Grupo T48

Bernardo Castiço ist196845

Hugo Rita ist196870

Pedro Pereira ist196905

Build Infrastructure

I. Business context

O tema do projeto é construir um serviço seguro denominado TheCork que permita aos seus usuários reservarem mesas para refeições nos restaurantes que planeiem ir comer.

II. Infrastructure overview

VM1 dos clientes: Client_T48 | IP: 192.168.0.100/24 que liga à Firewall_T48.

VM2 que funciona como Firewall: Firewall_T48 | IP: 192.168.0.10/24 para ligar à VM1 Client_T48 & IP: 192.168.1.254/24 para ligar à VM3 WebServerCork_T48 & IP: 192.168.2.254 para ligar à Database_T48.

VM3 que corre a aplicação: WebServerCork_T48 | IP: 192.168.1.1/24 que liga à Firewall_T48.

VM4 da base de dados: Database_T48 | IP: 192.168.2.4/24 que liga à Firewall_T48.

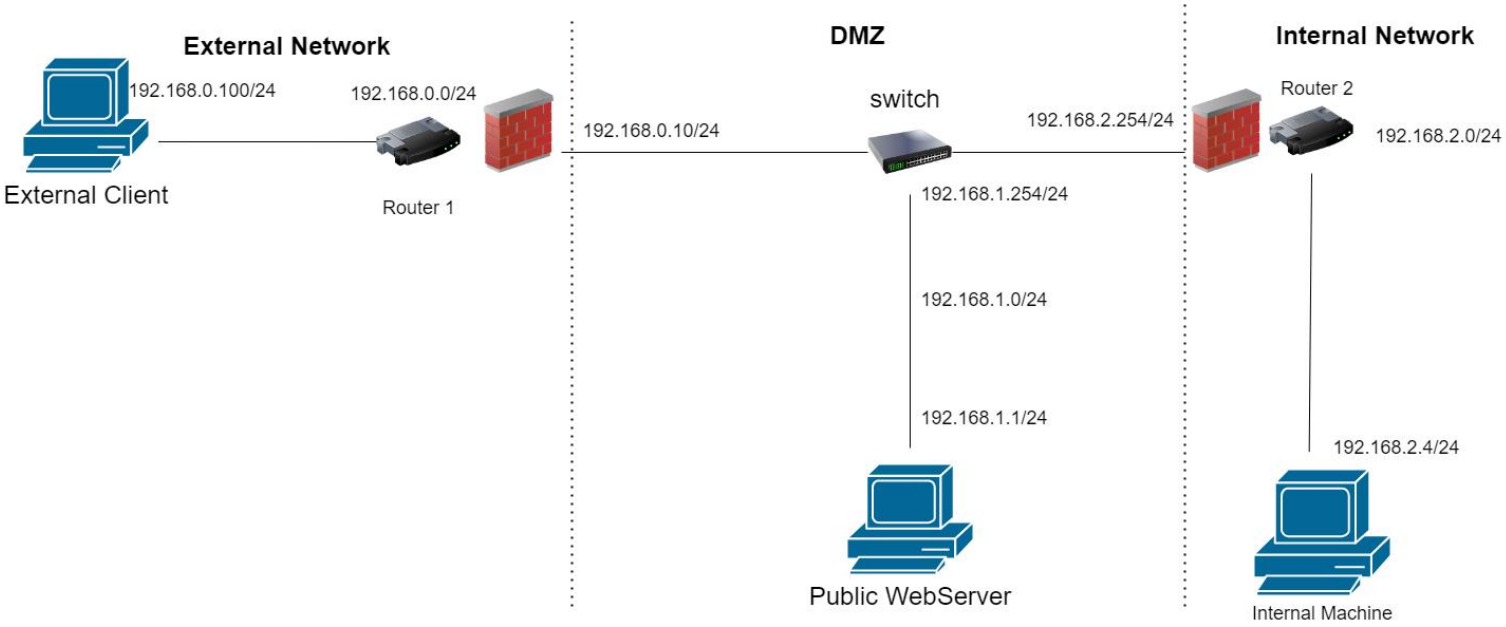
Na página em baixo temos uma imagem que mostra a nossa infraestrutura visualmente, no entanto, vamos também explicá-la agora por palavras.

A virtual machine responsável pelos pedidos dos clientes tem o nome de Client_T48 e a virtual machine da Firewall que se chama Firewall_T48 estão ligadas na mesma network através do sw-1.

Por sua vez, a virtual machine WebServerCork_T48 e a virtual machine Firewall_T48 também estão ligadas na mesma network, mas desta vez através do sw-2.

Por fim, a virtual machine Database_T48 e a virtual machine Firewall_T48 também estão ligadas na mesma network, mas desta vez através do sw-3.

A aplicação permite ao utilizador usufruir das seguintes 4 operações sobre as suas reservas: Create, Read, Update e Delete.



Firewall rules:

- A firewall apenas aceita pedidos ssh (port22) e http (port80) vindos da VM Client_T48.

- Todas as conexões http (port80) da VM Client_T48 são redirecionadas para a VM WebServerCork_T48.

- Todas as conexões ssh (port22) da VM Client_T48 são redirecionadas para a VM Database_T48.

- Pedidos da VM Database_T48 só são aceites se forem ssh (port22).

- A VM WebServerCork_T48 só pode começar conexões com a Internal Machine.

- A Internal Machine não pode começar conexões.

III. Secure Communications

What existing security protocol is being used?

O protocolo de segurança que decidimos usar é o TLS. Escolhemos este protocolo porque este ser um protocolo usado mundialmente para garantir privacidade e segurança nas comunicações através da internet.

Who is communicating?

O cliente e o webServer comunicam entre si e são as mensagens trocadas por ambos que pretendemos proteger.

What keys exist and how are they distributed?

Nas mensagens enviadas pelo cliente para o webServer, o cliente cifra as mensagens com a chave publica do webServer e o webServer decifra as mensagens com a sua chave privada.

Por outro lado, nas comunicações começadas pelo webServer e que tenham como destino o cliente, o webServer irá cifrá-las com a chave publica do cliente e o cliente irá decifrar as mensagens com a sua chave privada.

Como estamos a usar cifra de chave publica/privada as chaves publicas são conhecidas por todos. Por sua vez, as chaves privadas são conhecidas por quem as detém.

Ciframos e decifamos as mensagens usando o algoritmo RSA.

IV. Security Challenge

(i) TheCork has personal information about each customer, which needs to be kept private. There is a need for an authentication server that can support both the app level and the back-office level, to avoid illegitimate users to get access to restaurant's agenda / customer data.