



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

UNIVERSITY OF THE AEGEAN
DEPARTMENT OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

321-9703

Ασφάλεια Δικτύων Υπολογιστών και Τεχνολογίες
Προστασίας της Ιδιωτικότητας

Εργαστηριακή Άσκηση

3212018107 Κυριαζής Ιωάννης

3212018161 Παπαδόπουλος Παναγιώτης

Σάμος, Παρασκευή 31 Δεκεμβρίου, 2021



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

Κατάλογος Περιεχομένων

ΚΕΦΑΛΑΙΟ 1	Προετοιμασία	σελ. 03
ΚΕΦΑΛΑΙΟ 2	2.1. Ζητούμενο 1	σελ. 06
-----	2.2. Ζητούμενο 1 - Testing	σελ. 17
ΚΕΦΑΛΑΙΟ 3	3.1. Ζητούμενο 2	σελ. 19
-----	3.2. Ζητούμενο 2 - Testing	σελ. 24
ΚΕΦΑΛΑΙΟ 4	Σύγκριση	σελ. 25
ΚΕΦΑΛΑΙΟ 5	Βιβλιογραφία.....	σελ. 31



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 1

Προετοιμασία



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

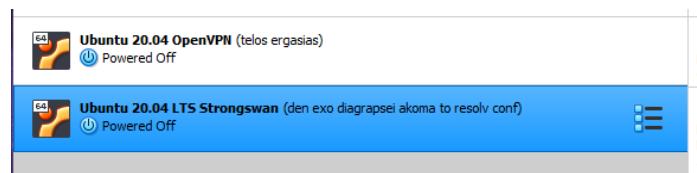
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 1^[1]

Προετοιμασία

Πριν προχωρήσουμε στα ζητούμενα της εργασίας, παραμετροποιήσαμε ορισμένες λειτουργίες που προσφέρονται από το λειτουργικό σύστημα Linux Ubuntu 20.04.

Αρχικά εγκαταστήσαμε το Ubuntu 20.04 OS δεν δύο virtual machines (1 για το 1^ο ζητούμενο και 1 για το 2^ο ζητούμενο). Και στις δύο περιπτώσεις εγκαταστήσαμε το Desktop λειτουργικό (γραφικό περιβάλλον).



Επίσης επιλέξαμε να έχουμε ξεχωριστές IP στην κάθε εικονική μηχανή (επιλογή της Bridged Adapter από τα Network Settings της κάθε εικονικής μηχανής).

Και στους δύο διακομιστές το hostname είναι panosioannis.

Στον κύριο χρήστη αποδόθηκαν grant δικαιώματα ώστε να έχει τον πλήρη έλεγχο του σέρβερ.

```
panosioannis@panosioannis:~$ usermod -aG sudo Panos Ioannis
Usage: usermod [options] LOGIN
Options:
  -b, --badnames      allow bad names
  -c, --comment COMMENT    new comment in the GECOS field
  -d, --home HOME_DIR   new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE  set password inactive after expiration
                           to INACTIVE
  -g, --gid GROUP       force use GROUP as new primary group
  -G, --groups GROUPS   new list of supplementary GROUPS
  -a, --append           append the user to supplemental GROUPS
                           mentioned by the -G option without removing
                           the user from other groups
  -h, --help             display this help message and exit
  -i, --login NEW_LOGIN  new value of the login name
  -l, --lock              lock the user account
  -m, --move-home        move contents of the home directory to the
                           new location (use only with -d)
  -o, --non-unique       allow using duplicate (non-unique) UID
  -p, --password PASSWORD  use encrypted password for the new password
  -R, --root CHROOT_DIR   directory to chroot into
  -P, --prefix PREFIX_DIR  new prefix where are located the /etc/* files
  -s, --shell SHELL       new shell for the user account
  -u, --uid UID           new uid for the user account
  -U, --unlock            unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER  new SELinux user mapping for the user account
```



Παραμετροποιήσαμε τις ρυθμίσεις του δικτύου και των δύο μηχανών. Συγκεκριμένα αποδώσαμε static IP διεύθυνση γιατί θα μας διευκολύνει σε άλλες παραμετροποίησεις.

The terminal window shows three sessions of command-line interaction:

- Session 1:** The user runs `ls /etc/netplan` to list files. The file `01-network-manager-all.yaml` is selected with a red box. The user then runs `sudo cp /etc/netplan/01-network-manager-all.yaml 01-network-manager-all.yaml.bak` to create a backup. Finally, they run `sudo nano /etc/netplan/01-network-manager-all.yaml`.
- Session 2:** The user runs `sudo netplan try`. A message asks if they want to keep the new settings. They press Enter to accept. The terminal then lists the current network configuration with `ip a`, showing interfaces like `lo` and `enp0s3`.
- Session 3:** The user runs `sudo netplan apply`. The terminal lists the updated network configuration again with `ip a`, showing the static IP address `inet 192.168.1.150/24 brd 192.168.1.255 scope global enp0s3`.

Με την 1^η εντολή βλέπουμε ποιο είναι το αρχείο το οποίο θα παραμετροποιήσουμε για να αποδώσουμε static IP.

Με την 2^η εντολή δημιουργούμε ένα backup του παραπάνω αρχείου έτσι ώστε σε περίπτωση λάθους να έχουμε τις προεπιλεγμένες ρυθμίσεις.

Με την 3^η εντολή ανοίγουμε το αρχείο έτσι ώστε να γράψουμε επάνω του.

Αφού δώσουμε στον OpenVPN Server την διεύθυνση 192.168.1.150 και στον StrongSwan Server την διεύθυνση 192.168.1.155, κάνουμε τα εξής:

Με την 1^η εντολή δοκιμάζουμε αν οι ρυθμίσεις έχουμε συντακτικά λάθη και αν λειτουργούν σωστά.

Με την 2^η εντολή κάνουμε apply τις ρυθμίσεις.

Με την 3^η εντολή βλέπουμε αν η διεύθυνση αποδόθηκε σωστά.

Η διεύθυνση αποδόθηκε σωστά. Οι ίδιες ρυθμίσεις έγιναν και στον StrongSwan Server οπότε ήταν περιττό να βάλουμε παραπάνω υλικό σε αυτή την ενότητα.

(ΣΕ ΟΛΑ ΤΑ ΠΑΡΑΠΑΝΩ ΣΤΙΓΜΙΟΤΥΠΑ ΦΑΙΝΟΝΤΑΙ ΟΙ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΕΙΣ ΣΤΟΝ OPENVPN SERVER)



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 2

Ζητούμενο 1



ΚΕΦΑΛΑΙΟ 2.1^{[2][3][5][7]}

Ζητούμενο 1

Αφού κάνουμε την παραπάνω προετοιμασία προχωρούμε στην επίλυση του 1^{ου} Ζητούμενου. Η παρουσίαση της πορείας της εργασίας από εδώ και πέρα θα γίνει με στιγμιότυπα και επεξηγήσεις.

```
Activities Terminal panosioannis@panosioannis: ~
[sudo] password for panosioannis:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
libccid opencsc opencsc-pkcs11 pcessd
The following NEW packages will be installed:
easy-rsa
```

Με αυτή την εντολή εγκαθιστούμε το easy-rsa. Το easy-rsa είναι ένα εργαλείο διαχείρισης της Certificate Authority που θα χρησιμοποιήσουμε για να δημιουργήσουμε ένα ιδιωτικό κλειδί και ένα δημόσιο πιστοποιητικό ρίζας, το οποίο στη συνέχεια θα χρησιμοποιήσουμε για να υπογράψουμε αιτήματα από πελάτες και διακομιστές που θα βασίζονται στην CA μας.

```
Activities Terminal panosioannis@panosioannis: ~
mkdir ~easy-rsa
ln -s /usr/share/easy-rsa/* ~easy-rsa/
```

Με την 1^η εντολή φτιάχνουμε έναν φάκελο.

Με την 2^η εντολή δημιουργούμε συμβολικούς συνδέσμους που θα δείχνουν τα αρχεία πακέτων easy-rsa που έχουμε εγκαταστήσει στο προηγούμενο βήμα.

```
Activities Terminal panosioannis@panosioannis: ~/easy-rsa
chmod 700 /home/panosioannis/easy-rsa
cd ~/easy-rsa
./easyrsa init-pki
```

Με την 1^η εντολή περιορίζουμε την πρόσβαση στον νέο μας κατάλογο PKI.

Με την 2^η εντολή αλλάζουμε directory.

Με την 3^η εντολή αρχικοποιούμε το PKI μέσα στον φάκελο easy-rsa.

```
Activities Terminal panosioannis@panosioannis: ~/easy-rsa
cd ~/easy-rsa
nano vars
```

Με την 1^η εντολή πηγαίνουμε στο directory easy-rsa.

Με την 2^η εντολή ένα αρχείο που ονομάζεται vars. Σε αυτό το αρχείο θα συμπληρώσουμε κάποιες προεπιλεγμένες τιμές.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal Noe 10 17:56
panosioannis@panosioannis: ~/easy-rsa vars
GNU nano 4.8
set_var EASYRSA_REQ_COUNTRY "GR"
set_var EASYRSA_REQ_PROVINCE "North Aegean"
set_var EASYRSA_REQ_CITY "Karlovasi"
set_var EASYRSA_REQ_ORG "PanosIoannis"
set_var EASYRSA_REQ_EMAIL "vicitysk.g@gmail.com"
set_var EASYRSA_REQ_OU "Community"
set_var EASYRSA_ALGO "ec"
set_var EASYRSA_DIGEST "sha512"

Activities Terminal Noe 10 18:01
panosioannis@panosioannis: ~/easy-rsa
panosioannis@panosioannis:~/easyrsa$ ./easyrsa build-ca
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020
Enter New CA Key Passphrase:
Enter New CA Key Passphrase:
read EC key
writing EC key
Can't load /home/panosioannis/easy-rsa/pki/rnd into RNG
id=0x10000000000000000000000000000000 error:2406F879:rnd:RAND_load_file:Cannot open file:../crypto/rand
file.c:98:File "/home/panosioannis/easy-rsa/pki/rnd" does not exist
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you do not have to answer all of them.
If some fields there will be a default value.
If you enter '.', the field will be left blank.
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:panosioannis
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/panosioannis/easy-rsa/pki/ca.crt
panosioannis@panosioannis:~/easy-rsa$ 

Activities Terminal Noe 10 18:06
panosioannis@panosioannis: ~ cat ~/easy-rsa/pki/ca.crt
-----BEGIN CERTIFICATE-----
MIICADCCAYMgAwIBAgIUBUesl647fuyzvMthwuhzk+jjxEcwCgYIKzj0EAwQw
FzEVMBMCa1UEAwMCgFub3Npb2FubnlzMB4XOTIxMTExME2DEwNVoXDTMxXTEw
ODE2DEwNVowfZEVMBMCa1UEAwMCgFub3Npb2FubnlzMHyWEAYHKoZizj0CAQYF
K4EACIDYgAEXXF2Eqh/ZsdwlNAQH8CqXewh1zJmke0DXNQLDHOgcJPLSGYesPy
7XmcSdbjIXNaofGTxREjHx8ZfweoB7TnQr97VxVky/PxdTrVGlb7jn7QgxWP125V6
RhoInzFXN/4o4GRMIGOMB0GA1uddqWBBRm2CsxAiAmNB3Ex050u4qpE0dwoTBS
BgNVHMESzBjBgBm3csXAtAmNB3Ex050u4qpE0dwoTBS
-----END CERTIFICATE-----
panosioannis@panosioannis:~$ 

Activities Terminal Noe 10 18:13
panosioannis@panosioannis: ~/practice-csr
[sudo] password for panosioannis:
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main andfd DEP-11 Metadata [29.0 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/universe andfd DEP-11 Metadata [107 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-updates/main andfd DEP-11 Metadata [2464 B]
Get:8 http://archive.ubuntu.com/ubuntu focal-updates/universe andfd DEP-11 Metadata [362 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal-security/multiverse andfd DEP-11 Metadata [940 B]
Get:10 http://archive.ubuntu.com/ubuntu focal-updates/multiverse andfd DEP-11 Metadata [204 kB]
Fetched 1075 kB in 2s (560 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
panosioannis@panosioannis:~$ sudo apt install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version (1:1.1f-1ubuntu2.8).
openssl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
panosioannis@panosioannis:~$ mdr ~/practice-csr
panosioannis@panosioannis:~/practice-csr$ 
panosioannis@panosioannis:~/practice-csr$ openssl gnrsa -out panosioannis-server.key
Invalid command 'gnrsa' type 'help' for list of available commands
openssl req -newkey rsa:2048 -nodes -keyout panosioannis-server.key
Generating RSA private key, 2048 bit long modulus
.....+
.....+
e is 65537 (0x10001)
panosioannis@panosioannis:~/practice-csr$ openssl req -new -key panosioannis-server.key -out panosioannis-server.req
panosioannis@panosioannis:~/practice-csr$ 

Activities Terminal Noe 10 18:26
panosioannis@panosioannis: ~
[sudo] password for panosioannis:
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal-security InRelease
Hit:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
panosioannis@panosioannis:~$ sudo apt install openvpn easy-rsa
Reading package lists... Done
Building dependency tree
Reading state information... Done
easy-rsa is already the newest version (3.0.6-1).
openvpn is already the newest version (2.4.7-1ubuntu2.20.04.3).
openvpn set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

Στο αρχείο που δημιουργήσαμε παραπάνω προσθέτουμε κάποια στοιχεία που αφορούν την έδρα του σέρβερ.

Με αυτή την εντολή δημιουργούμε το ζεύγος root δημόσιου και ιδιωτικού κλειδιού για την Certificate Authority. Βάζουμε έναν κωδικό που θα μας ζητείται κάθε φορά που αλληλεπιδράμε με την Certificate Authority. Για Common Name βάζουμε αφήνουμε το default.

Με αυτή την εντολή εμφανίζουμε τα περιεχόμενα του αρχείου ca.crt για να ελέγξουμε ότι δημιουργήθηκε το αρχείο.

Με την 1^η εντολή κάνουμε ενημέρωση το λειτουργικό μας.

Με την 2^η εντολή εγκαθιστούμε το OpenSSL. Το OpenSSL είναι ένα εργαλείο για να δημιουργήσουμε practice ιδιωτικό κλειδί και πιστοποιητικό.

Με την 3^η εντολή δημιουργούμε έναν φάκελο με όνομα practice-csr.

Με την 4^η εντολή αλλάζουμε directory και πάμε στο practice-csr.

Με την 5^η εντολή δημιουργούμε ένα ιδιωτικό κλειδί χρησιμοποιώντας το openssl.

Με την 6^η εντολή δημιουργούμε ένα αντίστοιχο CSR (Certificate Signing Request), χρησιμοποιώντας ξανά το βοηθητικό πρόγραμμα openssl. Στην συνέχεια θα μας ζητήσει κάποια στοιχεία σχετικά με την έδρα του σέρβερ.

Με την 1^η εντολή κάνουμε ενημέρωση το σύστημα.

Με την 2^η εντολή εγκαθιστούμε το OpenVPN.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal panosioannis@panosioannis:~/easy-rsa
panosioannis@panosioannis:~$ cd ~/easy-rsa
panosioannis@panosioannis:~/easy-rsa$ ./easyrsa gen-req server nopass
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
Generating an EC private key
writing new private key to /home/panosioannis/easy-rsa/pki/private/server.key.YGJChUfH'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (e.g: your user, host, or server name) [server]:
Keypair and certificate request completed. Your files are:
req: /home/panosioannis/easy-rsa/pki/reqs/server.req
key: /home/panosioannis/easy-rsa/pki/private/server.key
panosioannis@panosioannis:~/easy-rsa$ sudo cp /home/panosioannis/easy-rsa/pki/private/server.key /etc/openvpn/server/
panosioannis@panosioannis:~/easy-rsa$
```

```
Activities Terminal panosioannis@panosioannis:~/easy-rsa
panosioannis@panosioannis:~$ scp /home/panosioannis/easy-rsa/pki/reqs/server.req panosioannis@192.168.1.159:/tmp
The authenticity of host '192.168.1.159 (192.168.1.159)' can't be established.
ECDSA key fingerprint is SHA256:hfKd4Nb0FZetvFa3e0k734qPiogod03w6AjN9B0.
Are you sure you want to continue? (yes/no) [fingerprint]: yes
Warning: Permanently added '192.168.1.159' (ECDSA) to the list of known hosts.
panosioannis@192.168.1.159's password:
server.req
panosioannis@panosioannis:~/easy-rsa$ ./easyrsa import-req /tmp/server.req server
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
Easy-RSA error:
Unable to import the request as the destination file already exists.
Please choose a different name for your imported request file.
Existing file at: /home/panosioannis/easy-rsa/pki/reqs/server.req
panosioannis@panosioannis:~/easy-rsa$ ./easyrsa sign-req server server
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 1080 days:
subject=
    commonname = server
panosioannis@panosioannis:~/easy-rsa$
```

```
Activities Terminal panosioannis@panosioannis:~/easy-rsa
panosioannis@panosioannis:~$ Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
panosioannis@panosioannis:~$ You are about to sign the following certificate.
panosioannis@panosioannis:~$ Please check over the details shown below for accuracy. Note that this request
panosioannis@panosioannis:~$ has not been cryptographically verified. Please be sure it came from a trusted
panosioannis@panosioannis:~$ source or that you have verified the request checksum with the sender.
panosioannis@panosioannis:~$ Request subject, to be signed as a server certificate for 1080 days:
panosioannis@panosioannis:~$ subject=
panosioannis@panosioannis:~$     commonname = server
panosioannis@panosioannis:~$ Type the word 'yes' to continue, or any other input to abort.
panosioannis@panosioannis:~$ Confirm request details? [yes]: yes
panosioannis@panosioannis:~$ Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
panosioannis@panosioannis:~$ /home/panosioannis/easy-rsa/pki/openssl.cnf
panosioannis@panosioannis:~$ Enter pass phrase for /home/panosioannis/easy-rsa/pki/private/ca.key:
panosioannis@panosioannis:~$ Check that the request matches the signature
panosioannis@panosioannis:~$ Signature OK
panosioannis@panosioannis:~$ The Subject's Distinguished Name is as follows
panosioannis@panosioannis:~$ commonname :ASHA1 12:'server'
panosioannis@panosioannis:~$ Certificate is to be certified until Oct 25 16:44:41 2024 GMT (1080 days)
panosioannis@panosioannis:~$ Write out database with 1 new entries
panosioannis@panosioannis:~$ Data Base Updated
panosioannis@panosioannis:~$ Certificate created at: /home/panosioannis/easy-rsa/pki/issued/server.crt
panosioannis@panosioannis:~/easy-rsa$ scp pk/issued/server.crt panosioannis@192.168.1.159:/tmp/
panosioannis@192.168.1.159's password:
server.crt
panosioannis@panosioannis:~/easy-rsa$ scp pk/ca.crt panosioannis@192.168.1.159:/tmp/
panosioannis@192.168.1.159's password:
ca.crt
panosioannis@panosioannis:~/easy-rsa$ scp pk/ca.key panosioannis@192.168.1.159:/tmp/
panosioannis@192.168.1.159's password:
ca.key
panosioannis@panosioannis:~/easy-rsa$ sudo cp /tmp/{server.crt,ca.crt} /etc/openvpn/server/
panosioannis@panosioannis:~/easy-rsa$
```

Με την 1^η εντολή πηγαίνουμε στο directory easy-rsa.

Με την 2^η εντολή καλούμε το easyrsa με την επιλογή gen-req ακολουθούμενη από το Common Name του μηχανήματος. Αυτό θα δημιουργήσει ένα ιδιωτικό κλειδί για τον διακομιστή και ένα αρχείο αίτησης πιστοποιητικού που ονομάζεται server.req.

Με την 3^η εντολή αντιγράφουμε το server key στο /etc/openvpn/server.

Με την 1^η εντολή αντιγράφουμε το αίτημα πιστοποιητικού server.req στον διακομιστή CA για υπογραφή.

Με την 2^η εντολή πηγαίνουμε στο directory easy-rsa.

Με την 3^η εντολή κάνουμε εισαγωγή του αιτήματος πιστοποιητικού.

Με την 4^η εντολή υπογράφουμε το αίτημα.

Με την 1^η εντολή αντιγράφουμε το αρχείο server.crt από τον CA Server στον OpenVPN Server (στην περίπτωσή μας οι δύο αυτοί servers τρέχουν στο ίδιο μηχάνημα).

Με την 2^η εντολή αντιγράφουμε το αρχείο ca.crt από τον CA Server στον OpenVPN Server (στην περίπτωσή μας οι δύο αυτοί servers τρέχουν στο ίδιο μηχάνημα).

Με την 3^η εντολή αντιγράφουμε τα παραπάνω αρχεία στο μονοπάτι /etc/openvpn/server.

```
Activities Terminal panosioannis@panosioannis:~/easy-rsa
panosioannis@panosioannis:~$ openvpn --genkey --secret ta.key
panosioannis@panosioannis:~$ sudo cp ta.key /etc/openvpn/server
panosioannis@panosioannis:~$
```

Με την 1^η εντολή δημιουργούμε pre-shared κλειδί tls-crypt. Αυτό το κλειδί θα το χρησιμοποιούν όλοι οι clients και ο server. Χρησιμοποιείται από τον σερβερ για την εκτέλεση γρήγορων ελέγχων στα εισερχόμενα πακέτα: εάν έχει υπογραφεί χρησιμοποιώντας το pre-shared κλειδί, τότε ο διακομιστής το επεξεργάζεται. Εάν δεν είναι υπογεγραμμένο, τότε ο διακομιστής γνωρίζει ότι προέρχεται από μη αξιόπιστη πηγή και μπορεί να το απορρίψει χωρίς να χρειάζεται να εκτελέσει πρόσθιτη εργασία αποκρυπτογράφησης.

Με την 2^η εντολή αντιγράφουμε το παραγόμενο αρχείο ta.key στο μονοπάτι /etc/openvpn/server.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal panosIoannis@panosIoannis: ~easy-rsa
panosIoannis@panosIoannis: ~easy-rsa$ ./make-client-configs/keys
panosIoannis@panosIoannis: ~easy-rsa$ cd ./easy-rsa
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa gen-req client1 nopass
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
Generating an EC private key
writing new private key to '/home/panosIoannis/easy-rsa/pk/private/client1.key.evhx8SWdLC'
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [client1]:
Keypath and certificate request completed. Your files are:
read configuration from: ./vars
cp pk/client1.key ./client-configs/keys/
key: /home/panosIoannis/easy-rsa/pk/private/client1.key
panosIoannis@panosIoannis: ~easy-rsa$ cp pk/client1.key ./client-configs/keys/
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa import -req /tmp/client1.req client1
client1.req                                     100K 2972  2.9MB/s  00:00
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa import -req /tmp/client1.req client1
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
Easy-RSA error:
Unable to import the request as the destination file already exists.
Please choose a different name for your imported request file.
Existing file at: /home/panosIoannis/easy-rsa/pk/req/client1.req
```

```
Activities Terminal panosIoannis@panosIoannis: ~easy-rsa
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa sign-req client client1
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a client certificate for 1080 days:
subject:
  commonname = client1
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from: ./vars
Enter pass phrase for /home/panosIoannis/easy-rsa/pk/openssl.ca.key:
Check that the request matches the signature
Signature ok
The subject's Distinguished Name is as follows
commonName :ASH1 12::client1
Certificate is to be certified until Oct 25 16:59:54 2024 GMT (1080 days)
Write out database with 1 new entries
Data Base Updated
Certificate created at: /home/panosIoannis/easy-rsa/pk/issued/client1.crt
panosIoannis@panosIoannis: ~easy-rsa$ scp pk/issued/client1.crt panosIoannis@92.168.1.150:/tmp/
panosIoannis@92.168.1.150's password: 100K 2972  16.4MB/s  00:00
panosIoannis@panosIoannis: ~easy-rsa$ cp /tmp/client1.crt ./client-configs/keys/
panosIoannis@panosIoannis: ~easy-rsa$ sudo cp /etc/openssl/openssl.ca.crt ./client-configs/keys/
```

```
Activities Terminal panosIoannis@panosIoannis: ~easy-rsa
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a client certificate for 1080 days:
subject:
  commonname = client1
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from: ./vars
Enter pass phrase for /home/panosIoannis/easy-rsa/pk/openssl.ca.key:
Check that the request matches the signature
Signature ok
The subject's Distinguished Name is as follows
commonName :ASH1 12::client1
Certificate is to be certified until Oct 25 16:59:54 2024 GMT (1080 days)
Write out database with 1 new entries
Data Base Updated
Certificate created at: /home/panosIoannis/easy-rsa/pk/issued/client1.crt
panosIoannis@panosIoannis: ~easy-rsa$ scp pk/issued/client1.crt panosIoannis@92.168.1.150:/tmp/
panosIoannis@92.168.1.150's password: 100K 2972  16.4MB/s  00:00
panosIoannis@panosIoannis: ~easy-rsa$ cp ./tmp/client1.crt ./client-configs/keys/
panosIoannis@panosIoannis: ~easy-rsa$ sudo cp /etc/openssl/openssl.ca.crt ./client-configs/keys/
[sudo] password for panosIoannis:
panosIoannis@panosIoannis: ~easy-rsa$
```

```
Activities Terminal panosIoannis@panosIoannis: ~easy-rsa
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa gen-req client2 nopass
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
Generating an EC private key
writing new private key to '/home/panosIoannis/easy-rsa/pk/private/client2.key.VX01UKDvjr'
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [client2]:
Keypath and certificate request completed. Your files are:
read configuration from: ./vars
cp pk/client2.key ./client-configs/keys/
key: /home/panosIoannis/easy-rsa/pk/private/client2.key
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa import -req /tmp/client2.req client2
client2.req                                     100K 436  2.9MB/s  00:00
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa import -req /tmp/client2.req client2
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
Easy-RSA error:
Unable to import the request as the destination file already exists.
Please choose a different name for your imported request file.
Existing file at: /home/panosIoannis/easy-rsa/pk/req/client2.req
```

Με την 1^η εντολή δημιουργούμε μια δομή καταλόγου στον αρχικό μας κατάλογο για την αποθήκευση του πιστοποιητικού πελάτη και των αρχείων κλειδιών.

Με την 2^η εντολή, δεδομένου ότι θα αποθηκεύσουμε τα ζεύγη πιστοποιητικών/κλειδιών και τα αρχεία διαμόρφωσης των πελατών μας σε αυτόν τον κατάλογο, θα πρέπει να κλειδώσουμε τις άδειες του τώρα ως μέτρο ασφαλείας.

Με την 3^η εντολή πηγαίνουμε στο directory easy-rsa.

Με την 4^η εντολή εκτελούμε το script easyrsa για τον client1.

Με την 5^η εντολή αντιγράφουμε το client1.key στον φάκελο με τα κλειδιά των πελατών.

Με την 6^η εντολή μεταφέρουμε το αρχείο client1.req στον διακομιστή CA χρησιμοποιώντας μια ασφαλή μέθοδο.

Με την 7^η εντολή αντιγράφουμε το αρχείο client1.crt στον φάκελο tmp του σερβερ.

Με την 1^η εντολή υπογράφουμε το αίτημα του πελάτη 1.

Με την 2^η εντολή μεταφέρουμε το αρχείο client1.crt που δημιουργήθηκε στην πάνω εντολή, στον φάκελο tmp του σερβερ.

Με την 3^η εντολή αντιγράφουμε το αρχείο που μεταφέραμε στην πάνω εντολή στον φάκελο με τα κλειδιά των πελατών.

Με την 4^η εντολή αντιγράφουμε το αρχείο ta.key στον φάκελο με τα κλειδιά των πελατών.

Με την 1^η εντολή αντιγράφουμε το αρχείο ca.crt στον φάκελο με τα κλειδιά των πελατών.

Με την 2^η εντολή δίνουμε grant δικαιώματα στον τρέχον χρήστη για τον φάκελο με τα κλειδιά των πελατών.

Τα δύο επόμενα στιγμότυπα αποτυπώνουν τα ίδια βήματα και για τον πελάτη 2.

```
Activities Terminal panosIoannis@panosIoannis: ~easy-rsa
panosIoannis@panosIoannis: ~easy-rsa$ ./easy-rsa sign-req client client2
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a client certificate for 1080 days:
subject:
  commonname = client2
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from: ./vars
Enter pass phrase for /home/panosIoannis/easy-rsa/pk/openssl.ca.key:
Check that the request matches the signature
Signature ok
The subject's Distinguished Name is as follows
commonName :ASH1 12::client2
Certificate is to be certified until Oct 25 17:34:57 2024 GMT (1080 days)
Write out database with 1 new entries
Data Base Updated
Certificate created at: /home/panosIoannis/easy-rsa/pk/issued/client2.crt
panosIoannis@panosIoannis: ~easy-rsa$ scp pk/issued/client2.crt panosIoannis@92.168.1.150:/tmp/
panosIoannis@92.168.1.150's password: 100K 2972  15.0MB/s  00:00
panosIoannis@panosIoannis: ~easy-rsa$ cp /tmp/client2.crt ./client-configs/keys/
panosIoannis@panosIoannis: ~easy-rsa$
```



321-9703-Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal Noe 10 19:54 panosloannis@panosloannis: ~ panosloannis@panosloannis: ~ panosloannis@panosloannis: $ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/server/ [sudo] password for panosloannis: panosloannis@panosloannis: $ sudo gunzip /etc/openvpn/server/server.conf.gz panosloannis@panosloannis: $ sudo nano /etc/openvpn/server/server.conf
```

Με την 1η εντολή αντιγράφουμε το αρχείο server.conf.gz στον φάκελο που περιέχει το openvpn.

Με την 2^η εντολή αποσυμπιέζουμε το server.conf από το zip αρχείο.

Με την 3^η εντολή θα τροποποιήσουμε το αρχείο που αποσυμπιέσαμε πιο πάνω.

```
Activities Terminal Not 10:19:59
panoslois@panoslois ~
panoslois@panoslois:~$ /etc/openvpn/server/server.conf
GNU nano 4.8
keepalive 10 120
# For extra security beyond that provided
# by SSL/TLS, create an "HMAC Firewall"
# to help block DOS attacks and UDP port flooding.
# Generate with:
# openvpn --genkey --secret ta.key
# The server and each client must have
# a copy of this key.
# The second parameter should be '8'
# :tls-auth ta.key # This file is secret
# tls-crypt ta.key
# This certificate is for clients
# This certificate must be copied to
# the client config file as well.
# Note that v2.4 clients/server will automatically
# download the certificate if it is present.
# See also the --allow-linger option in the manpage
:cipher AES-256-CBC
:cipher AES-192-CBC
:auth SHA256
# Compresses traffic on the VPN link and push the
# compression option to the client (v2.4+ only, for earlier
# versions see below)
# compress lzo-v2
:push 'compress lzo-v2'

# For compression compatible with older clients use comp-lzo
# If you enable it here, you must also
# enable it in the client config file.
:comp-lzo

☰ Get Help ⌂ Exit ⌂ Write Out ⌂ Read File ⌂ Where Is ⌂ Replace ⌂ Cut Text ⌂ Paste Text ⌂ To Spell
```

```
Activities Terminal No 10 20:00
panosloannis@panosloannis: ~
$ nano 4.8
# and private keys. Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# via the "pkcs12" directive (in man page).
ca.crt
cert server.crt
key server.key # This file should be kept secret

# Diffie-Hellman parameters.
# Generate your own with:
# ./scripts/generate-dh dh2048.pem
dh dh2048.pem
dh none

# Default topology
# Should be subnet (addressing via IP)
# unless Windows clients v2.0.9 and lower have to
# use subnet (Windows clients v2.1.0 and higher per client)
# Defaults to mtu3 (not recommended)
;topology subnet

# Configure server mode and supply a VPN subnet
# For OpenVPN to draw client addresses from.
# The Server will take 10.8.0.1 for itself;
# clients will be available to 10.8.0.2-10.8.0.254.
# Each client will be able to reach the server
# on 10.8.0.1. Connect to the tunnel if you are
# experiencing connection issues. See man page for more info,
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file. If OpenVPN goes down or
# ...
# Get Help   Write Out   Where Is   Cut Paste Text   Justify
# Exit      Read File  Replace  To Selection  To Sel
```

```
 ④ nano /etc/openvpn/server/server.conf

[OpenVPN]
# If you enable it here, you must also
# enable it in the client config file.
# comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization,
# so you can uncomment this out on
# production systems.

#user nobody
#group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and reflushed every minute.
status /var/log/openvpn/openvpn-status.log

# By default, log messages will go to the syslog (or
# /var/log/syslog) unless you specify otherwise. You can go
# to the "Program Files\OpenVPN\log" directory.
# use log or log-append to override this default.
# log will truncate the log file when a new logging startup,
# while log-append will append to it, as new messages
# are generated.

⑤ Get Help   ⑥ Write Out  ⑦ Where Is  ⑧ Cut Text
⑨ Exit!  ⑩ Save File  ⑪ Redo!  ⑫ To Selection  ⑬ To Selection
```

Βάζουμε το σύμβολο «;» μπροστά από την
1^η γραμμή που είναι μέσα στο 1^ο κόκκινο
πλαίσιο.

Γράφουμε από κάτω από την πρώτη γραμμή την εντολή που βρίσκεται στην 2^η γραμμή.

Βάζουμε το σύμβολο «;» μπροστά από την

1^η γραμμή που είναι μέσα στο 2^o κόκκινο πλαίσιο.

Γράφουμε από κάτω από την πρώτη νοστιμή την εντολή που βοίσκεται στην 2^η

Γράφωντες από κάτω από την δεύτερη

Γραφούμε από κάτω από την οευτερή γραμμή την εντολή που βρίσκεται στην 3^η γραμμή.

Activities Terminal ▾

GNU nano 4.8

Βάζουμε το σύμβολο «;» μπροστά από την 1^η γραμμή που είναι μέσα στο 1^º κόκκινο

πλαίσιο.
Γράφουμε από κάτω από την πρώτη γραμμή την εντολή που βρίσκεται στην 2^η

γραμμή.

Προσθέτουμε αυτές τις δύο γραμμές έτσι ώστε να τρέξουμε το OpenVPN χωρίς προβλήμα.

Activities Terminal panosIoannis@panosIoannis: ~

```
GNU nano 4.8 /etc/openvpn/server/server.conf
#       from different clients. See man
#       page for more info on learn-address script.
;learn-address ./script

? # If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses. CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendnsc.com
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
;client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names. This is recommended
```

Βγάζουμε το σύμβολο «;» μπροστά από την γραμμή που είναι μέσα στο 1^o κόκκινο πλαίσιο. Αυτό επιτρέπει όλη την κυκλοφορία δεδομένων του πελάτη να περνάει μέσα από το OpenVPN.

Βγάζουμε το σύμβολο «;» μπροστά από την 1^η και 2^η γραμμή που είναι μέσα στο 2^ο κόκκινο πλαίσιο.



```
panosioannis@panosioannis:~$ sudo nano /etc/sysctl.conf
[5]+  Stopped                  sudo nano /etc/sysctl.conf
panosioannis@panosioannis:~$ sudo sysctl -p
net.ipv4.ip_forward=1
panosioannis@panosioannis:~$
```

Με την 1^η εντολή θα τροποποιήσουμε το αρχείο sysctl.conf που περιέχει το IP Forwarding.

```
panosioannis@panosioannis:~$ ip route list default
default via 192.168.1.1 dev enp0s3 proto static metric 100
panosioannis@panosioannis:~$ sudo nano /etc/ufw/before.rules
# rules.before
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward

# START OPENVPN RULES
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
# Masquerade traffic from OpenVPN client to endpoint (change to the interface you discovered!)
-A POSTROUTING -s 10.8.0.0/8 -o enp0s3 -j MASQUERADE
COMMIT

# END OPENVPN RULES

# Don't delete these required lines, otherwise there will be errors
#filter
#ufw-before-input - [0:0]
#ufw-before-output - [0:0]
#ufw-before-forward - [0:0]
#ufw-not-local - [0:0]
# End required lines

# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

panosioannis@panosioannis:~$
```

Με την 1^η εντολή μπορούμε να δούμε την είσοδο στον υπολογιστή μας από όπου έχουμε δίκτυο.

Με την 2^η εντολή θα τροποποιήσουμε το αρχείο before.rules.

Όπως βλέπουμε στο διπλανό στιγμιότυπο προσθέσαμε τις γραμμές μέσα στο κόκκινο πλαίσιο. Ουσιαστικά αυτές οι τροποποιήσεις θα ορίσουν την προεπιλεγμένη πολιτική για την αλυσίδα POSTROUTING στον πίνακα nat και θα καλύψουν κάθε κίνηση που προέρχεται από το VPN.

```
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# is accepted). You will need to 'disable' and then 'enable' the firewall for
# changes to take effect.
IPV6=yes

# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"

# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"

# Set the default forward policy to ACCEPT, DROP or REJECT. Please note that
# if you change this you will most likely want to adjust your rules.
DEFAULT_FORWARD_POLICY="ACCEPT"

# Set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
# note that setting this to a security 'REJECT' can be a security risk. See man ufw for
# details.
DEFAULT_APPLICATION_POLICY="SKIP"

# By default, ufw only touches its own chains. Set this to 'yes' to have ufw
# manage the built-in chains too. Warning: setting this to 'yes' will break
# existing user-defined firewall rules.
MANAGE_BUILTINS=no

# IPT backend
#
# only enable if using iptables backend
```

Με την ακριβώς πάνω εντολή θα τροποποιήσουμε το αρχείο του firewall.

Συγκεκριμένα, όπως βλέπουμε και στο ακριβώς δίπλα στιγμιότυπο, θα επιτρέψουμε στο firewall τα προωθημένα πακέτα by default.



```
panosioannis@panosioannis:~$ sudo ufw allow 1194/udp
Rule added
Rule added (v6)
panosioannis@panosioannis:~$ sudo ufw disable
Firewall stopped and disabled on system startup
panosioannis@panosioannis:~$ sudo ufw enable
Firewall is active and enabled on system startup
panosioannis@panosioannis:~$
```

Με την 1^η εντολή επιτρέπουμε την θύρα 1194 στο udp στο firewall. (1194 είναι η default θύρα του OpenVPN server).

Με την 2^η εντολή απενεργοποιούμε το firewall.

Με την 3^η εντολή ενεργοποιούμε το firewall.

ΣΗΜΕΙΩΣΗ: Μας έχουν διαφύγει 2 screenshots που γίνεται εγκατάσταση του OpenSSH και στην συνέχεια το επιτρέπουμε στο firewall. Συγκεκριμένα θα γραφτούν οι παρακάτω εντολές με την σειρά:

- sudo apt install openssh-server
- sudo systemctl status ssh
- sudo ufw allow OpenSSH
- sudo ufw disable

```
Activities Terminal Not 11 13:36
panosioannis@panosioannis:~$ sudo systemctl -f enable openvpn-server@server.service
[sudo] password for panosioannis:
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service → /lib/systemd/system/openvpn-server@.service.
panosioannis@panosioannis:~$ sudo systemctl start openvpn-server@server.service
panosioannis@panosioannis:~$ sudo systemctl status openvpn-server@server.service
● openvpn-server@server.service - openvpn service for server
   Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2021-11-11 13:36:10 EET; 13s ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/vk/v/OpenVPN24ManPage
             https://community.openvpn.net/openvpn/Mkt/HowTo
 Main PID: 2148 (openvpn)
   Status: "Initialization Sequence Completed"
   Tasks: 1 (limit: 4038)
      Memory: 1.9M
      CGroups: /system.slice/system-openvpn@x2dserver.slice/openvpn-server@server.service
              └─2148 /usr/sbin/openvpn --status /run/openvpn/server/status-server.log --status-version 2 -s

Nov 11 13:36:10 panosioannis openvpn[2148]: Listening for incoming TCP connection on [AF_INET][undef]:443
Nov 11 13:36:10 panosioannis openvpn[2148]: TCPv4 SERVER link local (bound): [AF_INET][undef]:443
Nov 11 13:36:10 panosioannis openvpn[2148]: TCPv4 SERVER link remote: [AF_UNSPEC]
Nov 11 13:36:10 panosioannis openvpn[2148]: GID set to nogroup
Nov 11 13:36:10 panosioannis openvpn[2148]: UID set to nobody
Nov 11 13:36:10 panosioannis openvpn[2148]: readpid called, r=256 w=256
Nov 11 13:36:10 panosioannis openvpn[2148]: IFCONFIG POOL: hexes10.8.0.4 size=62, ipv6=0
Nov 11 13:36:10 panosioannis openvpn[2148]: IFCONFIG POOL: hexes10.8.0.4 size=62, ipv6=0
Nov 11 13:36:10 panosioannis openvpn[2148]: MULTI: TCP INIT maxclients=1024 maxevents=1028
Nov 11 13:36:10 panosioannis openvpn[2148]: Initialization Sequence completed
[lines 1-23/23 (END)]
[1] Stopped sudo systemctl status openvpn-server@server.service

panosioannis@panosioannis:~$
```

Με την 1^η εντολή διαμορφώνουμε το OpenVPN ώστε να ξεκινά κατά την εκκίνηση, ώστε να μπορούμε να συνδεθούμε στο VPN ανά πάσα στιγμή, εφόσον ο διακομιστής λειτουργεί.

Με την 2^η εντολή ξεκινούμε τον OpenVPN server.

Με την 3^η εντολή ελέγχουμε αν ο OpenVPN server είναι ενεργοποιημένος.

```
Activities Terminal Not 11 13:40
panosioannis@panosioannis:~$ panosioannis@panosioannis:~$ mkdir -p ~/client-configs/files
panosioannis@panosioannis:~$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf
panosioannis@panosioannis:~$ nano ~/client-configs/base.conf
```

Με την 1^η εντολή δημιουργούμε έναν νέο κατάλογο όπου θα αποθηκεύσουμε αρχεία διαμόρφωσης πελάτη στον κατάλογο client-configs που δημιουργήσαμε νωρίτερα.

Με την 2^η εντολή αντιγράφουμε το αρχείο client.conf που αφορά ρύθμιση παραμέτρων πελάτη στον κατάλογο client-configs για να το χρησιμοποιήσουμε ως βασική διαμόρφωση.

Με την 3^η εντολή τροποποιούμε το αρχείο που αντιγράψαμε στην ακριβώς πάνω εντολή.



321-9703-Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

```
Activities Terminal NoeII 15:54 panosloannis@panosloannis:~/client-configs

CPU name: 4.8 /home/panosloannis/client-configs/base.conf
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel!
# http://www.microsoft.com/windows2000/sp2/
# you may need to disable the Firewall
# and turn off the network adapter.

udev mytun
# dev we may
# if we are connecting to a TCP or
# a UDP server we use the same setting as
# the TCP server.
# proto tcp
# proto udp

# the hostport/IP and port of the server;
# You can have multiple remote entries
# for different servers.
remote 192.168.1.159 194
remote my-server 2 194

# Choose a random host from the remote
# list for load-balancing. Otherwise,
# try hosts in the order specified.
# [remote-random]

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the Internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Don't keep user's config changes after initialization (non-Windows only)
user nobody
group nogroup

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to get to the Internet (openVPN
# server) put the proxy serverIP and
# port number here. See the man page
# for more details. The server requires
# authentication.
http-proxy-retry # retry on connection failures
http-proxy [proxy server] proxy port #]

# Wireless networks often produce a lot
# of duplicate broadcast frames. Set this
# to silence duplicate packet warnings.
# wireless

# Most clients don't need to bind to
# a specific local port number.

[ 0 Ext ] [ Write Out ] [ Where Is ] [ Cut Text ] [ Justify Left ] [ Paste Text ] [ To Spell ] [ Get Help ] [ Write Out ] [ Replace ] [ Where Is ] [ Cut Text ] [ Paste Text ] [ Justify Left ] [ To Spell ] [ Get Help ] [ Write Out ] [ Read File ] [ Replace ] [ Where Is ] [ Cut Text ] [ Paste Text ] [ Justify Left ] [ To Spell ] Activities Terminal NoeII 11:34 panosloannis@panosloannis:~

CPU name: 4.8 /home/panosloannis/client-configs/base.conf
# List for load-balancing. Otherwise
# try hosts in the order specified.
# [remote-random]

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the Internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.

[ 0 Ext ] [ Write Out ] [ Where Is ] [ Cut Text ] [ Justify Left ] [ Paste Text ] [ To Spell ] [ Get Help ] [ Write Out ] [ Replace ] [ Where Is ] [ Cut Text ] [ Paste Text ] [ Justify Left ] [ To Spell ] [ Get Help ] [ Write Out ] [ Read File ] [ Replace ] [ Where Is ] [ Cut Text ] [ Paste Text ] [ Justify Left ] [ To Spell ] Activities Terminal NoeII 13:54 panosloannis@panosloannis:~

CPU name: 4.8 /home/panosloannis/client-configs/base.conf
# List for load-balancing. Otherwise
# try hosts in the order specified.
# [remote-random]

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the Internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Verify server certificate by checking that the
# Common Name (CN) in the certificate matches
# this. This is an important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm

# To use this feature, you will need to generate
# your own certificate using the keygen set to
# digitalSignature, keyEncipherment
# and the extendedKeyUsage to
# clientAuth. See the man page
# for more details.
# EasyRSA can do this for you.
# remote-cert-tls server

# If a tls-auth key is used on the server,
# then the client must also have the key.
# [tls-auth tokey 1]

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
# http://openvpn.net/index.php?what=manual
# negotiate AES-256-GCM to TLS v1.2+.
# http://openvpn.net/index.php?what=manual
# cipher AES-256-CBC
cipher AES-256-GCM
auth SHA256

# Don't enable this unless it is also
# specified on the VPN link.
```

Ελέγχουμε αν είναι βγαλμένο το σύμβολο «;» από την 2^η γραμμή στο 1^ο κόκκινο πλαίσιο.

Στην 1^η γραμμή στο 2^o κόκκινο πλαίσιο βάζουμε την IP του σέρβερ και δίπλα την θύρα που είναι ο OpenVPN (1194).

Ελέγχουμε αν είναι βγαλμένο το σύμβολο «;» μπροστά από τις δυο γραμμές που περιέχονται στο κόκκινο πλαίσιο.

Ελέγχουμε αν είναι βαλμένο το σύμβολο «;» μπροστά από τις τρείς γραμμές που περιέχονται στο 1^ο κόκκινο πλαίσιο.

Ελέγχουμε αν είναι βαλμένο το σύμβολο «;» μπροστά από την γραμμή που περιέχεται στο 2^o κόκκινο πλαίσιο.

Πληκτρολογούμε ο,τι πληκτρολογήσαμε και στο αρχείο server.conf σε πιο πάνω στιγμιότυπο. (3^o κόκκινο πλαίσιο)

```
Activities Terminal No 11 13:11
panoioannis@panoioannis: ~
GNU nano 4.8 /home/panoioannis/client-configs/base.com
# then every client must also have the key.
;ts-auth take1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
# Note: The server and clients will automatically
# negotiate AES-256-GCM In TLS mode.
# See also the ncp-cipher option in the manpage
cipher AES-256-GCM
auth SHA256
# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
#comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20

key-direction 1

; script-security 2
; up /etc/openvpn/update-resolv.conf
; down /etc/openvpn/update-resolv-conf

; script-security 2
; up /etc/openvpn/update-systemd-resolved
; down /etc/openvpn/update-systemd-resolved
; resolvconf
; dhcp-option DOMAIN-ROUTE .
```

Προσθέτουμε την γραμμή που βρίσκεται μέσα στο 1^o κόκκινο πλαίσιο. Επιτρέπει στον VPN να λειτουργεί σωστά στην μηχανή του πελάτη.

Προσθέτουμε τις τρεις γραμμές που βρίσκονται μέσα στο 2^o κόκκινο πλαίσιο. Αυτή η ρύθμιση είναι για πελάτες που δεν χρησιμοποιούν systemd-resolved για τη διαχείριση DNS. Αυτοί οι πελάτες βασίζονται στο βοηθητικό πρόγραμμα resolvconf για την ενημέρωση των πληροφοριών DNS για πελάτες Linux.

Προσθέτουμε τις πέντε γραμμές που βρίσκονται μέσα στο 3^o κόκκινο πλαίσιο. Αυτή η ρύθμιση είναι για για πελάτες που χρησιμοποιούν systemd-resolved για ανάλυση DNS.

```
Activities Terminal Noe 11 13:56
panosloannis@panosloannis: ~
panosloannis@panosloannis:~$ mkdir -p ~/client-configs/files
panosloannis@panosloannis:~$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-c
onfigs/base.conf
panosloannis@panosloannis:~$ nano ~/client-configs/base.conf

? Use "fg" to return to nano.

[2]+ Stopped nano ~/client-configs/base.conf
panosloannis@panosloannis:~$ nano ~/client-configs/base.conf

Use "fg" to return to nano.

[3]+ Stopped nano ~/client-configs/base.conf
panosloannis@panosloannis:~$ nano ~/client-configs/base.conf

Use "fg" to return to nano.

[4]+ Stopped nano ~/client-configs/base.conf
panosloannis@panosloannis:~$ nano ~/client-configs/base.conf

Use "fg" to return to nano.

[5]+ Stopped nano ~/client-configs/base.conf
panosloannis@panosloannis:~$ nano ~/client-configs/make_config.sh
```

Με αυτή την εντολή θα δημιουργήσουμε ένα script που θα μεταγλωτίσει τη βασική διαμόρφωση με το σχετικό πιστοποιητικό, το κλειδί και τα αρχεία κρυπτογράφησης και στη συνέχεια θα τοποθετήσει τη διαμόρφωση που δημιουργήθηκε στον κατάλογο `~/client-configs/files`.



```
Activities Terminal panosioannis@panosioannis: ~
GNU nano 4.8 /home/panosioannis/client-configs/make_config.sh
#!/bin/bash

# First argument: Client identifier
KEY_DIR=/client-configs/keys
OUTPUT_DIR=/client-configs/files
BASE_CONFIG=/client-configs/base.conf

cat ${BASE_CONFIG} \
<echo -e <>ca.crt \
${KEY_DIR}/ca.crt \
<echo -e </ca>\n<cert> \
${KEY_DIR}/\$1.crt \
<echo -e </cert>\n<key> \
${KEY_DIR}/\$1.key \
<echo -e </key>\n<tls-crypt> \
${KEY_DIR}/ta.key \
<echo -e </tls-crypt> \
> ${OUTPUT_DIR}/\$(<).ovpn
```

```
Activities Terminal panosioannis@panosioannis: ~
panosioannis@panosioannis: $ mkdir -p ~/client-configs/files
panosioannis@panosioannis: $ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-conf
onfiles/base.conf
panosioannis@panosioannis: $ nano ~/client-configs/base.conf
[2]+ Stopped nano ~/client-configs/base.conf
panosioannis@panosioannis: $ nano ~/client-configs/base.conf

Use "fg" to return to nano.
[3]+ Stopped nano ~/client-configs/base.conf
panosioannis@panosioannis: $ nano ~/client-configs/base.conf

Use "fg" to return to nano.
[4]+ Stopped nano ~/client-configs/base.conf
panosioannis@panosioannis: $ nano ~/client-configs/base.conf

Use "fg" to return to nano.
[5]+ Stopped nano ~/client-configs/base.conf
panosioannis@panosioannis: $ nano ~/client-configs/make_config.sh
[6]+ Stopped nano ~/client-configs/make_config.sh
panosioannis@panosioannis: $ chmod 700 ~/client-configs/make_config.sh
panosioannis@panosioannis: $
```

Κάνουμε αντιγραφή επικόλληση το έτοιμο script που αντλήσαμε από την βιβλιογραφία στο αρχείο που δημιουργήσαμε στο ακριβώς πάνω στιγμιότυπο.

Αυτό το σενάριο θα δημιουργήσει ένα αντίγραφο του αρχείου base.conf που δημιουργήσαμε, θα συλλέξει όλα τα πιστοποιητικά και τα βασικά αρχεία που έχουμε δημιουργήσει για τον πελάτη, θα εξαγάγει τα περιεχόμενά τους, θα τα προσαρτήσει στο αντίγραφο του αρχείου base configuration και θα εξαγάγει όλο αυτό το περιεχόμενο σε ένα νέο client configuration αρχείο. Αυτό σημαίνει ότι, αντί να χρειάζεται να διαχειρίζόμαστε ξεχωριστά τις ρυθμίσεις παραμέτρων, το πιστοποιητικό και τα αρχεία κλειδιών του πελάτη, όλες οι απαιτούμενες πληροφορίες αποθηκεύονται σε ένα μέρος.

(ΜΟΝΟ Η ΤΕΛΕΥΤΑΙΑ ΕΝΤΟΛΗ ΕΧΕΙ ΒΑΣΗ ΣΕ ΑΥΤΟ ΤΟ ΣΤΙΓΜΙΟΤΥΠΟ. ΟΙ ΥΠΟΛΟΙΠΕΣ ΕΧΟΥΝ ΣΥΜΠΕΡΙΛΗΦΘΕΙ ΣΕ ΠΑΡΑΠΑΝΩ ΣΤΙΓΜΙΟΤΥΠΟ)

Με αυτή την εντολή επισημάνουμε το παραπάνω αρχείο ως εκτελέσιμο.

```
Activities Terminal panosioannis@panosioannis: ~/client-configs
panosioannis@panosioannis: $ cd ~/client-configs
panosioannis@panosioannis: ~/client-configs$ ./make_config.sh client1
panosioannis@panosioannis: ~/client-configs$ ls ~/client-configs/files
client1.ovpn
panosioannis@panosioannis: ~/client-configs$ ./make_config.sh client2
panosioannis@panosioannis: ~/client-configs$ ls ~/client-configs/files
client1.ovpn client2.ovpn
panosioannis@panosioannis: ~/client-configs$
```

Με την 1^η εντολή αλλάζουμε directory και πηγαίνουμε εκεί που είναι όλα τα configurations των πελατών.

Με την 2^η εντολή δημιουργούμε ένα config file για αυτά τα διαπιστευτήρια μεταβαίνοντας στον κατάλογο ~/client-configs και εκτελούμε το script που φτιάχαμε σε προηγούμενο στιγμιότυπο. Αυτό θα δημιουργήσει ένα αρχείο με το όνομα client1.ovpn στον κατάλογο ~/client-configs/files.

Με την 3^η εντολή ελέγχουμε αν δημιουργήθηκε το αρχείο client1.ovpn. (ΓΙΑ ΤΟΝ client2 ΑΚΟΛΟΥΘΟΥΜΕ ΤΑ ΙΔΙΑ ΒΗΜΑΤΑ)



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

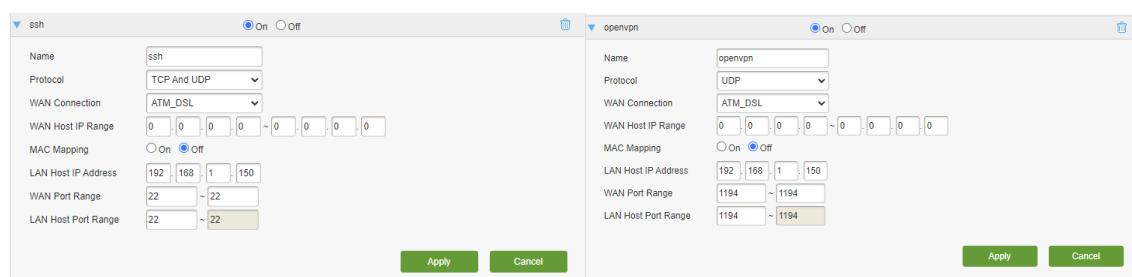
ΛΕΙΤΟΥΡΓΙΑ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΚΑΙ ΚΛΕΙΔΙΩΝ

Το PKI (Public Key Infrastructure) αποτελείται από ένα ξεχωριστό πιστοποιητικό (γνωστό και ως δημόσιο κλειδί) και ιδιωτικό κλειδί για τον διακομιστή και κάθε πελάτη, και ένα κύριο πιστοποιητικό και κλειδί Αρχής Έκδοσης Πιστοποιητικών (CA) που χρησιμοποιείται για την υπογραφή καθενός από τα πιστοποιητικά διακομιστή και πελάτη. Το OpenVPN υποστηρίζει αμφίδρομη ταυτοποίηση βάσει πιστοποιητικών, πράγμα που σημαίνει ότι ο πελάτης πρέπει να ελέγξει την ταυτότητα του πιστοποιητικού διακομιστή και ο διακομιστής πρέπει να ελέγξει την ταυτότητα του πιστοποιητικού πελάτη πριν δημιουργηθεί αμοιβαία εμπιστοσύνη. Τόσο ο διακομιστής όσο και ο πελάτης θα ελέγξουν την ταυτότητα του άλλου επιβεβαιώνοντας πρώτα ότι το παρουσιαζόμενο πιστοποιητικό υπογράφηκε από την αρχή του κύριου πιστοποιητικού (CA) και, στη συνέχεια, δοκιμάζοντας πληροφορίες στην κεφαλίδα πιστοποιητικού που έχει πλέον επικυρωθεί, όπως το κοινό όνομα πιστοποιητικού ή τύπος πιστοποιητικού (πελάτης ή σερβερ). Αυτό το μοντέλο ασφαλείας έχει μια σειρά από επιθυμητά χαρακτηριστικά από την άποψη του VPN:

- Ο διακομιστής χρειάζεται μόνο το δικό του πιστοποιητικό/κλειδί — δεν χρειάζεται να γνωρίζει τα μεμονωμένα πιστοποιητικά κάθε πελάτη που μπορεί να συνδεθεί σε αυτόν.
- Ο διακομιστής θα δέχεται μόνο πελάτες των οποίων τα πιστοποιητικά έχουν υπογραφεί από το κύριο πιστοποιητικό CA (το οποίο θα δημιουργήσουμε παραπάνω). Και επειδή ο διακομιστής μπορεί να εκτελέσει αυτήν την επαλήθευση υπογραφής χωρίς να χρειάζεται πρόσβαση στο ίδιο το ιδιωτικό κλειδί CA, είναι δυνατό το κλειδί CA (το πιο ευαίσθητο κλειδί σε ολόκληρο το PKI) να βρίσκεται σε ένα εντελώς διαφορετικό μηχάνημα, ακόμη και σε ένα χωρίς σύνδεση στο διαδίκτυο.

Πριν προχωρήσουμε στην δοκιμή της διαμόρφωσής μας, πρέπει να επισημάνουμε ότι πραγματοποιήσαμε Port Forwarding στον δρομολογητή μας έτσι ώστε να λειτουργήσει το VPN.

Συγκεκριμένα επιτρέψαμε τις θύρες 22 (SSH) και 1194 (default OpenVPN Port).





321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 2.2

Ζητούμενο 1 - Testing

Αφού κάνουμε την παραμετροποίηση του OpenVPN Server, θα πρέπει να τεστάρουμε τον σέρβερ να δούμε αν λειτουργεί. Δοκιμάσαμε σε 2 διαφορετικές συσκευές με διαφορετικά λειτουργικά συστήματα (1 smartphone Android OS και 1 λάπτοπ MacOS).

Android OS

The screenshots show the OpenVPN Connect app interface on an Android device. The left screenshot shows a 'Profiles' screen with a green 'CONNECTED' status, an 'OpenVPN Profile' section with the IP '192.168.1.150 (client1 (3))', and a 'CONNECTION STATS' section with a yellow line graph showing data transfer over time. The right screenshot shows a similar view with a yellow line graph showing data transfer rates of '4 B/S' for both bytes in and bytes out, and a duration of '00:12:08'. It also displays 'PACKET RECEIVED 2 sec ago' and 'YOUR PRIVATE IP 10.8.0.6'. The bottom of each screenshot shows the standard Android navigation bar.

Πριν δουλέψει το VPN, μεταφέραμε το αρχείο client1.ovpn στο κινητό τηλέφωνο, το εισαγάγαμε στην εφαρμογή του OpenVPN και δοκιμάσαμε να συνδεθούμε στο VPN.

Στα δύο στιγμιότυπα που φαίνονται πιο πάνω παρατηρούμε ότι το κινητό τηλέφωνο συνδέεται επιτυχώς στον σέρβερ.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

Mac OS

The screenshot displays two windows from the Tunnelblick application. The left window, titled 'PRIΝ ΤΗΝ ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΟΥ VPN', shows a table of DNS leak test results with 12 entries. The right window, titled 'ΜΕΤΑ ΤΗΝ ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΟΥ VPN', shows a table with 20 entries. Both tables include columns for IP, Hostname, ISP, and Country. The 'Country' column shows that all results are from Amsterdam, Netherlands, indicating a full DNS leak.

IP	Hostname	ISP	Country
83.235.71.83	ryma-dns1.ultranet.gr	Cosmote	Greece
83.235.71.84	ryma-dns2.ultranet.gr	Cosmote	Greece
83.235.71.85	ryma-dns10.ultranet.gr	Cosmote	Greece
83.235.71.86	ryma-dns19.ultranet.gr	Cosmote	Greece
83.235.71.87	ryma-dns18.ultranet.gr	Cosmote	Greece
83.235.71.88	ryma-dns17.ultranet.gr	Cosmote	Greece
83.235.71.89	ryma-dns16.ultranet.gr	Cosmote	Greece
83.235.71.90	ryma-dns15.ultranet.gr	Cosmote	Greece
83.235.71.91	ryma-dns14.ultranet.gr	Cosmote	Greece
83.235.71.92	ryma-dns13.ultranet.gr	Cosmote	Greece
83.235.71.93	ryma-dns12.ultranet.gr	Cosmote	Greece

IP	Hostname	ISP	Country
208.69.35.15	m53.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.19	m51.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.21	m511.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.45	m517.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.66	m527.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.67	m522.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.68	m529.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.70	m537.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.71	m51.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.72	m545.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.73	m548.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.74	m553.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.75	m557.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands
208.69.35.76	m511.ams.opendns.com	Cisco OpenDNS, LLC	Amsterdam, Netherlands

Πριν δουλέψει το VPN, μεταφέραμε το αρχείο client2.ovpn στο MacBook Pro, το εισαγάγαμε στην εφαρμογή Tunnelblick και δοκιμάσαμε να συνδεθούμε στο VPN. Για να ελέγχουμε την ορθή λειτουργία πήγαμε στην ιστοσελίδα dnsleaktest.com έτσι ώστε να δούμε τους DNS Servers που θα επικοινωνήσει το λάπτοπ πριν και μετά την ενεργοποίηση του VPN.

PRIΝ την ενεργοποίηση παρατηρούμε ότι οι DNS Servers που επικοινωνεί το λάπτοπ είναι οι σερβερούς της Cosmote. Αυτό σημαίνει ότι η Cosmote μπορεί να διαβάσει την περιήγησή μας στο διαδίκτυο.

META την ενεργοποίηση παρατηρούμε ότι οι DNS Servers που επικοινωνεί το λάπτοπ είναι οι σερβερούς OpenDNS που εδρεύουν στην Ολλανδία. Αυτό σημαίνει ότι η Cosmote δεν μπορεί να διαβάσει την περιήγησή μας στο διαδίκτυο.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 3

Ζητούμενο 2



ΚΕΦΑΛΑΙΟ 3.1^{[4][5][8]}

Ζητούμενο 2

Αφού κάνουμε την προετοιμασία της δεύτερης εικονικής μηχανής προχωρούμε στην επίλυση του 2^{ου} Ζητούμενου. Η παρουσίαση της πορείας της εργασίας από εδώ και πέρα θα γίνει με στιγμιότυπα και επεξηγήσεις.

```
panosloannis@panosloannis:~$ sudo apt install strongswan strongswan-pki libcharon-extra-plugins libcharon-exauth-plugins
[sudo] password for panosloannis:
Reading state information... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libstrongswan libstrongswan-standard-plugins strongswan-charon strongswan-libcharon
  strongswan-starter
The following NEW packages will be installed:
  libcharon-exauth-plugins libcharon-extra-plugins libcupic libstrongswan libstrongswan-extras-plugins
  libstrongswan-standard-plugins strongswan strongswan-charon strongswan-libcharon strongswan-pki
  strongswan-starter
0 upgraded, 11 newly installed, 0 to remove and 4 not upgraded.
Need to get 1564 kB of archives.
```

Με αυτή την εντολή κάνουμε εγκατάσταση το StrongSwan μαζί με όλα τα απαραίτητα πακέτα προκειμένου να λειτουργεί σωστά. Το πρόσθετο πακέτο libcharon-exauth-plugins χρησιμοποιείται για να διασφαλιστεί ότι διαφοροί πελάτες μπορούν να πραγματοποιήσουν έλεγχο ταυτότητας στον διακομιστή χρησιμοποιώντας ένα κοινόχρηστο όνομα χρήστη και φράση πρόσβασης. Το πακέτο libstrongswan-extra-plugins περιλαμβάνεται έτσι ώστε το Strongswan να υποστηρίζει σουίτες κρυπτογράφησης ελλεπτικών καμπυλών που χρησιμοποιούν τη σουίτα κρυπτογράφησης Curve25519.

```
panosloannis@panosloannis:~$ chmod 700 -R /pk1
```

Με την 1^η εντολή δημιουργούμε μερικούς καταλόγους για να αποθηκεύσουμε όλα τα στοιχεία που θα εργαστούμε.

Με την 2^η εντολή κλειδώνουμε τα δικαιώματα έτσι ώστε τα ιδιωτικά μας αρχεία να μην είναι ορατά από άλλους χρήστες.

```
panosloannis@panosloannis:~$ pkitab --gen --type rsa --size 4096 --output pen > /pk1/private/ca-key.pen
> --type rsa --dn "CN=VPN root CA" --output pen > /pk1/certs/ca-cert.pen
panosloannis@panosloannis:~$ pkitab --gen --type rsa --size 4096 --output pen > /pk1/private/server-key.pen
panosloannis@panosloannis:~$ pkitab --list-all
> | pkitab --list-all
> | > ca-cert: /pk1/certs/ca-cert.pen \
> | > ca-key: /pk1/private/ca-key.pen \
> | > server-auth: 192.168.1.155 --san 192.168.1.155 \
> | > .flag serverAuth .flag tkipIntermediate --output pen \
> | > /pk1/certs/server-cert.pen
panosloannis@panosloannis:~$ sudo cp -r /pk1/* /etc/ipsec.d/
panosloannis@panosloannis:~$
```

Με την 1^η εντολή δημιουργούμε ένα βασικό κλειδί.

Με την 2^η εντολή δημιουργούμε root CA χρησιμοποιώντας το κλειδί που μόλις δημιουργήσαμε για να υπογράψουμε το root πιστοποιητικό.

Με την 3^η εντολή δημιουργούμε ένα ιδιωτικό κλειδί για τον διακομιστή VPN.

Με την 4^η εντολή δημιουργούμε και υπογράφουμε το πιστοποιητικό διακομιστή VPN με το κλειδί της CA που δημιουργήσαμε στο προηγούμενο βήμα.

Με την τελευταία εντολή μετακινούμε τα αρχεία στον κατάλογο /etc/ipsec.d.

```
panosloannis@panosloannis:~$ sudo mv /etc/ipsec.conf{,.original}
panosloannis@panosloannis:~$ sudo nano /etc/ipsec.conf
```

Με την 1^η εντολή κάνουμε backup το αρχείο ipsec.conf διότι δεν θέλουμε να χαθούν οι προεπιλεγμένες ρυθμίσεις.

Με την 2^η εντολή δημιουργούμε και ανοίγουμε ένα νέο κενό αρχείο διαμόρφωσης χρησιμοποιώντας το πρόγραμμα επεξεργασίας κειμένου. Κάνουμε αντιγραφή επικόλληση από την βιβλιογραφία.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

The screenshot shows two terminal windows side-by-side. Both windows are running on an Ubuntu 20.04 LTS system. The left window is titled 'panosioannis@panosioannis: ~' and shows the contents of the file '/etc/ipsecc.conf'. The right window is also titled 'panosioannis@panosioannis: ~' and shows the contents of the file '/etc/ipsecc.conf'. Both files contain configuration for an IKEv2 VPN connection named 'ikev2-vpn'. The configuration includes parameters like 'auto=add', 'compress=no', 'fragmentation=yes', 'forceencaps=yes', 'fragmentation-clear', 'ddpdelay=300s', 'rekey=no', 'leftid=any', 'leftcert=server-cert.pem', 'leftsendertagsalways', 'leftsubonet=0.0.0.0/0', 'rightid=any', 'rightauth=mschapv2', 'rightdns=8.8.8.8,8.8.4.4', 'rightsubnet=0.0.0.0/24', and 'rightsendertagsnever'. The right window also includes a section for 'modpsk' and 'esp-psk'. The bottom of both terminals shows standard Linux terminal navigation keys.

Με το 1^o κόκκινο πλαίσιο λέμε στον StrongSwan να καταγράφει καταστάσεις deamon για εντοπισμό σφαλμάτων και να επιτρέπει διπλότυπες συνδέσεις.

Με το 2^o κόκκινο πλαίσιο δημιουργούμε μια ενότητα διαμόρφωσης για το VPN μας. Λέμε επίσης στον StrongSwan να δημιουργήσει IKEv2 VPN Tunnels και να φορτώσει αυτόματα αυτήν την ενότητα διαμόρφωσης κατά την εκκίνηση.

Με το 3^o κόκκινο πλαίσιο διαμορφώνουμε επίσης την ανίχνευση dead-peer για την εκκαθάριση τυχόν "dangling" συνδέσεων σε περίπτωση που ο πελάτης αποσυνδέθει απροσδόκητα.

Με το 4^o κόκκινο πλαίσιο διαμορφώνουμε τις παραμέτρους IPSec της «αριστερής» πλευράς του διακομιστή. Καθεμία από τις ακόλουθες παραμέτρους διασφαλίζει ότι ο διακομιστής έχει ρυθμιστεί ώστε να δέχεται συνδέσεις από πελάτες και να αναγνωρίζει τον εαυτό του σωστά.

Με το 5^o κόκκινο πλαίσιο διαμορφώνουμε τις παραμέτρους IPSec της «δεξιάς» πλευράς του πελάτη. Καθεμία από τις ακόλουθες παραμέτρους λέει στον διακομιστή πώς να δέχεται συνδέσεις από πελάτες, πώς πρέπει να γίνεται έλεγχος ταυτότητας των πελατών στο διακομιστή και τις ιδιωτικές περιοχές διευθύνσεων IP και τους διακομιστές DNS που θα χρησιμοποιούν οι πελάτες.

Με το 6^o κόκκινο πλαίσιο λέμε στον StrongSwan να ζητήσει από τον πελάτη διαπιστευτήρια χρήστη όταν συνδεθεί.

Στο 7^o κόκκινο πλαίσιο προσθέτουμε τις ακόλουθες γραμμές για την υποστήριξη πελατών Linux, Windows, macOS, iOS και Android. Αυτές οι γραμμές καθορίζουν τους διάφορους αλγόριθμους ανταλλαγής κλειδιών, κατακερματισμού, ελέγχου ταυτότητας και κρυπτογράφησης (που συνήθως αναφέρονται ως Cipher Suites) που το StrongSwan θα επιτρέπει σε διαφορετικούς πελάτες να χρησιμοποιούν.

The screenshot shows two terminal windows. The left window is titled 'panosioannis@panosioannis: ~' and shows the command 'sudo nano /etc/ipsecc.secrets'. The right window is also titled 'panosioannis@panosioannis: ~' and shows the contents of the file '/etc/ipsecc.secrets'. The file contains the following text:
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 "server-key.pem"
icsd18107 : EAP "icsd18161"
The bottom of both terminals shows standard Linux terminal navigation keys.

(ΑΡΙΣΤΕΡΟ ΣΤΙΓΜΙΟΤΥΠΟ): Με την 1^η εντολή ανοίγουμε το αρχείο που θα περιέχει τα credentials κάθε πελάτη προκειμένου να συνδεθεί στο VPN.

(ΔΕΞΙ ΣΤΙΓΜΙΟΤΥΠΟ): Λέμε στον StrongSwan που να βρει το ιδιωτικό μας κλειδί και πώς να το αναλύσει. Στην συνέχεια ορίζουμε τα διαπιστευτήρια χρήστη.

(ΑΡΙΣΤΕΡΟ ΣΤΙΓΜΙΟΤΥΠΟ): Με την 2^η εντολή επανεκκινούμε την υπηρεσία VPN, ώστε να εφαρμοστεί η διαμόρφωσή μας.



321-9703-Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal Noe 11 17:48
panosioannis@panosioannis:~$ sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
panosioannis@panosioannis:~$ sudo ufw enable
Firewall is active and enabled on system startup
panosioannis@panosioannis:~$ sudo ufw allow 500,4500/udp
Rule added
Rule added (v6)
panosioannis@panosioannis:~$ ip route show default
default via 192.168.1.1 dev enp0s3 proto static metric 100
panosioannis@panosioannis:~$ sudo nano /etc/ufw/before.rules
Use "fg" to return to nano.

[5]+ Stopped sudo nano /etc/ufw/before.rules
panosioannis@panosioannis:~$ sudo nano /etc/ufw/sysctl.conf

Use "fg" to return to nano.

[6]+ Stopped sudo nano /etc/ufw/sysctl.conf
panosioannis@panosioannis:~$ sudo ufw disable
Firewall stopped and disabled on system startup
panosioannis@panosioannis:~$ sudo ufw enable
Firewall is active and enabled on system startup
panosioannis@panosioannis:~$
```

Με την 1^η εντολή επιτρέπουμε το OpenSSH στο firewall.

Με την 2^η εντολή ενεργοποιούμε το firewall.

Με την 3^η εντολή επιτρέπουμε τις θύρες 500 και 4500 κατά υδρ στο firewall.

Με την 4η εντολή βρήσκουμε ποια διεπαφή δικτύου στον διακομιστή μας χρησιμοποιείται για πρόσβαση στο Διαδίκτυο.

Με την 5^η εντολή ανοίγουμε ένα από τα αρχεία διαμόρφωσης του UFW για να προσθέσουμε μερικές πολιτικές χαμηλού επιπέδου για τη δρομολόγηση και την προώθηση πακέτων IPSec. (ΣΤΙΓΜΙΟΤΥΠΑ META)

Με την 6η εντολή ανοίγουμε το αρχείο διαμόρφωσης παραμέτρων πυρήνα του UFW. (ΣΤΙΓΜΙΟΤΥΠΟ ΜΕΤΑ)

Με την 7^η εντολή απενεργοποιούμε το firewall.

Με την 8^η εντολή ενεργοποιούμε το firewall.

5^η ΕΝΤΟΛΗ ΑΠΟ ΤΟ ΠΑΡΑΠΑΝΩ ΣΤΙΓΜΙΟΤΥΠΟ (αρχείο: before.rules)

```
panosloannis@panosloannis: ~
```

```
GNU nano 4.8
```

```
rules.before
```

```
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   - ufw-before-input
#   - ufw-before-output
#   - ufw-before-forward
```

```
*nat
```

```
-A POSTROUTING -s 10.10.10.0/24 -o enp0s3 -m policy --pol ipsec --dir out -j ACCEPT
-A POSTROUTING -s 10.10.10.0/24 -o enp0s3 -j MASQUERADE
COMMIT
```

```
*mangle
```

```
-A FORWARD -m policy --dir in -s 10.10.10.0/24 -o enp0s3 -p tcp --tcp-flags SYN,RST
COMMIT
```

```
# Don't delete these required lines, otherwise there will be errors
#filter
#ufw-before-input - [0:0]
#ufw-before-output - [0:0]
#ufw-before-forward - [0:0]
#ufw-not-local - [0:0]
#end required lines
```

```
-A ufw-before-forward -m policy --pol ipsec --dir in --proto esp -s 10.10.10.0/24 -j ACCEPT
-A ufw-before-forward -m policy --pol ipsec --dir out --proto esp -d 10.10.10.0/24 -j ACCEPT
```

```
# allow all on interface
-A ufw-before-forward -l lo -j ACCEPT
-A ufw-before-output -l lo -j ACCEPT
```

```
Get Help ⌘ + F1 Write Out ⌘ + F2 Where Is ⌘ + F3 Cut Text ⌘ + X Paste Text ⌘ + V Justify ⌘ + J To Spell ⌘ + S Go To Pos ⌘ + G Undo ⌘ + Z Redo ⌘ + Y
```

```
panosloannis@panosloannis: ~
```

```
GNU nano 4.8
```

```
rules.before
```

```
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   - ufw-before-input
#   - ufw-before-output
#   - ufw-before-forward
```

```
*nat
```

```
-A POSTROUTING -s 10.10.10.0/24 -o enp0s3 -m policy --pol ipsec --dir out -j ACCEPT
-A POSTROUTING -s 10.10.10.0/24 -o enp0s3 -j MASQUERADE
COMMIT
```

```
*mangle
```

```
-A SYN,RST SYN -m tcpmss --nss 1361:1536 -j TCPMSS --set-mss 1360
COMMIT
```

```
# Don't delete these required lines, otherwise there will be errors
#filter
#ufw-before-input - [0:0]
#ufw-before-output - [0:0]
#ufw-before-forward - [0:0]
#ufw-not-local - [0:0]
#end required lines
```

```
-A ufw-before-forward -m policy --pol ipsec --dir in --proto esp -s 10.10.10.0/24 -j ACCEPT
-A ufw-before-forward -m policy --pol ipsec --dir out --proto esp -d 10.10.10.0/24 -j ACCEPT
```

```
# allow all on interface
-A ufw-before-forward -l lo -j ACCEPT
-A ufw-before-output -l lo -j ACCEPT
```

```
Get Help ⌘ + F1 Write Out ⌘ + F2 Where Is ⌘ + F3 Cut Text ⌘ + X Paste Text ⌘ + V Justify ⌘ + J To Spell ⌘ + S Go To Pos ⌘ + G Undo ⌘ + Z Redo ⌘ + Y
```

Με το 1^o κόκκινο πλαίσιο, οι γραμμές *nat δημιουργούν κανόνες έτσι ώστε το τείχος προστασίας να μπορεί να δρομολογεί και να χειρίζεται σωστά την κυκλοφορία μεταξύ των πελατών VPN και του Διαδικτύου. Η γραμμή *mangle προσαρμόζει το μέγιστο μέγεθος τιμήματος πακέτου για να αποτρέψει πιθανά προβλήματα με συγκεκριμένους πελάτες VPN.

Με το 2^o κόκκινο πλαίσιο λέμε στο τείχος προστασίας να προωθήσει την κυκλοφορία ESP (Encapsulating Security Payload) έτσι ώστε οι πελάτες VPN να μπορούν να συνδεθούν. Το ESP παρέχει πρόσθετη ασφάλεια για τα πακέτα VPN μας καθώς διασχίζουν μη αξιόπιστα δίκτυα.

```
Activities Terminal └── panosIoannis@panosIoannis: ~
  └── nano 4.8
    └── /etc/ipv4/conf/all/forwarding=1
      └── /etc/ufw/sysctl.conf

  # Disable ICMP redirects. ICMP redirects are rarely used but can be used in
  # MITM (man-in-the-middle) attacks. Disabling ICMP may disrupt legitimate
  # traffic.
  net/ipv4/conf/all/accept_redirects=0
  net/ipv4/conf/default/accept_redirects=0
  net/ipv4/conf/all/accept_redirects=0
  net/ipv4/conf/default/accept_redirects=0

  # Ignore bogus ICMP errors
  net/ipv4/icmp_echo_ignore_broadcasts=1
  net/ipv4/icmp_echo_ignore_replies=1
  net/ipv4/icmp_echo_ignore_all=0

  # Don't log Martians Packets (impossible addresses)
  # packets
  net/ipv4/conf/all/log_martians=0
  net/ipv4/conf/default/log_martians=0

  # Set IPv4 TCP fin_timeout=30
  #net/ipv4/tcp_keepalive_time=1000

  # Uncomment this to turn off IPv6 autoconfiguration
  #net/ipv6/conf/default/autocfg=1
  #net/ipv6/conf/all/autocfg=1

  # Uncomment this to enable IPv6 privacy addressing
  #net/ipv6/conf/default/use_tempaddr=2
  #net/ipv6/conf/default/use_tempaddr=2

  #net/ipv4/ip_forward=1
  net/ipv4/conf/all/accept_redirects=0
  net/ipv4/conf/all/send_redirects=0
  net/ipv4/ip_no_pmtu_disc=1

  └── Get Help └── Ext └── Write Out └── Where Is └── Cut Text └── Justify
    └── Read File └── Reply └── Paste Text └── To Spell
```

Στο κορκτό πλαίσιο με την Τ. γράμμη συνεργειώσαμε την Κρεωποτή πακέτων μεταξύ διεπαφών.

Στο αύγουστο του 1981 οι πρώτες διαδικασίες για την επένδυση στην Ελλάδα έγιναν στην Αθήνα.



321-9703-Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

Με αυτή την εντολή βλέπουμε αν όντως έχει δημιουργηθεί επιτυχώς τα πιστοποιητικά CA.

ΛΕΙΤΟΥΡΓΙΑ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΚΑΙ ΚΛΕΙΔΙΩΝ

Τα ψηφιακά πιστοποιητικά παρέχουν ένα μέσο για τον ψηφιακό έλεγχο ταυτότητας συσκευών και μεμονωμένων χρηστών. Αυτά τα πιστοποιητικά λειτουργούν σαν ένα διαδικτυακό διαβατήριο—είναι στεγανά και δεν μπορούν να πλαστογραφηθούν. Ένα άτομο που επιθυμεί να στείλει κρυπτογραφημένα δεδομένα αποκτά ψηφιακό πιστοποιητικό από μια Αρχή Έκδοσης Πιστοποιητικών (CA). Η CA εκδίδει ένα κρυπτογραφημένο ψηφιακό πιστοποιητικό που περιέχει το δημόσιο κλειδί του αιτούντος και μια ποικιλία άλλων πληροφοριών αναγνώρισης. Η CA καθιστά το δικό της δημόσιο κλειδί άμεσα διαθέσιμο. Ο παραλήπτης του κρυπτογραφημένου μηνύματος χρησιμοποιεί το δημόσιο κλειδί της CA για να αποκωδικοποιήσει το ψηφιακό πιστοποιητικό που επισυνάπτεται στο μήνυμα, το επαληθεύει ότι έχει εκδοθεί από την CA και, στη συνέχεια, λαμβάνει το δημόσιο κλειδί του αποστολέα και τις πληροφορίες αναγνώρισης που βρίσκονται στο πιστοποιητικό. Με αυτές τις πληροφορίες, ο παραλήπτης μπορεί να στείλει μια κρυπτογραφημένη απάντηση. Η υποδομή δημόσιου κλειδιού (PKI) είναι ο ενεργοποιητής για τη διαχείριση ψηφιακών πιστοποιητικών για την ανάπτυξη IPSec VPN.

Πριν προχωρήσουμε στην δοκιμή της διαμόρφωσής μας, πρέπει να επισημάνουμε ότι πραγματοποιήσαμε Port Forwarding στον δρομολογητή μας έτσι ώστε να λειτουργήσει τα VPN.

Συγκεκριμένα επιτρέψαμε τις θύρες 22 (SSH) και 4500 (default IPSec Port).

<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>																
<p>ipsecash</p> <p><input checked="" type="radio"/> On <input type="radio"/> Off</p> <table border="1"> <tr> <td>Name</td> <td>ipsecash</td> </tr> <tr> <td>Protocol</td> <td>TCP And UDP</td> </tr> <tr> <td>WAN Connection</td> <td>ATM_DSL</td> </tr> <tr> <td>WAN Host IP Range</td> <td>0.0.0.0 - 0.0.0.0</td> </tr> <tr> <td>MAC Mapping</td> <td><input type="radio"/> On <input checked="" type="radio"/> Off</td> </tr> <tr> <td>LAN Host IP Address</td> <td>192.168.1.155</td> </tr> <tr> <td>WAN Port Range</td> <td>22 - ~22</td> </tr> <tr> <td>LAN Host Port Range</td> <td>22 - ~22</td> </tr> </table>			Name	ipsecash	Protocol	TCP And UDP	WAN Connection	ATM_DSL	WAN Host IP Range	0.0.0.0 - 0.0.0.0	MAC Mapping	<input type="radio"/> On <input checked="" type="radio"/> Off	LAN Host IP Address	192.168.1.155	WAN Port Range	22 - ~22	LAN Host Port Range	22 - ~22
Name	ipsecash																	
Protocol	TCP And UDP																	
WAN Connection	ATM_DSL																	
WAN Host IP Range	0.0.0.0 - 0.0.0.0																	
MAC Mapping	<input type="radio"/> On <input checked="" type="radio"/> Off																	
LAN Host IP Address	192.168.1.155																	
WAN Port Range	22 - ~22																	
LAN Host Port Range	22 - ~22																	
<p>ipseca4500</p> <p><input checked="" type="radio"/> On <input type="radio"/> Off</p> <table border="1"> <tr> <td>Name</td> <td>ipseca4500</td> </tr> <tr> <td>Protocol</td> <td>UDP</td> </tr> <tr> <td>WAN Connection</td> <td>ATM_DSL</td> </tr> <tr> <td>WAN Host IP Range</td> <td>0.0.0.0 - 0.0.0.0</td> </tr> <tr> <td>MAC Mapping</td> <td><input type="radio"/> On <input checked="" type="radio"/> Off</td> </tr> <tr> <td>LAN Host IP Address</td> <td>192.168.1.155</td> </tr> <tr> <td>WAN Port Range</td> <td>4500 - ~4500</td> </tr> <tr> <td>LAN Host Port Range</td> <td>4500 - ~4500</td> </tr> </table>			Name	ipseca4500	Protocol	UDP	WAN Connection	ATM_DSL	WAN Host IP Range	0.0.0.0 - 0.0.0.0	MAC Mapping	<input type="radio"/> On <input checked="" type="radio"/> Off	LAN Host IP Address	192.168.1.155	WAN Port Range	4500 - ~4500	LAN Host Port Range	4500 - ~4500
Name	ipseca4500																	
Protocol	UDP																	
WAN Connection	ATM_DSL																	
WAN Host IP Range	0.0.0.0 - 0.0.0.0																	
MAC Mapping	<input type="radio"/> On <input checked="" type="radio"/> Off																	
LAN Host IP Address	192.168.1.155																	
WAN Port Range	4500 - ~4500																	
LAN Host Port Range	4500 - ~4500																	



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 3.2

Ζητούμενο 2 - Testing

Αφού κάνουμε την παραμετροποίηση του StrongSwan Server, θα πρέπει να τεστάρουμε τον σέρβερ να δούμε αν λειτουργεί. Δοκιμάσαμε σε 1 συσκευή με Android OS .

Android OS

3:12 PM

dnsleaktest.com/results.html

Status: Connected
Profile: 192.168.1.155

DISCONNECT

192.168.1.155
Server: 192.168.1.155
Username: icsd18107

Test complete

Query round	Progress...	Servers found
1	0
2	0
3	0
4	0
5	0
6	0

#	Hostname	IP	Country
02.235.71.83	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.84	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.85	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.86	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.87	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.88	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.89	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.90	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.91	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.92	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.93	resolver01.cloudflare.com	Cloudflare	Greece
02.235.71.94	resolver01.cloudflare.com	Cloudflare	Greece

What do the results of this test mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address everytime you enter a website address in your browser.
- The owners of the servers above have the ability to associate your personal IP address with the names of all the sites you connect to and store this data indefinitely. This does not mean that they do log or store it indefinitely **but they may and you need to trust whatever their policy says.**
- If you are connected to a VPN service and ANY of the servers listed above are not provided by the VPN service then you have a DNS leak and are choosing to trust the owners of the above servers with your private data.

Dnsleaktest.com is proudly brought to you by [VPN](#), an open-source, audited, no BS, no logs, VPN provider run by privacyv

3:04 PM

dnsleaktest.com/results.html

Status: Connected
Profile: 192.168.1.155

DISCONNECT

192.168.1.155
Server: 192.168.1.155
Username: icsd18107

Test complete

#	Hostname	IP	Country
172.237.33.102	None	Google	Frankfurt am Main, Germany
172.237.33.199	None	Google	Frankfurt am Main, Germany
172.237.33.197	None	Google	Frankfurt am Main, Germany
172.237.33.198	None	Google	Frankfurt am Main, Germany
172.237.33.194	None	Google	Frankfurt am Main, Germany
172.237.33.195	None	Google	Frankfurt am Main, Germany
172.237.33.196	None	Google	Frankfurt am Main, Germany
172.237.33.197	None	Google	Frankfurt am Main, Germany
172.237.33.198	None	Google	Frankfurt am Main, Germany
172.237.33.199	None	Google	Frankfurt am Main, Germany
172.237.33.190	None	Google	Frankfurt am Main, Germany
172.237.45.131	None	Google	Frankfurt am Main, Germany
172.237.45.130	None	Google	Frankfurt am Main, Germany
172.237.45.190	None	Google	Frankfurt am Main, Germany
172.237.45.191	None	Google	Frankfurt am Main, Germany
172.237.45.192	None	Google	Frankfurt am Main, Germany
172.237.45.193	None	Google	Frankfurt am Main, Germany
172.237.45.194	None	Google	Frankfurt am Main, Germany
172.237.45.195	None	Google	Frankfurt am Main, Germany
172.237.45.196	None	Google	Frankfurt am Main, Germany
172.237.45.197	None	Google	Frankfurt am Main, Germany
172.237.45.198	None	Google	Frankfurt am Main, Germany
172.237.45.199	None	Google	Frankfurt am Main, Germany
172.237.45.195	None	Google	Frankfurt am Main, Germany
172.237.18.199	None	Google	Frankfurt am Main, Germany
172.235.187.1	None	Google	Frankfurt am Main, Germany
172.235.187.2	None	Google	Frankfurt am Main, Germany
172.235.187.3	None	Google	Frankfurt am Main, Germany
172.235.189.9	None	Google	Frankfurt am Main, Germany
172.235.190.4	None	Google	Frankfurt am Main, Germany
172.235.190.5	None	Google	Frankfurt am Main, Germany
172.235.235.30	None	Google	Frankfurt am Main, Germany
172.235.235.35	None	Google	Frankfurt am Main, Germany
192.130.187.102	None	Google	Frankfurt am Main, Germany

What do the results of this test mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address everytime

Πριν δουλέψει το VPN, μεταφέραμε το αρχείο ca-cert.pem στο κινητό τηλέφωνο, το εισαγάγαμε στην εφαρμογή του StrongSwan, βάλαμε τα διεπιστευτήρια χρήστη και δοκιμάσαμε να συνδεθούμε στο VPN.

Στο ΜΕΣΑΙΟ στιγμιότυπο που φαίνεται πιο πάνω παρατηρούμε ότι το κινητό τηλέφωνο συνδέεται επιτυχώς στον σέρβερ.

ΠΡΙΝ την ενεργοποίηση (ΑΡΙΣΤΕΡΟ ΣΤΙΓΜΙΟΤΥΠΟ) παρατηρούμε ότι οι DNS Servers που επικοινωνεί το κινητό είναι οι σερβερς της Cosmote. Αυτό σημαίνει ότι η Cosmote μπορεί να διαβάσει την περιήγησή μας στο διαδίκτυο.

ΜΕΤΑ την ενεργοποίηση (ΔΕΞΙ ΣΤΙΓΜΙΟΤΥΠΟ) παρατηρούμε ότι οι DNS Servers που επικοινωνεί το κινητό είναι οι σερβερς της Google που εδρεύουν στην Γερμανία. Αυτό σημαίνει ότι η Cosmote δεν μπορεί να διαβάσει την περιήγησή μας στο διαδίκτυο.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 4

Σύγκριση

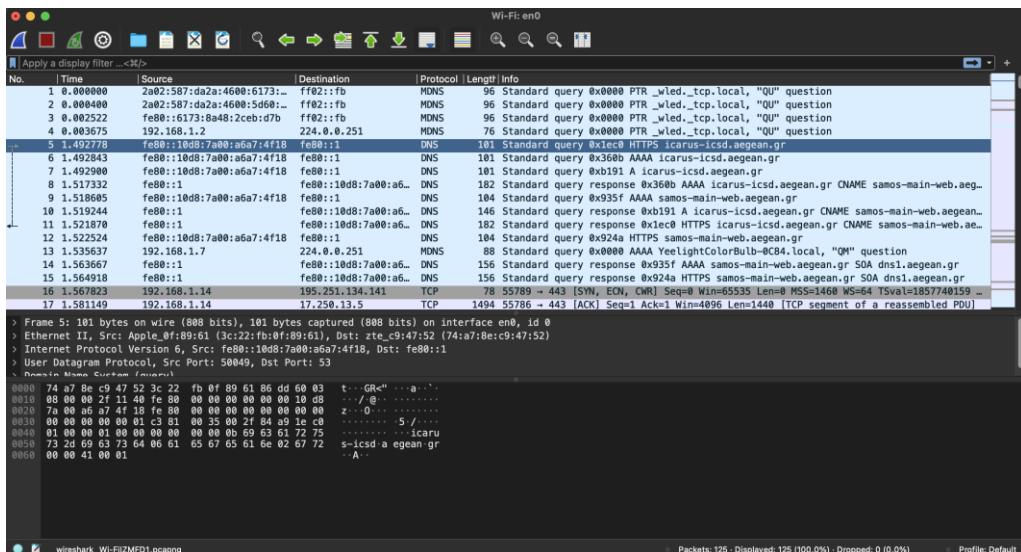


ΚΕΦΑΛΑΙΟ 4^[6]

Σύγκριση

Αφού τελειώσαμε και τα δύο ζητούμενα και έχουμε δοκιμάσει ότι όλα λειτουργούν επιτυχώς, πρέπει να συγκρίνουμε τα δύο αυτά VPNs. Όλοι οι έλεγχοι θα γίνουν πάνω σε μηχάνημα που θα έχει πρόσβαση και στα δύο VPNs. Συγκεκριμένα οι έλεγχοι θα γίνουν πάνω στο λάπτοπ MacBook Pro με Mac OS και με την χρήση της εφαρμογής Wireshark.

ΠΡΙΝ ΤΗΝ ΕΝΕΡΓΟΠΟΙΗΣΗ ΟΠΟΙΟΥΔΗΠΟΤΕ VPN

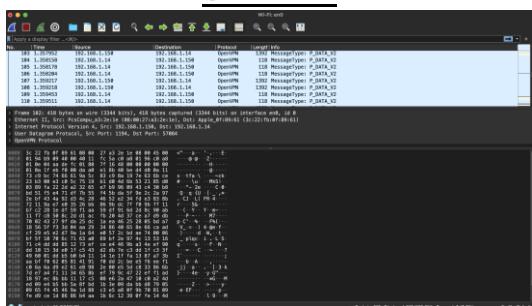


Στο παραπάνω στιγμιότυπο που δεν υπάρχει ενεργοποιημένο κάποιο VPN παρατηρούμε ότι χρησιμοποιείται το πρωτόκολλο DNS μέσω της Cosmote προκειμένου να μπούμε στην σελίδα icarus-icsd.aegean.gr. Μας δίνει, επιπλέον, πληροφορίες για τα πακέτα που ανταλλάσσονται προκειμένου να επιτευχθεί η σύνδεση μας στην ιστοσελίδα καθώς και το URL της. Γενικά οι πληροφορίες είναι εύκολα προσβάσιμες από όποιον τρέχει το Wireshark εκείνη την στιγμή.

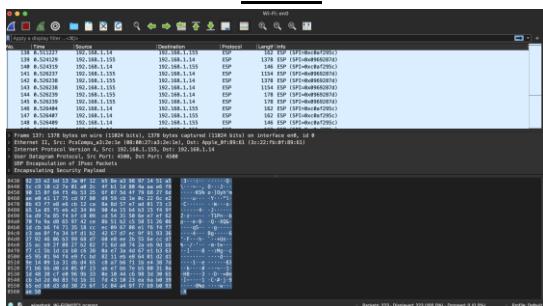


ΕΝΕΡΓΟΠΟΙΗΣΗ VPN

OPENVPN



IPSEC



Στο ΑΡΙΣΤΕΡΟ στιγμιότυπο παρατηρούμε ότι όλες οι πληροφορίες σχετικά με το URL της ιστοσελίδας icarus-icsd.aegean.gr δεν υπάρχουν. Επίσης το πρωτόκολλο έχει αλλάξει σε αυτό που προσφέρει το OpenVPN (UDP). Επιπλέον οι πληροφορίες σχετικά με τα πακέτα που ανταλλάσσονται ανάμεσα στην ιστοσελίδα και τον υπολογιστή μας, δεν υπάρχουν πλέον. Σε σύγκριση με το στιγμιότυπο που δεν είχαμε ενεργοποιήσει το VPN παρατηρούμε ότι αποστέλλονται και εμφανίζονται περισσότερα πακέτα (όχι VPN: 125 πακέτα, με VPN: 217 πακέτα). Επιπρόσθετα έχουν αλλάξει οι θύρες επικοινωνίας. Τα πακέτα προωθούνται από την θύρα 1194 σε αντίθεση με το απενεργοποιημένο VPN που προωθούνται στην θύρα 53 (κλασική DNS θύρα). Τέλος όλα τα πακέτα στέλνονται στον VPN σέρβερ και μετά από εκεί φεύγουν για την ιστοσελίδα σε αντίθεση με το απενεργοποιημένο VPN που στέλνονται στους DNS Servers της Cosmote.

Στο ΔΕΞΙ στιγμιότυπο, σε σύγκριση με το ΑΡΙΣΤΕΡΟ, παρατηρούμε ότι έχει μειωμένο χρόνο αποστολής και λήψης πακέτων (μόλις 0,5 δευτερόλεπτα σε σύγκριση με 1,358 του OpenVPN). Επίσης το πρωτόκολλο έχει αλλάξει σε ESP (Encapsulating Security Payload (UDP)). Επιπλέον παρατηρούμε ότι αποστέλλονται και εμφανίζονται περισσότερα πακέτα (OpenVPN: 217 πακέτα, IPsec: 223 πακέτα). Η θύρα που προωθούνται τα πακέτα είναι η 4500. Επιπρόσθετα παρατηρείται ότι το IPsec λαμβάνει και στέλνει περισσότερα bytes σε αντίθεση με το OpenVPN (OpenVPN: 418 bytes, IPsec: 1378 bytes).



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

Πίνακας Σύγκρισης OpenVPN και IPSec

ΛΕΙΤΟΥΡΓΙΑ	IPSec	OpenVPN
Εύκολος Αποκλεισμός	Ναι	Όχι
Συμβατότητα	Ενσωματωμένη υποστήριξη για μεγάλη ποικιλία λειτουργικών συστημάτων και συσκευών	Χωρίς ενσωματωμένη υποστήριξη
Κρυπτογράφηση	Έως 256-bit	Έως 256-bit
Χρήση	μέσω OS/συσκευής built-in client ή εγγενούς εφαρμογής VPN από τον πάροχο VPN	μέσω third-party εφαρμογής ή εγγενούς εφαρμογής VPN από πάροχο VPN
Ταχύτητα	Γενικά γρήγορες ταχύτητες	Το OpenVPN μέσω UDP προσφέρει καλύτερες ταχύτητες από το OpenVPN μέσω TCP
Σταθερότητα	Σταθερό	Πολύ σταθερό σε όλα τα δίκτυα
Υποστηριζόμενες Συσκευές (ΛΣ)	Windows, Mac, iOS, Android, Linux, Solaris, FreeBSD, OpenBSD, κ.α.	Windows, Mac, iOS, Android, Linux, Solaris, FreeBSD, OpenBSD, κ.α.
Ευπάθειες Ασφαλείας	Έχει τη δυνατότητα να παραβιαστεί από το NSA	Δεν υπάρχουν γνωστά τρωτά σημεία ασφαλείας
Κατάλληλο για	Μέτριοι χρήστες του Διαδικτύου	Καθημερινή χρήση, όπου η ασφάλεια και η ταχύτητα είναι απαραίτητες



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

Πλεονεκτήματα IPSec

- ✓ Οι ταχύτητες είναι γενικά πιο γρήγορες από το OpenVPN από πολλές απόψεις, αλλά εξαρτώνται επίσης από άλλες μεταβλητές όπως οι προδιαγραφές της συσκευής, η προβλεπόμενη χρήση κ.λπ.
- ✓ Ισχυρή ασφάλεια, με την προϋπόθεση ότι έχει ρυθμιστεί σωστά. Το IPSec υποστηρίζει μια ποικιλία αλγορίθμων και κρυπτογράφησης όπως HMAC-SHA1/SHA2, RSA, PSK, ECDH, AES-CTR και AES-CBC.
- ✓ Δεν απαιτεί εφαρμογή τρίτου κατασκευαστή για να ξεκινήσει και να λειτουργεί, καθώς πολλά λειτουργικά συστήματα επιτραπέζιων υπολογιστών και κινητών την υποστηρίζουν εγγενώς.

Μειονεκτήματα IPSec

- Η διαδικασία εγκατάστασης μπορεί να είναι περίπλοκη με βάση το τι σκοπεύετε να το χρησιμοποιήσετε. Ωστόσο, οι μέσοι χρήστες που προσπαθούν να συνδεθούν με τους διακομιστές της υπηρεσίας VPN τους δεν θα πρέπει να αντιμετωπίσουν κανένα πρόβλημα.
- Εικάζεται ότι η Υπηρεσία Εθνικής Ασφάλειας (NSA) εργάζεται ενεργά για να εισαγάγει τρωτά σημεία στο IPSec, κάτι που αν ισχύει, σας αφήνει ευάλωτους στη στοχευμένη παρακολούθηση.

Πλεονεκτήματα OpenVPN

- ✓ Είναι πολύ δύσκολο να αποκλειστεί καθώς το OpenVPN μπορεί να ρυθμιστεί ώστε να εκτελείται σε οποιαδήποτε θύρα χρησιμοποιώντας TCP και UDP, επιτρέποντάς σας να το αποκρύψετε εύκολα ως κίνηση HTTPS.
- ✓ Αξιόπιστη ασφάλεια καθώς χρησιμοποιεί το OpenSSL, το οποίο υποστηρίζει μια ποικιλία κρυπτογράφησης και αλγορίθμων όπως ChaCha20, AES, Camellia και Blowfish.
- ✓ Μεγάλη σταθερότητα όσον αφορά την περιαγωγή μέσω Wi-Fi και δικτύων κινητής τηλεφωνίας, καθώς και εκείνων όπου η συμφόρηση και η απώλεια πακέτων είναι συνήθης.

Μειονεκτήματα OpenVPN

- Η μη αυτόματη ρύθμιση παραμέτρων μπορεί να είναι μια μπερδεμένη και περίπλοκη διαδικασία, ειδικά για τους first-time χρήστες του OpenVPN.
- Το πρωτόκολλο δεν είναι πολύ ελαφρύ, επομένως ενδέχεται να αντιμετωπίσετε προβλήματα με τις ταχύτητες σύνδεσης. Εάν το χρησιμοποιείτε μέσω TCP, η εναλλαγή σε UDP βοηθά.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

Συμπέρασμα

Το IPSec θα πρέπει να χρησιμοποιείται μόνο εάν έχει ρυθμιστεί από κάποιον που ξέρει πώς να το κάνει σωστά. Προσφέρει αρκετά γρήγορες ταχύτητες και ασφάλεια συγκρίσιμης με το OpenVPN, αν και το πρωτόκολλο φέρεται να έχει αποδυναμωθεί από την NSA.

Το OpenVPN είναι το καλύτερο ολοκληρωμένο VPN, καθιστώντας το ιδανική επιλογή για τους περισσότερους χρήστες. Ενώ συχνά απαιτεί έναν πελάτη τρίτου μέρους, πολλοί πάροχοι VPN ενσωματώνουν το πρωτόκολλο απευθείας στις εφαρμογές τους, έτσι ώστε η χρήση του να είναι απρόσκοπτη.



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 5

Βιβλιογραφία



321-9703– Ασφάλεια Δικτύων και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Τίτλος Μελέτης: Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

ΚΕΦΑΛΑΙΟ 5

Βιβλιογραφία

[1]: <https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-20-04>

[2]: <https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-a-certificate-authority-ca-on-ubuntu-20-04>

[3]: <https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-ubuntu-20-04>

[4]: <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-ikev2-vpn-server-with-strongswan-on-ubuntu-20-04>

[5]: <https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-20-04/>

[6]: <https://www.purevpn.com/blog/ipsec-vs-openvpn/>

[7]: <https://openvpn.net/community-resources/setting-up-your-own-certificate-authority-ca/>

[8]: <https://www.ciscopress.com/articles/article.asp?p=421514&seqNum=4>

ΠΕΡΑΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ



Kyriazis Ioannis | Papadopoulos Panagiotis

Copyright © 2021 – All Rights Reserved