Implementação de zonas de segurança em redes LAN

Raul Ferreira da Silva Junior [1, 2], Renan França Gomes Nogueira [1]
[1] Faculdade de Tecnologia Prof. Waldomiro May, Cruzeiro,SP
[2] INPE-CPTEC - Instituto Nacional de Pesquisas Espaciais, Cachoeira Paulista,SP
raul.ferreira@cptec.inpe.br, renan.nogueira@fateccruzeiro.edu.br

1. Objetivos

A implementação de zonas de segurança em uma rede LAN equaciona a questão de restrição e limitação de acessos a dados corporativos sigilosos e essenciais. Em especial, a criação de uma zona desmilitarizada (DMZ– DeMilitarized Zone) que, através de um eficaz controle de acesso permite que todo o tráfego entre os servidores corporativos e a web estejam devidamente isolados por um firewall e por essa zona desmilitarizada, com regras de segurança específicas para hosts críticos. No presente trabalho, propõe-se a criação uma VLAN específica e com faixa de IPs dedicados, que irá conectar 03 equipamentos configurados como servidores WEB, DNS externo e SMTP e também a formulação e testes com alternativas de configuração de mais de um serviço em um mesmo servidor (Ex: DNS + SMTP), medição de custo computacional dos serviços e determinação da melhor relação custo-benefício.

A figura a seguir dá uma idéia da rede a ser montada e testada para o trabalho.

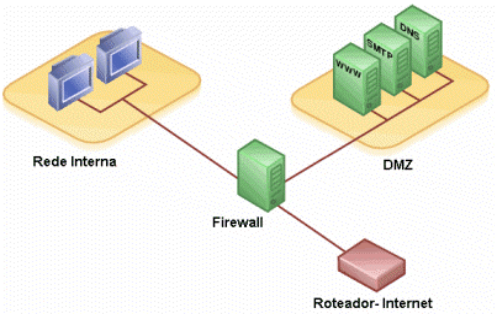

Figura 1 – PINHEIRO, José Maurício <www.projetoderedes.com.br/artigos/>

2. Métodos/Procedimentos

A metodologia consiste em: (1) projeto documentado da rede com equipamentos, cabeamento e protocolos; (2) montagem e testes rápidos da rede básica; (3) formulação das alternativas de configuração; (4) formulação dos critérios de medição e especificação de hardware/software utilizado; (5) desenvolvimento e ativação do plano de testes; (6) comparação de resultados; (7) implantação da 1ª configuração a testar; (8) testes documentados da 1ª configuração; (9) implantação da 2ª configuração a testar; (10) testes documentados da 2ª configuração; (11) comparação dos resultados e opção pela melhor configuração.

3. Resultados

Após a implementação e testes em ambiente paralelo e também em ambiente de produção, espera-se obter as informações necessárias para desenvolver um projeto de segurança para uma rede de médio/grande porte. Esse projeto incluirá, além das atividades usuais: (1) uma bateria de testes rigorosos; (2) desenvolvimento de ferramentas de manutenção do sistema.

4. Conclusões

É possível desenvolver um projeto piloto de uma DMZ em rede de teste e extrapolá-la para uma rede de maior porte. Tal rede piloto pode mesmo se tornar uma ferramenta permanente de testes contra ameaças externas, e é possível usar de proatividade, conceber possíveis ataques, defesas e situações adversas na rede-piloto. Ao efetivamente “isolar” a rede interna da web por meio de um segmento de rede dedicado, adiciona uma camada de segurança bastante útil aos administradores de rede para a análise, identificação e bloqueio de intrusões.

5. Referências Bibliográficas

[1]PINHEIRO, José Maurício. Biometria nos Sistemas Computacionais. Editora Ciência Moderna, 2003.

[2]TANENBAUM, Andrew S. Redes de Computadores. Editora Prentice-Hall. 4ª Edição, 2003.

[3] NEMETH, Evi.; *et al.* Manual Completo do Linux –Guia do Administrador. Editora Prentice-Hall, 2ª Edição, 2007.