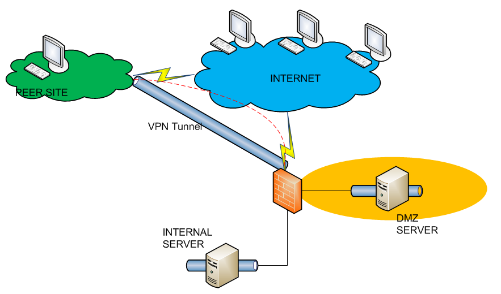
**O que é DMZ?**

Uma DMZ é uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável, normalmente a internet. Quaisquer dispositivos situados nesta área, isto é, entre a rede confiável (geralmente a rede privada local) e a rede não confiável (geralmente a Internet), está na zona desmilitarizada.

A função de uma DMZ é manter todos os serviços que possuem acesso externo (tais como servidores [HTTP](https://pt.wikipedia.org/wiki/HTTP), [FTP](https://pt.wikipedia.org/wiki/FTP), de correio eletrônico, etc.) junto em uma rede local, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um invasor. Para atingir este objetivo os computadores presentes em uma DMZ não devem conter nenhuma forma de acesso à rede local.

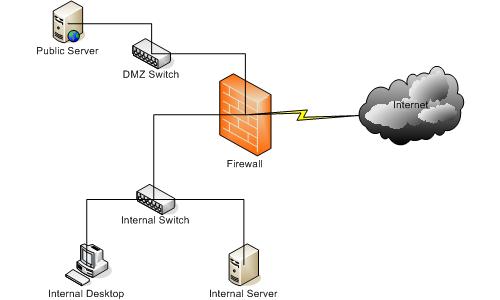
A configuração é realizada através do uso de equipamentos de firewall, que vão realizar o controle de acesso entre a rede local, a internet e a DMZ (ou, em um modelo genérico, entre as duas redes a serem separadas e a DMZ). Os equipamentos na DMZ podem estar em um switch dedicado ou compartilhar um switch da rede, porém neste último caso devem ser configuradas redes virtuais distintas dentro do equipamento, também chamadas de VLANs.



Tipos de DMZ

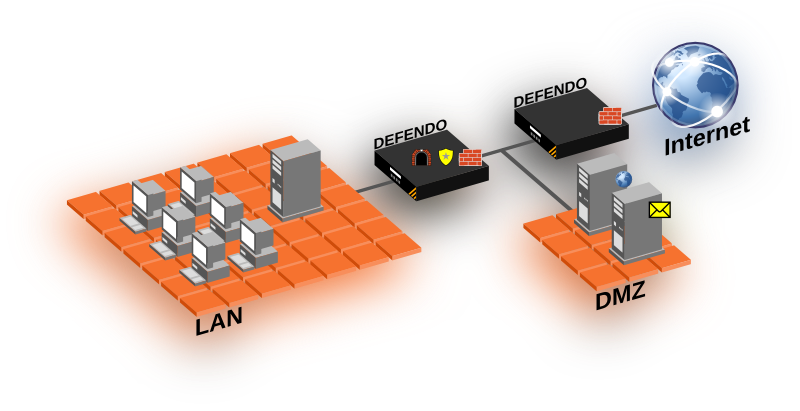
* Single Firewall

É a arquitetura apresentada na figura a baixo. Qualquer firewall com pelo menos 3 interfaces de rede pode formar uma arquitetura desse tipo. Neste caso, A primeira interface de rede conecta a firewall à internet através do ISP, a segunda interface forma a rede interna e a terceira interface é usada para criar a DMZ. Este tipo de arquitetura é considerado vulnerável devido ao facto da firewall ter que lidar com as requisições para a rede interna e para a DMZ, sendo um ponto óbvio de ataque na arquitetura de segurança da rede.



* Multiple Firewall

É a arquitetura mais segura quando se utiliza uma DMZ. Utiliza mais de uma firewall (geralmente duas), onde a primeira, também chamada de firewall exterior é utilizada para direcionar o tráfego da internet para a DMZ apenas, enquanto as outras são utilizadas para direcionar o tráfego da DMZ para a rede interna. Este tipo de arquitetura é a mais segura pois para que a rede interna seja comprometida, é necessário que as duas ou mais firewalls sejam comprometidas. Por isso, quando essa arquitetura é utilizada, é comum que se usem firewalls de fabricantes diferentes, pois é mais difícil que as falhas de segurança encontradas num equipamento de um fabricante sejam encontradas no equipamento de outro, tornando assim a rede mais segura e confiável



Bibliografia

<https://pt.wikipedia.org/wiki/DMZ_(computa%C3%A7%C3%A3o)>

<http://gigacom.servehttp.com/gct/index.php/2017/03/24/o-que-e-uma-dmz/>