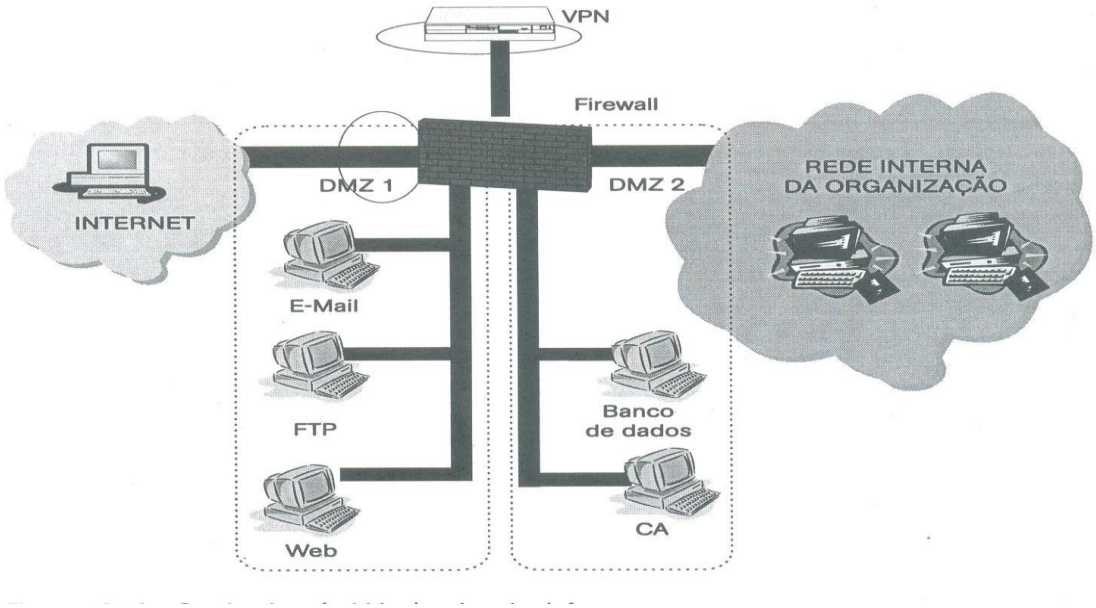
Prova B – Segurança de Rede

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: 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)

   - Para o quarto nível de defesa devemos usar algum método de autenticação dos usuários para acesso aos serviços internos.
   - O primeiro nível de defesa corresponde à filtragem de pacotes TCP/IP pelo fierewall.
   - O segundo nível de defesa consiste autenticação do usuários para acesso aos serviços públicos na DMZ-1.
   - 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.

- O acesso à DMZ-2 são tratadas no . por regras do firewall no terceiro nível de defesa.

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

   - (Verdade/Falso) – Os acessos para serviços públicos disponíveis na DMZ-1 são realizados via filtragem de pacotes TCP-IP, no **segundo nível** (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 quando os acessos usam a Internet ou acesso ADSL).

   - (Verdade/Falso) – Os acessos para serviços públicos disponíveis na DMZ-2 são realizados no **primeiro nível segundo nível** (no primeiro) de defesa.

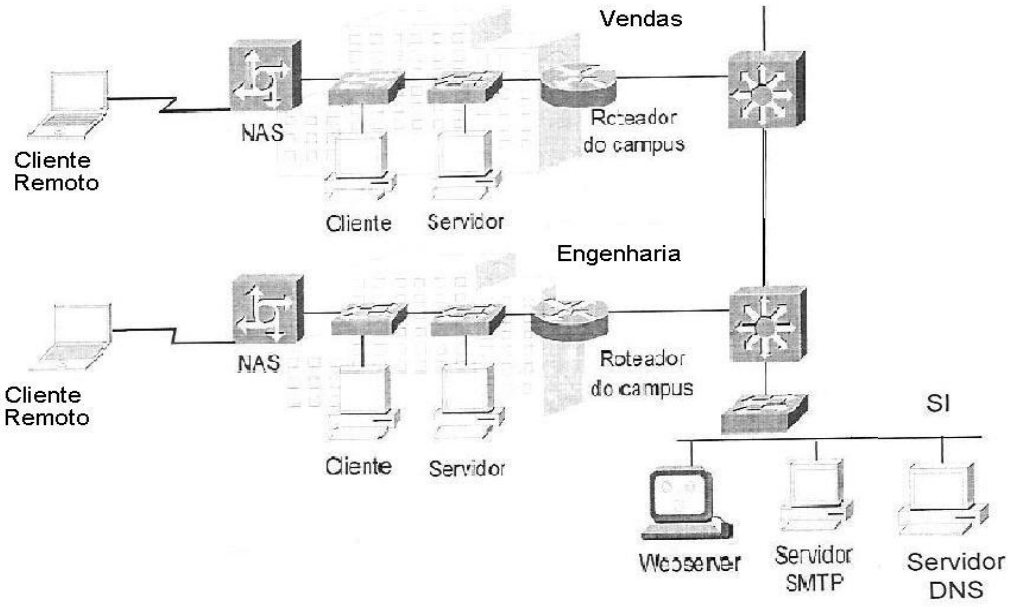
   - (Verdade/Falso) - A comunicação entre o BD na DMZ-2 e um servidor Web na DMZ-1 é realizada via o segundo nível hierárquico.

3. Suponha que você é um profissional da área de segurança, responsável por implantar os níveis apontados na política de segurança de uma empresa XYZ. Então, indique, visualizando a rede XYZ desprotegida na figura abaixo, como a política de segurança pode ser implementada para se ter (desenhe ou descreva): (1,75)

   (a) uma segurança de perímetro definindo uma DMZ mais externa. Ou seja, em que pode consistir a DMZ mais externa ? (roteador de perímetro, Host de segunça, IDS) (1,00)

   (b) uma política segura de acesso, 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 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