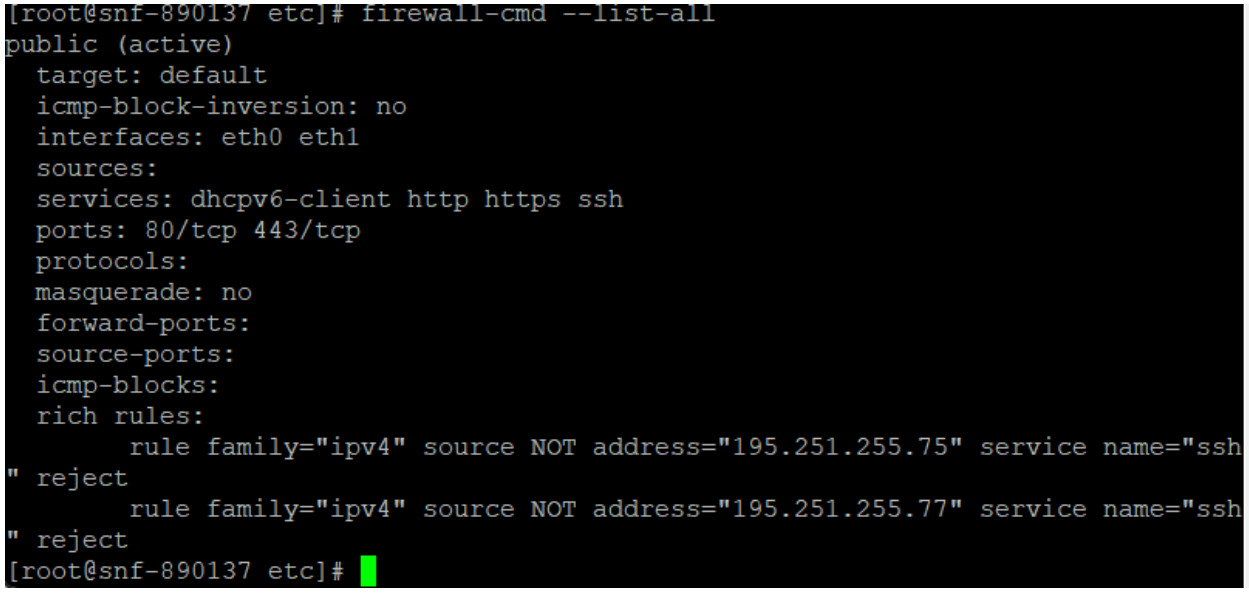
   <VirtualHost *:80>

   ServerName www.snf-890137.gr

   Redirect "/" "https://83.212.97.112"

   </VirtualHost>

2. Παρακάτω φαίνεται ο κανόνας με τον οποίο προστέθηκε ένα rich rule που κάνει reject όλες τις IPv4 που προσπαθούν να συνδεθούν με ssh στο vm, εκτός από την IP Address που δόθηκε.



3.
   a. openssl req -new -x509 -days 365 -key /etc/pki/CA/private/myCA.key -out /etc/pki/CA/certs/myCA.crt → Με αυτή την εντολή έφτιαξα το CA.
   b. openssl req -new -key /etc/pki/tls/private/web-server.key -out /etc/pki/tls/web-server.csr → Με αυτή την εντολή έφτιαξα το CSR
   c. openssl x509 -req -in web-server.csr -CA /etc/pki/CA/certs/myCA.crt -CAkey /etc/pki/CA/private/myCA.key -CAcreateserial -out web-server.crt -days 365 → Και με αυτή την εντολή υπέγραψα το CRS με το CA μου και έφτιαξα το τελικό SSL Certificate.

4. Είναι μια στατική σελίδα https://83.212.97.112 με χρήση html, css, javascript. Ένα input για να γίνει εισαγωγή του ΑΜ και ένα button για submit, με javascript γίνεται ο έλεγχος αν είναι το ΑΜ μου, αν ναι κάνει alert με success αλλιώς fail, επίσης τα κάνει και console.log().