Securi-Pi: Raspberry Pi használata biztonságos végpontként

Linux Journal – 2015. december 09. Szerző: Bill Childers

http://www.linuxjournal.com/content/securi-pi-using-raspberry-pi-secure-landing-point

Mint sok Linux Journal olvasó napjainkban, én is egy kissé techno-nomád életstílusra tértem át az elmúlt néhány év alatt – hálózatról hálózatra, csatlakozási pontról csatlakozási pontra ugrálva, ahogy a világban ide-oda vándorolva fenntartom az Internet, és más, naponta használt hálózatom elérését. Újabban azt vettem észre, hogy egyre több és több hálózat kezdi blokkolni az SMTP-hez (25-ös port), SSH-hoz (22-es port) használt és hasonló külső portokat. Nagyon zavaró lehet, amikor betérsz egy internetes kávézóba arra számítva, hogy elindíthatod a SSH-kliensedet és elvégezhetsz néhány dolgot, de nem tudod, mert a hálózat blokkol téged.

Emellett át kell jutnom olyan hálózaton, ami blokkolja a HTTPS elérést (443-as port). Egy kicsit vacakolva otthon a Raspberry Pi 2-mmel, képes voltam egy szép, tiszta megoldást találni, amivel különféle szolgáltatásokat indíthattam el a Raspberry Pi 443-as portján keresztül – lehetővé téve számomra a blokkolt portok és korlátozott hálózatok megkerülését, ami által el tudom végezni a szükséges dolgokat. Dióhéjban, úgy állítottam be a Raspberry pi-t, hogy OpenVPN és SSH végpontként, illetve Apache szerverként működjön – mindegyik a 443-as porton figyelve, ami által a hálózati korlátozások nem akadályoznak.

Megjegyzések:

Ez a megoldás a legtöbb hálózat esetében működik, de az olyan tűzfalak, amik a kimenő forgalomra mélyreható csomagellenőrzést végeznek, esetleg blokkolhatják az ilyen módon csatornázott forgalmat. Ugyanakkor én még nem találkoztam ilyen rendszerrel ... egyelőre. Emellett, noha több titkosítás alapú megoldás alkalmazok itt (OpenVPN, HTTPS, SSH), ebben az felállásban nem alkalmaztam szigorú biztonsági ellenőrzést. Például a DNS-en keresztül lehet információszivárgás, és még lehetnek olyan dolgok, amikre még nem gondoltam. Nem ajánlom ezt arra a célra, hogy elrejtsd a forgalmadat – én csak arra használom, hogy az Internetre szabadon csatlakozhassak, amikor távol vagyok.

Kezdeti lépések

Kezdjük azzal, hogy mire van szükség, hogy ezt összehozd. Én otthon egy Raspberry Pi 2-ön használom ezt, a legfrissebb Raspbian-t futtatva, de ennek jól kell működnie Raspberry Pi B modellen is. Könnyen ráfér egy 512 MB-s RAM-ra, ugyanakkor, a futása egy kicsit lassabb lehet, mivel a Raspberry Pi B modell egymagos CPU-val bír, ellentétben a Pi 2-vel

ami négymagos. A Raspberry Pi 2-öm az otthoni router-em, tűzfalam mögött ül, ennek köszönhetően további előny, hogy a gépeimet otthon is elérem. Ez azt is jelenti, hogy a teljes Internetre küldött forgalom láthatóan az otthoni router-em IP-céméről érkezik, vagyis nem alkalmas a névtelenség megőrzésére. Ha nincs Raspberry Pi-d, vagy ezt nem akarod otthonról futtatni, ez teljes egészében futtatható egy kisebb felhő szerverről is. Csak arra vigyázz, hogy a szerveren Debian, vagy Ubuntu fusson, mivel ezek az utasítások Debian-alapú disztribúciót céloznak meg.

1. kép A Raspberry Pi készen arra, hogy titkosított hálózati végpont legyen.

A BIND telepítése és beállítása

Amikor a platform kész és fut – lett légyen az Raspberry Pi, vagy más – következőkben a BIND-ot kell telepítened, a névkiszolgálót, ami nagymértékben kihasználja az Internetet. A BIND-ot csak gyorsítótárazó névkiszolgálóként telepíted és nem szolgál ki Internetről érkező kéréseket. A BIND telepítve ad egy olyan névkiszolgálót, amire az OpenVPN kliensek mutathatnak, amikor az OpenVPN-es lépéshez érünk. A BIND telepítése könnyű, csak az apt-get parancs kell hozzá:

```
root@test:~# apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

```
The following extra packages will be installed:
    bind9utils
Suggested packages:
    bind9-doc resolvconf ufw
The following NEW packages will be installed:
    bind9 bind9utils
0 upgraded, 2 newly installed, 0 to remove and
  ↪0 not upgraded.
Need to get 490 kB of archives.
After this operation, 1,128 kB of additional disk
  ↪space will be used.
Do you want to continue [Y/n]? y
```

Mielőtt a BIND képes lenne gyorsítótárazó névkiszolgálóként működni, két apró módosítást kell elvégezni az egyik beállító fájlon. Mindkét változtatás az /etc/bind/named.conf.options-ban történik. Először megjegyzésből ki kell venni a fájl „forwarders” szakaszát és meg kell adni egy névkiszolgálót az Interneten, amihez a kéréseket továbbítja. Ez esetben a Google DNS-ét (8.8.8.8) adom hozzá. A fájl „forwarders” része így kell, hogy kinézzen:

```
forwarders {
   8.8.8.8;
};
```

A második változtatás, amit végrehajtunk, engedélyezi a lekérdezést a belső hálózatról és a localhost-ról. Egyszerűen add ezt a sort a konfigurációs fájl végéhez a fájlt lezáró } elé közvetlenül:

```
allow-query { 192.168.1.0/24; 127.0.0.0/16; };
```

A fenti sor lehetővé teszi ennek a névkiszolgálónak a lekérdezését a saját hálózatáról (ebben az esetben az én hálózatom a tűzfal mögül) és a localhost-ról. Ezután egyszerűen csak újra kell indítani a BIND-ot:

```
root@test:~# /etc/init.d/bind9 restart
[....] Stopping domain name service...: bind9waiting
  ↪for pid 13209 to die
. ok
[ ok ] Starting domain name service...: bind9.
```

Most teszteld az nslookup -ot, hogy meggyőződj a szerver működéséről:

```
root@test:~# nslookup
> server localhost
Default server: localhost
Address: 127.0.0.1#53
> www.google.com
Server:         localhost
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 173.194.33.176
Name:   www.google.com
Address: 173.194.33.177
Name:   www.google.com
Address: 173.194.33.178
Name:   www.google.com
Address: 173.194.33.179
Name:   www.google.com
Address: 173.194.33.180
```

Ez az! Van már működő névkiszolgáló a gépen. Most térjünk át az OpenVPN-re.

OpenVPN telepítése és beállítása

Az OpenVPN egy nyílt forráskódú VPN megoldás, ami SSL/TLS-re támaszkodik kulcsváltás tekintetében. Linux alatt telepíteni és működésre bírni szintén egyszerű. Az OpenVPN beállítása egy kicsit szörnyű, de nem térünk el túlságosan az alap beállításoktól. Indításként futtass egy apt-get parancsot és telepítsd az OpenVPN-t:

```
root@test:~# apt-get install openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
   liblzo2-2 libpkcs11-helper1
```

```
Suggested packages:
    resolvconf
The following NEW packages will be installed:
    liblzo2-2 libpkcs11-helper1 openvpn
0 upgraded, 3 newly installed, 0 to remove and
  ↪0 not upgraded.
Need to get 621 kB of archives.
After this operation, 1,489 kB of additional disk
  ↪space will be used.
Do you want to continue [Y/n]? y
```

Most, hogy az OpenVPN települt, be kell állítani. Az OpenVPN SSL-alapú és a futásához mind szerver, mind kliens oldalon tanúsítvány szükséges. Ezen tanúsítványok létrehozásához be kell állítani a Certificate Authority-t (CA) a gépen. Szerencsére az OpenVPN rendelkezik néhány, „easy-rsa”-ként ismert csomagoló szkripttel, ami segít a folyamat végrehajtásában. Előbb létre kell hozni egy könyvtárat a fájlrendszerben az easy-rsa szkript elhelyezésére és másold a sablon (template) könyvtárból a szkripteket oda:

```
root@test:~# mkdir /etc/openvpn/easy-rsa
root@test:~# cp -rpv
  ↪/usr/share/doc/openvpn/examples/easy-rsa/2.0/*
  ↪/etc/openvpn/easy-rsa/
```

Ezután a vars fájlról készíts mentést:

```
root@test:/etc/openvpn/easy-rsa# cp vars vars.bak
```

Most szerkeszd a vars-t, hogy a rendszerednek megfelelő információkat tartalmazza. Csak azokat a sorokat mutatom példa adatokkal, amiket szerkeszteni kell:

```
KEY_SIZE=4096
KEY_COUNTRY="US"
KEY_PROVINCE="CA"
KEY_CITY="Silicon Valley"
KEY_ORG="Linux Journal"
KEY_EMAIL="bill.childers@linuxjournal.com"
```

A következő lépés a vars fájl felhasználása, hogy a fájl környezeti változói az aktuális

környezeti váltózóba kerüljenek:

```
root@test:/etc/openvpn/easy-rsa# source ./vars
NOTE: If you run ./clean-all, I will be doing a
  ↪rm -rf on /etc/openvpn/easy-rsa/keys
```

A Certificate Authority elkészítése

Most a környezeti változó kitisztításhoz a clean-all futtatása kell, majd felépítjük a CA-t. Vedd észre, hogy a changeme (változtass meg) prompt-ot a rendszer szempontjából megfelelőre változtatom:

	Az üzenetek tartalma:
root@test:/etc/openvpn/easy-rsa# ./clean-all	
root@test:/etc/openvpn/easy-rsa# ./build-ca	
Generating a 4096 bit RSA private key	4096 bites RSA személyes kulcs készítése
.....++	
.....++	
writing new private key to 'ca.key'	Az új személyes kulcs ca.key-be írása
-----	
You are about to be asked to enter information that	Rákérdez néhány információra, amit a hitelesítő kérésedbe beépít.
will be incorporated into your certificate request.	
What you are about to enter is what is called a	Amit be kell vinned, azt Distinguished Name-nek (azonosító/megkülönböztető név), vagy DN-nek hívják.
Distinguished Name or a DN.	
There are quite a few fields but you can leave some	Sok mező van, de párat üresen lehet hagyni. Némely alapértékkel rendelkezik. Ha „.”-t írsz be, akkor az üresen marad.
blank. For some fields there will be a default value,	
If you enter '.', the field will be left blank.	

Country Name (2 letter code) [US]:	Országnév (2 betű kód) [US]
State or Province Name (full name) [CA]:	Állam, vagy tartomány [CA]
Locality Name (eg, city) [Silicon Valley]:	Helységnév (pl. város) [Silicon Valley]
Organization Name (eg, company) [Linux Journal]:	Szervezet neve: ...
Organizational Unit Name (eg, section)	Szervezeti egység neve: …
↪[changeme]:SecTeam	
Common Name (eg, your name or your server's hostna	Közös név (pl. saját neved, vagy a szervered host name-je): ...
↪[changeme]:test.linuxjournal.com	
Name [changeme]:test.linuxjournal.com	Név (változtass meg): …
Email Address [bill.childers@linuxjournal.com]:	Email-cím: ...

A szerver tanúsítvány elkészítése

Mihelyst a CA elkészült, fel kell építeni az OpenVPN szerver tanúsítványát:

```
root@test:/etc/openvpn/easy-rsa#
  ↪./build-key-server test.linuxjournal.com
Generating a 4096 bit RSA private key
.....................................................++
writing new private key to 'test.linuxjournal.com.key'
-----
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.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [Silicon Valley]:
Organization Name (eg, company) [Linux Journal]:
Organizational Unit Name (eg, section)
  ↪[changeme]:SecTeam
Common Name (eg, your name or your server's hostname)
  ↪[test.linuxjournal.com]:
Name [changeme]:test.linuxjournal.com
Email Address [bill.childers@linuxjournal.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from
  ↪/etc/openvpn/easy-rsa/openssl-1.0.0.cnf
```

A CA résznél leírtakon túli információk:

Add meg a tanúsítványkéréseddel megküldendő további extra attribútumokat

Elvárt jelszó (?): …
Opcionális szervezeti név: …

A használt konfigurációs fájl /etc/openvpn/easy-rsa/openssl-1.0.0.cnf

```
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'Silicon Valley'
organizationName      :PRINTABLE:'Linux Journal'
organizationalUnitName:PRINTABLE:'SecTeam'
commonName            :PRINTABLE:'test.linuxjournal.com'
name                  :PRINTABLE:'test.linuxjournal.com'
emailAddress
  ↪:IA5STRING:'bill.childers@linuxjournal.com'
Certificate is to be certified until Sep  1
  ↪06:23:59 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

```
Ellenőrizd a kérés aláírását
Aláírás oké
A cél Distinguished Name-je (?)
a következő

.... KIÍRANDÓ ... „US”
.....
..... stb.

A tanúsítványt szeptember 1-
jéig kell tanúsítani.
...

A tanúsítványt aláírja?

1-ből 1 tanúsítványkérés
tanúsítva, alkalmazza? ...
Adatbázis kiírása egy új tétellel
Adatbázis frissítve
```

A következő lépés, az OpenVPN számára a Diffie-Hellman kulcs elkészítése hosszabb ideig tarthat. Hagyományos asztali gépszintű CPU-n néhány perc, de a Raspberry Pi ARM processzora számára ez sokkal tovább tarthat. Nyugalom, amíg a terminálon a pontok haladnak, a rendszer építi a Diffie-Hellman kulcsot (megjegyzem, a példámban számos pontot kihagytam).

```
root@test:/etc/openvpn/easy-rsa# ./build-dh
Generating DH parameters, 4096 bit long safe prime,
  ↪generator 2
This is going to take a long time
.....+
<snipped out many more dots>
```

Kliens tanúsítvány elkészítése

Most generálunk egy kliens tanúsítványt, amit az OpenVPN-re bejelentkezésre kell használni. Az OpenVPN jellemzően tanúsítvány alapú azonosításra van beállítva, ahol a

kliens bemutatja a tanúsítványt, amit egy jóváhagyott Certificate Authority adott ki (Ford: a tanúsítvány készítése során a korábban már megismert folyamat zajlik le, és a kérdések, megadandó információk ugyanazok, mint a CA elkészítésekor.):

```
root@test:/etc/openvpn/easy-rsa# ./build-key
  ↪bills-computer
Generating a 4096 bit RSA private key
.....................................................++
.....................................................++
writing new private key to 'bills-computer.key'
-----
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.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [Silicon Valley]:
Organization Name (eg, company) [Linux Journal]:
Organizational Unit Name (eg, section)
  ↪[changeme]:SecTeam
Common Name (eg, your name or your server's hostname)
  ↪[bills-computer]:
Name [changeme]:bills-computer
Email Address [bill.childers@linuxjournal.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from
```

```
  ↪/etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'Silicon Valley'
organizationName      :PRINTABLE:'Linux Journal'
organizationalUnitName:PRINTABLE:'SecTeam'
commonName            :PRINTABLE:'bills-computer'
name                  :PRINTABLE:'bills-computer'
emailAddress
  ↪:IA5STRING:'bill.childers@linuxjournal.com'
Certificate is to be certified until
  ↪Sep  1 07:35:07 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified,
  ↪commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@test:/etc/openvpn/easy-rsa#
```

Most létrehozunk egy HMCA kódot megosztott kulcsként, hogy tovább fokozzuk a rendszer biztonságát:

```
root@test:~# openvpn --genkey --secret
  ↪/etc/openvpn/easy-rsa/keys/ta.key
```

A szerver konfigurálása

Végül eljutunk a lényeghez, az OpenVPN szerver beállításához. Készíteni kell egy új fájlt, a „/etc/openvpn/server.conf”-ot, aminek a nagyobb részében az alapbeállításokat meghagyjuk. A leglényegesebb változtatás, amit eszközölünk, hogy az OpenVPN-t UDP helyett TCP használatára állítjuk be. Erre szükség van ahhoz, hogy a következő jelentősebb

lépés működjön – az OpenVPN használata internetes kommunikációra TCP nélkül nem képes a 443-as portot beüzemelni. Tehát készítsünk egy /etc/openvpn/server.conf nevű fájlt a következő beállítással benne:

```
port 1194
proto tcp
dev tun
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/test.linuxjournal.com.crt ## or whatever
  ↪your hostname was
key easy-rsa/keys/test.linuxjournal.com.key  ## Hostname key
  ↪- This file should be kept secret
management localhost 7505
dh easy-rsa/keys/dh4096.pem
tls-auth /etc/openvpn/certs/ta.key 0
server 10.8.0.0 255.255.255.0 # The server will use this
  ↪subnet for clients connecting to it
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp" # Forces clients
  ↪to redirect all traffic through the VPN
push "dhcp-option DNS 192.168.1.1" # Tells the client to
  ↪use the DNS server at 192.168.1.1 for DNS -
  ↪replace with the IP address of the OpenVPN
  ↪machine and clients will use the BIND
  ↪server setup earlier
keepalive 30 240
comp-lzo # Enable compression
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Végül engedélyezzük a szerveren az IP forwarding-ot, úgy beállítva az OpenVPN-t, hogy a rendszer betöltésekor induljon és induljon el az OpenVPN szolgáltatás:

```
root@test:/etc/openvpn/easy-rsa/keys# echo
  ↪"net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
```

```
root@test:/etc/openvpn/easy-rsa/keys# sysctl -p
  ↪/etc/sysctl.conf
net.core.wmem_max = 12582912
net.core.rmem_max = 12582912
net.ipv4.tcp_rmem = 10240 87380 12582912
net.ipv4.tcp_wmem = 10240 87380 12582912
net.core.wmem_max = 12582912
net.core.rmem_max = 12582912
net.ipv4.tcp_rmem = 10240 87380 12582912
net.ipv4.tcp_wmem = 10240 87380 12582912
net.core.wmem_max = 12582912
net.core.rmem_max = 12582912
net.ipv4.tcp_rmem = 10240 87380 12582912
net.ipv4.tcp_wmem = 10240 87380 12582912
net.ipv4.ip_forward = 0
net.ipv4.ip_forward = 1

root@test:/etc/openvpn/easy-rsa/keys# update-rc.d
  ↪openvpn defaults
update-rc.d: using dependency based boot sequencing

root@test:/etc/openvpn/easy-rsa/keys#
  ↪/etc/init.d/openvpn start
[ ok ] Starting virtual private network daemon:.
```

OpenVPN kliensek létrehozása

A kliens telepítése függ az alkalmazott op. rendszertől, ám a kliens tanúsítványát és kulcsát, amit korábban hoztunk létre, be kell másolni, és importálnod kell azokat a tanúsítványokat, valamint létrehozni az adott kliens beállításait. Minden kliens és kliens op. rendszer egy kicsit más, ezek dokumentálása meghaladja a cikk tárgyát, azaz az adott kliens futtatásához tanulmányozd a dokumentációját. Források részben a fontosabb op. rendszerek OpenVPN klienseinek leírásában megtalálható.

SSLH telepítése — a „mágikus” Protocol Multiplexer

A megoldás valóban izgalmas része az SSLH. Az SSLH egy protokoll többszöröző – a 443-

as porton figyeli a forgalmat és képes azonosítani, hogy egy bejövő csomag SSH, HTTP, vagy OpenVPN csomag-e, illetve képes a csomagot továbbítani a megfelelő szolgáltatás felé. Ez az, ami lehetővé teszi a megoldás számára a legtöbb port-blokkolás átlépését – a HTTPS portot használod a teljes forgalom számra, mivel azt a legritkábban blokkolják.

Indításként apt-get install SSLH

```
root@test:/etc/openvpn/easy-rsa/keys# apt-get
  ↪install sslh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
    apache2 apache2-mpm-worker apache2-utils
      ↪apache2.2-bin apache2.2-common
    libapr1 libaprutil1 libaprutil1-dbd-sqlite3
      ↪libaprutil1-ldap libconfig9
Suggested packages:
    apache2-doc apache2-suexec apache2-suexec-custom
      ↪openbsd-inetd inet-superserver
The following NEW packages will be installed:
    apache2 apache2-mpm-worker apache2-utils
      ↪apache2.2-bin apache2.2-common
    libapr1 libaprutil1 libaprutil1-dbd-sqlite3
      ↪libaprutil1-ldap libconfig9 sslh
0 upgraded, 11 newly installed, 0 to remove
  ↪and 0 not upgraded.
Need to get 1,568 kB of archives.
After this operation, 5,822 kB of additional
  ↪disk space will be used.
Do you want to continue [Y/n]? y
```

Az SSLH telepítését követően a csomagtelepítő meg fogja kérdezni, hogy inetd-ben, vagy önálló módban akarod-e futtatni. Válaszd az önálló módot, mivel az SSLH-t saját folyamatként kell futtatni. Ha nincs Apache telepítve, akkor a Debian (Rapbian) SSLH csomag automatikusan behúzza, noha arra nincs feltétlen szükség. Ha már van futó és beállított Apache-od, akkor győződj meg arról, hogy kizárólag a localhost interfészen hallgatózik-e és

nem az összes interfészen (ellenkező esetben az SSLH nem tud elindulni, mert nem köthető a 443-as porthoz). Telepítés után egy ilyen hibaüzenetet kapsz:

```
[....] Starting ssl/ssh multiplexer: sslhsslh disabled,
  ↪please adjust the configuration to your needs
[FAIL] and then set RUN to 'yes' in /etc/default/sslh
  ↪to enable it. ... failed!
Failed!
```

Ez valójában nem hiba – az SSLH közli, hogy nincs beállítva és nem tud elindulni. Az SSLH beállítása elég egyszerű. A beállításokat a /etc/default/sslh tartalmazza és csak a RUN és a DAEMON_OPTS változókat kell beállítani. Az én SSLH beállításom így néz ki:

```
# Default options for sslh initscript
# sourced by /etc/init.d/sslh

# Disabled by default, to force yourself
# to read the configuration:
# - /usr/share/doc/sslh/README.Debian (quick start)
# - /usr/share/doc/sslh/README, at "Configuration" section
# - sslh(8) via "man sslh" for more configuration details.
# Once configuration ready, you *must* set RUN to yes here
# and try to start sslh (standalone mode only)

RUN=yes

# binary to use: forked (sslh) or single-thread
  ↪(sslh-select) version
DAEMON=/usr/sbin/sslh

DAEMON_OPTS="--user sslh --listen 0.0.0.0:443 --ssh
  ↪127.0.0.1:22 --ssl 127.0.0.1:443 --openvpn
  ↪127.0.0.1:1194 --pidfile /var/run/sslh/sslh.pid"
```

Save the file and start SSLH:

```
root@test:/etc/openvpn/easy-rsa/keys#
```

```
↪/etc/init.d/sslh start
[ ok ] Starting ssl/ssh multiplexer: sslh.
```

Most már képes kell legyél ssh-zni a 443-as portra, és az SSLH segítségével tovább jutsz:

```
$ ssh -p 443 root@test.linuxjournal.com
root@test:~#
```

Az SSLH most a 443-as porton hallgat és képes továbbítani a forgalmat az SSH, az Apache, vagy az OpenVPN felé a hozzá eljutó csomagok alapján. Most már készen vagy a futtatásra!

Következtetések

Most már elindíthatod az OpenVPN-t és beállíthatod az OpenVPN klienst a 443-as portra, az SSLH át fogja irányítani az OpenVPN szerverhez az 1194-es portra. Ugyanakkor, mivel a szerveredhez a 443-as porton fordulsz, ezért a VPN-forgalmadat nem blokkolják. Most már betelepedhetsz egy ismeretlen kávézóba, egy ismeretlen városban abban a tudatban, hogy az Internet működni fog, amikor az OpenVPN-t elindítod és a Raspberry Pi-dre irányít. Emellett kapsz némi titkosítást a vonaladra, ami némileg megvédi a kapcsolatodat. Élvezd a szörfölést a neten az új végpontodon keresztül!

Források

OpenVPN telepítése és beállítása: **https://wiki.debian.org/OpenVPN és http://cryptotap.com/articles/openvpn**

OpenVPN kliens letöltése: **https://openvpn.net/index.php/open-source/downloads.html**

OpenVPN iOS számára: **https://itunes.apple.com/us/app/openvpn-connect/id590379981?mt=8**

OpenVPN Android számára: **https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en**

Tunnelblick Mac OS X-hez (OpenVPN kliens): **https://tunnelblick.net**

SSLH—Protocol Multiplexer: **http://www.rutschle.net/tech/sslh.shtml és https://github.com/yrutschle/sslh**