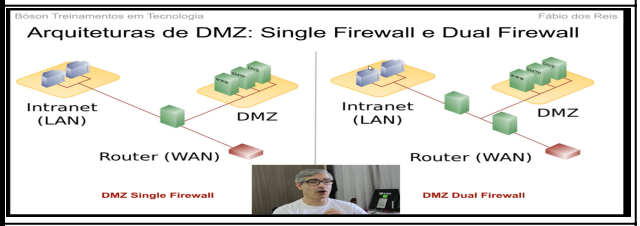
| DMZ - SEGURANÇA DE REDES DE COMPUTADORES | DMZ - SEGURANÇA DE REDES DE COMPUTADORES |
|---|---|
| O que é uma **DMZ**? | DMZ ou **De-Militarized Zone** (**Zona Desmilitarizada**), faz referência aquelas **zonas neutras entre dois países**, como por exemplo a zona neutra entre coréia do norte e do sul. Assim como essas zonas fazem divisão entre uma **parte protegida** do país e outra **desprotegida**, as DMZ's digitais são zonas onde podemos armazenar dispositivos que podem ser acessados tantos por **zonas protegidas** (**intranet's**) quanto por **zonas desprotegidas** (**Internet**). Porém, dispositivos dentro das DMZ's **não podem acessar zonas protegidas**, eles conseguem acessar somente zonas desprotegidas. Os servidores dentro das DMZ's são chamados de "**Bastion Hosts**" (**Nós de Posto Avançado**). |
| Qual é o **Objetivo Principal** de uma DMZ? | O objetivo principal de uma DMZ é justamente tornar informações **disponíveis tanto do lado de dentro da intranet quanto no lado de fora, para a internet**. Por isso que os servidores da DMZ são chamados de Bastion Hosts, por que eles são como um Posto Avançado de uma nação, fazendo frente á ela numa zona neutra, **não são seguros como os prédios e muralhas de uma nação**, mas entregam certa medida de segurança para tornar informações disponíveis do lado de fora da intranet. Mas vale lembrar que **informações de alta segurança não podem ser colocadas na DMZ**, somente aquelas que **não causarão dano a intranet** e que tenham a **real necessidade de serem disponibilizadas na internet**. |
| Que tipo de informações e serviços **podem ser disponibilizados** na DMZ e quais **jamais devem ser disponibilizados**? | **PODEM ser Disponibilizados**<br><br>- Servidor Web;<br>- Servidor DNS;<br>- Servidor de E-mail;<br>- Servidor FTP;<br>- Servidor VoIP;<br>- Bancos de Dados pouco relevante;<br>- Proxy Reversos;<br><br>**NÃO DEVEM ser Disponibilizados**<br><br>- Bancos de Dados de Alta Segurança;<br>- Dados Pessoais;<br>- Senhas;<br>- Informações Corporativas;<br>- Dados Financeiros; |
| Como as Redes DMZ conferem certa medida de **segurança**? | As redes DMZ utilizam **firewalls** tanto físicos como digitais, para se proteger de ataques maliciosos. Nesse quesito podemos encontrar redes DMZ utilizando arquiteturas de segurança com 1, 2 ou até mais firewalls. Mas as arquiteturas mais utilizadas são as:<br>**- Single Firewall:** com apenas 1 firewall fazendo a proteção entre o caminho para a rede interna, a DMZ e a Internet;<br>**- Dual Firewall:** com 2 firewalls, um firewall "Externo" fazendo a proteção para a entrada na DMZ e para o caminho para a rede Intranet, e um firewall "Interno" criando uma 2ª camada de proteção para a rede interna (intranet); |
| **Ilustre as Arquiteturas Single e Dual Firewall** |  |
| Que **Tipo de Dispositivos** vamos utilizar para o trabalho com DMZ's? | **- Servidores Bation:** servidores para guardar as informações que desejamos ter acessíveis dentro da DMZ, é importante lembrar que quando trabalhamos numa arquitetura Dual Frame, seria interessante utilizar servidores de marcas diferentes, isso iria aumentar a nossa segurança contra invasões;<br>**- Roteadores com porta de função DMZ integrada;**<br>**- Switch L3:** para criação de VLAN's como se fossem redes DMZ; (Não recomendado, oferece uma segurança mínima)<br>**- Firewall com porta de função DMZ integrada;**<br>**- Firewall comum**: usados em pares para criação de arquitetura Dual Firewall; |
| O que é um **DMZ Host?** | DMZ Host é uma **função existente em algumas aplicações de roteadores domésticos**, onde os roteadores podem **separar uma porta qualquer** do roteador para servir como um DMZ. Mas na realidade não é um DMZ de verdade, afinal **não confere a segurança por através de Firewall**. Nessa aplicação, o programa simplesmente **reserva uma porta para receber um tráfego de rede direcionado somente para a estação ao qual a ponta está interligada**, mensagens enviadas para essa porta não são direcionadas para as outras portas da rede interna. |
| Quais são algumas **desvantagens** na implantação de uma rede DMZ? | Algumas desvantagens são:<br>**- Queda na Performace da Rede:** como o aumento de dispositivos e conferências de segurança a velocidade do fluxo de dados vai cair;<br>**- Custo Elevado:** o custo com equipamento, manutenção, software e especialistas em segurança da informação;<br>**- Determinar o que proteger:** pode ser confuso e desgastante; |
| | |
| | |