Eric Younger
Jonas Brunvoll Larsson
Thomas Bakken Moe

Øving - 15. VPN

Oppsett:

- Eric sin maskin kjørte VPN - serveren.
- Jonas sin maskin var VPN - klient, som koblet seg til Eric sin maskin.
- Thomas sin maskin var ekstern klient , som prøvde å koble seg til Eric sin maskin uten VPN.

Fremgangsmåte: Vi satt opp OpenVPN - VPN-serveren på Eric sin maskin, samt en webserver man kun kan aksessere med port 8000. Jonas sin maskin var VPN - klient og Thomas sin maskin hadde ingen VPN

```
eric@eric-macbook:~/Desktop/øving13$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [12/Oct/2020 14:42:53] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [12/Oct/2020 14:42:54] code 404, message File not found
127.0.0.1 - - [12/Oct/2020 14:42:54] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [12/Oct/2020 14:42:59] "GET /pwned.png HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:44:14] "GET / HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:44:14] code 404, message File not found
10.8.0.2 - - [12/Oct/2020 14:44:14] "GET /favicon.ico HTTP/1.1" 404 -
i10.22.11.35 - - [12/Oct/2020 14:44:55] "GET / HTTP/1.1" 200 -
10.22.11.35 - - [12/Oct/2020 14:44:55] code 404, message File not found
10.22.11.35 - - [12/Oct/2020 14:44:55] "GET /favicon.ico HTTP/1.1" 404 -
10.22.11.35 - - [12/Oct/2020 14:44:58] "GET /Screenshot%20from%202020-10-05%2010-53-44.png HTTP/1.1" 200 -
10.22.11.35 - - [12/Oct/2020 14:45:01] "GET /pwned.png HTTP/1.1" 200 -
127.0.0.1 - - [12/Oct/2020 14:45:40] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [12/Oct/2020 14:45:41] code 404, message File not found
127.0.0.1 - - [12/Oct/2020 14:45:41] "GET /favicon.ico HTTP/1.1" 404 -
10.8.0.2 - - [12/Oct/2020 14:50:17] "GET / HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:50:18] "GET / HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:50:19] "GET / HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:50:19] "GET / HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:50:25] "GET / HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:50:28] "GET / HTTP/1.1" 200 -
10.8.0.2 - - [12/Oct/2020 14:50:42] "GET / HTTP/1.1" 200 -
```

Tjenesten som deler at innholdet i øving13 mappen blir delt gjennom python sin http tjener på port 8000.

```
eric@eric-macbook:/etc/openvpn$ sudo openvpn --config server.conf
Mon Oct 12 14:40:29 2020 disabling NCP mode (--ncp-disable) because not in P2MP client or server mode
Mon Oct 12 14:40:29 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2019
Mon Oct 12 14:40:29 2020 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Mon Oct 12 14:40:29 2020 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher
 with a larger block size (e.g. AES-256-CBC).
Mon Oct 12 14:40:29 2020 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher
 with a larger block size (e.g. AES-256-CBC).
Mon Oct 12 14:40:29 2020 TUN/TAP device tun0 opened
Mon Oct 12 14:40:29 2020 /sbin/ip link set dev tun0 up mtu 1500
Mon Oct 12 14:40:29 2020 /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
Mon Oct 12 14:40:29 2020 Could not determine IPv4/IPv6 protocol. Using AF_INET
Mon Oct 12 14:40:29 2020 UDPv4 link local (bound): [AF_INET][undef]:1194
Mon Oct 12 14:40:29 2020 UDPv4 link remote: [AF_UNSPEC]
Mon Oct 12 14:40:42 2020 Peer Connection Initiated with [AF_INET]10.22.213.242:1194
Mon Oct 12 14:40:42 2020 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Mon Oct 12 14:40:42 2020 Initialization Sequence Completed
Mon Oct 12 14:42:13 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:42:16 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:42:21 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:42:29 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:42:45 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:48:13 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:48:15 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:48:20 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:48:28 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:48:45 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:54:13 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:54:16 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:54:19 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
Mon Oct 12 14:54:27 2020 Authenticate/Decrypt packet error: packet HMAC authentication failed
```

Her kjører VPN tjeneren med server.conf som konfigurasjonsfil. Man kan også se at Jonas koblet seg på VPN-tjeneren 14:40:42 med linjen “Peer connection Initiated with [AF_INET][]undef:1194” på bildet over.

```
eric@eric-macbook:/etc/openvpn$ ls
client  client.conf  server  server.conf  static.key  update-resolv-conf
eric@eric-macbook:/etc/openvpn$
```

```
eric@eric-macbook:/etc/openvpn$ sudo cat server.conf
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret static.key
```

For å kjøre VPN-serveren med konfigurasjonsfil så genererte vi en static.key som er lik hos både server og client. Denne nøkkelen blir referert til gjennom server.conf konfigurasjons-filen som open VPN-server kjører med som parameter.

```
eric@eric-macbook:~/Desktop/øving13$ sudo iptables -I INPUT -p tcp ! -s 10.8.0.2 --dport 8000 -j DROP
eric@eric-macbook:~/Desktop/øving13$
```

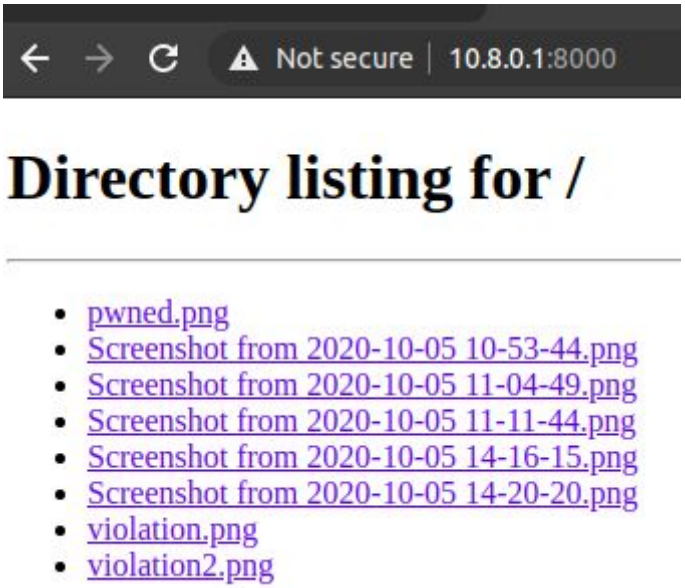
Brannmuren satt vi opp med iptables til å blokkere alle på port 8000 utenom ip-addressen 10.8.0.2 som er vpn gateway tilkoblingen.

```
jonasbl@jonasbl-MacBookAir:~/Documents$ cat halloiHanoi.conf
remote 10.24.2.16
dev tun
ifconfig 10.8.0.2 10.8.0.1
secret static.key
jonasbl@jonasbl-MacBookAir:~/Documents$
```

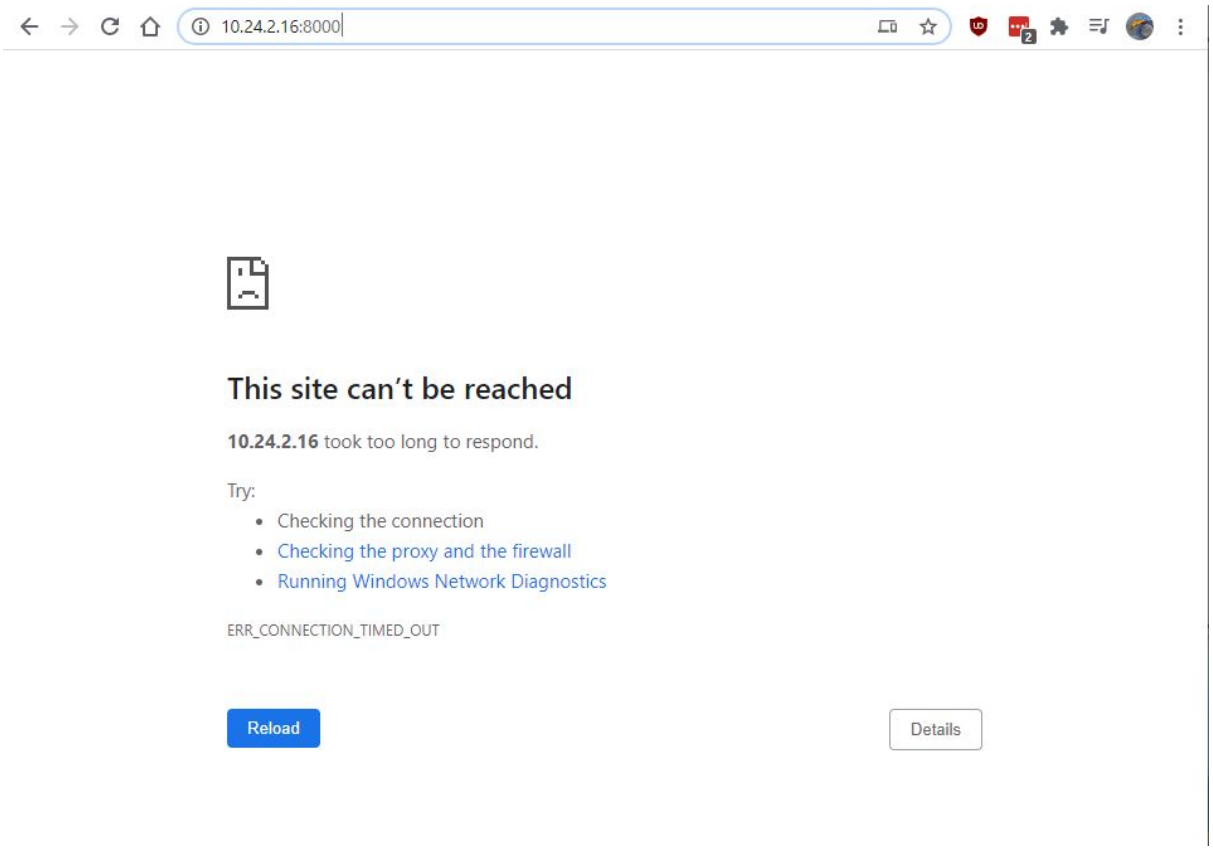
Klient config filen.

```
jonasbl@jonasbl-MacBookAir:~/Documents$ sudo openvpn --config halloiHanoi.conf
[sudo] password for jonasbl:
Mon Oct 12 15:21:27 2020 disabling NCP mode (--ncp-disable) because not in P2MP
client or server mode
Mon Oct 12 15:21:27 2020 WARNING: file 'static.key' is group or others accessibl
e
Mon Oct 12 15:21:27 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO]
 [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2019
Mon Oct 12 15:21:27 2020 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Mon Oct 12 15:21:27 2020 WARNING: INSECURE cipher with block size less than 128
bit (64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher w
ith a larger block size (e.g. AES-256-CBC).
Mon Oct 12 15:21:27 2020 WARNING: INSECURE cipher with block size less than 128
bit (64 bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher w
ith a larger block size (e.g. AES-256-CBC).
Mon Oct 12 15:21:27 2020 TUN/TAP device tun0 opened
Mon Oct 12 15:21:27 2020 /sbin/ip link set dev tun0 up mtu 1500
Mon Oct 12 15:21:27 2020 /sbin/ip addr add dev tun0 local 10.8.0.2 peer 10.8.0.1
Mon Oct 12 15:21:27 2020 TCP/UDP: Preserving recently used remote address: [AF_I
NET]10.24.2.16:1194
Mon Oct 12 15:21:27 2020 UDP link local (bound): [AF_INET][undef]:1194
Mon Oct 12 15:21:27 2020 UDP link remote: [AF_INET]10.24.2.16:1194
Mon Oct 12 15:21:37 2020 Peer Connection Initiated with [AF_INET]10.24.2.16:1194
Mon Oct 12 15:21:39 2020 WARNING: this configuration may cache passwords in memo
ry -- use the auth-nocache option to prevent this
Mon Oct 12 15:21:39 2020 Initialization Sequence Completed
```

Tjenesten som kun var tilgjengelig om man koblet til Eric sin maskin med VPN.



Jonas får til å hente web - ressursen Eric kjører.



Her prøver Thomas (ekstern klient) å koble seg til tjenesten som Eric tilbyr.

Kilder: https://openvpn.net/community-resources/static-key-mini-howto/