FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D COIMBRA

# Relatório

*Trabalho Prático #1*

**Segurança em Tecnologias da Informação**

**2019/2020**


Duarte Guerreiro 2016231778

João Tomás 2016225021

# Índice

# Introdução

No âmbito do primeiro trabalho prático da unidade curricular de Segurança em Tecnologias da Informação implementámos dois tipos de cenários de comunicação segura, sendo estes Roadwarrior e o outro Gateway-to-Gateway. Para tal foi utilizada a tecnologia *OpenVPN*, em conjunto com uma Autoridade de Certificação privada e um servidor OCSP. Para aumentar o nível de segurança, iremos implementar *Two-Factor Authentication*, tendo o roadwarrior que fornecer, para além de um certificado válido fornecido pela Autoridade de Certificação privada, uma password e uma *one-time password*, fornecida pela aplicação *Google Authenticator.*

# 1. Arquitetura do Projeto

O nosso projeto utiliza **4 ficheiros** de configuração para implementar os diferentes intervenientes do nosso projeto:

- **Roadwarrior** é implementado no ficheiro client.conf
- **Gateway de Coimbra** foi implementada utilizando dois ficheiros, sendo um o server.conf, que comunica com o roadwarrior e servertolisb.conf, que comunica com a Gateway de Lisboa
- **Gateway de Lisboa**, implementada através do ficheiro client.conf

# 2. Como executar o projeto

Para que seja possível executar o trabalho implementado, é necessário ligar as três máquinas virtuais, sendo que:

- Na máquina virtual destinada ao **Roadwarrior** é apenas necessário executar o openvpn com o ficheiro de configuração do roadwarrior (client.conf). Para tal é utilizado o comando **openvpn --config server.conf**
- Na máquina virtual referente à **Gateway de Coimbra** é necessário começar por colocar o servidor OCSP no porto pretendido (**openssl ocsp -index index.txt -port 8080 -CA CertAuth.crt -rsigner CertAuth.crt -rkey CertAuth.key -resp_text**) e, de seguida, executar o openvpn com o ficheiro de configuração do servidor que liga Coimbra ao roadwarrior (server.conf) e o ficheiro de configuração do servidor que liga Coimbra a Lisboa (servertolisb.conf) . Isto é feito através dos comandos **openvpn --config server.conf** e **openvpn --config servertolisb.conf**
- Na máquina virtual na qual se encontra o **Gateway de Lisboa** será apenas necessário executar o openvpn com o ficheiro de configuração do cliente (client.conf), utilizando o comando **openvpn --config client.conf**

# 3. Configuração da máquina virtual

Cada um dos intervenientes no cenário do nosso projeto (roadwarrior, gateway de Coimbra e de Lisboa) encontram-se numa máquina virtual, existindo, portanto, um total de três máquinas virtuais. Para tornar possível a comunicação entre as diferentes máquinas

foram configurados adaptadores de redes internas em cada uma das máquinas virtuais, da seguinte forma:

- **Roadwarrior** - Adaptador NAT e adaptador Internal Network, com o nome *intnet*, para permitir a comunicação com a gateway de Coimbra
- **Gateway de Coimbra** - Adaptador NAT e 3 adaptadores Internal Network, sendo que aquele com nome *intnet* se destina à comunicação com o roadwarrior, o de nome *intnet2* destina-se à comunicação com a Gateway de Lisboa e o *intnet3* serve para a rede interna de Coimbra, na qual estará a correr o servidor OCSP
- **Gateway de Lisboa** - Adaptador NAT e 2 adaptadores Internal Network, sendo o adaptador de nome *intnet2* utilizado para comunicar com a Gateway de Coimbra e aquele com nome *intnet4* será utilizado para a rede interna de Lisboa

Após criar cada uma destas interfaces foi necessário atribuir os devidos endereços de IP estáticos, sendo tudo isto foi efetuado na diretoria **/etc/sysconfig/network-scripts**, em cada um dos ficheiros com o nome da respetiva interface (ifcfg-enp0s**x**).

Na figura que se segue são apresentados todos os endereços IP atribuídos, sendo assim possível dar a entender todo o ambiente do nosso projeto.

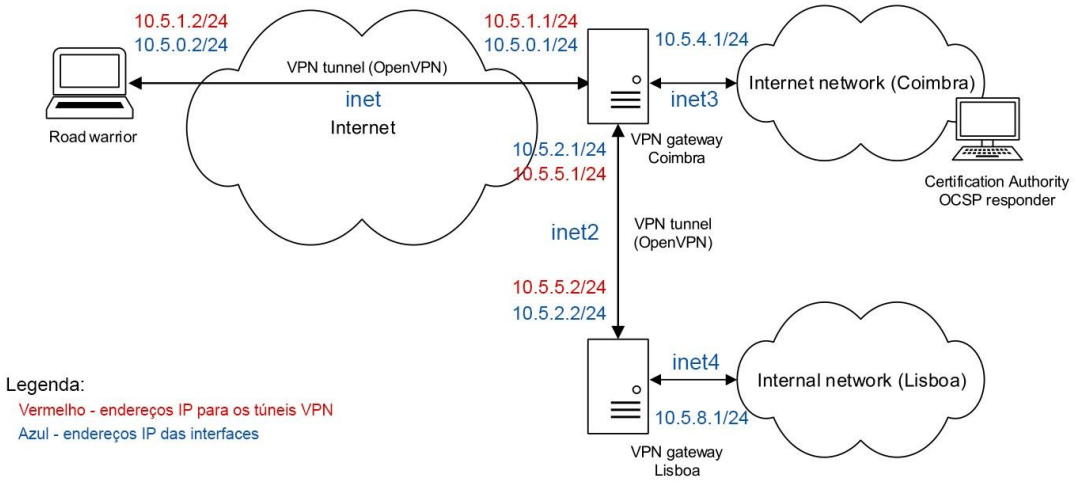


*Figura 1 - Esquema representativo do ambiente do nosso projeto*

Como é possível observar na figura, a gama de endereços 10.5.0.0/24 está reservada para a rede na qual ocorre a comunicação entre o roadwarrior e Coimbra (inet), a gama 10.5.2.0/24 está reservada para a rede onde ocorre a comunicação entre Coimbra e Lisboa (inet2), a gama 10.5.4.0/24 está reservada para a rede interna de Coimbra (inet3) e a gama 10.5.8.0/24 está reservada para a rede interna de Lisboa (inet4). É ainda possível observar que o servidor de Coimbra, que comunica com o Roadwarrior, atribui endereços de IP para o túnel VPN na gama 10.5.1.0/24 e o que comunica com a Gateway de Lisboa atribui endereços na gama 10.5.5.0/24.

Quanto ao **encaminhamento** necessário efetuar para que, quando o túnel VPN fosse estabelecido, o Roadwarrior conseguisse comunicar com a Gateway de Lisboa, foi necessário, em todas as máquinas, desativar a firewall (**systemctl stop firewalld**) e efetuar o comando **echo 'net.ipv4.ip_forward = 1' >> /etc/sysctl.conf**, o qual ativa o encaminhamento dos pacotes IP. Foram ainda necessários outros comandos adicionais que

serão descritos na secção 4.3, quando referirmos os procedimentos de implementação de cada um dos intervenientes do projeto.

# 4. Implementação

Nesta secção iremos explicar em pormenor todos os detalhes que tornaram possível implementar as funcionalidades descritas nas secções anteriores.

## 4.1 Autoridade de Certificação Privada

Para que fosse possível gerar os certificados que seriam usados pelo roadwarrior, gateway de Coimbra e de Lisboa foi criada uma Autoridade de Certificação Privada, utilizando OpenSSL, seguindo os seguintes comandos:

- **openssl genrsa -out CertAuth.key 2048 -des3** - criação de uma chave de 2048 bits (RSA) encriptada com o algoritmo 3DES
- **openssl req -new -key CertAuth.key -out CertAuth.csr** - criação do certificate signing request
- **openssl x509 -req -days 3650 -in CertAuth.csr -out CertAuth.crt -signkey CertAuth.key** - criação de um certificado *self-signed*, visto que a nossa autoridade de certificação é a entidade maior e como tal tem que ser esta a assinar o seu próprio certificado. Importante ainda referir que a o certificado da autoridade foi criado com uma validade de 10 anos (-days 3650)

Como iremos ver mais em detalhe, na secção 4.4, a autoridade de certificação irá trabalhar em conjunto com o OCSP para verificar a validade dos certificados apresentados pelo roadwarrior.

## 4.2 Certificados

Através da utilização da Autoridade de Certificação Privada criada foi depois possível gerar os certificados do Roadwarrior, da Gateway de Coimbra e de Lisboa. Para que tal fosse possível foram utilizados os seguintes comandos:

- **sudo openssl genrsa -out coimbra.key 2048 -des3** - criação de uma chave de 2048 bits (RSA) encriptada com o algoritmo 3DES
- **sudo openssl req -new -key coimbra.key -out coimbra.csr** - criação do certificate signing request
- **sudo openssl ca -in coimbra.csr -cert CertAuth.crt -keyfile CertAuth.key -out apache.crt** - criação do certificado (neste caso, da Gateway de Coimbra) utilizando a Autoridade de Certificação Privada

Todos os certificados foram gerados pela dita Autoridade de Certificação Privada e fornecidos a cada um dos intervenientes do nosso projeto. Foi importante que todos fossem gerados na máquina virtual de Coimbra para que ficassem no ficheiro **index.txt**, visto que este ficheiro serve como uma espécie de base de dados, onde estará um registo dos certificados criados por esta autoridade, o estado dos mesmos (válido ou revogado) e o seu número de série, a partir do qual cada um dos certificados será identificado.

De forma a revogar um certificado foi utilizado o comando **openssl ca -keyfile CertAuth.key -cert CertAuth.crt -revoke revwarrior.crt**

## 4.3 Criação dos intervenientes do nosso projeto

### 4.3.1 Roadwarrior

A criação do Roadwarrior foi feita com base nos ficheiros de configuração-exemplo fornecidos pelo openvpn, sendo necessário inicialmente, neste ficheiro, associar o certificado da Autoridade de Certificação Privada, o certificado do Roadwarrior e a chave privada do mesmo. Foi também importante adicionar a linha que permite que este se ligue ao servidor de Coimbra remotamente: **remote 10.5.0.1 1194.** Em todos os ficheiros de configuração foi utilizada a interface **tun** que é adequada para routing e foram utilizadas as diretivas **user nobody** and **group nobody** para melhorar a segurança. O protocolo de comunicação escolhido foi **udp**. Foram ainda adicionadas as linhas **remote-cert-tls server** e **tls-auth /etc/pki/CA/ta.key 1**, as quais fazem parte do processo de configuração do OCSP, em conjunto com outro conjunto de linhas que iremos adicionar no ficheiro de configuração do servidor de Coimbra, como iremos ver de seguida.

### 4.3.2 Gateway de Coimbra

Na Gateway de Coimbra existem dois ficheiros, sendo que um se destina ao servidor que se liga diretamente ao roadwarrior e o outro serve para estabelecer ligação com Lisboa. No ficheiro relativo ao **servidor que comunica com o roadwarrior**, começámos por especificar o endereço de IP no qual o servidor estará à escuta (local 10.5.0.1) e o porto associado (port 1194). Foram depois associados os certificados da Autoridade de Certificação Privada, da Gateway de Coimbra e a chave privada da mesma. Foi ainda definida a topologia subnet e definida a gama de endereços IP na qual o OpenVPN iria fornecer endereços (server 10.5.1.0 255.255.255.0). Para que o roadwarrior tivesse conhecimento das restantes redes do nosso cenário, foi necessário efetuar o comando push route da rede interna de Coimbra, de Lisboa, de ligação de Coimbra com Lisboa e da rede do túnel VPN que liga Coimbra a Lisboa. Para que depois fosse possível configurar o servidor para contactar o OCSP, foi necessário definir as linhas que se seguem, de forma a que o script criado seja executado:

**script-security 2**
**tls-verify /etc/pki/CA/check_ocsp.sh**
**tls-auth /etc/pki/CA/ta.key 0 # This file is secret**

Por fim, foi ainda utilizado um plugin que nos permitiu executar um ficheiro que irá tratar da Two-Factor Authentication, através do comando **plugin usr/lib64/openvpn/plugins/ openvpn-plugin-auth-pam.so /etc/pam.d/openvpn2** à configuração do servidor

No ficheiro que configura o **servidor que efetua a comunicação entre Coimbra e Lisboa**, voltamos a definir o endereço IP no qual este estará à escuta (local 10.5.2.1) e respetivo porto (port 1194). De seguida, definimos os ficheiros dos certificados da Autoridade de Certificação, do da Gateway de Coimbra e a chave privada da mesma. Foi definida mais uma vez a topologia subnet e configurado o servidor para fornecer endereços na gama 10.5.5.0/24, com o comando **server 10.5.5.0 255.255.255.0**. Foram depois indicadas ao cliente quais as redes que se encontram por detrás do servidor, sendo estas a rede interna de Coimbra, a rede interna de comunicação entre o roadwarrior e Coimbra e a

rede do túnel VPN (**push "route 10.5.4.0 255.255.255.0", push "route 10.5.0.0 255.255.255.0", push "route 10.5.1.0 255.255.255.0").**

Por fim, para que o roadwarrior conseguisse estabelecer ligação com a rede interna de Lisboa foi necessário criar um ficheiro com o Common Name do cliente Lisboa na diretoria ccd, introduzindo no interior do mesmo o comando **iroute 10.5.8.0 255.255.255.0** e configurando, no ficheiro do servidor, as linhas **client-config-dir /etc/openvpn/ccd** e **route 10.5.8.0 255.255.255.0.** O comando iroute controla o encaminhamento do servidor OpenVPN para os clientes remotos, enquanto que o comando route controla o encaminhamento do kernel para o servidor openVPN.

### 4.3.3 Gateway de Lisboa

Esta gateway foi configurada como sendo um cliente que se liga ao servidor de Coimbra. Deste modo, indicámos o endereço IP remoto ao qual esta se deveria ligar e o respetivo porto (remote 10.5.2.1 1194) e de seguida configurámos quais os certificados do cliente e da autoridade de certificação e qual a chave privada do cliente Lisboa.

## 4.3 OCSP

O servidor OCSP foi criado e executado na máquina virtual de Coimbra, estando este associado ao endereço de IP da interface da rede interna de Coimbra. Para que fosse possível configurar o mesmo, utilizámos um script (check_ocsp.sh), o qual irá ser executado quando o servidor de Coimbra for executado, sendo neste script indicado qual o endereço de IP e o porto onde o servidor vai estar a correr e onde são indicadas e efetuadas as diversas verificações quanto ao estado dos certificados. Antes disso, é necessário colocar o servidor OCSP a correr com o comando **openssl ocsp -index index.txt -port 8080 -CA CertAuth.crt -rsigner CertAuth.crt -rkey CertAuth.key -resp_text** , que irá dizer qual a Autoridade de Certificação utilizada e qual o ficheiro index.txt que deve ser verificado para consultar o estado dos certificados. Desta forma, se o cliente apresentar um certificado que não tenha sido revogado e que tenha sido fornecido pela Autoridade de Certificação privada, este poder-se-á ligar ao servidor, caso contrário a ligação não será estabelecida.

## 4.4 Autenticação do Roadwarrior

Para além da verificação dos certificados efetuada pelo servidor OCSP, é ainda utilizada uma camada de proteção adicional, sendo esta fornecida pela Two-Factor Authentication, sendo que o roadwarrior tem que fornecer o seu nome de utilizador e palavra-passe, a qual consiste na agregação da palavra-passe com um código temporário fornecido pela aplicação móvel *Google Authenticator.* Isto foi possível através da criação de um ficheiro na diretoria /etc/pam.d/ com o nome **openvpn,** que irá ter as indicações do que deve ser tido em conta para realizar a autenticação do roadwarrior. De seguida foi necessário alterar o ficheiro de configuração do servidor para que este corresse o plugin de autenticação com o ficheiro criado, tendo sido acrescentadas as linhas **script-security-2** e **plugin openvpn-plugin-auth-pam.so openvpn.** Foi também necessário alterar o ficheiro de configuração do cliente, para que este tenha que fornecer o seu nome de utilizador e a palavra-passe, através da linha **auth-user-pass.**

De seguida foi instalado o *Google Authenticator* através do comando **yum install google-authenticator**. Depois foi efetuado o setup do mesmo, executando o comando **google-authenticator.** Utilizando a aplicação do Google Authenticator no smartphone, foi feito scan do QR code apresentado na linha de comandos, ficando assim com um código a ser gerado de 30 em 30 segundos nesta mesma aplicação. Antes de prosseguirmos com o setup, verificámos se o código funcionava corretamente, colocando o código apresentado no smartphone na linha de comandos. Após esta etapa ser concluída com sucesso, terminámos a configuração respondendo com N, Y e N às perguntas apresentadas.

# 5. Testes efetuados

## 5.1 Comunicação entre máquinas virtuais

De forma a verificar que as máquinas virtuais adjacentes comunicam entre si, foram efetuados ping's entre as interfaces internas das mesmas, tendo sido recebidas as respostas aos pings como seria esperado. Logo, a partir do roadwarrior conseguimos pingar Coimbra e vice-versa (10.5.0.2 consegue pingar 10.5.0.1 e 10.5.0.1 consegue pingar 10.5.0.2) e a partir de Coimbra conseguimos pingar Lisboa e vice-versa (10.5.2.1 consegue pingar 10.5.2.2 e 10.5.2.2 consegue pingar 10.5.2.1).

## 5.2 Comunicação do roadwarrior com Coimbra e Lisboa

Para comprovar que o roadwarrior consegue comunicar tanto com a Gateway de Coimbra como de Lisboa através do túnel, foram executados os ficheiros de configuração do roadwarrior, servidores da Gateway de Coimbra e cliente de Lisboa e foram efetuados pings para a rede interna de Coimbra (10.5.4.1) e de Lisboa (10.5.8.1) com sucesso. Foi ainda utilizado o wireshark como podemos ver nas figuras 2 e 3 para comprovar que os pings eram recebidos corretamente e que, escutando na interface tun0, era possível observar informação detalhada sobre os pacotes enviados, mas, se escutássemos na interface enp0s8, estes estavam encriptados.

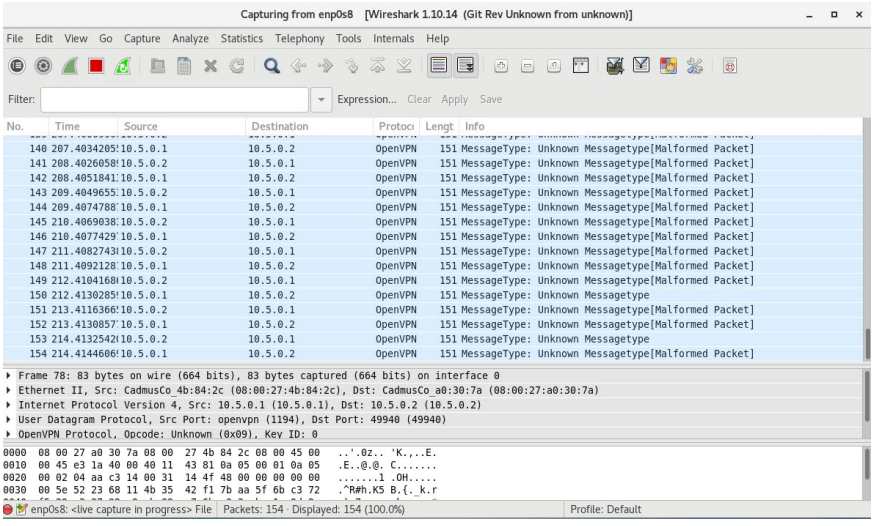


*Figura 2 - Wireshark à escuta na interface enp0s8*

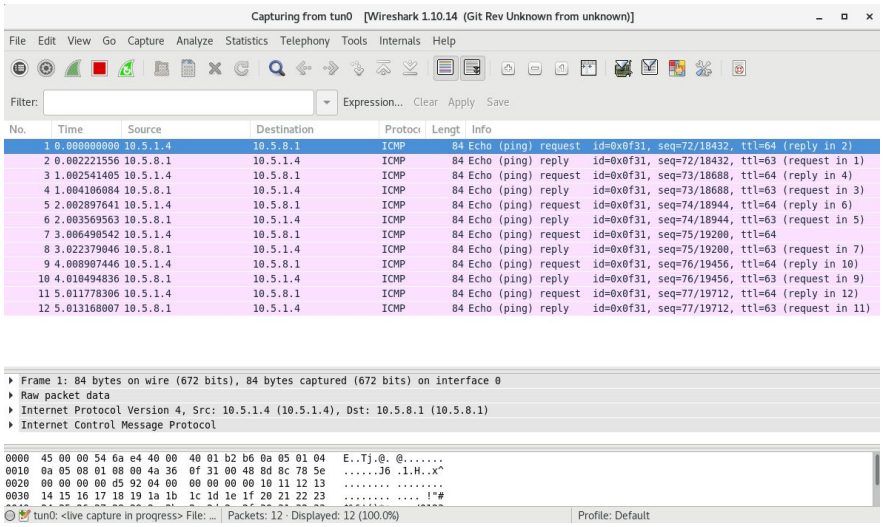


*Figura 3 - Wireshark à escuta na interface tun0*

## 5.3 Comunicação Gateway-to-Gateway

Tal como aconteceu na secção anterior, entre as Gateways de Lisboa e de Coimbra também foi possível efetuar os pings corretamente e foram efetuados testes utilizando o wireshark, obtendo resultados de sucesso semelhantes aos da secção anterior.

## 5.4 Verificação dos certificados apresentados pelo roadwarrior

Foram criados dois certificados para o roadwarrior, sendo que um deles se encontra válido e o outro foi revogado. Tentando efetuar a ligação a Coimbra com o certificado válido, esta é concluída com sucesso. Por outro lado, se tentarmos utilizar o certificado que se encontra revogado, a ligação não é estabelecida.

## 5.5 Autenticação do roadwarrior utilizando 2FA

Foi executado o ficheiro de configuração do roadwarrior e do servidor de Coimbra, sendo depois inserido o respetivo nome de utilizador e palavra-passe do mesmo (palavra-passe concatenada com a One-Time Password fornecida pelo Google Authenticator). Ao inserir as credenciais corretas, o login seria efetuado e a ligação é estabelecida, caso contrário a ligação é rejeitada.

# Conclusão

A realização deste trabalho permitiu compreender como deve ser configurado um cenário de comunicação segura utilizando um VPN (no nosso caso, o OpenVPN), para ser utilizado tanto num cenário remoto (Roadwarrior) ou numa comunicação Gateway-to-Gateway. Compreendemos também a importância de possuir um servidor OCSP para garantir que apenas são estabelecidas ligações com clientes que forneçam certificados válidos e que sejam fornecidos pela autoridade de certificação privada. Por fim, ao utilizar Two-Factor Authentication é garantida uma camada de segurança adicional e,

como sabemos, nos tempos atuais, nos quais existem ataques constantes à segurança dos utilizadores, toda a segurança adicional é bem vinda.

# Bibliografia

**[1]**https://openvpn.net/community-resources/how-to/#starting-up-the-vpn-and-testing-for-initial-connectivity