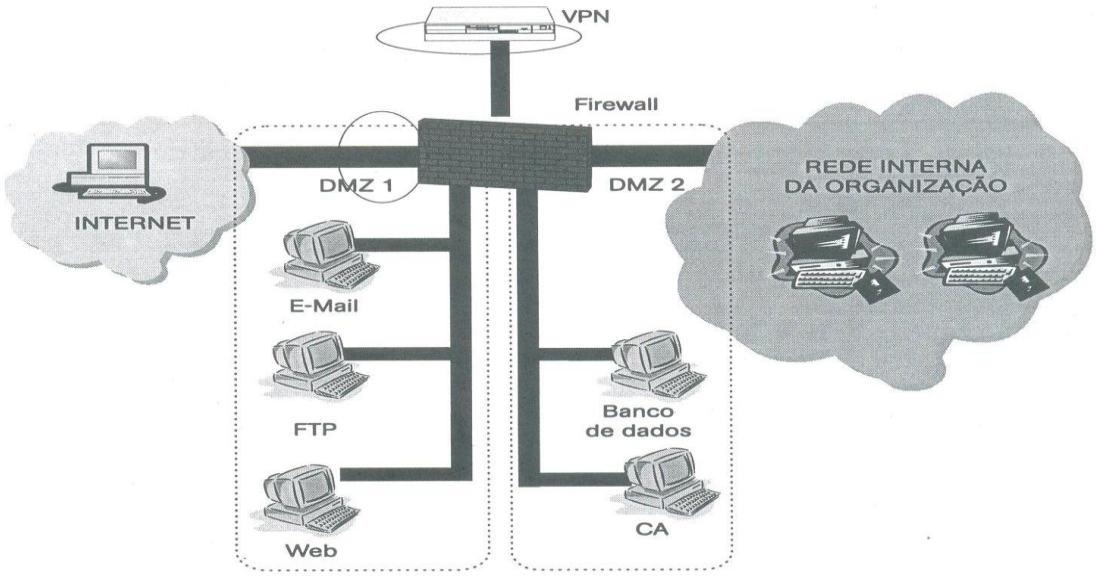
Prova A – Segurança de Rede

Seja a arquitetura de um firewall cooperativo como mostrado na figura seguinte:



Cinco níveis hierárquicos de defesa são definidos para auxiliar na definição das proteções para os três tipos de recursos num ambiente cooperativo (públicos, privados e internos): recursos públicos, disponibilizados para acesso via Internet e localizados na DMZ-1; recursos privados, disponibilizados para acesso via Internet e localizados na DMZ-2 e recursos internos, localizados na rede interna e acessados externamente via VPN. O firewall cooperativo é uma arquitetura de segurança que, em conjunto com esses cinco níveis, facilita a definição e a implementação das medidas de segurança necessárias. Uma DMZ é uma rede intermediária entre a rede corporativa e a Internet, criada pelos dispositivos de segurança de perímetro que serve também para disponibilizar recursos públicos ou privados aos usuários de uma corporação. CA é uma autoridade certificadora privada que a empresa utiliza.

1. Complete as proposições: (0,25 cada correta)

   - O primeiro nível de defesa corresponde a filtragem de pacotes TCP/IP pelo firewall, considerando que é um firewall filtro de pacotes.
   - O segundo nível de defesa consiste na autenticação do usuários para acesso aos serviços públicos na DMZ-1.
   - O acesso à DMZ-2 são tratadas por regras do firewall no terceiro nível de defesa.
   - Para o quarto nível de defesa devemos usar algum método de autenticação dos usuários para acesso aos serviços internos.
   - Firewalls internos ou IDS nos segmentos ou hosts (IDSs são mais utilizados, já que na organização da rede dada, já se poderia contar com um firewall potente, protegendo os elementos de rede no *backbone* - *os switches-routers* -

da rede), podem ser disponibilizados para proteger segmentos da rede interna da corporação.

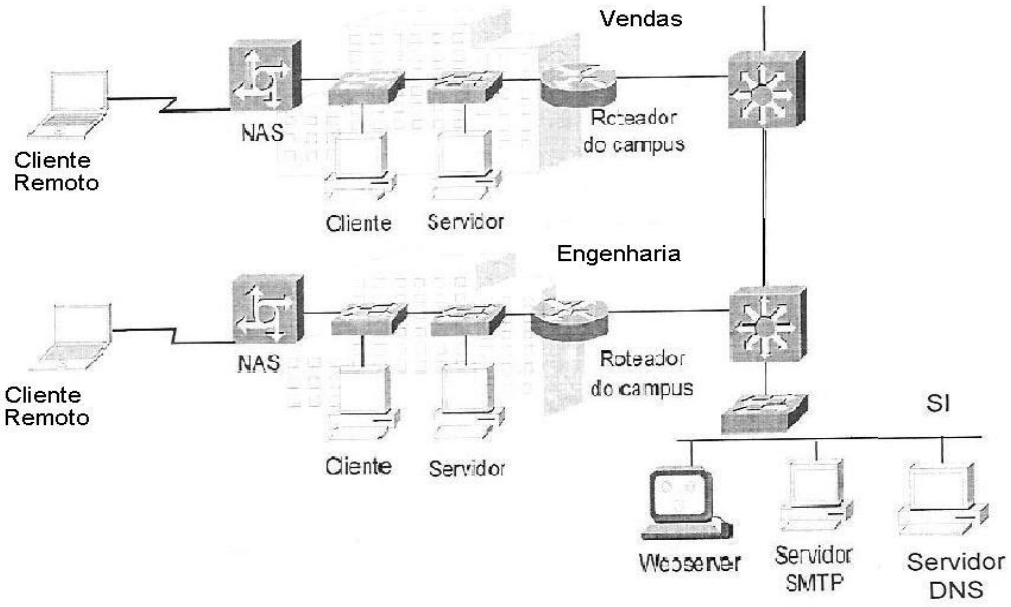
2. Indique verdade/falso e corrija, ligeiramente, quando encontrar proposições falsas. (2,00, sendo 0,5 cada questão correta)

   - (Verdade/Falso) – Os acessos externos para serviços públicos disponíveis na DMZ-2 (seria DMZ-1) são realizados no primeiro nível de defesa.
   - (Verdade/Falso) – Os acessos para serviços privados disponíveis na DMZ-2 são realizados no terceiro nível de defesa, via VPN (se são serviços privados, úteis para internos, VPN não precisa, VPN se usa entre ambientes de uma mesma organização sobre a Internet ou acesso ADSL).
   - (Verdade/Falso) – Os acessos para serviços públicos disponíveis na DMZ-1 são realizados via filtragem de pacotes TCP-IP, no segundo nível (no primeiro nível) de defesa.
   - (Verdade/Falso) - A comunicação entre um servidor Web na DMZ-1 com o BD na DMZ-2 é realizada via o segundo nível hierárquico. (o servidor Web autentica o usuário para acesso ao BD).

3. Considere o cenário, sem segurança, de uma rede corporativa da empresa XYZ, ilustrando a rede interna de uma corporação, como sendo a figura abaixo. Suponha que você é um profissional da área de segurança, responsável por implantar os níveis de segurança apontados na política de segurança de uma empresa XYZ. Então, indique na figura abaixo, como a política de segurança deve ser seguida para se ter:

   (a) Uma política de detecção de intrusões, na parte DMZ da rede de perímetro. (Basta colocar algum IDS na DMZ pública). (1,00)

   (b) uma política segura de acesso remoto, supondo que um cliente remoto tem acesso via linha telefônica até chegar no servidor NAS (Servidor de Acesso de Rede). Ou seja, como a empresa XYZ pode aumentar a segurança de acesso remoto ? (usar uma VPN entre a máquina do usuário e o NAS) (0,75)


Vendas
Cliente
Remoto
NAS
Cliente
Servidor
Roteador
do campus
Engenharia
Cliente
Remoto
NAS
Cliente
Servidor
Roteador
do campus
SI
Webserver
Servidor
SMTP
Servidor
DNS