FICHA TRABALHO 5

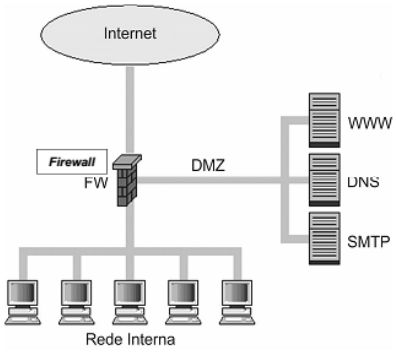
MODALIDADE:	Jovem + Digital	Não aplicável	
CURSO:	J+D 2/2026 Cibersegurança		
UFCD:	Cibersegurança Ativa	CÓDIGO UFCD:	9196
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Saber como utilizar uma DMZ (Zona Desmilitarizada)
- Saber como configurar DMZ nos routers

Uma rede DMZ (zona desmilitarizada), é uma sub-rede na infraestrutura de rede de uma organização localizada entre a rede interna protegida e uma rede não confiável (geralmente a Internet). A rede DMZ de uma organização contém serviços voltados ao público (websites, servidores DNS, emails, entre outros) e foi projetada para ajudar a proteger as redes internas.

Um conceito muito importante de frisar é que o DMZ é um conceito e não um hardware ou software.



Uma DMZ é projetada para fornecer serviços que pertencem a uma organização, mas são menos confiáveis ou mais expostos a comprometimentos. Exemplos de sistemas implementados com uma DMZ:

- Servidor da Web
- Servidor DNS
- Servidor de e-mail
- Servidor FTP

Estes sistemas devem ser acessíveis ao público. Uma DMZ permite que uma organização exponha funcionalidades voltadas para a Internet sem colocar em risco a rede interna com os outros sistemas.

Embora os sistemas localizados na DMZ possam ter acesso a sistemas internos e dados confidenciais – como os dados de clientes armazenados em base de dados e usados por aplicações web – as

conexões entre esses sistemas baseados na DMZ e os sistemas internos passam por inspeção adicional por forma a detetar conteúdo malicioso.

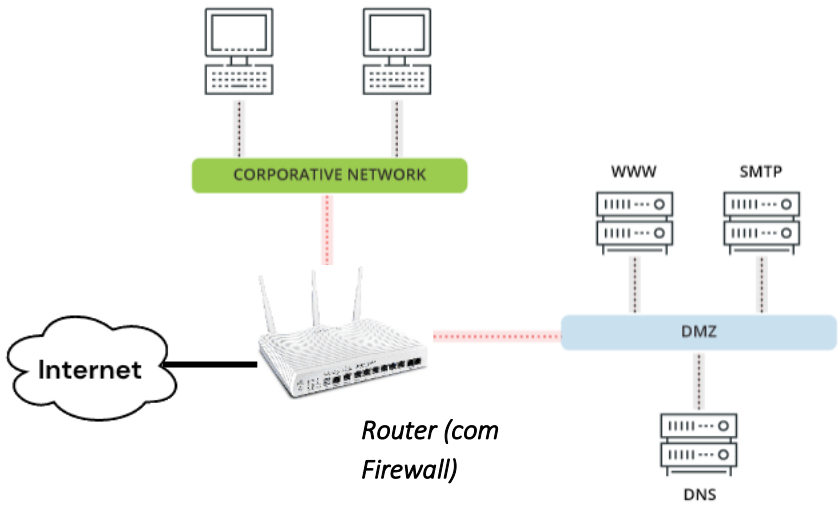
Um dos cenários mais frequentes de utilização de DMZ e firewalls, prende-se ao facto de queremos impedir todo e qualquer acesso de utilizadores localizados na Internet a recursos internos de uma rede privada de uma dada organização. No entanto, por que essa informação deseja disponibilizar informação para o exterior (exemplo: informação acessível por HTTP), é criada uma zona especial, designada por DMZ, onde se localizam servidores de acesso público. Da mesma forma, o tráfego do interior da rede para o exterior vai passar, também, por servidores localizados na DMZ. As máquinas localizadas nesta zona são designadas por bastion hosts, devemos estar devidamente preparadas para resistir a ataques. Na eventualidade de um ataque bem-sucedido a essas máquinas, os estragos ficarão limitados a elas, não enfrentando serviços internos da rede.

Casos Práticos de DMZ e Firewalls:

Exemplo 1 – Router com Firewall incorparada (sem firewalls dedicadas)

Neste exemplo, é apresentada uma arquitetura de acesso bastante simples, baseada na utilização de um router que executa as funções de firewall. Neste caso, o router executa, basicamente, funções de filtragem de pacotes, com base nos endereços IP de origem e destino, no protocolo utilizado, nos portos e nas interfaces.

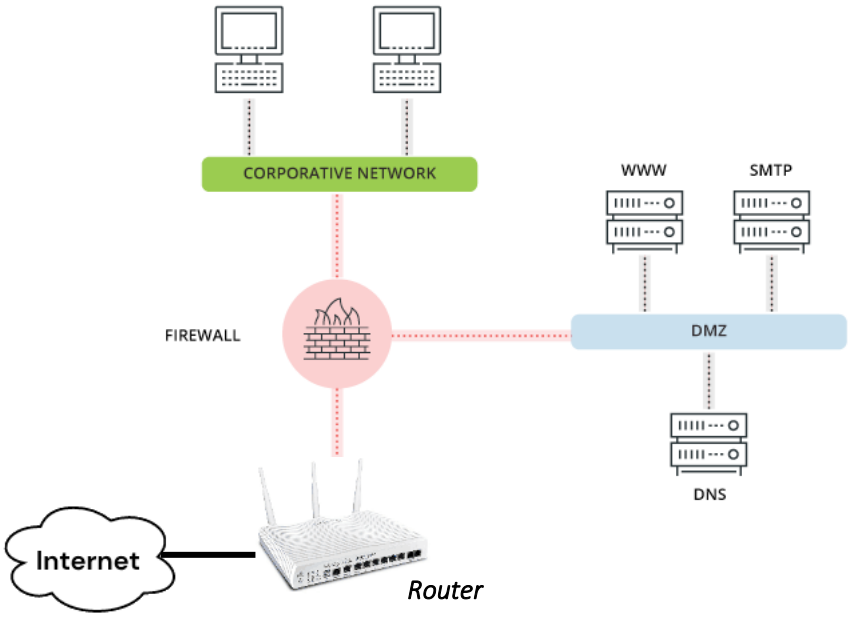
Neste exemplo pode observar-se que o Firewall possui 3 interfaces: uma para acesso à Internet, outra para acesso a uma sub-rede onde se encontra os serviços de acesso público (zona desmilitarizada - DMZ), e outra para acesso à rede privada.



A principal fragilidade dessa configuração reside no fato de a firewall constituir um ponto único de segurança. Na eventualidade de um utilizador não autorizado conseguir ultrapassar as proteções estabelecidas, toda a rede privada fica imediatamente exposta.

Exemplo 2 – Router com Firewall com firewall dedicada

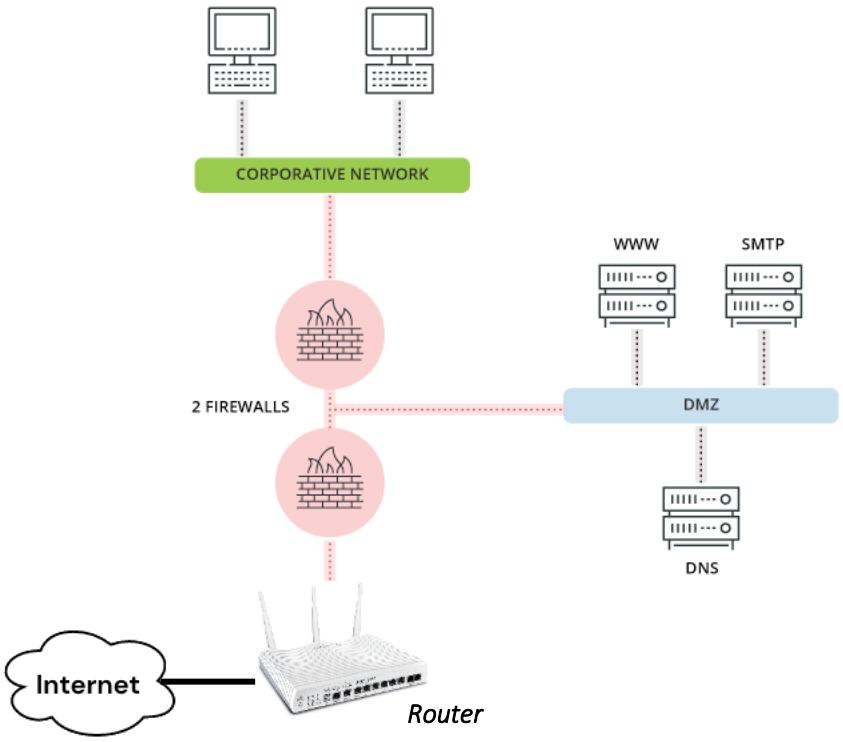
Neste caso, é apresentada uma arquitetura de acesso mais fiável, que resolve o problema do ponto único de segurança. Assim, o roteiro externo constitui um primeiro filtro de tráfego, deixando passar apenas os pacotes que obedecem às regras impostas pela sua lista de acesso.



O tráfego que consegue passar por este router é que chegará à firewall, que constitui a segunda linha de segurança e que implementa, normalmente, mecanismos de filtragem mais elaborados, como por exemplo, mecanismos ao nível de aplicação ou sistemas dinâmicos.

Exemplo 3 – Router com Firewall com várias firewalls estrategicamente implementadas

Neste caso, é apresentada uma configuração com diversas linhas de defesa, fornecendo um elevado nível de segurança. Como primeira linha de defesa é utilizado um router. Num segundo nível é utilizado uma firewall que dá acesso a uma DMZ e uma segunda firewall de entrada na rede privada. Estas duas firewalls deverão utilizar tecnologias diferentes (caso seja possível), pois desta forma, a utilização de um determinado mecanismo terá menos probabilidades de ser bem-sucedida em ambas as firewalls.



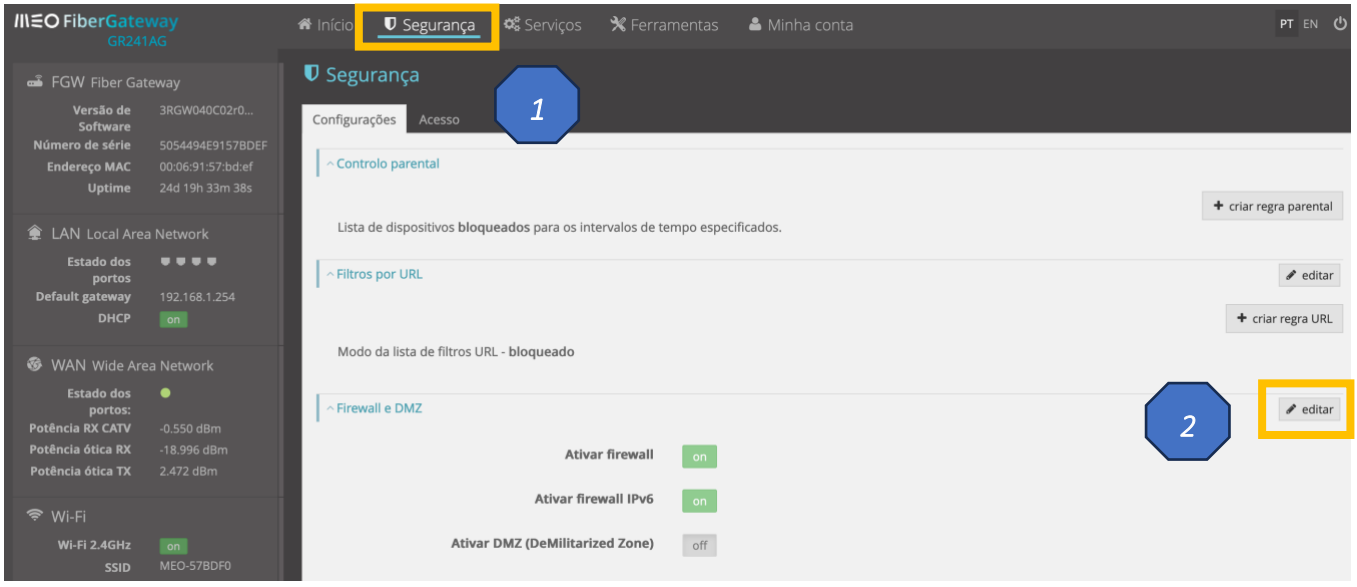
Como ativar DMZ nos routers?

Exemplo Router MEO FiberGateway GR241AG

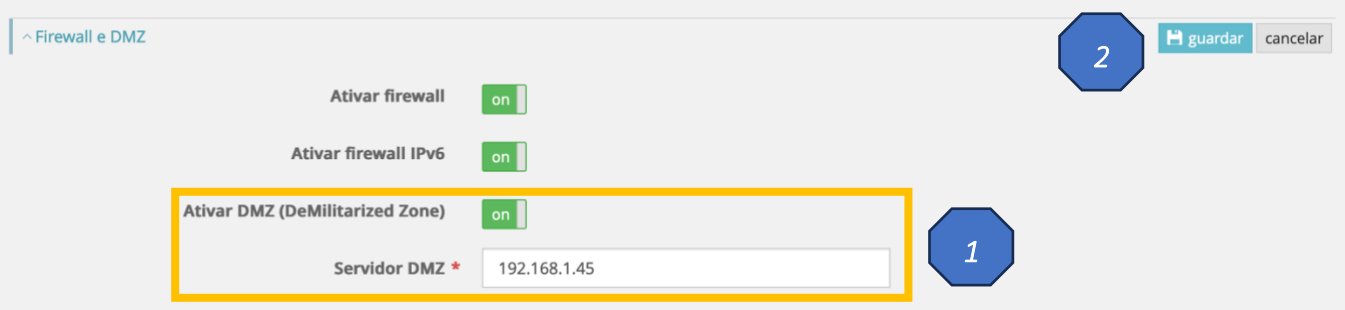
Passo 1 – Aceder ao endereço 192.168.1.254 (normalmente) e colocar os dados de acesso

Passo 2 – Na página inicial, mais especificamente, no canto direito da aplicação, temos os links rápidos para as configurações da aplicação. Uma dessas hiperligações é a "DMZ (zona desmilitarizada).

Também podem aceder no menu superior e clicar na opção Segurança:



Passo 3 – Após clicar no botão editar, ative a opção "Ativar DMZ (DeMilitarized Zone)" para ON e coloque o endereço IP a isolar da rede em causa.

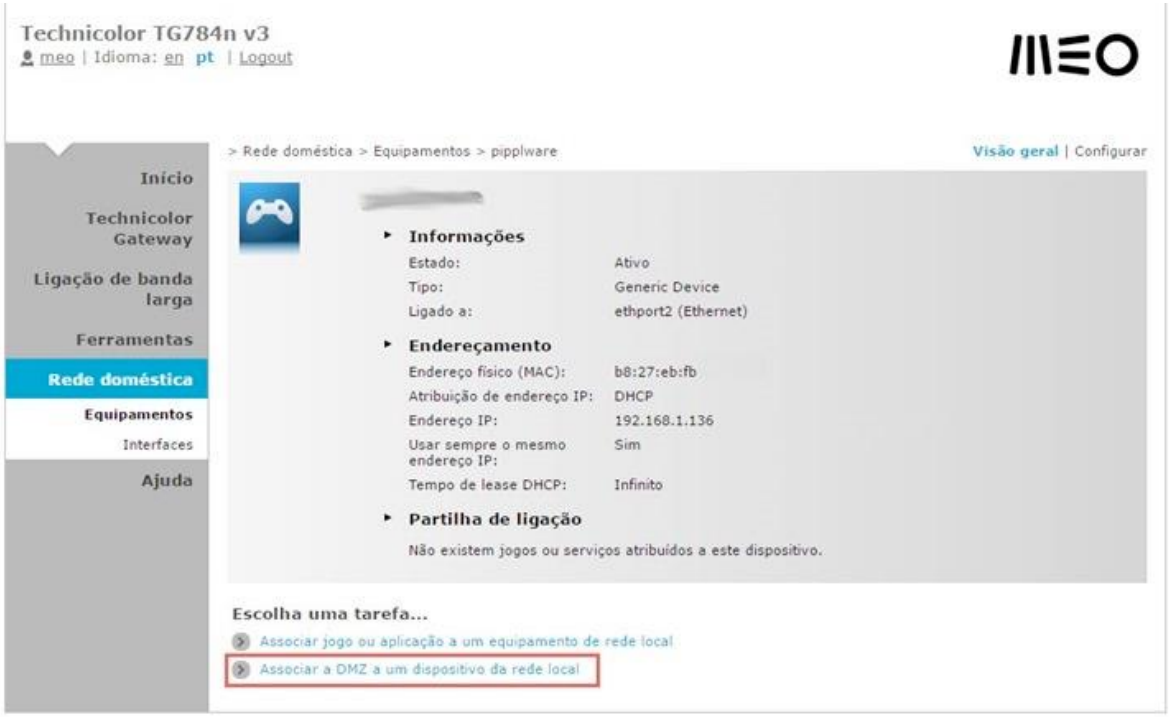


No final, não esquecer de gravar as alterações que foram modificadas.

Exemplo Router Technicolor tg784n

Passo 1 – Para acederem à página de administração do router devem, a partir de um PC ligado a rede, abrir um browser e colocar o endereço IP: 192.168.1.254 (normalmente).

Passo 2 – De seguida, devem ir ao lado esquerdo da página, encontrar o menu Rede Doméstica → Dispositivos e depois selecionar o dispositivo ao qual querem associar o endereço público do router MEO. Depois, carreguem em Associar a DMZ a um dispositivo da rede local

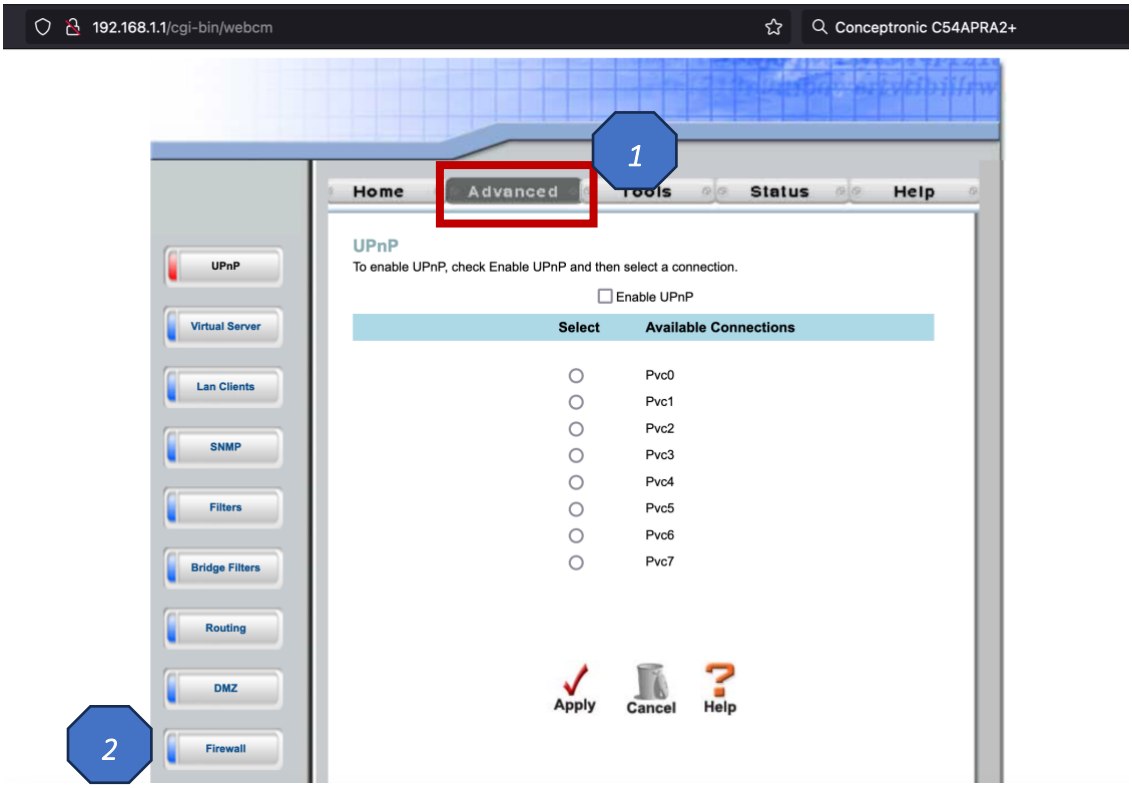


Passo 3 – Ao carregarem na opção anterior, vai ser apresentada a interface para colocar o endereço IP a isolar da rede em causa:

Exemplo Router Conceptronic C54APRA2+

Passo 1 – Para acederem à página de administração do router devem abrir um browser e colocar o endereço IP: 192.168.1.1 (segundo o manual de configuração).

Passo 2 – Na página principal, clicar no menu superior “Advanced” e de seguida a opção “DMZ”:



Passo 3 **–** Nesta página, deve ativar o DMZ clicando na opção Enabled e indicar o endereço IP. Não esqueça de gravar as alterações.