

# Practical Network Defense - Lab 5

Alessandro Serpi - 1647244

29 March 2019

## Contents





<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>VPN for the road warriors</b>	<b>2</b>
2.1	Users . . . . .	2
2.2	Server . . . . .	2
2.3	Firewall rules . . . . .	3
2.4	Clients . . . . .	4
<b>3</b>	<b>VPN for the firewall tunnel</b>	<b>5</b>
3.1	Phase 1 . . . . .	5
3.2	Phase 2 . . . . .	6
3.3	Firewall rules . . . . .	7
3.4	Routes . . . . .	7
<b>4</b>	<b>Test of the configuration</b>	<b>7</b>
<b>5</b>	<b>Final remarks</b>	<b>8</b>
<b>6</b>	<b>Update: OpenVPN in the remote infrastructure</b>	<b>8</b>

# 1 Introduction

In this assignment we have to set up two VPNs: one for road warriors (people who work outside the office and travel for business) and another between the two firewall. The assignment has been carried out on a local environment, please refer to the previous report for the network topology and configuration.

## 2 VPN for the road warriors

### 2.1 Users

Username	Full name	Groups
 <code>alice</code>	Alice	road_warriors
 <code>bob</code>	Bob	road_warriors
 <code>root</code>	System Administrator	admins
 <code>susan</code>	Susan	road_warriors

Create the three new users *alice*, *bob* and *susan* in System → Access → Users. All fields except username and password are optional and may be omitted. Then, create the group *road\_warriors* and add to it the newly created users.

### 2.2 Server

Create a new server in VPN → OpenVPN → Servers and populate it with the following options. The encryption settings provide additional security with respect to the default (except for the password-only authentication mode, which has been decided with smart-phones in mind), while the subnet `10.10.0.0/24` has been chosen without a precise reason.

<b>Description</b>	Road warriors
<b>Server Mode</b>	Remote Access ( User Auth )
<b>Backend for authentication</b>	Local Database
<b>Enforce local group</b>	road_warriors
<b>Protocol</b>	UDP
<b>Device Mode</b>	tun
<b>Interface</b>	WAN
<b>Local port</b>	1194
<hr/>	
<b>DH Parameters Length</b>	2048 bit
<b>Encryption algorithm</b>	AES-256-CBC (256 bit key, 128 bit block)
<b>Auth Digest Algorithm</b>	SHA256 (256-bit)
<hr/>	
<b>Tunnel Settings</b>	
<b>IPv4 Tunnel Network</b>	100.64.253.0/24
<b>IPv6 Tunnel Network</b>	
<b>Redirect Gateway</b>	<input type="checkbox"/>
<b>IPv4 Local Network</b>	100.64.0.0/16

## 2.3 Firewall rules

Firstly, it is necessary to allow incoming OpenVPN packets from the internet. To do so, create a new rule for interface WAN that accepts UDP packets with destination port

1194, the standard OpenVPN port.

	Protocol	Source	Port	Destination	Port
▶	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)

Then, allow access to *client* and *internal server* networks for road warriors. Given that the specifics are not clear about the type of access the road warriors have and that they may have different needs than normal employees, allowing all TCP/UDP packets was considered a good compromise between security and functionality.

Since communications may be started from both the road warriors network and the internal networks, we must add rules in all affected interfaces (the automatically-generated OpenVPN one and those in 100.64.254.0/30, 100.64.1.0/24 and 100.64.2.0/24).

	Protocol	Source	Port	Destination	Port
▶	IPv4 TCP/UDP	*	*	client_net 🚩	*
▶	IPv4 TCP/UDP	*	*	server_net 🚩	*
✗ ⓘ	IPv4 *	*	*	*	*

## 2.4 Clients

In VPN → OpenVPN → Client Export it is possible to download the OpenVPN configuration files. Obviously, it is necessary to insert the public IP for the WAN interface, which is usually fixed for enterprise networks.

To start a new connection, execute the command `openvpn --config FILE.ovpn` and insert a pair of valid credentials.

```
~/Downloads/Road_warriors_alice ➤ sudo openvpn --config Road_warriors_alice.ovpn
Wed Jul 31 17:07:39 2019 OpenVPN 2.4.7 [git:makepkg/2b8aec62d5db2c17+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 19 2019
Wed Jul 31 17:07:39 2019 library versions: OpenSSL 1.1.1c 28 May 2019, LZO 2.10
Enter Auth Username: alice
Enter Auth Password: *****
Wed Jul 31 17:07:44 2019 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.6:1194
Wed Jul 31 17:07:44 2019 UDP link local (bound): [AF_INET][undef]:0
Wed Jul 31 17:07:44 2019 UDP link remote: [AF_INET]192.168.1.6:1194
Wed Jul 31 17:07:44 2019 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Wed Jul 31 17:07:44 2019 [Road warriors VPN] Peer Connection Initiated with [AF_INET]192.168.1.6:1194
Wed Jul 31 17:07:45 2019 TUN/TAP device tun0 opened
Wed Jul 31 17:07:45 2019 /usr/bin/ip link set dev tun0 up mtu 1500
Wed Jul 31 17:07:45 2019 /usr/bin/ip addr add dev tun0 local 10.10.0.6 peer 10.10.0.5
Wed Jul 31 17:07:45 2019 Initialization Sequence Completed
```

## 3 VPN for the firewall tunnel

### 3.1 Phase 1

In VPN → IPsec → Tunnel Settings create a new phase 1 connection. In the general settings, insert the following data for *mainfw* and the inverse for *intfw*.

General information	
Disabled	<input type="checkbox"/> Disable this phase1 entry
Connection method	default ▼
Key Exchange version	V2 ▼
Internet Protocol	IPv4 ▼
Interface	internal ▼
Remote gateway	100.64.254.2
Dynamic gateway	<input type="checkbox"/> Allow any remote gateway to connect
Description	ipsec-intfw

Proposal settings must be identical in both firewalls, otherwise the session negotiation will fail.

Phase 1 proposal (Authentication)	
Authentication method	Mutual PSK ▼
My identifier	My IP address ▼
Peer identifier	Peer IP address ▼
Pre-Shared Key	openvpn-psk

Phase 1 proposal (Algorithms)	
Encryption algorithm	AES
	256
Hash algorithm	SHA256

Since phase 2 will be route-based, untick the Install policy checkbox.

Advanced Options	
Install policy	<input type="checkbox"/>

## 3.2 Phase 2

In VPN → IPsec → Tunnel Settings, create a new phase 2 configuration. Since *intfw* must use *mainfw* as the default gateway, it is not possible to use a tunnel connection: the two networks must not overlap but 0.0.0.0/0 contains all possible subnets. Instead, use a route-based setup using 100.64.247.0/30 addresses.

General information	
Disabled	<input type="checkbox"/>
Mode	Route-based
Description	ipsec-intfw
Tunnel network	
Local Address	10.64.247.1
Remote Address	10.64.247.2

In both firewalls, in order to increase security set up the proposal settings as follows. MD5 and SHA1 are insecure and should be avoided, AES-128 is acceptable but AES-256 is better.

**Phase 2 proposal (SA/Key Exchange)**

**Protocol** ESP

**Encryption algorithms**

☒ AES

256 bits

☐ aes128gcm16

☐ aes192gcm16

☐ aes256gcm16

☐ Blowfish

auto

☐ 3DES

☐ CAST128

☐ DES

☐ NULL (no encryption)

**Hash algorithms** SHA256, SHA384, SHA512

### 3.3 Firewall rules

Transfer in both firewall the rules from the interfaces in 100.64.254.0/30 to the newly-generated IPsec ones. Add to the old interfaces the rules that allow IPsec traffic.

	Protocol	Source	Port	Destination	Port
▶	IPv4 ESP	*	*	intfw_address 🚩	*
▶	IPv4 TCP/UDP	*	*	intfw_address 🚩	500 (ISAKMP)
▶	IPv4 TCP/UDP	*	*	intfw_address 🚩	4500 (IPsec NAT-T)

### 3.4 Routes

In *mainfw*, change the 100.64.0.0/16 route from the internal interface to the IPsec one. In *intfw*, change the default gateway to the IPsec interface.

## 4 Test of the configuration

IPsec was tested with the same files as the previous laboratory because the allowed traffic did not change. For OpenVPN, a `road_warriors.test` file, which uses the same return

codes, was executed on the local machine. FTP and SSH services were tested manually for the reasons already expressed in the previous report.

## 5 Final remarks

OpenVPN is one of the most commonly used VPN protocols thanks to its security and ease of use. Therefore, it is a sensible choice for road warriors, since they must have a safe and reliable communication channel with the base office.

IPsec, on the other hand, is less flexible and more difficult to configure. Since it encrypts IP packets, it is more suited to use cases where both endpoints are fixed. In this particular case, assuming that both firewalls are located in the same secure compound and that the communication channel does not leave its premises, IPsec is an overkill. The additional – and superfluous – security does not justify the substantial latency increase.

## 6 Update: OpenVPN in the remote infrastructure

In the remote infrastructure, the OpenVPN server was configured differently in order to authenticate users through certificates.

Firstly, we created an internal Certificate Authority in System → Trust → Authorities, then we used it to create a new server certificate in System → Trust → Certificates. Similarly, we generated a certificate for every Road Warrior user.

The server mode was changed to **Remote Access (SSL/TLS)** and we used the previously-generated certificates in the cryptographic settings.