Universidade de Coimrba

• U  C •

Universidade de Coimbra

Segurança e Tecnologias de Informação

Trabalho Práctico I

Gonçalo Santos
2012140860 - gdsantos@student.dei.uc.pt

Ana Inês Mesquita Fidalgo
2013134819 - aimf@student.dei.uc.pt

12 de Março de 2017

Conteúdo

Capítulo 1

Introdução

Este projecto foi realizado no âmbito da cadeira Segurança em Teconologias de Informação, STI, inserida no plano de estudos do Mestrado em Engenharia Informática da Universidade de Coimbra, lecionada pelos Professores Doutores João Paulo da Silva Machado Garcia Vilela e António Jorge da Costa Granjal, no ano lectivo de 2016/2017.

O projecto acima referido tem como objetivo explorar as tecnologias VPN e OCSP, que garantem ao controlo de acessos através de certificados, privacidade e segurança.

Capítulo 2

Arquitectura

Este projecto está dividido em três partes, o cliente Road Warrior, o servidor Coimbra e o cliente Lisboa. Tanto o servidor Coimbra como o cliente Lisboa têm ainda uma rede interna. Consequentemente foram criadas três máquinas de CentOS 6.8 para realizar as diversas rotas pedidas. Estas máquinas estão ainda ligadas por várias redes criadas manualmente:

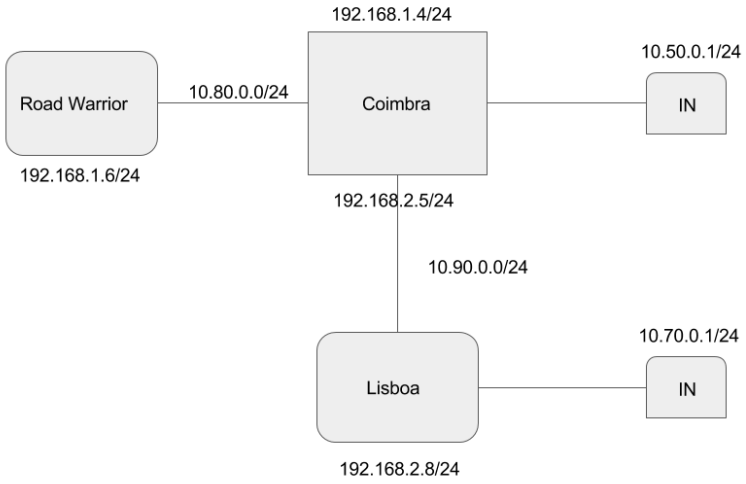

Fig. 1 Mapa da Rede

2.1 Simulação da Arquitectura

Para simular a arquitetura do sistema, tal como já tinha sido referido anteriormente, foram criadas três maquinas virtuais correspondentes às máquina apresentadas na figura 1, onde se criaram os seguintes IPs fixos:

	IP	Máscara
Gateway Road Warrior	192.168.1.6	255.255.255.0
Tunnel OpenVPN RR-L	10.80.0.0	255.255.255.0
Gateway Coimbra	192.168.1.4	255.255.255.0
Gateway Coimbra-Lisboa	192.168.2.5	255.255.255.0
Gateway Lisboa	192.168.2.8	255.255.255.0
IN Coimbra	10.50.0.1	255.255.255.0
IN Lisboa	10.70.0.1	255.255.255.0
Tunel OpenVPN C-L	10.90.0.0	255.255.255.0

Tabela 2.1: IPs Utilizados

Capítulo 3

Autoridade de Certitificados

Neste trabalho foram gerados certificados tanto para Coimbra, como para Lisboa e Road Warrior. A validade dos mesmos é posteriormente verificada por OCSP, sendo estes emitidos ou revogados pela Autoridade de Certificados (CA).

3.0.1 Servidor Coimbra

- Criar Chave: *openssl genrsa -out coimbra.key 1024 -des3*
- Criar o Request: *openssl req -new -key user.key -out coimbra.csr*
  - Country: PT
  - State: Coimbra
  - City: Coimbra
  - Organization name: UC
  - Org. Unit Name: DEI
  - Common Name: Coimbra
  - E-mail: coimbra@dei.uc.pt
- Criar Certificado Assinado pela CA: *openssl ca -in coimbra.csr -cert ca.crt -keyfile ca.key -out coimbra.crt*

3.0.2 Cliente Road Warrior

- Criar Chave: *openssl genrsa -out roadwarrior.key 1024 -des3*
- Criar o Request: *openssl req -new -key roadwarrior.key -out roadwarrior.csr*
  - Country: PT
  - State: Coimbra
  - City: Coimbra
  - Organization name: UC
  - Org. Unit Name: DEI
  - Common Name: Road Warrior
  - E-mail: roadwarrior@dei.uc.pt
- Criar Certificado Assinado pela CA: *openssl ca -in roadwarrior.csr -cert ca.crt -keyfile ca.key -out roadwarrior.crt*

3.0.3 Cliente Lisboa

- Criar Chave: *openssl genrsa -out lisboa.key 1024 -des3*
- Criar o Request: *openssl req -new -key lisboa.key -out lisboa.csr*
  - Country: PT
  - State: Coimbra
  - City: Coimbra
  - Organization name: UC
  - Org. Unit Name: DEI
  - Common Name: Lisboa
  - E-mail: lisboa@dei.uc.pt
- Criar Certificado Assinado pela CA: *openssl ca -in lisboa.csr -cert ca.crt -keyfile ca.key -out lisboa.crt*

Capítulo 4

Virtual Private Network

Uma Virtual Private Network permite que um cliente se ligue a outro utilizador através da rede pública e transferir informação mas de forma segura. Neste trabalho foi utilizada a tecnologia OpenVPN para realizar as ligações Road Warrior-Coimbra e Coimbra-Lisboa.

4.1 Open Virtual Private Network

Na máquina Road Warrior foi criada manualmente a rede com o IP 192.168.1.6, sendo que esta máquina contém uma configuaração do tipo cliente com o porto 1194. Na máquina de Coimbra, foram criados três redes. Uma para a rede interna de Coimbra, 10.50.0.1, outra para o IP 192.168.1.4 e outra para 192.168.2.5. Estas duas últimas redes correspondem ao endereço local dos dois servidores criados em Coimbra.

Foram criados dois ficheiros de configuração do tipo servidor. A primeira configuração contém o IP 192.168.1.4, no porto 1194 onde é criado o tunel com o IP 10.80.0.0, por onde é realizada a ligação com o Cliente Road Warrior. O segundo servidor, com o IP local 192.168.2.5, foi criado o tunel VPN com o IP 10.90.0.0 que permite realizar a rota Coimbra-Lisboa.

No cliente Lisboa foram criadas suas redes, uma para a sua gateway, com o IP 192.168.2.8, e outra para a sua rede interna, com o IP 10.70.0.1.

4.2 Push Routes Necessários

Para que Road Warrior e Lisboa soubessem quais as redes que existiam, foi necessário realizar vários push routes das redes desconhecidas em cada servidor na Máquina Coimbra.

4.2.1 Servidor Coimbra 1

- push "route 10.50.0.0 255.255.255.0"
- push "route 10.70.0.0 255.255.255.0"
- push "route 192.168.2.0 255.255.255.0"
- push "route 10.90.0.0 255.255.255.0"

4.2.2 Servidor Coimbra 2

- push "route 10.50.0.0 255.255.255.0"
- push "route 10.80.0.0 255.255.255.0"
- push "route 192.168.1.0 255.255.255.0"

Com estas configurações já era possível realizar ping do cliente Road Warrior para o servidor Coimbra e do cliente Lisboa para o servidor Coimbra. Para conseguirmos dar ping do Road Warrior até ao cliente Lisboa realizamos os seguintes passos:

- Criação de uma pasta ccd na directoria /etc/openvpn, onde foi criado um ficheiro com o nome do Common Name escolhido aquando da criação do certeficado do cliente Lisboa, neste caso, foi criado um ficheiro "Lisboa"onde está contida o seguinte comando:
  - *iroute 10.70.0.0 255.255.255.0*
- Posteriormente foi adicionado ao ficheiro de configuração Coimbra-Lisboa os seguintes comandos:
  - client-config-dir ccd
  - *route 10.70.0.0 255.255.255.0*

Com isto foi possível realizar então ping do Servidor 2 de Coimbra para a rede interna de Lisboa e consequentemente do cliente Road Warrior para a rede interna de Lisboa.

Para a realização do ping entre as rotas foi ainda necessário desactivar a firewall com o seguinte comando:

- service iptables stop

Para simular estas configurações foram utilizadas variâncias do seguinte comando, neste caso para iniciar o servidor Coimbra-RoadWarrior:

- *openvpn –config /etc/openvpn/server.conf*

Capítulo 5

Two-factor User Authentication

Quando o cliente Road Warrior se conecta à gateway de Coimbra, este é autenticado por dois mecanismos:

- Username e password válida;
- One-time password;

Esta password é gerada através do algoritmo TOTP, Time-based One-time Password, que cria uma chave secreta partilhada entre o cliente e a gateway, sendo esta chave apenas válida durante um curto espaço de tempo.

Para gerar esta password foi utilizada a aplicação *Google Authenticator*. A realização de ping entre cliente e servidor apenas será autorizada caso o cliente introduza as credenciais válidas.

Para implementar esta funcionalidade seguimos apenas um tutorial online, instalando também a versão android do *Google Authenticator*.

Capítulo 6

Online Certificate Status Protocol

O OCSP é um protocolo Internet usado para obter a revogação de um certificado X.509. Para que o cliente Road Warrior realize ping para o servidor Coimbra, a gateway do mesmo contacta o OCSP para a validação do certeficado do cliente Road Warrior. Para realizar esta funcionalidade foram realizados os seguintes passos:

- Realização de download do script ocsh.sh, onde foram realizadas as seguintes alterações:
  - *ocsp_url = "http://192.168.1.4:1194"*
  - *issuer = "/etc/pki/CA/ca.crt"*
  - *verify = "/etc/pki/CA/ca.crt"*
- Geração da chave ta.key no servidor Coimbra através do comando:
  - openvpn –genkey –secret ta.key
- Copiar esse ta.key para a máquina Road Warrior.
- Alteração do ficheiro de configuração do servidor Coimbra:
  - script-security 2
  - tls-verify /etc/openvpn/my_keys/ocsp.sh

  - tls-auth ta.key 0

- Alteração do ficheiro de configuração cliente do Road Warrior:
  - *remote-cert-ku server*
  - *tls-auth ta.key 1*
- Inicialização do OCSP
  - *openssl ocsp -index index.txt -CA ca.crt -rsigner ca.crt -rkey ca.key -port 1194 -resp_text*
- Revogação dos certificados
  - openssl ca -revoke newcerts/00.pem -keyfile ca.key -cert ca.crt

Capítulo 7

Testes

	Gateway Road Warrior	Gateway 1 Coimbra	Gateway 2 Coimbra	Rede Interna Coimbra	Gateway Lisboa	Rede Interna Lisboa	Openvpn C-L	Openvpn R-C
Cliente Road Warrior		Sim	Sim	Sim		Sim	Sim	
Servidor Coimbra	Sim			Sim	Sim	Sim	Sim	Sim
Cliente Lisboa		Sim	Sim	Sim		Sim	Sim	Sim

Tabela 7.1: Tabela das Rotas Estabelecidas

Capítulo 8

Anexos

- https://openvpn.net/index.php/open-source/documentation/howto.html#scope
- http://www.letsvirt.com/2016/09/24/how-to-configure-2fa-using-google-authenticator-rhelcent-os/
- https://github.com/OpenVPN/openvpn/blob/master/contrib/OCSP_check/OCSP_check.sh