

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Δικτύων και Επικοινωνιών**

Αρ. Άσκησης – Τίτλος Άσκησης	1η Άσκηση - Υλοποίηση IPSec-based VPN με τη χρήση του strongswan
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Ανδριανόπουλος Βασίλειος – ΜΠΚΕΔ2303
	Τσουτσουλιανούδης Γεώργιος – ΜΠΚΕΔ2347
Ημερομηνία παράδοσης	Κυριακή 17 Δεκεμβρίου 2023



Εκφώνηση της άσκησης

Περιγραφή: Σε αυτή την εργασία, καλείστε να εγκαταστήσετε και να παραμετροποιήσετε IPsec συνδέσεις σε περιβάλλον linux, χρησιμοποιώντας το λογισμικό strongswan (δείτε εδώ το αντίστοιχο εργαστηριακό παράδειγμα [1]).

Η δημιουργία των συνδέσεων προτείνεται να γίνει με τη χρήση του Versatile IKE Control Interface (vici plugin) και του εργαλείου εντολών swanctl με το πρωτόκολλο IKEv2 (δείτε εδώ για ενδεικτικά παραδείγματα [2]).

(I) Δημιουργία και εγκατάσταση κλειδιών

- Δημιουργήστε μία Αρχή Πιστοποίησης (ΑΠ - CA) η οποία θα χρησιμοποιήσει τον αλγόριθμο RSA για τη δημιουργία του ιδιωτικού κλειδιού της μήκους 2048 bit. Η ΑΠ μπορεί να δημιουργηθεί στον έναν από τους δύο κόμβους που θα χρησιμοποιήσετε στην άσκηση.
- Δημιουργήστε ένα self-signed πιστοποιητικό για την ΑΠ.
- Μέσω της ΑΠ να δημιουργήσετε, για κάθε άκρο της σύνδεσης τα ιδιωτικά κλειδιά και τα αντίστοιχα πιστοποιητικά. Για τα δύο άκρα της σύνδεσης τα κλειδιά να είναι κλειδιά RSA μήκους 2048 bit.
- Αντιγράψτε σε κάθε άκρο της σύνδεσης, στους αντίστοιχους φακέλους του ipsec τα εξής: το ιδιωτικό κλειδί του κόμβου, το πιστοποιητικό του και τέλος το πιστοποιητικό της ΑΠ.

Σημείωση: Μπορείτε να δημιουργήσετε τα απαραίτητα κλειδιά και πιστοποιητικά, είτε χρησιμοποιώντας την υπηρεσία pki του strongswan είτε χρησιμοποιώντας το openssl, δείτε ενδεικτικά παραδείγματα στο [2].

(II) Δημιουργία και δοκιμή συνδέσεων

Δημιουργήστε και δοκιμάστε διαδοχικά τις παρακάτω συνδέσεις (connections) που περιγράφονται στα βήματα (Α) και (Β). Εκκινήστε διαδοχικά κάθε μία από τις παρακάτω συνδέσεις και επαληθεύστε την με τη βοήθεια ενός packet snifer (πχ wireshark). Στο τελικό σας παραδοτέο να περιλαμβάνονται τα αρχεία διαμόρφωσης του ipsec από τα δύο άκρα, με όλες τις παραπάνω συνδέσεις και οποιοδήποτε άλλο αρχείο πιθανώς απαιτείται. Χρήσιμα παραδείγματα μπορείτε να βρείτε στα [2], [3] [4].

(Α) Σύνδεση host-to-host (κόμβος-με-κόμβο) με IKE2 και με τη χρήση των παραπάνω πιστοποιητικών. Σε αυτή την περίπτωση θα χρειαστεί να δημιουργήσετε 2 VM.

(Β) Σύνδεση site-to-site (δίκτυο-με-δίκτυο) με IKE2 και με τη χρήση των παραπάνω πιστοποιητικών. Σε αυτή την περίπτωση θα χρειαστεί να δημιουργήσετε 4 VM. Θα πρέπει να ρυθμίσετε το κάθε VM που έχει το ρόλο του εσωτερικού host, να βλέπει τον αντίστοιχο Gateway ως default gateway και επίσης οι gateway να δρομολογούν τα πακέτα που λαμβάνουν (δείτε εδώ για βοηθητικές ρυθμίσεις [5]).

Οδηγίες/ Υποδείξεις:

- Μπορείτε να εργαστείτε ατομικά ή σε ομάδες 2 ατόμων. Για κάθε ομάδα θα υποβληθεί μία φορά η εργασία (από ένα μέλος της ομάδας) μέσω του e-class.
- Χρησιμοποιείτε το πρότυπο συγγραφής εργασιών που βρίσκεται στην ενότητα «Έγγραφο\Βοηθητικά Έγγραφα». Στην απάντησή σας θα περιλάβετε ενδεικτικά screenshot από την υλοποίησή σας.
- Αντί για screenshots, μπορείτε εναλλακτικά να δημιουργήσετε σύντομο video επίδειξης και να περιλάβετε στο παραδοτέο σας σύνδεσμο σε κάποια πλατφόρμα διαμοιρασμού για να μπορέσουμε να κατεβάσουμε από εκεί το σχετικό video.
- Πριν την υλοποίηση της άσκησης εκτελέστε τις εντολές: **apt-get update** και **apt-get install**



strongswan strongswan-pki , σε περίπτωση που παρατηρήσετε ότι η υπηρεσία αυτή δεν λειτουργεί.

Πηγές

- [1] <https://pithos.oceanos.grnet.gr/public/KFTegMmilW2yk2AisrlsI4>
- [2] <https://docs.strongswan.org/docs/5.9/index.html>
- [3] <https://docs.strongswan.org/docs/5.9/config/IKEv2.html>
- [4] <https://github.com/strongswan/strongswan>
- [5] <https://gunet2.cs.unipi.gr/modules/document/document.php?course=CDS101&openDir=/618e3a7bIUwh>



ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

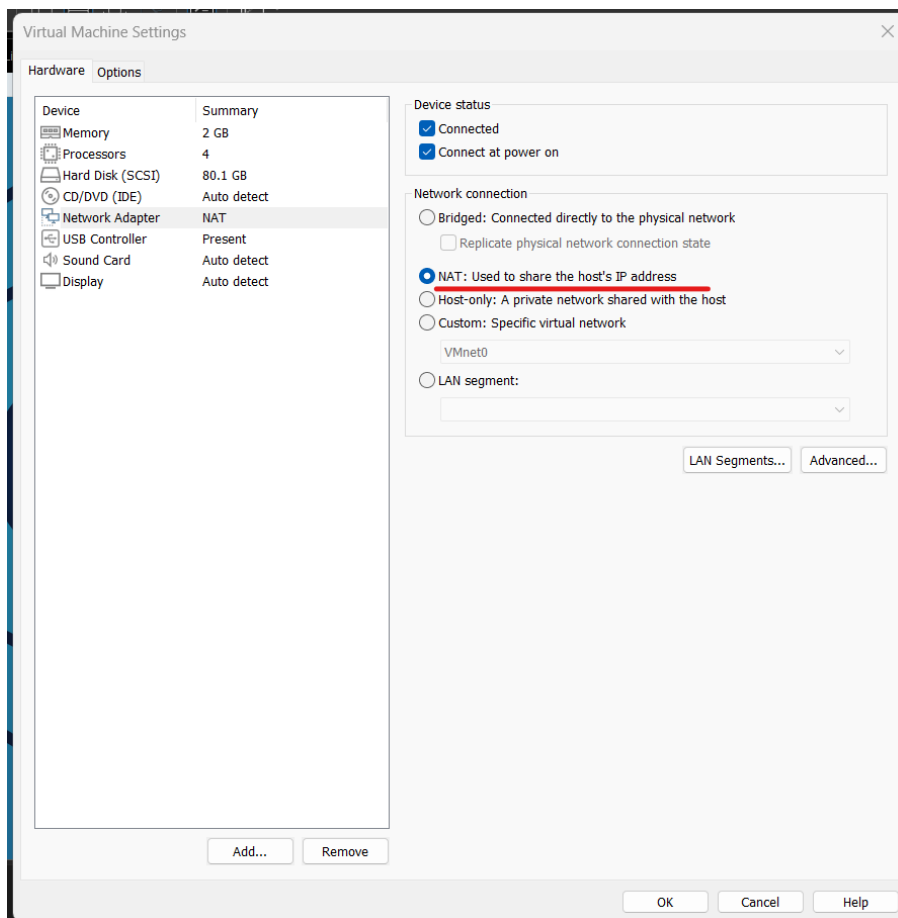
1	Εικονικό Περιβάλλον με 2 κόμβους linux	4
1.1	Εγκατάσταση IPSec (strongswan)	6
1.2	Δημιουργία και διαχείριση κλειδιών	6
1.2.1	Δημιουργία δοκιμαστικής Αρχής Πιστοποίησης	6
1.2.2	Δημιουργία ζεύγους κλειδιών και πιστοποιητικού για το αριστερό άκρο.....	9
1.2.3	Δημιουργία ζεύγους κλειδιών και πιστοποιητικού για το δεξί άκρο	11
1.2.4	Αντιγραφή κλειδιών και πιστοποιητικών στα δύο μέρη της σύνδεσης	13
1.3	Διαμόρφωση αρχείων σύνδεσης	14
1.3.1	Διαμόρφωση αρχείου /etc/ipsec.conf.....	14
1.3.2	Διαμόρφωση αρχείου /etc/ipsec.secrets	17
1.4	Εκκίνηση σύνδεσης	19
1.5	Επιβεβαίωση σύνδεσης IPSec.....	20
2	Εικονικό Περιβάλλον με 4 κόμβους linux	21
2.1	Ορισμός εικονικών μηχανών για τη Site-to-Site σύνδεση.....	21
2.2	Παραμετροποίηση Gateways' IP	22
2.3	Εκκίνηση σύνδεσης	27
2.4	Επιβεβαίωση σύνδεσης	28

1 Εικονικό Περιβάλλον με 2 κόμβους linux

Στην παρούσα ενότητα, θα εγκαταστήσουμε την IPSec σύνδεση σε 2 κόμβους linux κάτω από το ίδιο δίκτυο.

Πριν ξεκινήσουμε την εγκατάσταση του πακέτου Strongswan, θα βεβαιωθούμε πως τα δύο εικονικά μηχανήματα μοιράζονται τις ίδιες NAT ρυθμίσεις.

Επιβεβαιώνουμε επομένως τις ρυθμίσεις και των δύο εικονικών μηχανημάτων, πρώτα από το virtualization software και μετά από τα shells των δύο kali machines.



Εικόνα 1. Επιβεβαίωση NAT ρύθμισης των δύο machines από το Virtualization Software

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.242.128 netmask 255.255.255.0 broadcast 192.168.242.25  
5  
    inet6 fe80::ae8d:7a9d:fd8:87d5 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:6a:c1:a6 txqueuelen 1000 (Ethernet)  
    RX packets 1574 bytes 229152 (223.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 86 bytes 21073 (20.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 24 bytes 1240 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 1240 (1.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

Εικόνα 2. Επιβεβαίωση στο kali machine 1

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~] /usr/strongswan/d/myTestCA  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.242.129 netmask 255.255.255.0 broadcast 192.168.242.25  
5  
    inet6 fe80::28f:10fa:9b4c:ce3 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:a9:f9:d2 txqueuelen 1000 (Ethernet)  
    RX packets 1594 bytes 243253 (237.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 115 bytes 23600 (23.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

Εικόνα 3. Επιβεβαίωση στο kali machine 2

Επομένως, από την Εικόνα 2 και την Εικόνα 3 επιβεβαιώνουμε πως τα 2 machines βρίσκονται στο ίδιο local network και άρα θα μπορούν να επικοινωνήσουν μεταξύ τους.



1.1 Εγκατάσταση IPSec (strongswan)

Εγκαθιστούμε το strongswan και στα δύο μηχανήματα.

Ανοίγοντας ένα shell με root δικαιώματα, και στα δύο machines, μπορούμε να τρέξουμε την εντολή,

apt-get install strongswan

Ωστόσο, είναι ήδη προ εγκατεστημένο στα συστήματα kali και άρα αυτό που θα μπορούσαμε να κάνουμε είναι να ελέγχουμε για ενημερώσεις τρέχοντας τις εντολές,

sudo apt update

sudo apt upgrade strongswan

1.2 Δημιουργία και διαχείριση κλειδιών

Για την υλοποίηση της IPSec σύνδεσης, με τη βοήθεια του strongswan, θα δημιουργήσουμε μία δοκιμαστική Αρχή Πιστοποίησης σε ένα από τα 2 εικονικά μηχανήματα και στη συνέχεια με τη βοήθεια αυτής της Αρχής πιστοποίησης, θα πιστοποιήσουμε τα κλειδιά των δύο άκρων της IPSec σύνδεσης.

1.2.1 Δημιουργία δοκιμαστικής Αρχής Πιστοποίησης

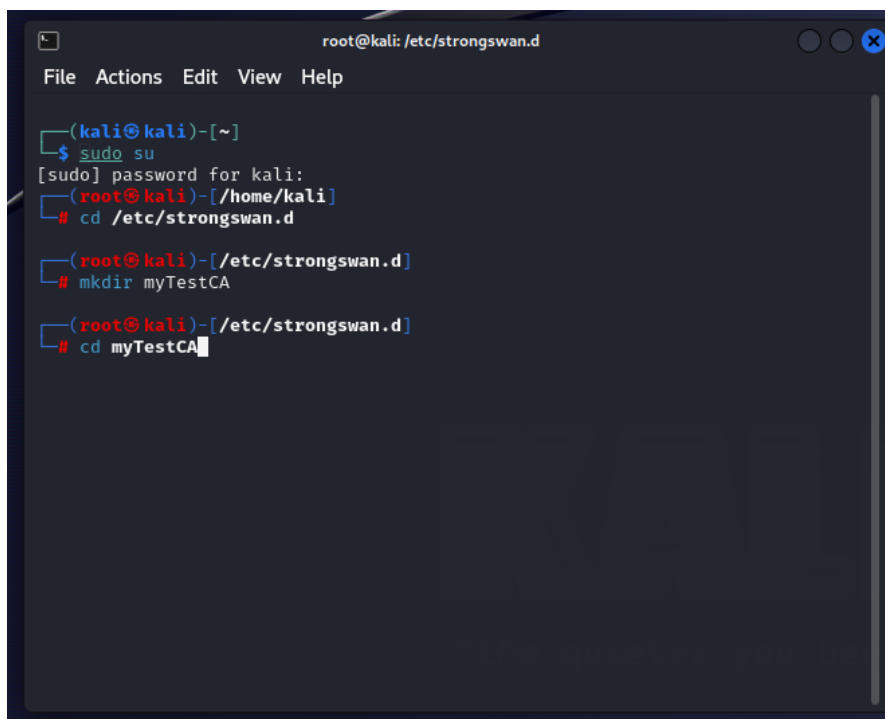
Μεταβαίνουμε στο εικονικό μηχάνημα που θα έχει τον ρόλο της Αρχής Πιστοποίησης

1. Δημιουργία Φακέλου για την Αρχή Πιστοποίησης και στη συνέχεια μεταβαίνουμε σε αυτόν. Στο shell με root δικαιώματα εκτελούμε με τη σειρά

cd /etc/strongswan.d

mkdir myTestCA

cd myTestCA



```
root@kali: /etc/strongswan.d
File Actions Edit View Help

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# cd /etc/strongswan.d

(root@kali)-[/etc/strongswan.d]
# mkdir myTestCA

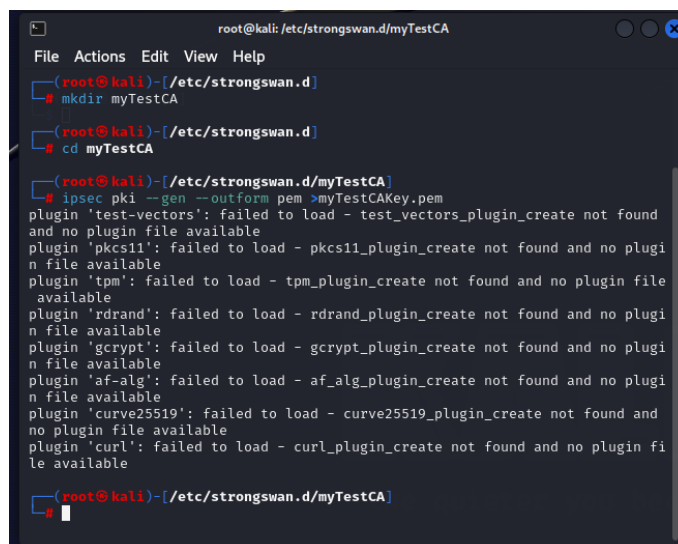
(root@kali)-[/etc/strongswan.d]
# cd myTestCA
```

Εικόνα 4. Επιβεβαίωση δημιουργίας του φακέλου myTestCA

2. Δημιουργία κλειδιού της ΑΠ (σε pem format)

Στο ίδιο shell εκτελούμε

ipsec pki --gen --outform pem >myTestCAKey.pem



```
root@kali: /etc/strongswan.d/myTestCA
File Actions Edit View Help

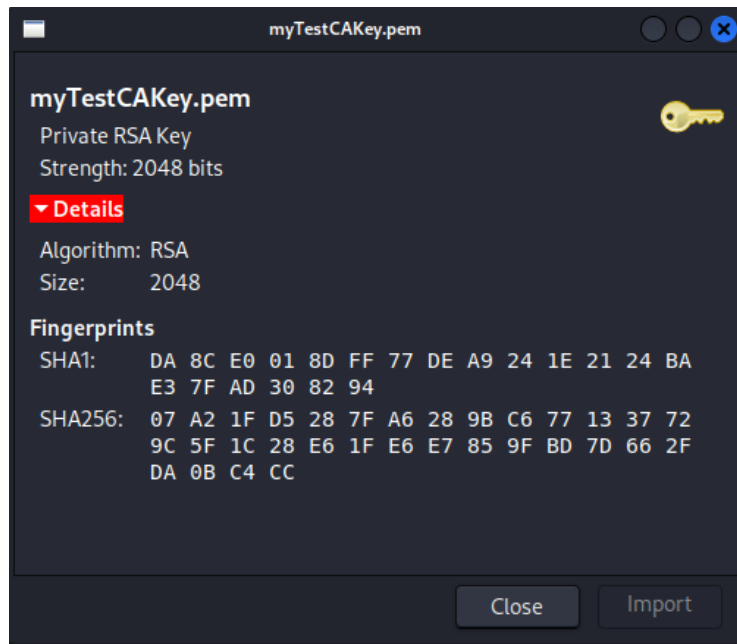
(root@kali)-[/etc/strongswan.d]
# mkdir myTestCA

(root@kali)-[/etc/strongswan.d]
# cd myTestCA

(root@kali)-[/etc/strongswan.d/myTestCA]
# ipsec pki --gen --outform pem >myTestCAKey.pem
plugin 'test-vectors': failed to load - test_vectors_plugin_create not found
and no plugin file available
plugin 'pkcs11': failed to load - pkcs11_plugin_create not found and no plugin
file available
plugin 'tpm': failed to load - tpm_plugin_create not found and no plugin file
available
plugin 'rdrand': failed to load - rdrand_plugin_create not found and no plugin
file available
plugin 'gcrypt': failed to load - gcrypt_plugin_create not found and no plugin
file available
plugin 'af-alg': failed to load - af_alg_plugin_create not found and no plugin
file available
plugin 'curve25519': failed to load - curve25519_plugin_create not found and
no plugin file available
plugin 'curl': failed to load - curl_plugin_create not found and no plugin fi
le available

(root@kali)-[/etc/strongswan.d/myTestCA]
#
```

Εικόνα 5. Επιβεβαίωση εκτέλεσης της εντολής για δημιουργία του κλειδιού της ΑΠ

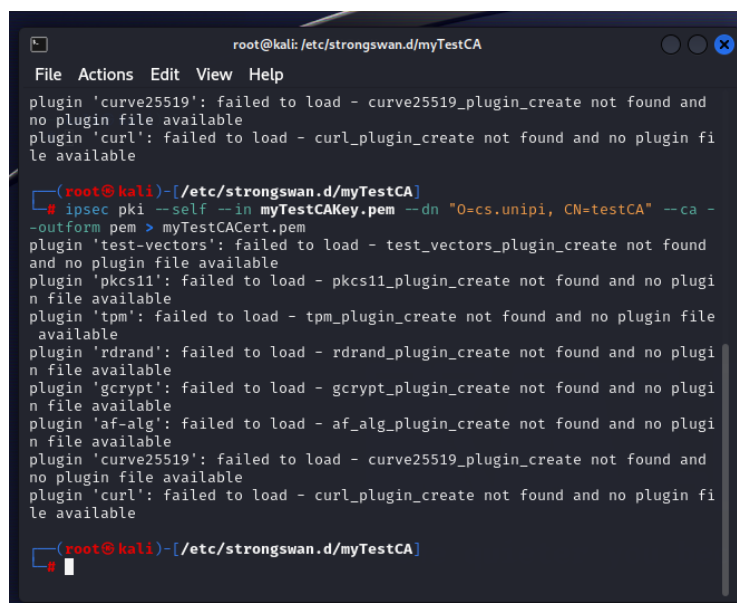


Εικόνα 5. Επιβεβαίωση δημιουργίας του κλειδιού της ΑΠ

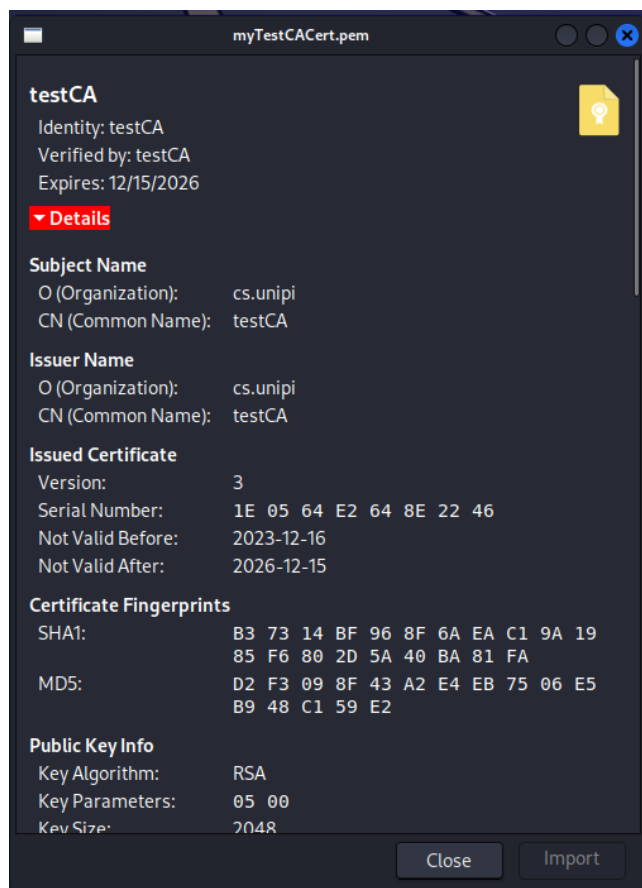
3. Δημιουργία αυτό-υπογεγραμμένου πιστοποιητικού για την ΑΠ.

Στο ίδιο shell εκτελούμε:

```
ipsec pki --self --in myTestCAKey.pem --dn "O=cs.unipi, CN=testCA" --ca --outform pem  
> myTestCACert.pem
```



Εικόνα 6. Επιβεβαίωση εκτέλεσης της εντολής για δημιουργία του πιστοποιητικού



Εικόνα 7. Επιβεβαίωση δημιουργίας του υπογεγραμμένου πιστοποιητικού

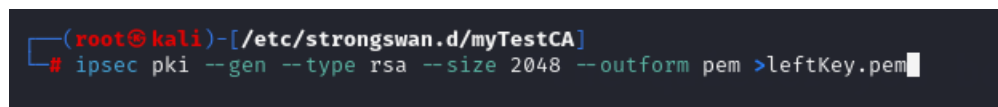
1.2.2 Δημιουργία ζεύγους κλειδιών και πιστοποιητικού για το αριστερό άκρο

Στο ίδιο εικονικό μηχανήμα που έχει τον ρόλο της Αρχής Πιστοποίησης εκτελούμε στο shell με root δικαιώματα τα παρακάτω βήματα.

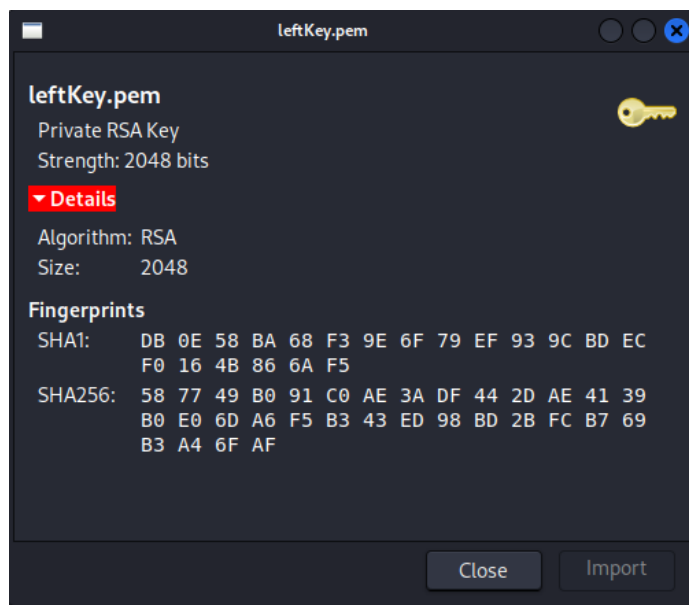
1. Δημιουργία μυστικού κλειδιού αριστερού άκρου

Εκτέλεση εντολής:

ipsec pki --gen --type rsa --size 2048 -- outform pem >leftKey.pem



Εικόνα 8. Επιβεβαίωση εκτέλεσης της εντολής για δημιουργία του μυστικού κλειδιού



Εικόνα 9. Επιβεβαίωση δημιουργίας του μυστικού κλειδιού για το αριστερό άκρο

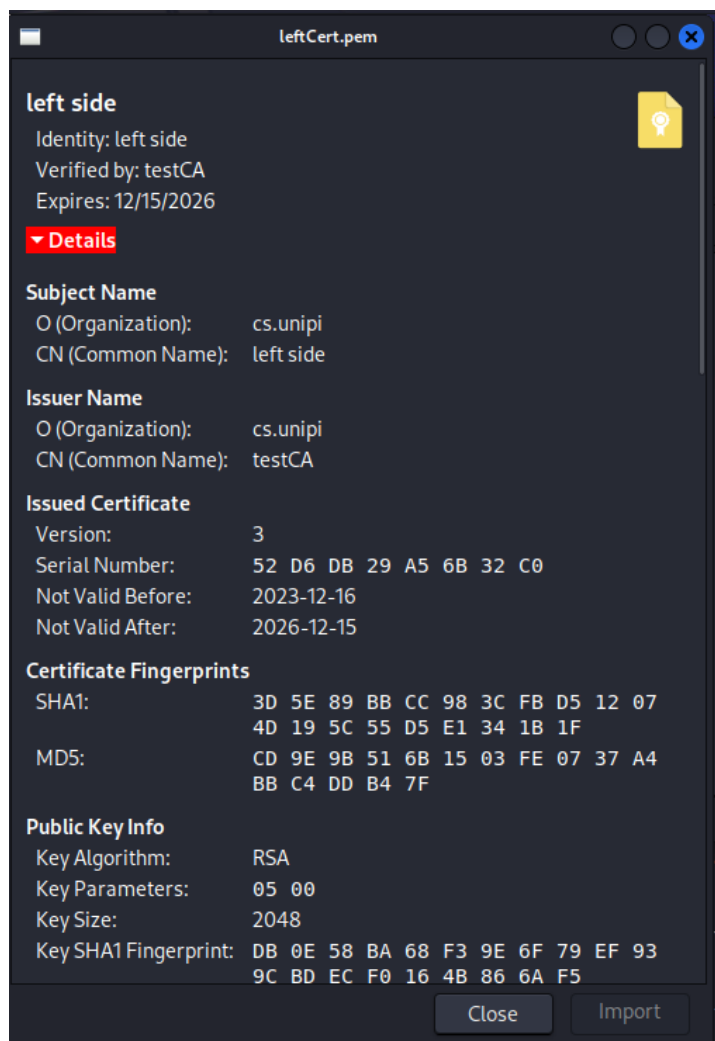
2. Εξαγωγή δημόσιου κλειδιού και Δημιουργία/Υπογραφή πιστοποιητικού για το αριστερό άκρο, από την ΑΠ.

Εκτελούμε την εντολή:

```
ipsec pki --pub --in leftKey.pem | ipsec pki --issue --cacert myTestCACert.pem --cakey myTestCAKey.pem --dn "O=cs.unipi, CN=left side" --flag ikeIntermediate --flag serverAuth --outform pem > leftCert.pem
```

```
(root@kali)-[/etc/strongswan.d/myTestCA]  
# ipsec pki --pub --in leftKey.pem | ipsec pki --issue --cacert myTestCACert.pem --cakey myTestCAKey.pem --dn "O=cs.unipi, CN=left side" --flag ikeIntermediate --flag serverAuth --outform pem > leftCert.pem
```

Εικόνα 10. Επιβεβαίωση εκτέλεσης της εντολής για δημιουργία/υπογραφή του πιστοποιητικού για το αριστερό άκρο



Εικόνα 11. Επιβεβαίωση δημιουργίας και υπογραφής του πιστοποιητικού για το αριστερό άκρο

1.2.3 Δημιουργία ζεύγους κλειδιών και πιστοποιητικού για το δεξί άκρο

Στο ίδιο εικονικό μηχανήμα που έχει τον ρόλο της Αρχής Πιστοποίησης εκτελούμε στο shell με root δικαιώματα τα παρακάτω βήματα.

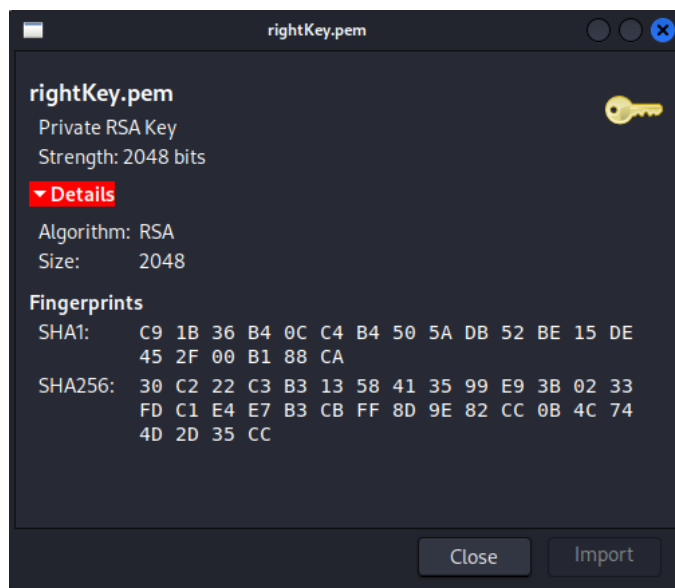
1. Δημιουργία μυστικού κλειδιού δεξιού άκρου

Εκτέλεση εντολής:

```
ipsec pki --gen --type rsa --size 2048 -- outform pem > rightKey.pem
```

```
(root@kali)-[/etc/strongswan.d/myTestCA]
# ipsec pki --gen --type rsa --size 2048 --outform pem > rightKey.pem
```

Εικόνα 12. Επιβεβαίωση εκτέλεσης της εντολής για δημιουργία του μυστικού κλειδιού



Εικόνα 13. Επιβεβαίωση δημιουργίας του μυστικού κλειδιού για το δεξί άκρο

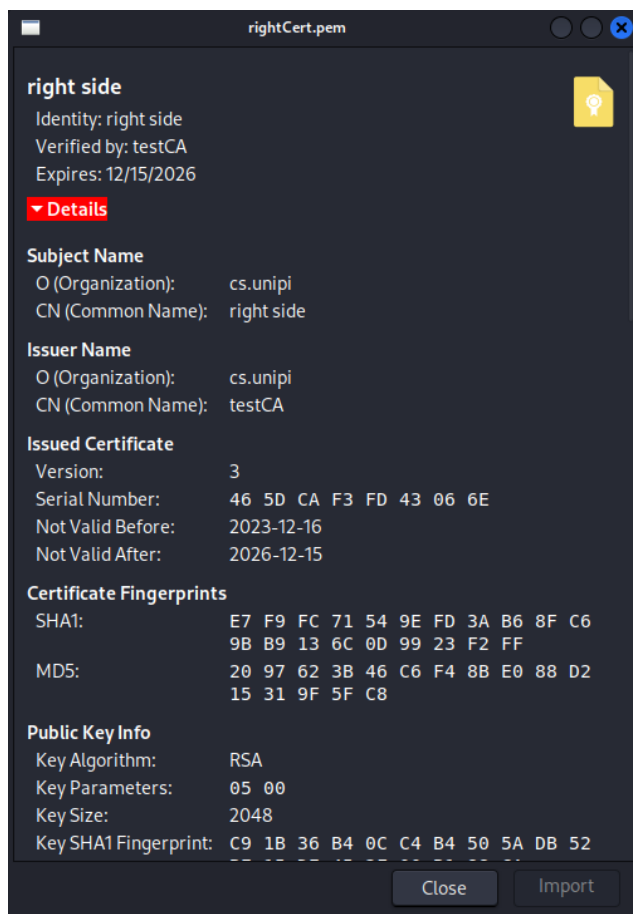
2. Εξαγωγή δημόσιου κλειδιού και Δημιουργία/Υπογραφή πιστοποιητικού για το δεξιό άκρο, από την ΑΠ.

Εκτελούμε την εντολή:

```
ipsec pki --pub --in rightKey.pem | ipsec pki --issue --cacert myTestCACert.pem --  
cakey myTestCAKey.pem --dn "O=cs.unipi, CN=right side" --flag ikeIntermediate --  
flag serverAuth --outform pem > rightCert.pem
```

```
(root@kali)-[/etc/strongswan.d/myTestCA]
# ipsec pki --pub --in rightKey.pem | ipsec pki --issue --cacert myTestCACe  
rt.pem --cakey myTestCAKey.pem --dn "O=cs.unipi, CN=right side" --flag ikeInt  
ermediate --flag serverAuth --outform pem > rightCert.pem
```

Εικόνα 14. Επιβεβαίωση εκτέλεσης της εντολής για δημιουργία/υπογραφή του πιστοποιητικού για το δεξί άκρο



Εικόνα 15. Επιβεβαίωση δημιουργίας και υπογραφής του πιστοποιητικού για το δεξί άκρο

1.2.4 Αντιγραφή κλειδιών και πιστοποιητικών στα δύο μέρη της σύνδεσης

Εκτελούμε και στα δύο μηχανήματα τα παρακάτω βήματα.

Αριστερό άκρο (Kali 1 που είχε και τον ρόλο της Αρχής Πιστοποίησης)

1. Στον φάκελο **/etc/ipsec.d/private** αντιγράφουμε το ιδιωτικό κλειδί **leftKey.pem**
2. Στον φάκελο **/etc/ipsec.d/certs** αντιγράφουμε το πιστοποιητικό **leftCert.pem**
3. Στο φάκελο **/etc/ipsec.d/cacerts** αντιγράφουμε το πιστοποιητικό της ΑΠ **myTestCACert.pem**



```
(root@kali)~[/etc/strongswan.d/myTestCA]
# cp leftKey.pem /etc/ipsec.d/private

(root@kali)~[/etc/strongswan.d/myTestCA]
# cp leftCert.pem /etc/ipsec.d/certs

(root@kali)~[/etc/strongswan.d/myTestCA]
# cp myTestCACert.pem /etc/ipsec.d/cacerts
```

Εικόνα 16. Επιβεβαίωση εκτέλεσης εντολών αντιγραφής των παραπάνω αρχείων

Δεξί άκρο (Kali 2)

Αντιγράφουμε από το Kali 1 στο Kali 2 τα αρχεία που παράξαμε στην υποενότητα 1.2.3 και εκτελούμε τα ίδια βήματα.

1. Στον φάκελο **/etc/ipsec.d/private** αντιγράφουμε το ιδιωτικό κλειδί **rightKey.pem**
2. Στον φάκελο **/etc/ipsec.d/certs** αντιγράφουμε το πιστοποιητικό **rightCert.pem**
3. Στο φάκελο **/etc/ipsec.d/cacerts** αντιγράφουμε το πιστοποιητικό της ΑΠ **myTestCACert.pem**

1.3 Διαμόρφωση αρχείων σύνδεσης

1.3.1 Διαμόρφωση αρχείου /etc/ipsec.conf

Παραμετροποιούμε και στα 2 μηχανήματα της σύνδεσης, το αρχείο **ipsec.conf** εκτελώντας τα παρακάτω βήματα.

Αριστερό άκρο (kali 1)

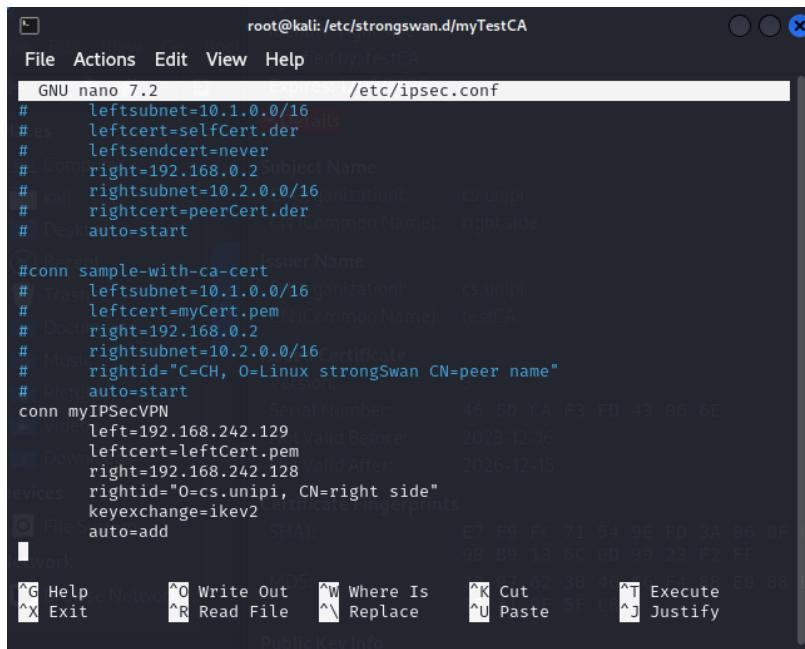
1. Εκτελούμε την παρακάτω εντολή στο shell με δικαιώματα root
nano /etc/ipsec.conf

2. Προσθέτουμε την ακόλουθη σύνδεση

```
conn myIPSecVPN
    left=192.168.242.129
    leftcert=leftCert.pem
    right=192.168.242.128
    rightid="O=cs.unipi, CN=right side"
```

keyexchange=ikev2

auto=add



```
root@kali: /etc/strongswan.d/myTestCA
File Actions Edit View Help
GNU nano 7.2 /etc/ipsec.conf
# leftsubnet=10.1.0.0/16
# leftcert=selfCert.der
# leftsendcert=never
# right=192.168.0.2
# rightsubnet=10.2.0.0/16
# rightcert=peerCert.der
# auto-start

#conn sample-with-ca-cert
# leftsubnet=10.1.0.0/16
# leftcert=myCert.pem
# right=192.168.0.2
# rightsubnet=10.2.0.0/16
# rightid="C=CH, O=Linux strongSwan CN=peer name"
# auto-start
conn myIPSecVPN
left=192.168.242.129
leftcert=leftCert.pem
right=192.168.242.128
rightid="O=cs.unipi, CN=right side"
keyexchange=ikev2
auto=add
```

Εικόνα 17. Επιβεβαίωση εκτέλεσης της παραπάνω παραμετροποίησης στο αριστερό άκρο

Δεξί άκρο (kali 2)

1. Εκτελούμε την παρακάτω εντολή στο shell με δικαιώματα root

nano /etc/ipsec.conf

2. Προσθέτουμε την ακόλουθη σύνδεση

conn myIPSecVPN

left=192.168.242.129

leftcert=leftCert.pem

right=192.168.242.128

rightid="O=cs.unipi, CN=right side"

keyexchange=ikev2

auto=add



```
root@kali: /home/kali/Desktop
File Actions Edit View Help

root@kali: /home/kali
File Actions Edit View Help

GNU nano 7.2 /etc/ipsec.conf
# right=192.168.0.2
# rightsubnet=10.2.0.0/16
# rightid="C=CH, O=Linux strongSwan CN=peer name"
# auto=start
conn myIPSecVPN
left=192.168.242.129
leftid="O=cs.unipi, CN=left side"
right=192.168.242.128
rightcert=rightCert.pem
keyexchange=ikev2
auto=add
```

Εικόνα 19. Επιβεβαίωση εκτέλεσης της παραπάνω παραμετροποίησης στο δεξί άκρο

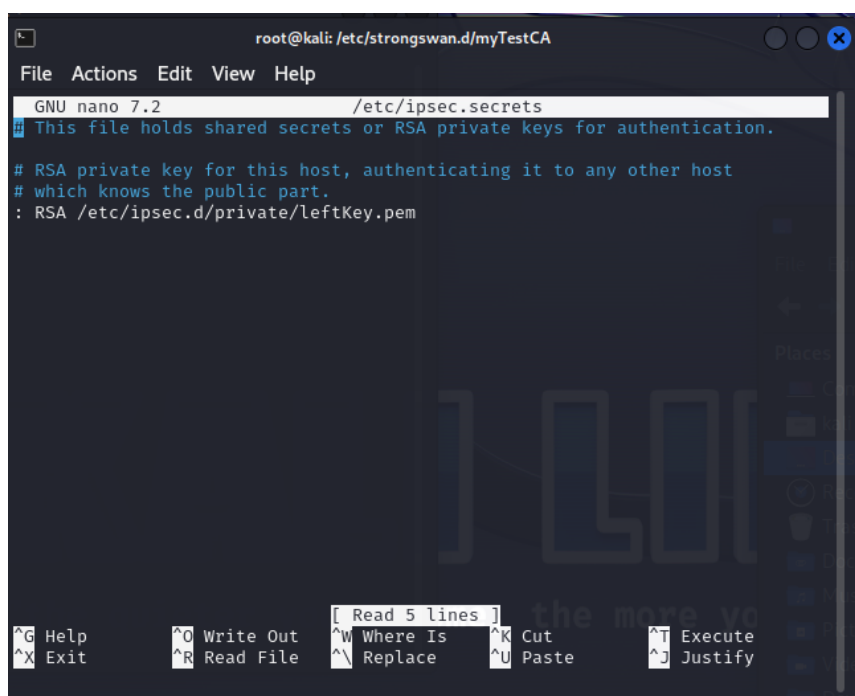
1.3.2 Διαμόρφωση αρχείου `/etc/ipsec.secrets`

Παραμετροποιούμε και στα 2 μηχανήματα της σύνδεσης, το αρχείο ***ipsec.secrets*** εκτελώντας τα παρακάτω βήματα.

Αριστερό Άκρο (Kali 1)

1. Στο αρχείο ***/etc/ipsec.secrets*** προσθέτουμε ένα δείκτη προς το RSA ιδιωτικό κλειδί του αριστερού άκρου.

: RSA /etc/ipsec.d/private/leftKey.pem



Εικόνα 20. Επιβεβαίωση εκτέλεσης της παραπάνω παραμετροποίησης στο αριστερό άκρο

Δεξί Άκρο (Kali 2)

1. Στο αρχείο ***/etc/ipsec.secrets*** προσθέτουμε ένα δείκτη προς το RSA ιδιωτικό κλειδί του δεξί άκρου.

: RSA /etc/ipsec.d/private/rightKey.pem



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
GNU nano 7.2 /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.
# RSA private key for this host, authenticating it to any other host
# which knows the public part.
: RSA /etc/ipsec.d/private/rightKey.pem

[ Read 6 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Εικόνα 21. Επιβεβαίωση εκτέλεσης της παραπάνω παραμετροποίησης στο δεξί άκρο

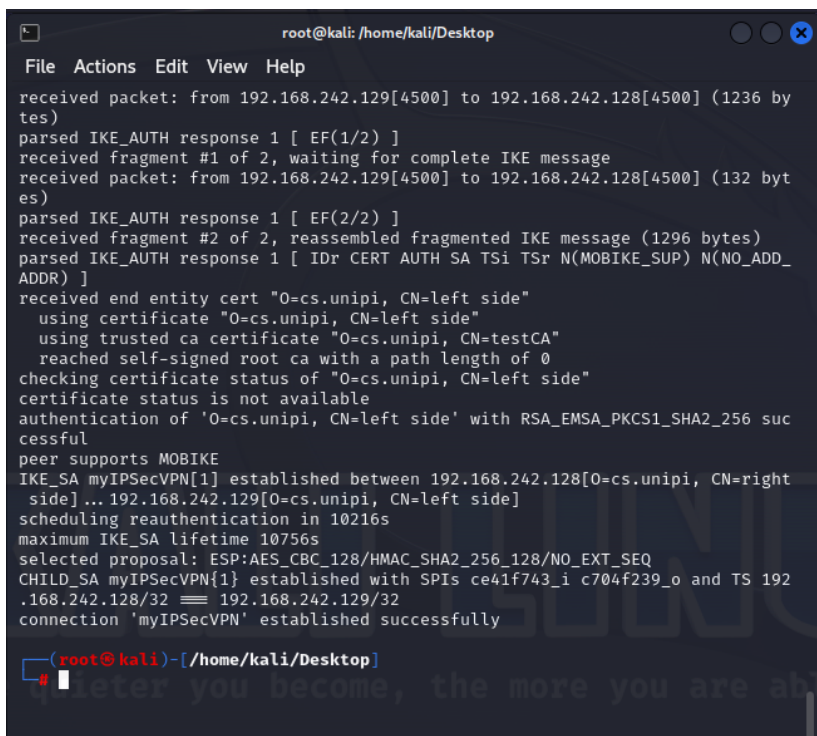


1.4 Εκκίνηση σύνδεσης

Εκτελούμε και στα 2 μηχανήματα της σύνδεσης, τις παρακάτω εντολές στο shell με root δικαιώματα, για την εκκίνηση του IPSec.

ipsec restart

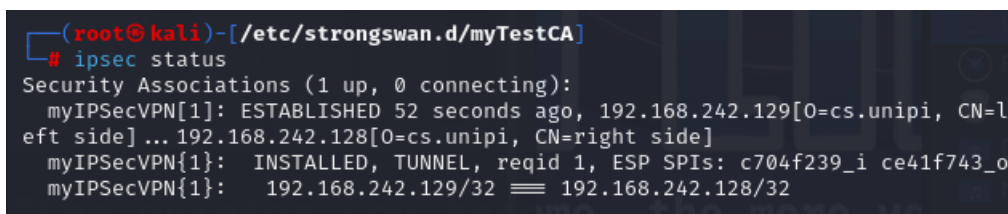
ipsec up myIPSecVPN



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
received packet: from 192.168.242.129[4500] to 192.168.242.128[4500] (1236 bytes)
parsed IKE_AUTH response 1 [ EF(1/2) ]
received fragment #1 of 2, waiting for complete IKE message
received packet: from 192.168.242.129[4500] to 192.168.242.128[4500] (132 bytes)
parsed IKE_AUTH response 1 [ EF(2/2) ]
received fragment #2 of 2, reassembled fragmented IKE message (1296 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH SA TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
received end entity cert "O=cs.unipi, CN=left side"
using certificate "O=cs.unipi, CN=left side"
using trusted ca certificate "O=cs.unipi, CN=testCA"
reached self-signed root ca with a path length of 0
checking certificate status of "O=cs.unipi, CN=left side"
certificate status is not available
authentication of 'O=cs.unipi, CN=left side' with RSA_EMSA_PKCS1_SHA2_256 successful
peer supports MOBIKE
IKE_SA myIPSecVPN[1] established between 192.168.242.128[O=cs.unipi, CN=right side]... 192.168.242.129[O=cs.unipi, CN=left side]
scheduling reauthentication in 10216s
maximum IKE_SA lifetime 10756s
selected proposal: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SEQ
CHILD_SA myIPSecVPN{1} established with SPIs ce41f743_i c704f239_o and TS 192.168.242.128/32 == 192.168.242.129/32
connection 'myIPSecVPN' established successfully

(root@kali)-[/home/kali/Desktop]
#
```

Εικόνα 22. Επιβεβαίωση εκκίνησης IPSec στο kali 1



```
(root@kali)-[/etc/strongswan.d/myTestCA]
# ipsec status
Security Associations (1 up, 0 connecting):
myIPSecVPN[1]: ESTABLISHED 52 seconds ago, 192.168.242.129[O=cs.unipi, CN=left side]... 192.168.242.128[O=cs.unipi, CN=right side]
myIPSecVPN{1}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c704f239_i ce41f743_o
myIPSecVPN{1}: 192.168.242.129/32 == 192.168.242.128/32
```

Εικόνα 23. Επιβεβαίωση εκκίνησης IPSec στο kali 2

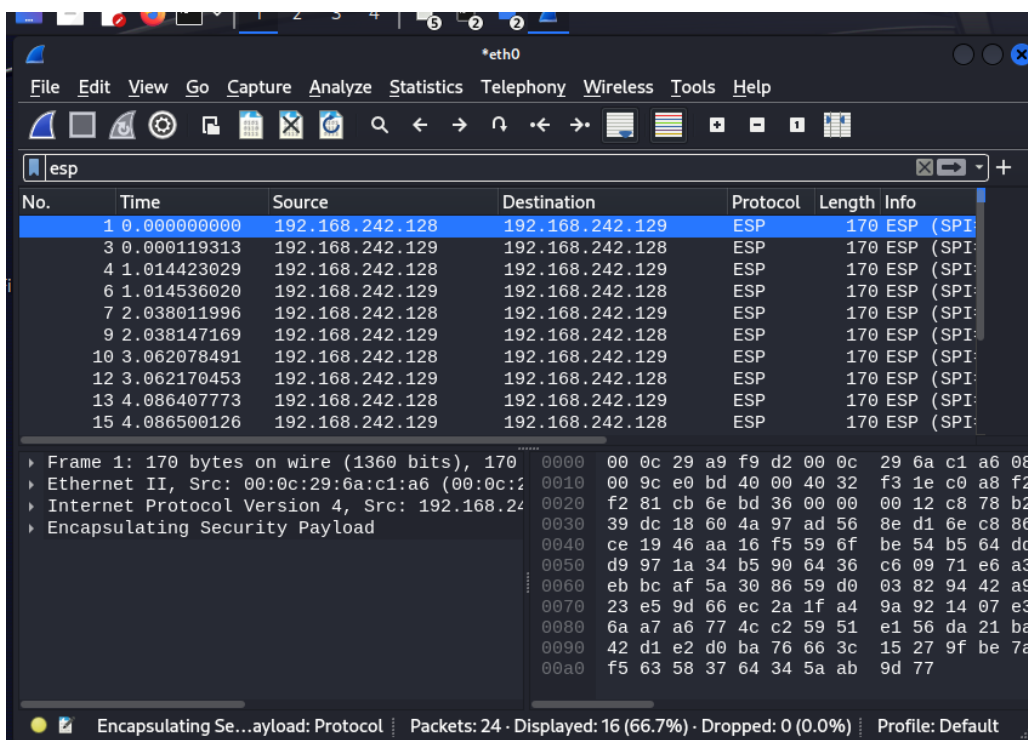
1.5 Επιβεβαίωση σύνδεσης IPSec

Μεταβαίνουμε σε ένα από τα δύο μηχανήματα της σύνδεσης IPSec και κάνουμε ping το 2^ο μηχάνημα.

```
(kali@kali)-[~]
$ ping 192.168.242.129
PING 192.168.242.129 (192.168.242.129) 56(84) bytes of data.
64 bytes from 192.168.242.129: icmp_seq=1 ttl=64 time=1.68 ms
64 bytes from 192.168.242.129: icmp_seq=2 ttl=64 time=0.401 ms
64 bytes from 192.168.242.129: icmp_seq=3 ttl=64 time=0.521 ms
64 bytes from 192.168.242.129: icmp_seq=4 ttl=64 time=0.750 ms
64 bytes from 192.168.242.129: icmp_seq=5 ttl=64 time=55.2 ms
64 bytes from 192.168.242.129: icmp_seq=6 ttl=64 time=0.723 ms
64 bytes from 192.168.242.129: icmp_seq=7 ttl=64 time=0.319 ms
64 bytes from 192.168.242.129: icmp_seq=8 ttl=64 time=0.347 ms
64 bytes from 192.168.242.129: icmp_seq=9 ttl=64 time=0.584 ms
64 bytes from 192.168.242.129: icmp_seq=10 ttl=64 time=0.788 ms
64 bytes from 192.168.242.129: icmp_seq=11 ttl=64 time=0.518 ms
64 bytes from 192.168.242.129: icmp_seq=12 ttl=64 time=0.464 ms
64 bytes from 192.168.242.129: icmp_seq=13 ttl=64 time=0.477 ms
64 bytes from 192.168.242.129: icmp_seq=14 ttl=64 time=0.391 ms
64 bytes from 192.168.242.129: icmp_seq=15 ttl=64 time=0.431 ms
64 bytes from 192.168.242.129: icmp_seq=16 ttl=64 time=0.359 ms
64 bytes from 192.168.242.129: icmp_seq=17 ttl=64 time=0.767 ms
64 bytes from 192.168.242.129: icmp_seq=18 ttl=64 time=0.479 ms
64 bytes from 192.168.242.129: icmp_seq=19 ttl=64 time=0.499 ms
64 bytes from 192.168.242.129: icmp_seq=20 ttl=64 time=0.667 ms
64 bytes from 192.168.242.129: icmp_seq=21 ttl=64 time=0.276 ms
```

Εικόνα 24. Αποστολή ping πακέτων από το kali 2 στο kali 1

Επιβεβαιώνουμε με το wireshark στο kali 2 πως τα πακέτα είναι κρυπτογραφημένα.



Εικόνα 25. Επιβεβαίωση κρυπτογράφησης στο kali 1



2 Εικονικό Περιβάλλον με 4 κόμβους linux

2.1 Ορισμός εικονικών μηχανών για τη Site-to-Site σύνδεση

Στο ήδη παραμετροποιημένο περιβάλλον σύνδεσης IPSec που δημιουργήσαμε στην Ενότητα 1, θα μετανομάσουμε τα μηχανήματα kali 1 και kali 2 σε GW-1 και GW-2 αντίστοιχα.

Σκοπός, είναι να συνδέσουμε διακριτά 2 νέα μηχανήματα linux στα GW-1 και GW-2, αντιστοίχως.

Έτσι θα έχουμε μία site-to-site IPSec σύνδεση.

Τους 2 νέους κόμβους θα τους ονομάσουμε Kali 3 και Kali 4

Ωστόσο, για να επιτευχθεί η επικοινωνία των ακριανών κόμβων Kali 3 και Kali 4 θα πρέπει να παραμετροποιήσουμε τις gateways ip των 2 αυτών μηχανημάτων.

2.2 Παραμετροποίηση Gateways' IP

Εκτελούμε στο κάθε άκρο της σύνδεσης, τα παρακάτω βήματα

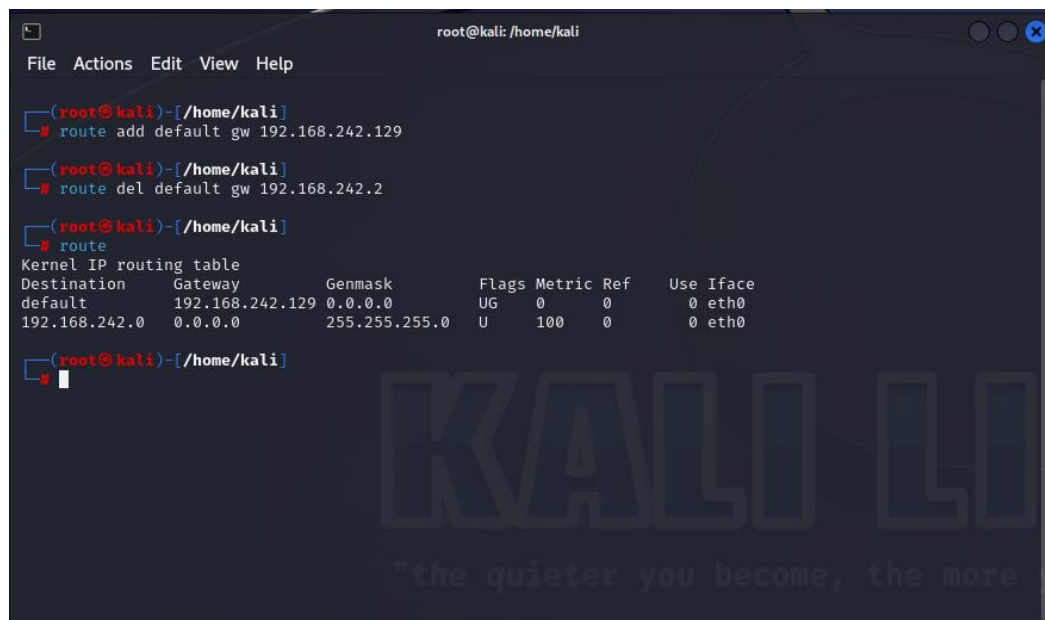
Αριστερό Άκρο (Kali 3)

1. Αλλαγή του Default Gateway στην IP του GW-1

Εκτελούμε τις εντελές στο shell με root δικαιώματα:

```
route add default gw 192.168.242.129
```

```
route del default gw 192.168.242.2
```



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# route add default gw 192.168.242.129
(root@kali)-[/home/kali]
# route del default gw 192.168.242.2
(root@kali)-[/home/kali]
# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.242.129 0.0.0.0 UG 0 0 0 eth0
192.168.242.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
(root@kali)-[/home/kali]
#
```

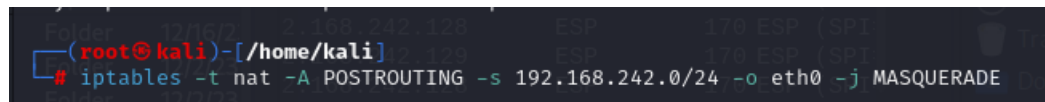
Εικόνα 26. Επιβεβαίωση εκτέλεσης εντολών στο kali 3

Αριστερό Gateway (GW-1)

1. Μετατροπή του πίνακα nat στο iptables ώστε να υποστηρίζει nat

Εκτελούμε την εντολή :

```
iptables -t nat -A POSTROUTING -s 192.168.242.0/24 -o eth0 -j MASQUERADE
```



```
(root@kali)-[/home/kali]
# iptables -t nat -A POSTROUTING -s 192.168.242.0/24 -o eth0 -j MASQUERADE
```

Εικόνα 27. Επιβεβαίωση εκτέλεσης εντολής στο GW-1

```
(root@kali)-[/home/kali]
# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
MASQUERADE all -- 192.168.242.0/24 anywhere
```

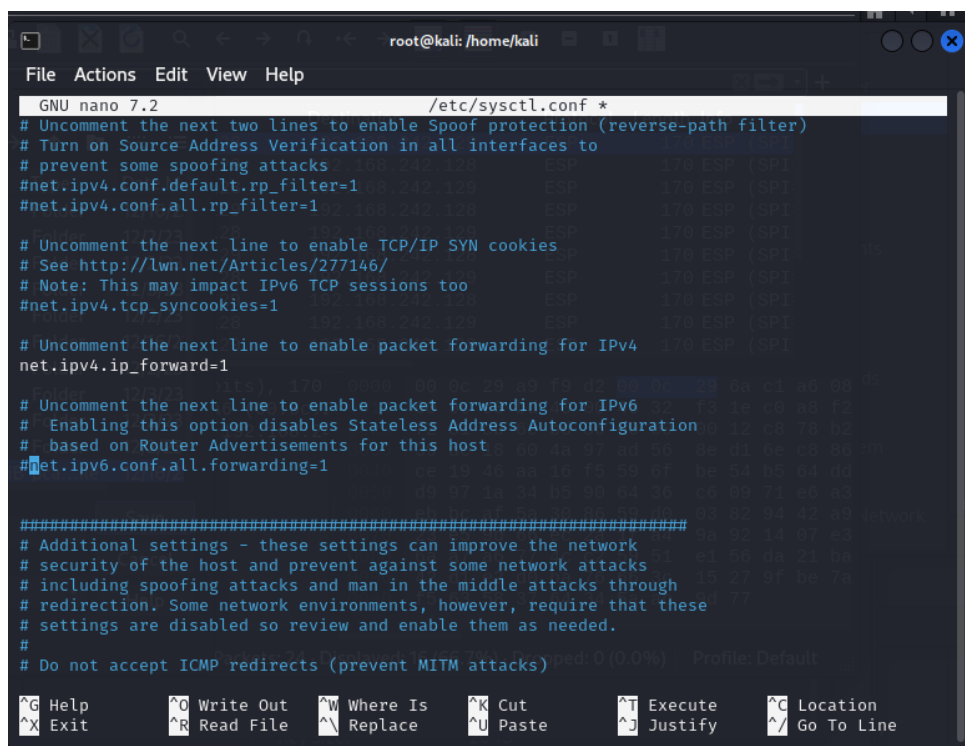
Εικόνα 28. Επιβεβαίωση στο iptables

2. Ενεργοποίηση ip forwarding

Στο αρχείο `/etc/sysctl.conf` βρίσκουμε τη γραμμή: `net.ipv4.ip_forward=1` και την ενεργοποιούμε.

Εκτελούμε:

`nano /etc/sysctl.conf`



```
GNU nano 7.2 /etc/sysctl.conf *
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
```

Εικόνα 29. Ενεργοποίηση της γραμμής `net.ipv4.ip_forward=1`



Τέλος στο shell εκτελούμε:

sysctl -p

```
(root@kali)-[/home/kali]
# sysctl -p
net.ipv4.ip_forward = 1
```

Εικόνα 30. Επιβεβαίωση εκτέλεσης της εντολής ***sysctl -p***

Δεξί Άκρο (Kali 4)

2. Αλλαγή του Default Gateway στην IP του GW-2

Εκτελούμε τις εντελές στο shell με root δικαιώματα:

route add default gw 192.168.242.128

route del default gw 192.168.242.2

Δεξί Gateway (GW-2)

3. Μετατροπή του πίνακα nat στο iptables ώστε να υποστηρίζει nat

Εκτελούμε την εντολή :

iptables -t nat -A POSTROUTING -s 192.168.242.0/24 -o eth0 -j MASQUERADE

```
(root@kali)-[/home/kali]
# iptables -t nat -A POSTROUTING -s 192.168.242.0/24 -o eth0 -j MASQUERADE
```

Εικόνα 31. Επιβεβαίωση εκτέλεσης εντολής στο GW-2

```
(root@kali)-[/home/kali]
# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
MASQUERADE all -- 192.168.242.0/24 anywhere
```

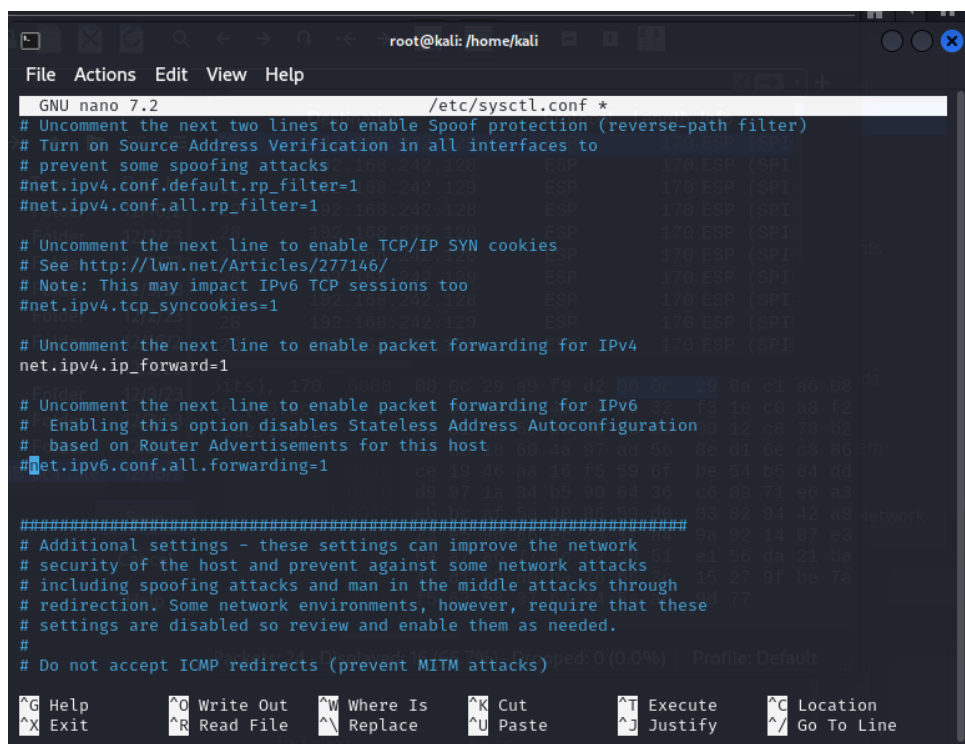
Εικόνα 32. Επιβεβαίωση στο iptables

4. Ενεργοποίηση ip forwarding

Στο αρχείο `/etc/sysctl.conf` βρίσκουμε τη γραμμή: `net.ipv4.ip_forward=1` και την ενεργοποιούμε.

Εκτελούμε:

`nano /etc/sysctl.conf`



```
GNU nano 7.2 /etc/sysctl.conf *
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
```

Εικόνα 33. Ενεργοποίηση της γραμμής `net.ipv4.ip_forward=1`

Τέλος στο shell εκτελούμε:



sysctl -p

```
(root@kali)-[/home/kali]
# sysctl -p
net.ipv4.ip_forward = 1
```

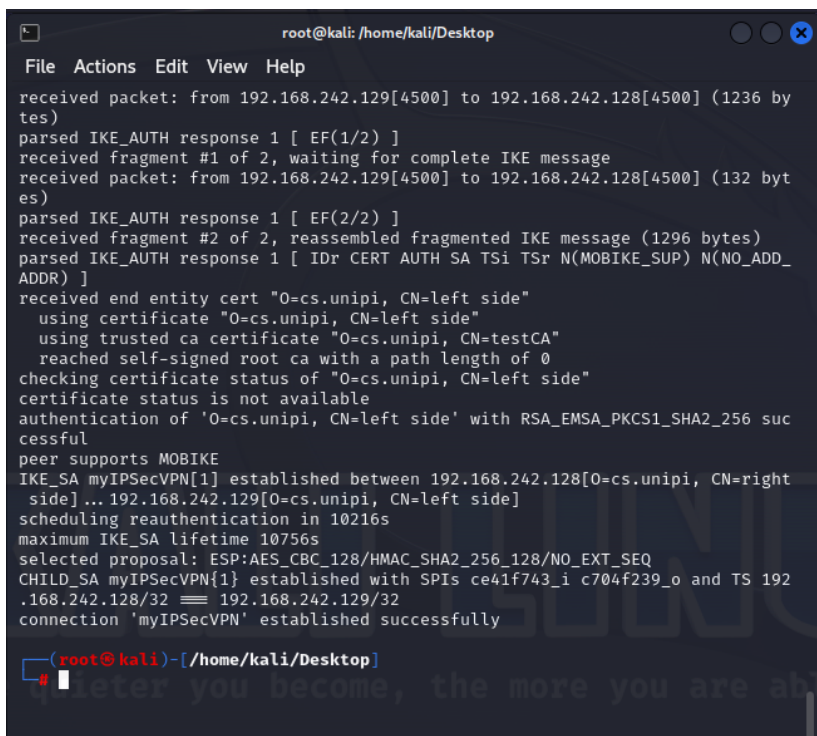
Εικόνα 34. Επιβεβαίωση εκτέλεσης της εντολής *sysctl -p*

2.3 Εκκίνηση σύνδεσης

Εκτελούμε και στα 2 Gateways της σύνδεσης, τις παρακάτω εντολές στο shell με root δικαιώματα, για την εκκίνηση του IPSec.

ipsec restart

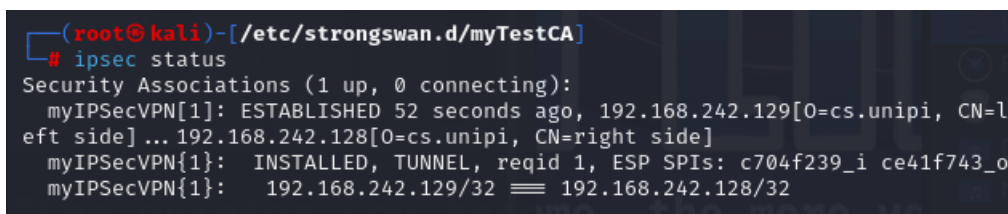
ipsec up myIPSecVPN



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
received packet: from 192.168.242.129[4500] to 192.168.242.128[4500] (1236 bytes)
parsed IKE_AUTH response 1 [ EF(1/2) ]
received fragment #1 of 2, waiting for complete IKE message
received packet: from 192.168.242.129[4500] to 192.168.242.128[4500] (132 bytes)
parsed IKE_AUTH response 1 [ EF(2/2) ]
received fragment #2 of 2, reassembled fragmented IKE message (1296 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH SA TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
received end entity cert "O=cs.unipi, CN=left side"
using certificate "O=cs.unipi, CN=left side"
using trusted ca certificate "O=cs.unipi, CN=testCA"
reached self-signed root ca with a path length of 0
checking certificate status of "O=cs.unipi, CN=left side"
certificate status is not available
authentication of 'O=cs.unipi, CN=left side' with RSA_EMSA_PKCS1_SHA2_256 successful
peer supports MOBIKE
IKE_SA myIPSecVPN[1] established between 192.168.242.128[O=cs.unipi, CN=right side]... 192.168.242.129[O=cs.unipi, CN=left side]
scheduling reauthentication in 10216s
maximum IKE_SA lifetime 10756s
selected proposal: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SEQ
CHILD_SA myIPSecVPN{1} established with SPIs ce41f743_i c704f239_o and TS 192.168.242.128/32 == 192.168.242.129/32
connection 'myIPSecVPN' established successfully

(root@kali)-[/home/kali/Desktop]
#
```

Εικόνα 22. Επιβεβαίωση εκκίνησης IPSec στο kali 1



```
(root@kali)-[/etc/strongswan.d/myTestCA]
# ipsec status
Security Associations (1 up, 0 connecting):
myIPSecVPN[1]: ESTABLISHED 52 seconds ago, 192.168.242.129[O=cs.unipi, CN=left side]... 192.168.242.128[O=cs.unipi, CN=right side]
myIPSecVPN{1}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c704f239_i ce41f743_o
myIPSecVPN{1}: 192.168.242.129/32 == 192.168.242.128/32
```

Εικόνα 23. Επιβεβαίωση εκκίνησης IPSec στο kali 2



2.4 Επιβεβαίωση σύνδεσης

Μεταβαίνουμε σε έναν από τους δύο ακριανούς κόμβους της σύνδεσης, kali 3 ή kali 4 και ελέγχουμε αν μπορούν να επικοινωνήσουν μεταξύ τους.

Εκτελούμε από το Kali 4 την παρακάτω εντολή , για να ελέγξουμε την επικοινωνία με τον άλλον ακριανό κόμβο με IP **192.168.242.130**

ping 192.168.242.130

```
(kali㉿kali)-[~]  
$ ping 192.168.242.130  
PING 192.168.242.130 (192.168.242.130) 56(84) bytes of data.  
64 bytes from 192.168.242.130: icmp_seq=1 ttl=64 time=1.45 ms  
64 bytes from 192.168.242.130: icmp_seq=2 ttl=64 time=0.601 ms  
64 bytes from 192.168.242.130: icmp_seq=3 ttl=64 time=0.381 ms  
64 bytes from 192.168.242.130: icmp_seq=4 ttl=64 time=1.17 ms  
64 bytes from 192.168.242.130: icmp_seq=5 ttl=64 time=0.279 ms  
64 bytes from 192.168.242.130: icmp_seq=6 ttl=64 time=0.657 ms  
64 bytes from 192.168.242.130: icmp_seq=7 ttl=64 time=1.61 ms  
64 bytes from 192.168.242.130: icmp_seq=8 ttl=64 time=0.438 ms  
64 bytes from 192.168.242.130: icmp_seq=9 ttl=64 time=0.368 ms  
^C
```

Εικόνα 24. Επιβεβαίωση επικοινωνία kali 3 με kali 4