



SAPIENZA
UNIVERSITÀ DI ROMA

DEPARTMENT OF CYBERSECURITY

Assignment 1

ACME-02

PRACTICAL NETWORK DEFENSE

Professor:

Angelo Spognardi

Students:

Federica Bianchi, 1891952

Giovanna Camporeale, 2086227

Francesco Rizzo, 1955615

Alessio Vigilante, 1839055

Contents

1	Brainstorming	2
1.1	Users creation	2
1.2	Road-Warriors VPN	2
1.3	Main-Internal VPN	3
1.4	Firewall	4
2	Details about the VPN setup for the ROAD WARRIORS	6
2.1	Creation of Users:	6
3	Details about the VPN for the MAIN INTERNAL VPN TUNNEL	9
3.1	In the Main-Firewall	9
3.1.1	Phase1:	9
3.1.2	Phase 2:	11
3.2	In the Internal Firewall	12
3.3	Firewall's Rules	13
4	Test of the new configuration	14
4.1	OpenVPN	14
4.1.1	Testing for the Operators: Alice	14
4.1.2	Testing for the Employees: Bob	16
4.2	IPsec	18
5	Final remarks	19

1 Brainstorming

First of all, we started analyzing the topology of the network and how the different subnetworks were linked to each other. In particular, we have identified the local and remote subnetworks of the Main Firewall-Router and the Internal Firewall-Router and to which of them the VPN users of the company have access.

1.1 Users creation

Since we needed to distinguish the access to the networks based on the type of users, we've decided to create two different groups for them: "operators" and "employees". After that we have created the users Alice, Bob and Charles and associated them to the respective groups, so Alice in the operators and Bob and Charles in the employees.

We decided to create different groups for the users in order to be able to distinguish them in an easier and cleaner way and in particular for the creation of the road warrior vpn. In fact, our idea was to make it impossible for the employees to access the vpn of the operators (and viceversa) and we could do this by restricting access to the vpn to users in a selected local group.

1.2 Road-Warriors VPN

First of all, we observed that we needed a way to distinguish the traffic belonging to the operators and the one belonging to the employees, because the latter cannot access the Internal servers network. In order to do this, we have analyzed two main strategies:

- There can be created two separated vpn tunnels (and so we set two different VPN servers, one for the employees and one for the operators) with different settings, in order to distinguish the privileges associated to the users, in particular which user can access the internal network and which can't;
- There can be created a single vpn tunnel and vpn server. In this way, we give full access to all the users and then we need to enforce the limitation on the access of the users using firewall's rules.

In general, the choice between using two separate VPNs or a single VPN with a firewall to divide access depends on the specific security needs of your environment. Using two separate VPNs can provide a higher level of security, as each VPN will have its own authentication credentials and security policies. Additionally, using separate VPNs can allow for greater control over access to network resources, as each VPN could be restricted to accessing only specific network resources and/or areas. On the other hand, using a single VPN with a firewall may be simpler to manage and configure, as

it would require fewer hardware and software components. Additionally, a firewall can offer greater flexibility in defining access rules, allowing you to block or allow access to specific network resources based on specific criteria.

In our specific case, we decided to implement the first option and so to create two separate vpn (with two different addresses, one for the operators and one for the employees). We made this choice because, even if the configuration with a single vpn may be easier, for our requirements we needed to regulate the access to the network only for two different types of users, so it was straightforward. In addition, by dividing the vpn, we can also enforce our policy using multiple levels of security: one on the vpn and one on the firewalls.

For what regards the creation of the certificates for the two different vpn, at the beginning we decided to create two different Certification Authorities, one for the operators and one for the employees. But then we realized that actually it wasn't necessary to have two CAs because we could use just one that issues the certificates of both employees and operators.

1.3 Main-Internal VPN

For what regards the IPsec tunnel, we needed to decide the details of the implementation and the level of security of IPsec. We mainly discussed two different ways to implement the tunnel, one using pre-shared keys and the other using RSA public keys (so certificates).

We evaluated the pros and cons of the two different methods. The main pro of the pre-shared keys is that they are easier to implement and use, since it's not necessary to obtain a certificate. The cons are mainly linked to the security of the key: if the key is compromised, unauthorized access to the network may be obtained and there is no way to automatically notify the IPsec peers the pre-shared key has been compromised. In addition, there are more opportunities to get the key because it's stored on all the IPsec peer systems and also replacing the key itself can be tedious, because it requires the update of all the systems.

For what regard the certificates, the only cons we could find is that creating/obtaining a certificate is more complicated, time consuming and potentially expensive than using a preshared key. But certificates have a lot of pros: the key used to generate certificates is stored in a single location, separate from the systems using the certificate. Thus, a compromised certificate only needs to be replaced on the system to which the certificate belongs and all systems may be notified of a certificate's compromise via a certificate revocation list (CRL). In addition, the public key embedded in a certificate may be larger than a pre-shared key (1024, 2048, 4096, or more).

So, we saw that, even though pre-shared keys are easier to work with, they are generally considered less secure than a certificate. For this reason we have decided to use certificates with RSA public keys.

First of all, we have decided the authentication and algorithms settings for our IPsec tunnel (in the phase 1 of the tunnel set up). Then, in the second phase, we created the two endpoints of the tunnel. As we do not define a local and remote network, we just use tunnel addresses, in this case we use 10.111.1.1 and 10.111.1.2. These will be the gateway addresses used for routing.

1.4 Firewall

Once we have set up the road-warrior vpn and the IPsec vpn, we decided also to enforce the security policies for the access to the network through the firewall rules.

Before starting to add the rules, in order to understand better how and if the tunnel was correctly working, we decided to test the IP address seen by the Internal Firewall if we ping it using a user. We saw that the IP was actually the one assigned to the vpn (namely the subnet 100.100.253.0/24) so we've seen that we could create new firewall's rules based on the IP address of the vpn.

At first, we decided to allow every incoming packet from the vpn users and then block only the access of the employees to the Internal servers network. In this way, we would have less rules on the firewall but as we know, by default, a firewall should block everything and you only permit certain traffic. For this reason, we've chosen this second option, which implements a more secure and clean policy.

In order to allow the access to all the networks to the operators and block the access of the employees to the Internal network, we first of all inserted the rules on the Main Firewall. We decided to follow the common strategy for the rules mentioned above: in order to provide better security, we've blocked the incoming traffic in the firewall from all the IP address sources except from the one of the vpn. Of course, as OpenVPN rules are evaluated on a first-match basis, we need to insert our "pass" rules at the beginning. For the operators we only needed to insert one rule: the firewall needed to accept all the incoming packets of the operators' vpn (based on the IP address) to any possible destination. For the employees, instead, we needed to add three different rules, for the External Service Network, the DMZ network and the Client network. In this way, all the incoming packets of the employees with destination addresses in the Internal Server Network are discarded. The rule that blocks all incoming traffic is already done by default by the firewall, so we didn't need to add that.

We decided to apply the same rules also in the Internal Firewall, even though it is redundant, in order to provide another additional level of security.

As regards the firewall's rules for the WAN, we thought it would be better to block all the traffic from the WAN to the networks of the corporation, except for the DMZ (for the nature itself of this type of network). So we added another rule on the firewall for that. For testing everything we used the common port 1994 and 1995 (for the two vpn), but then we changed them using other UDP ports, 4937 and 4938. For the

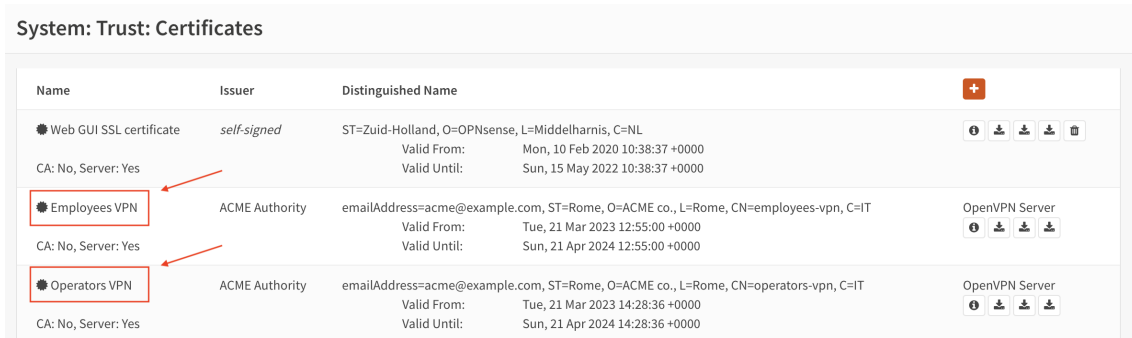
incoming packet on the Main Firewall, we added a rule to accept only the ones coming on port 4937 and 4938, so of the two VPNs.

Finally we added the rules regarding the IPsec tunnel. First of all we needed to make sure that all the traffic between the Main Firewall and the Internal Firewall is only made of IPsec packets, in other words that all the packets belong to the IPsec tunnel. To enforce an higher security, we also add in the Main Firewall a rule to accept only incoming packets with source the Internal Firewall and vice versa for the Internal.

2 Details about the VPN setup for the ROAD WARRIORS

2.1 Creation of Users:

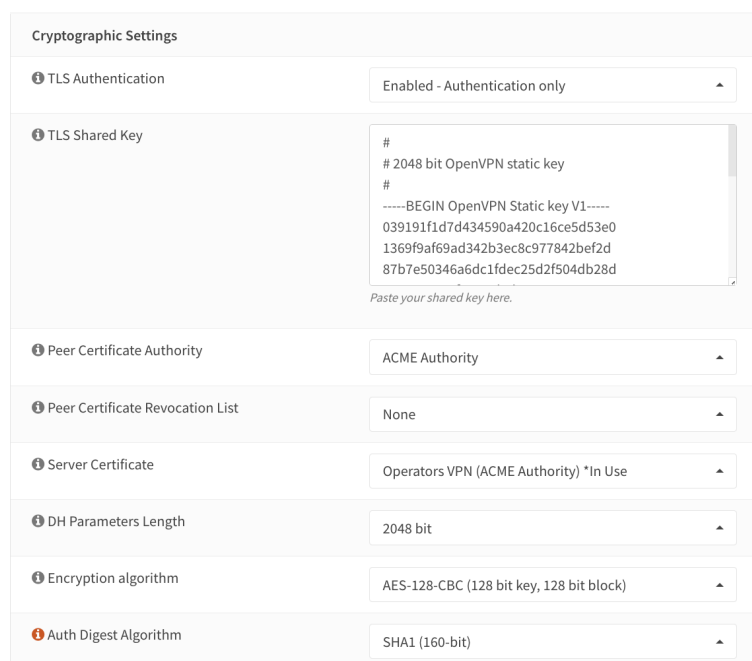
First of all, after the creation of the users and the groups, we have created the certificate for both the operators vpn server and the employees vpn server, by accessing the section System → Trust → Certificates.



Name	Issuer	Distinguished Name	
Web GUI SSL certificate	self-signed	ST=Zuid-Holland, O=OPNsense, L=Middelharnis, C=NL	
Valid From: Mon, 10 Feb 2020 10:38:37 +0000			
Valid Until: Sun, 15 May 2022 10:38:37 +0000			
CA: No, Server: Yes			
Employees VPN	ACME Authority	emailAddress=acme@example.com, ST=Rome, O=ACME co., L=Rome, CN=employees-vpn, C=IT	OpenVPN Server
Valid From: Tue, 21 Mar 2023 12:55:00 +0000			
Valid Until: Sun, 21 Apr 2024 12:55:00 +0000			
CA: No, Server: Yes			
Operators VPN	ACME Authority	emailAddress=acme@example.com, ST=Rome, O=ACME co., L=Rome, CN=operators-vpn, C=IT	OpenVPN Server
Valid From: Tue, 21 Mar 2023 14:28:36 +0000			
Valid Until: Sun, 21 Apr 2024 14:28:36 +0000			
CA: No, Server: Yes			

Figure 1: Creation of users

Then we created the two servers for the OpenVPN in VPN → OpenVPN → Servers. Here we have defined the cryptographic settings and inserted the TLS shared key and the server certificates.



Cryptographic Settings	
TLS Authentication	Enabled - Authentication only
TLS Shared Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 039191f1d7d434590a420c16ce5d53e0 1369f9af69ad342b3ec8c977842bef2d 87b7e50346a6dc1fdec25d2f504db28d</pre> <small>Paste your shared key here.</small>
Peer Certificate Authority	ACME Authority
Peer Certificate Revocation List	None
Server Certificate	Operators VPN (ACME Authority) *In Use
DH Parameters Length	2048 bit
Encryption algorithm	AES-128-CBC (128 bit key, 128 bit block)
Auth Digest Algorithm	SHA1 (160-bit)

Figure 2: Cryptographic settings

Then we have setted all the local networks that are reachable from the operators vpn and the employees vpn. The operators can access all the ACME network:

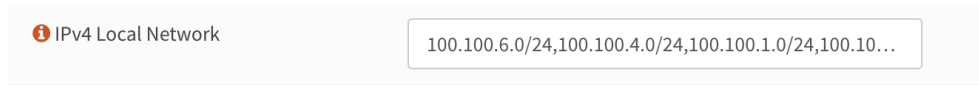


Figure 3: Local network for operators

The employees, instead, cannot access the Internal servers network (100.100.1.0/24)

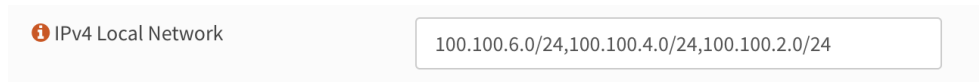


Figure 4: Local network for employees

So as we can see, here we haven't added that network.

We've divided the pool of addresses associated with the openvpn in two subnetworks: one for the employees and one for the operators. As we can see from the image, we associated the subnet 100.100.253.0/25 to the operators using port 4937 and the subnet 100.100.253.128/25 to the employees using port 4938.







VPN: OpenVPN: Servers			
Protocol / Port	Tunnel Network	Description	
UDP / 4937	100.100.253.0/25	Operators VPN Server	  
UDP / 4938	100.100.253.128/25	Employees VPN Server	  

Figure 5: Association of subnet to users

After we've completed the setup of the Road Warrior vpn, we defined the firewall's rules in order to better regulate the traffic of the operators and employees VPNs (as we described in the Introduction).

In the Main Firewall, on the OpenVPN interface we've added the following rules:









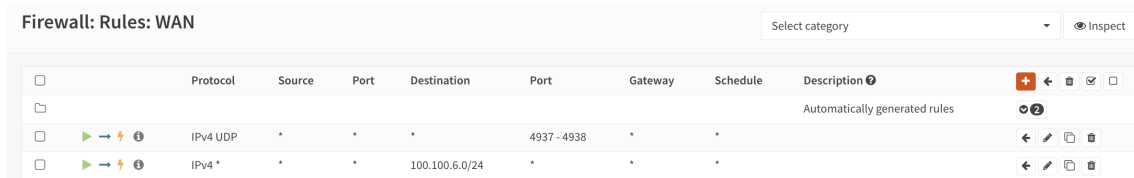
Firewall: Rules: OpenVPN									Select category
<input type="checkbox"/>		Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description ?
<input type="checkbox"/>	 	IPv4 *	100.100.253.0/25	*	*	*	*	*	Allows the operators to access all the ACME corporation networks
<input type="checkbox"/>	 	IPv4 *	100.100.253.128/25	*	100.100.2.0/24	*	*	*	Allows the employees to access the Clients Network
<input type="checkbox"/>	 	IPv4 *	100.100.253.128/25	*	100.100.4.0/24	*	*	*	Allows the employees to access the External services network
<input type="checkbox"/>	 	IPv4 *	100.100.253.128/25	*	100.100.6.0/24	*	*	*	Allows the employees to access the DMZ network

Figure 6: Main Firewall's rules

As we can see, these rules handle the access of the different users to the subnetworks.

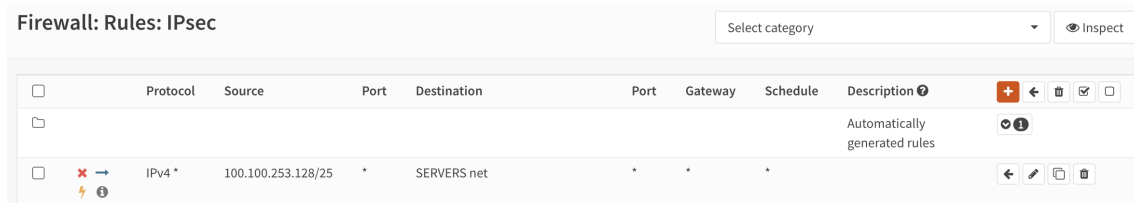
In the WAN, instead, we added a rule to allow only the traffic on the ports 4937 and 4938 to connect to the VPNs. The second rule is used to allow, from the WAN, only the access to DMZ. This is coherent with the concept of DMZ first.



	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
								Automatically generated rules	
	IPv4 UDP	*	*	*	4937 - 4938	*	*		
	IPv4 *	*	*	100.100.6.0/24	*	*	*		

Figure 7: WAN's rules

On the Internal Firewall, on the IPSec interface, we enforced the security blocking the access of the employees. This is an additional precaution for managing the access of the employees in the Internal Servers Network.



	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
								Automatically generated rules	
	IPv4 *	100.100.253.128/25	*	SERVERS net	*	*	*		

Figure 8: IPSec's rules

3 Details about the VPN for the MAIN INTERNAL VPN TUNNEL

3.1 In the Main-Firewall

First of all we create our first endpoint of the IPsec tunnel in the Main Firewall. We accessed the section VPN → IPsec → Tunnel Settings in order to define the tunnel settings.

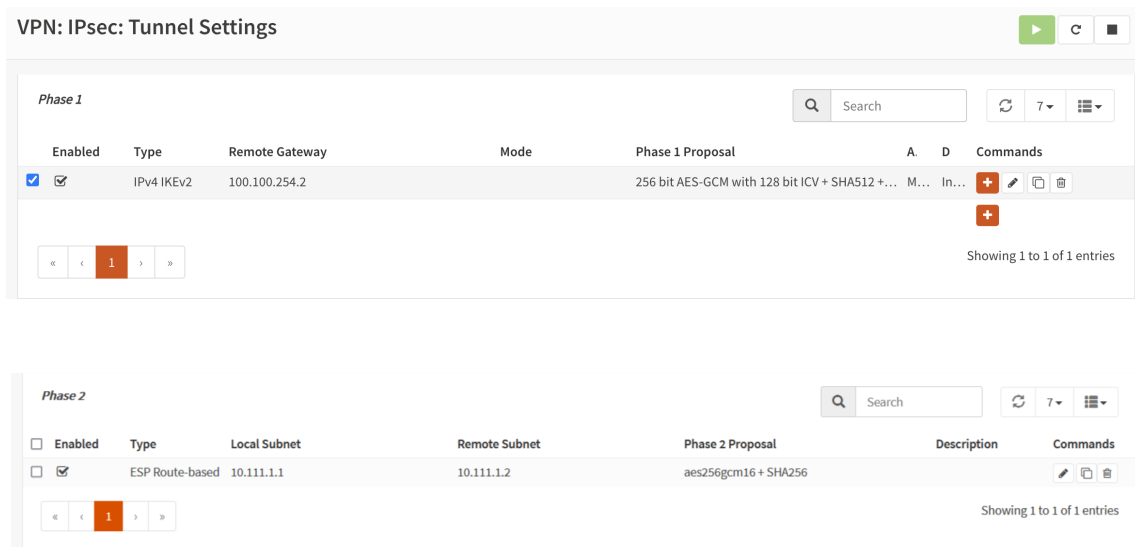


Figure 9: IPsec tunnel in the Main Firewall

3.1.1 Phase1:

In the phase 1, the main features that we've defined are:

- the internal interface of the Main Firewall,
- the remote gateway, set as the IP address of the "EXTERNAL" interface of the Internal Firewall (100.100.254.2),
- the authentication method: Mutual public key (for the motivation described in the section of **Brainstorming**),
- the encryption algorithms (256 bit AES and SHA512) as they are the ones that offer the higher level of security.

VPN: IPsec: Tunnel Settings

General information

- i** Disabled ☐ Disable this phase1 entry
- i** Connection method
- i** Key Exchange version
- i** Internet Protocol
- i** Interface
- i** Remote gateway
- i** Dynamic gateway ☐ Allow any remote gateway to connect
- i** Description

Phase 1 proposal (Authentication)

- i** Authentication method
- i** My identifier
- i** Peer identifier
- i** Local Key Pair
- i** Peer Key Pair

Phase 1 proposal (Algorithms)

- i** Encryption algorithm
- i** Hash algorithm
- i** DH key group
- i** Lifetime

Figure 10: Phase 1

3.1.2 Phase 2:

In the phase 2 the main features that we've defined are (in the image there is an example of one of the phase2):

- Route-based mode;
- The address of the local network for the tunnel, namely 10.111.1.1;
- In the remote network 10.111.1.2;
- Then we select the protocol ESP and the information about the encryption algorithms.

VPN: IPsec: Tunnel Settings

General information [full help](#)

Disabled ☐

Mode: Route-based

Description:

Tunnel network

Local Address: 10.111.1.1

Remote Address: 10.111.1.2

Figure 11: Phase 2.a

Phase 2 proposal (SA/Key Exchange)

Protocol: ESP

Encryption algorithms: aes256gcm16

Hash algorithms: SHA256

PFS key group: off

Lifetime: 3600 seconds

Figure 12: Phase 2.b

After that we added the RSA key pairs in the section VPN → IPsec → RSA Key Pairs:

Name	Key Type	Key Size	Key Fingerprint	Commands
InternalFirewall	RSA	4096	63:be:dd:1c:d2:b8:e6:4f:ea:d1:10:14:dd:3d:7e:a...	[Edit] [Copy] [Delete]
MainFirewall	RSA	4096	08:f9:57:97:8f:ac:2e:89:b3:f8:23:58:69:99:25:fe:0...	[Edit] [Copy] [Delete]

Figure 13: RSA Key Pairs

For the Internal Firewall, we added only the Public key (because we are in the Main Firewall) taken from the section System→Trust →Certificates, while for the Main Firewall we inserted both the private and public key.

After that, we created the routes and the gateways in the System section of OPNsense.

Name	Interface	Protocol	Port	IPV4 Address	IPV6 Address	MTU	Filter Rule	Filter Action	Status	Actions
GW_INTERNAL	InternalFirewallTunnel	IPv4	255	10.111.1.2	10.111.1.2	0.9 ms	0.7 ms	0.0 %	Online	[Edit] [Copy] [Delete]
	100.100.2.0/24			GW_INTERNAL - 10.111.1.2						[Edit] [Copy] [Delete]
	100.100.1.0/24			GW_INTERNAL - 10.111.1.2						[Edit] [Copy] [Delete]

3.2 In the Internal Firewall

We created our second endpoint of the IPsec tunnel in the Internal Firewall. Both the phases 1 and 2 have been done in the same way as in the Main Firewall, with the corresponding IP addresses and also the gateways and the routes.

At the end of the set up, we've obtained the following tunnel:

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.	Data
100.100.254.1	100.100.254.2	ESP	cb3207ae	aes-gcm-16	replay=0	0 hard: B
100.100.254.2	100.100.254.1	ESP	cf4d230f	aes-gcm-16	replay=4	0 hard: B

Figure 14: Security Association Database

3.3 Firewall's Rules

After the set up of the IPsec tunnel, we've added the rules in the two firewalls to enforce our company policy.

In the Main Firewall, in the INTERNAL interface, we've added the following rules:

Firewall: Rules: INTERNAL										Select category	Inspect
<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>		
Automatically generated rules											
<input type="checkbox"/>	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> IPv4 ESP	100.100.254.2	*	*	*	*	*			<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	
<input type="checkbox"/>	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> IPv4 TCP/UDP	100.100.254.2	*	*	500 (ISAKMP)	*	*			<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	
<input type="checkbox"/>	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> IPv4 TCP/UDP	100.100.254.2	*	*	4500 (IPsec NAT-T)	*	*			<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	

Figure 15: Rules of Internal interface

With these rules we have blocked all the traffic on the IPsec tunnel except the one belonging to the protocol ESP and the one on port 500 and 4500, which are the ones used by IPsec.

So only the IPsec traffic can pass through the tunnel between the Main Firewall and the Internal Firewall. In addition, to enforce even higher security, we accept only the packets with source IP address of the Internal Router.

In the Internal Firewall, on the EXTERNAL interface, we've added the same rules:

Firewall: Rules: EXTERNAL

Select category

Inspect

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description ⓘ	<div><div>+</div><div>←</div><div>↻</div><div>🗑</div><div>□</div></div>
📁	Automatically generated rules								<div><div>ⓘ</div></div>
<input type="checkbox"/>	<div><div>▶</div><div>⚡</div><div>ⓘ</div></div> IPv4 ESP	100.100.254.1	*	*	*	*	*		<div><div>←</div><div>✎</div><div>🗑</div><div>📄</div></div>
<input type="checkbox"/>	<div><div>▶</div><div>⚡</div><div>ⓘ</div></div> IPv4 TCP/UDP	100.100.254.1	*	*	500 (ISAKMP)	*	*		<div><div>←</div><div>✎</div><div>🗑</div><div>📄</div></div>
<input type="checkbox"/>	<div><div>▶</div><div>⚡</div><div>ⓘ</div></div> IPv4 TCP/UDP	100.100.254.1	*	*	4500 (IPsec NAT-T)	*	*		<div><div>←</div><div>✎</div><div>🗑</div><div>📄</div></div>

Figure 16: Rules of Internal interface

The logic is the same as the one in the Main Firewall.

4 Test of the new configuration

4.1 OpenVPN

In order to test the OpenVPN tunnel, we checked for a member of the operators (Alice) and a member of the employees (Bob), which subnets could reach, to see if the policy was satisfied.

4.1.1 Testing for the Operators: Alice

Accessing the Alice VPN, we tried to ping all the four networks: Alice, as an operator, is allowed to access every one of them. Ping to the Web Server of the DMZ Network:

```
[(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.6.2
PING 100.100.6.2 (100.100.6.2): 56 data bytes
64 bytes from 100.100.6.2: icmp_seq=0 ttl=63 time=66.907 ms
64 bytes from 100.100.6.2: icmp_seq=1 ttl=63 time=87.815 ms
64 bytes from 100.100.6.2: icmp_seq=2 ttl=63 time=243.004 ms
64 bytes from 100.100.6.2: icmp_seq=3 ttl=63 time=166.923 ms
^C
--- 100.100.6.2 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 66.907/141.162/243.004/69.633 ms
```

Figure 17: Ping to the Web Server of the DMZ

Ping to the DNS Server of the Internal servers network:

```
(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.1.2
PING 100.100.1.2 (100.100.1.2): 56 data bytes
64 bytes from 100.100.1.2: icmp_seq=0 ttl=62 time=230.665 ms
64 bytes from 100.100.1.2: icmp_seq=1 ttl=62 time=112.685 ms
64 bytes from 100.100.1.2: icmp_seq=2 ttl=62 time=102.740 ms
64 bytes from 100.100.1.2: icmp_seq=3 ttl=62 time=57.524 ms
^C
--- 100.100.1.2 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 57.524/125.904/230.665/63.957 ms
```

Figure 18: Ping to the DNS Server of the Internal servers network

Ping to the Client ext 1 of the External services network:

```
(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.4.100
PING 100.100.4.100 (100.100.4.100): 56 data bytes
64 bytes from 100.100.4.100: icmp_seq=0 ttl=63 time=486.257 ms
64 bytes from 100.100.4.100: icmp_seq=1 ttl=63 time=127.746 ms
64 bytes from 100.100.4.100: icmp_seq=2 ttl=63 time=138.011 ms
64 bytes from 100.100.4.100: icmp_seq=3 ttl=63 time=147.367 ms
64 bytes from 100.100.4.100: icmp_seq=4 ttl=63 time=103.084 ms
^C
--- 100.100.4.100 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 103.084/200.493/486.257/143.644 ms
```

Figure 19: Ping to the Client ext 1 of the External servers network

Ping to the Kali PC of the Clients network:

```
(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.2.100
PING 100.100.2.100 (100.100.2.100): 56 data bytes
64 bytes from 100.100.2.100: icmp_seq=0 ttl=62 time=105.267 ms
64 bytes from 100.100.2.100: icmp_seq=1 ttl=62 time=95.025 ms
64 bytes from 100.100.2.100: icmp_seq=2 ttl=62 time=112.268 ms
64 bytes from 100.100.2.100: icmp_seq=3 ttl=62 time=80.974 ms
^C
--- 100.100.2.100 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
```

Figure 20: Ping to the Kali PC of the Clients network

When we were connected to the VPN of Alice, we also checked the Connection Status in the section VPN → OpenVPN → Connection Status.

VPN: OpenVPN: Connection Status						
Operators VPN Server UDP:4937 Client connections ▶ ⌂ ⌵						
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	
alice	100.101.0.5:54589	100.100.253.6	2023-03-31 12:43:13	1.72 MB	171 KB	✕
▼ Operators VPN Server UDP:4937 Routing Table						
Employees VPN Server UDP:4938 Client connections ▶ ⌂ ⌵						
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	
No OpenVPN clients are connected to this instance.						

Figure 21: Connection status

4.1.2 Testing for the Employees: Bob

Accessing the Bob VPN, we tried to ping all the four networks: Bob, as an employee, is allowed to access only in the DMZ network, in the External services and in the Clients newtork. Ping to the Web Server of the DMZ Network:

```
utun7: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST>mtu 1500
    inet 100.100.253.134 --> 100.100.253.133 netmask 0xffffffff
(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.6.2
PING 100.100.6.2 (100.100.6.2): 56 data bytes
64 bytes from 100.100.6.2: icmp_seq=0 ttl=63 time=164.989 ms
64 bytes from 100.100.6.2: icmp_seq=1 ttl=63 time=92.568 ms
64 bytes from 100.100.6.2: icmp_seq=2 ttl=63 time=93.244 ms
64 bytes from 100.100.6.2: icmp_seq=3 ttl=63 time=100.724 ms
^C
--- 100.100.6.2 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 92.568/112.881/164.989/30.254 ms
```

Figure 22: Ping to the Web Server of the DMZ

Ping to the DNS Server of the Internal servers network:

```
(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.1.2
PING 100.100.1.2 (100.100.1.2): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
^C
--- 100.100.1.2 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
```

Figure 23: Ping to the DNS Server of the Internal servers network

Ping to the Client ext 1 of the External services network:

```
(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.4.100
PING 100.100.4.100 (100.100.4.100): 56 data bytes
64 bytes from 100.100.4.100: icmp_seq=0 ttl=63 time=106.350 ms
64 bytes from 100.100.4.100: icmp_seq=1 ttl=63 time=138.044 ms
64 bytes from 100.100.4.100: icmp_seq=2 ttl=63 time=108.731 ms
^C
--- 100.100.4.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 106.350/117.708/138.044/14.412 ms
```

Figure 24: Ping to the Client ext 1 of the External servers network

Ping to the Kali PC of the Clients network:

```
(base) MacBook-Pro-di-Federica:~ federica$ ping 100.100.2.100
PING 100.100.2.100 (100.100.2.100): 56 data bytes
64 bytes from 100.100.2.100: icmp_seq=0 ttl=62 time=116.316 ms
64 bytes from 100.100.2.100: icmp_seq=1 ttl=62 time=157.695 ms
64 bytes from 100.100.2.100: icmp_seq=2 ttl=62 time=112.270 ms
64 bytes from 100.100.2.100: icmp_seq=3 ttl=62 time=102.854 ms
^C
--- 100.100.2.100 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 102.854/122.284/157.695/21.020 ms
```

Figure 25: Ping to the Kali PC of the Clients network

When we were connected to the VPN of Bob, we also checked the Connection Status in the section VPN → OpenVPN → Connection Status.

VPN: OpenVPN: Connection Status					
Operators VPN Server UDP:4937 Client connections ▶ ⌂ ⌵					
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
No OpenVPN clients are connected to this instance.					
Employees VPN Server UDP:4938 Client connections ▶ ⌂ ⌵					
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
bob	100.101.0.5:50675	100.100.253.134	2023-05-02 15:00:48	2.06 MB	110 KB
▼ Employees VPN Server UDP:4938 Routing Table					

Figure 26: Connection status

4.2 IPsec

In order to check the IPsec connection, we first of all accessed the section VPN → IPsec → Status Overview:

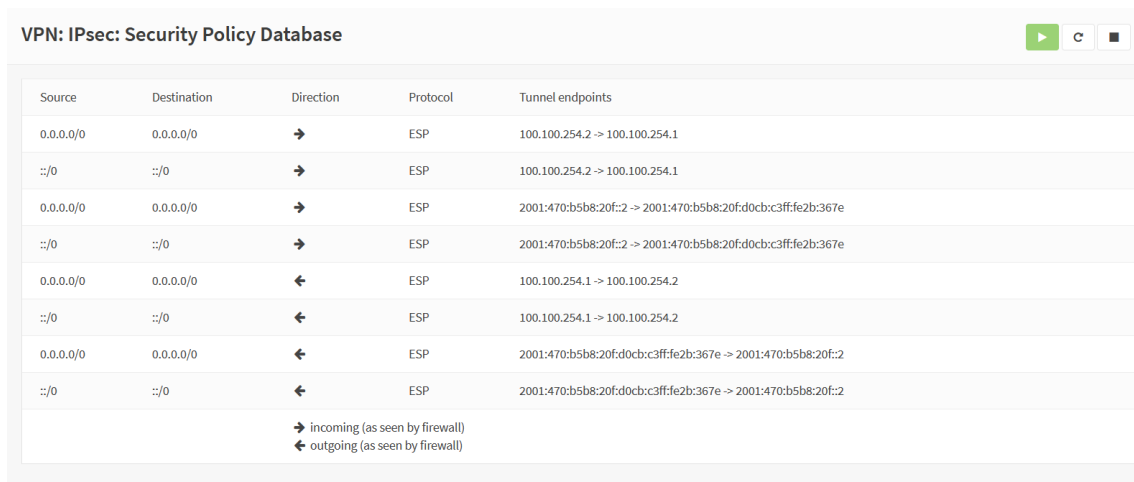
VPN: IPsec: Status Overview

Connection	Version	Local ID	Local IP	Remote ID	Remote IP	Local Auth	Remote Auth	Status
Main Firewall Tunnel (con1)	IKEv2	100.100.254.2	100.100.254.2	100.100.254.1	100.100.254.1	public key	public key	<div><div></div><div></div><div></div></div>
Remote Host	Local subnets	SPI(s)	Remote subnets	State	Stats			
100.100.254.1	0.0.0.0/0	in : c35e275f out : c89ab494	0.0.0.0/0	INSTALLED Routed	Time : 1085 Bytes in : 50273 Bytes out : 199140			
100.100.254.1	0.0.0.0/0	in : c08b87fd out : ca09d608	• 0.0.0.0/0	INSTALLED Routed	Time : 927 Bytes in : 255641 Bytes out : 1173400			

Figure 27: Status Overview

Then, because there isn't an intermediate node between the Main Firewall and the Internal firewall that we can access, we can't check if the traffic is encrypted. So in order to have a further check on the tunnel, we looked at the Security Policy Database in the section VPN → IPsec → Security Policy Database.

In the Main Firewall we have:



Source	Destination	Direction	Protocol	Tunnel endpoints
0.0.0.0/0	0.0.0.0/0	→	ESP	100.100.254.2 -> 100.100.254.1
::/0	::/0	→	ESP	100.100.254.2 -> 100.100.254.1
0.0.0.0/0	0.0.0.0/0	→	ESP	2001:470:b5b8:20f::2 -> 2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e
::/0	::/0	→	ESP	2001:470:b5b8:20f::2 -> 2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e
0.0.0.0/0	0.0.0.0/0	←	ESP	100.100.254.1 -> 100.100.254.2
::/0	::/0	←	ESP	100.100.254.1 -> 100.100.254.2
0.0.0.0/0	0.0.0.0/0	←	ESP	2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e -> 2001:470:b5b8:20f::2
::/0	::/0	←	ESP	2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e -> 2001:470:b5b8:20f::2

→ incoming (as seen by firewall)
← outgoing (as seen by firewall)

Figure 28: Security Policy Database Main Firewall

In the Internal Firewall we have:

Source	Destination	Direction	Protocol	Tunnel endpoints
0.0.0.0/0	0.0.0.0/0	➔	ESP	100.100.254.1 -> 100.100.254.2
::/0	::/0	➔	ESP	100.100.254.1 -> 100.100.254.2
0.0.0.0/0	0.0.0.0/0	➔	ESP	2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e -> 2001:470:b5b8:20f:2
::/0	::/0	➔	ESP	2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e -> 2001:470:b5b8:20f:2
0.0.0.0/0	0.0.0.0/0	➔	ESP	100.100.254.2 -> 100.100.254.1
::/0	::/0	➔	ESP	100.100.254.2 -> 100.100.254.1
0.0.0.0/0	0.0.0.0/0	➔	ESP	2001:470:b5b8:20f:2 -> 2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e
::/0	::/0	➔	ESP	2001:470:b5b8:20f:2 -> 2001:470:b5b8:20f:d0cb:c3ff:fe2b:367e
		➔ incoming (as seen by firewall) ➔ outgoing (as seen by firewall)		

Figure 29: Security Policy Database Internal Firewall

5 Final remarks

The creation of the users and the groups was straightforward. Regarding the Road Warriors VPN, the implementation was pretty simple but it was more interesting and challenging the brainstorming part, where we needed to decide how to design the VPN for the employees and the operators.

Finally, the IPsec tunnel was a little more difficult for us, also for the implementation itself, which wasn't as simple as the one for the OpenVPN. In addition, we encountered more difficulties also for the testing part, in particular to verify that all the traffic was actually passing through the internal tunnel. In fact, we needed also to add some firewall's rules in order to accomplish that.