VPN Assignment - Group 09

Student Names and Numbers:

- Alessio Civica, Mat: 1916744 - civica.1916744@studenti.uniroma1.it

- Antonio Giorgino, Mat: 2126475 - giorgino.2126475@studenti.uniroma1.it

- Federico Detomaso, Mat: 1903906 - detomaso.1903906@studenti.uniroma1.it

Brainstorming and policy evaluation

We started by reading the assignment and dividing it into steps to follow to implement. These step are the following

1. Gathering information to understand the VPN to implement inside the system
2. Understand which services to use for VPN implementation and understand how opnsense could implement them
3. VPN realization

For this assignment we've chosen to use *Aliases,* named lists of networks, hosts or ports that can be used as one entity by selecting the alias name in the various supported sections of the firewall, to refer to the given users and groups of the trace in order to have a better and more orderly reference within the firewall rules. Using this method we've the two groups employees and operator.

In order to give a better security of the VPN, we've chosen to implement it using the TCP protocol that ensures reliability and security of connections in line with our proposed security and authentication rules. To reinforce this concept, where provided with the use of OpenVPN and IPSec, we decided to set up authentication procedures with the aim of greater security and easier access control, choosing SHA512 in OpenVPN and Mutual PSK in IPSec.

Studying the encryption algorithms on opnsense, we decided to use the AES256 algorithm as the encryption algorithm for OpenVPN and IPSec VPNs as we found it to be the most secure and suitable for our needs. The SHA512 algorithm was chosen to be the hashing algorithm for the IPSec VPN and the Auth Digest Algorithm for authenticating communications in the OpenVPN configuration. In addition, for the two VPNs, it was deemed consonant to use Diffie-Hellman Group 14 for key negotiation in IPSec and the use of two certificates, one for the client and one for the server, for the configuration in OpenVPN.

Realization of the VPN system

Authorities Server configuration

We started the VPN configuration by the certificate authority, as we know for certificate the truthfulness of a host we have to use a certificate that ensures our identity. For our VPN we have implemented our certificate authority via *Authorities* option provided by the opnsense main firewall and we used this *Authorities* to release and authenticate four certificates for our VPN server and after we have generated three certificates for the designated user of the trace.

OpenVPN configuration

With this certificate we've enabled the OpenVPN server inside our opnsense main firewall and pass it to the server certificate generated a few minutes before. The OpenVPn server is configured in this way: the OpenVPN server, configured on standard port 1194, has as server mode, that we decided during the brainstorming, setted to *Remote Access (SSL/TLS + User Auth)* that enables an authentication, using the local database, to permit the user to connect to the ACME VPN. For better security performance the OpenVPN server uses the protocol TCP for its communication with the connected host and is configured in order to encrypt the IP layer via a virtual *tun interface.*
The IP range assigned to the OpenVPN server is the 100.100.253.0/24 with a domain name equal to *roadwarriorsserver* and enabled to provide a list of DNS servers to the connected clients that are owned by the ACME network.
Then it has been configured with all the cryptographic certificates and algorithms. The *Peer Certificate Authority* and the *Server Certificate* are configured to be the one that have been locally created by us moments before the OpenVPN configuration. The *Encryption Algorithm,*as we already know, is the AES-256-GCM as one of the most secure and SHA512 was set as the Auth Digest Algorithm

IPSec configuration

To configure the IPSec VPN, before starting the configuration, we added three firewall rules on the INTERNAL interface of the Main Firewall and EXTERNAL interface of the Internal Firewall to allow all the UDP packets on port 500 (for ISAKMP) and 4500 (for NAT-T) and we also allowed the passthrough of all the packet sent with protocol ESP. By allowing this packets on our firewall, we enabled the possibility, with ISAKMP, for establishing security association (SA) and cryptographic keys in an Internet environment; with NAT-T to allow IPSec traffic to pass through NAT devices.
Inside the *Tunnel Settings* section of opnsense for the IPSec configuration and then we followed the two phases for both of the routers to set the secure tunnel for the VPN.

1. In the first phase is created the tunnel between the two routers by settings requested parameters like Key Exchange Version, the Internet Protocol setted to IPv4, the remote

gateway setted to 100.100.254.2. Then we configured the security part of the VPN by setting Mutual PSK (which allows a secret key to be shared before the connection between the two parties to the vpn) as the authentication method; generating the Pre-Shared key according to a password generated specifically for use with Mutual PSK; setting the encryption algorithms to AES256 and the Hashing algorithm to SHA512; and, finally, choosing group 14 (which uses 2048-bit chaivi) for key exchange with Diffie-Hellman.

2. In the second phase, the networks that will be used by this tunnel were configured, in particular, all the possible directions in will be possible to generate the VPN tunnel such as, for example, the tunnel from the DMZ network to the CLIENTS network. For the sake of clarity the tunnel that will be used will be the one set up in phase one, in this phase the networks, and directions, enabled to use the tunnel are entered

As we already said this two phases has been repeated on both of the firewall inside the network, the only difference between the main and the internal firewall configuration is that the remote gateway is setted to 100.100.254.1 (inside the internal firewall)

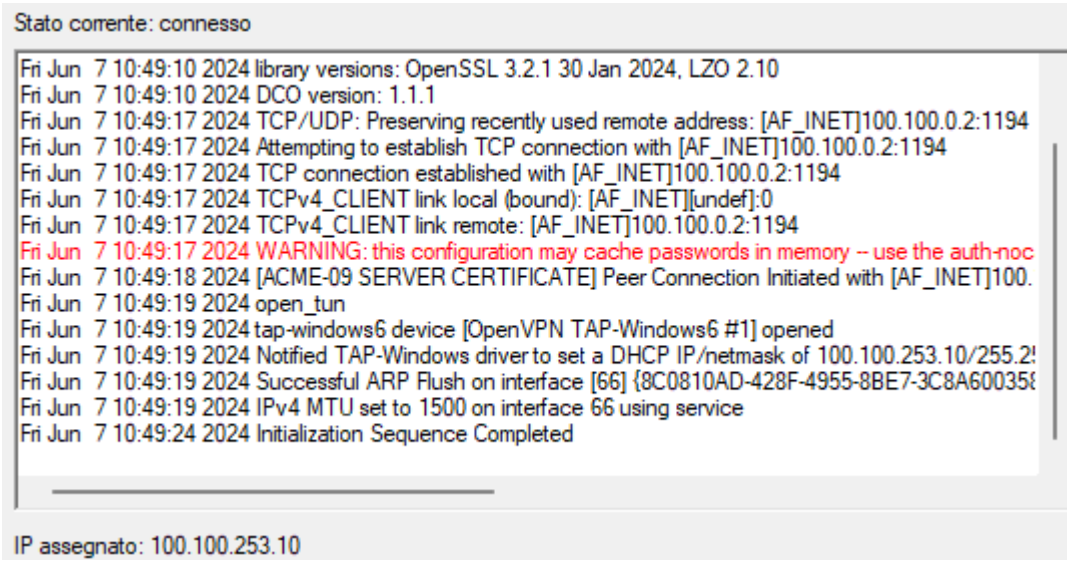
Account setup

To generate users, we used the authorities generated via OpenVPN. Starting from that, we then created the three accounts: Alice, Bob and Charles by inserting them into the OpenVPN configuration and generating, for each of them, a certificate that they could use to authenticate when using the VPN. Once the users were created, the employees and operators groups were then created and each user was assigned to the designated group. Following the credential configuration

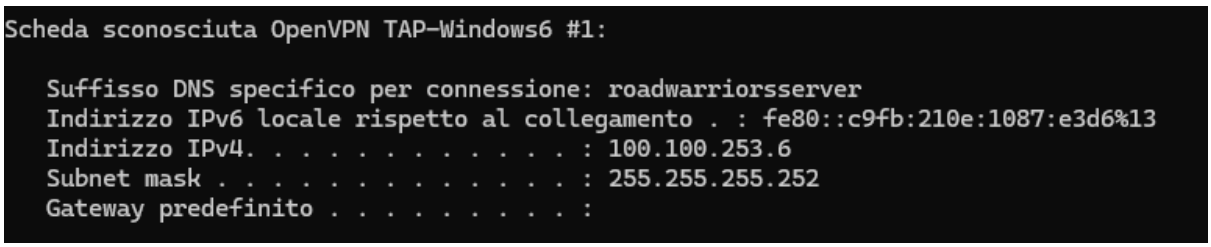
Username	**Password**
Alice	Alice
Bob	Bob
Charles	Charles

Configuration test

This image shows the correct connection to the VPN with the Alice account and credentials. The ip reserved for this connection is inside the assigned range and is setted up to 100.100.253.2

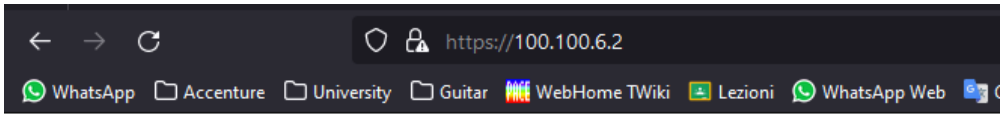


This images shows the virtual interface enabled after the Alice connection to the OpenVPN server

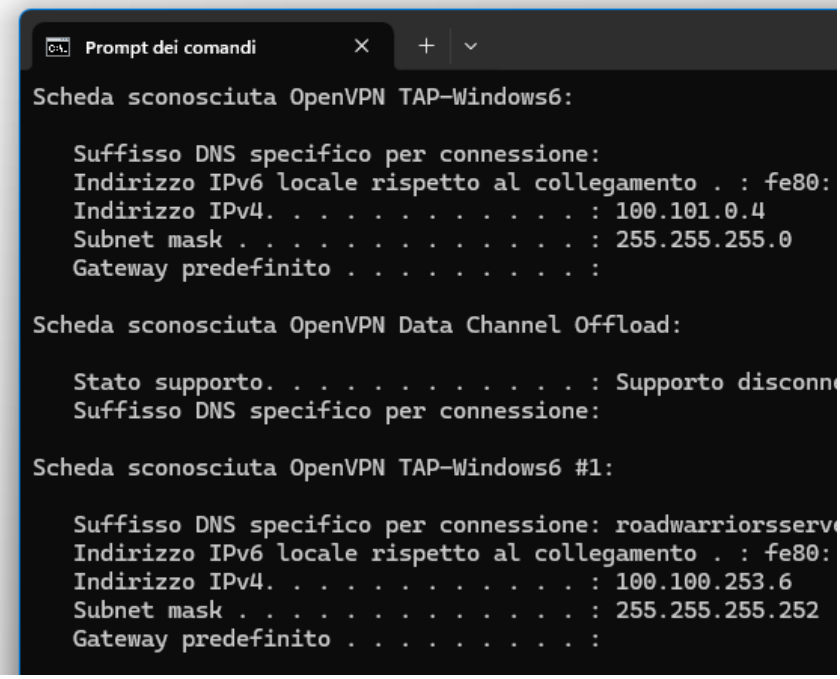


And after the connection, here are shown a correct ping inside the network and a correct https connection to the internal web server

```
C:\Users\feder>ping 100.100.1.2

Esecuzione di Ping 100.100.1.2 con 32 byte di dati:
Risposta da 100.100.1.2: byte=32 durata=62ms TTL=62
Risposta da 100.100.1.2: byte=32 durata=71ms TTL=62
Risposta da 100.100.1.2: byte=32 durata=85ms TTL=62
Risposta da 100.100.1.2: byte=32 durata=69ms TTL=62

Statistiche Ping per 100.100.1.2:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 62ms, Massimo =  85ms, Medio =  71ms

C:\Users\feder>ping 100.100.4.100

Esecuzione di Ping 100.100.4.100 con 32 byte di dati:
Risposta da 100.100.4.100: byte=32 durata=68ms TTL=63
Risposta da 100.100.4.100: byte=32 durata=75ms TTL=63
Risposta da 100.100.4.100: byte=32 durata=81ms TTL=63
Risposta da 100.100.4.100: byte=32 durata=72ms TTL=63

Statistiche Ping per 100.100.4.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 68ms, Massimo =  81ms, Medio =  74ms
```



I'm working!



This screen shows the correct communication between the two router inside the IPSec VPN

2024-06-07T08:48:34	Informational	charon	10[NET] <con1|5> received packet: from 100.100.254.2[4500] to 100.100.254.1[4500] (96 bytes)
2024-06-07T08:48:33	Informational	charon	10[NET] <con1|5> sending packet: from 100.100.254.1[4500] to 100.100.254.2[4500] (448 bytes)
2024-06-07T08:48:33	Informational	charon	10[ENC] <con1|5> generating CREATE_CHILD_SA response 2 [SA No KE]
2024-06-07T08:48:33	Informational	charon	10[IKE] <con1|5> IKE_SA con1[6] rekeyed between 100.100.254.1[100.100.254.1]...100.100.254.2[100.100.254.2]
2024-06-07T08:48:33	Informational	charon	10[IKE] <con1|5> maximum IKE_SA lifetime 15037s
2024-06-07T08:48:33	Informational	charon	10[IKE] <con1|5> scheduling rekeying in 13597s
2024-06-07T08:48:33	Informational	charon	10[CFG] <con1|5> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_2048
2024-06-07T08:48:33	Informational	charon	10[IKE] <con1|5> 100.100.254.2 is initiating an IKE_SA