Grupo de Resposta a Incidentes de Segurança

Segurança em DMZ

Nome: Augusto Cesar da F. dos Santos

Grupo de Respostas a Incidentes de Segurança

Departamento de Ciência da Computação

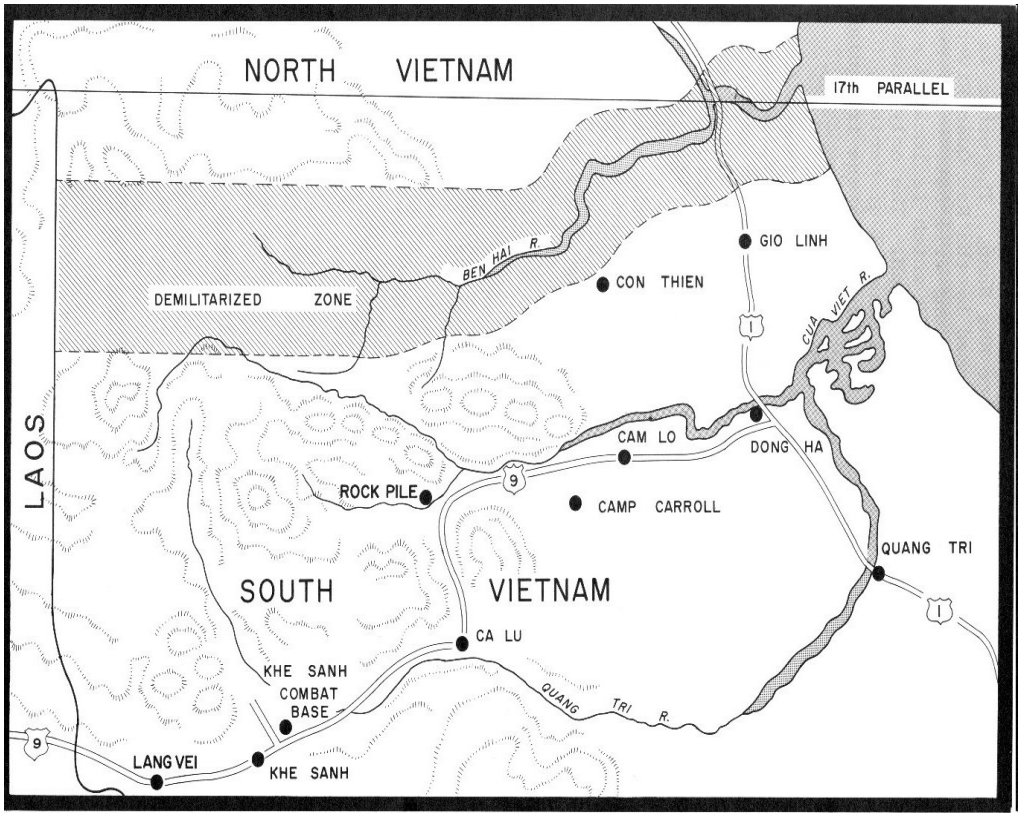
Instituto de Matemática

Universidade Federal do Rio de Janeiro

augusto@gris.dcc.ufrj.br

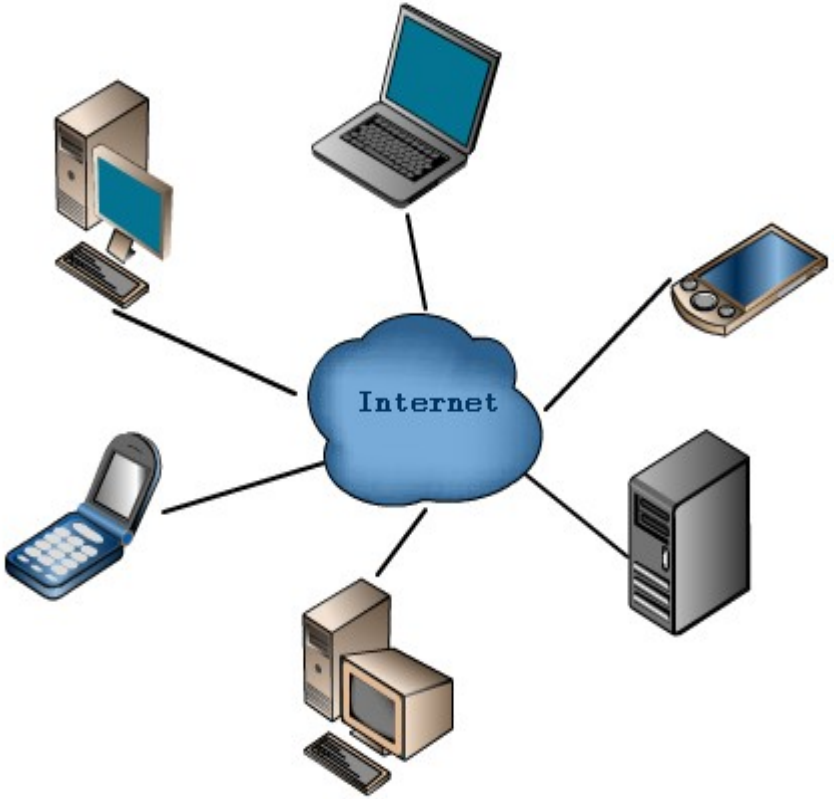
DMZ Conceito Geopolitico

- Geopoliticamente - Zona Desmilitarizada (De-Militarized Zone)
- Vietnã do Sul X Vietnã do Norte
- Atividade Bélica Proibida – Armistício
- Na Segurança da Informação (Zona de Perímetro ou Zona Neutra)



A Internet

- Rede Mundial de Computadores
- Rede Externa (Não Confiável)
- Confiabilidade e Segurança
- Riscos e Atividades Maliciosas



http://eb23svformoso.ccbi.com.pt/blog/?p=92

A DMZ (Zona Desmilitarizada)

- O que é?

- Sub-redes que hospedam servidores com seus respectivos serviços, protegidos por regras de Firewal

- O que existe na DMZ?

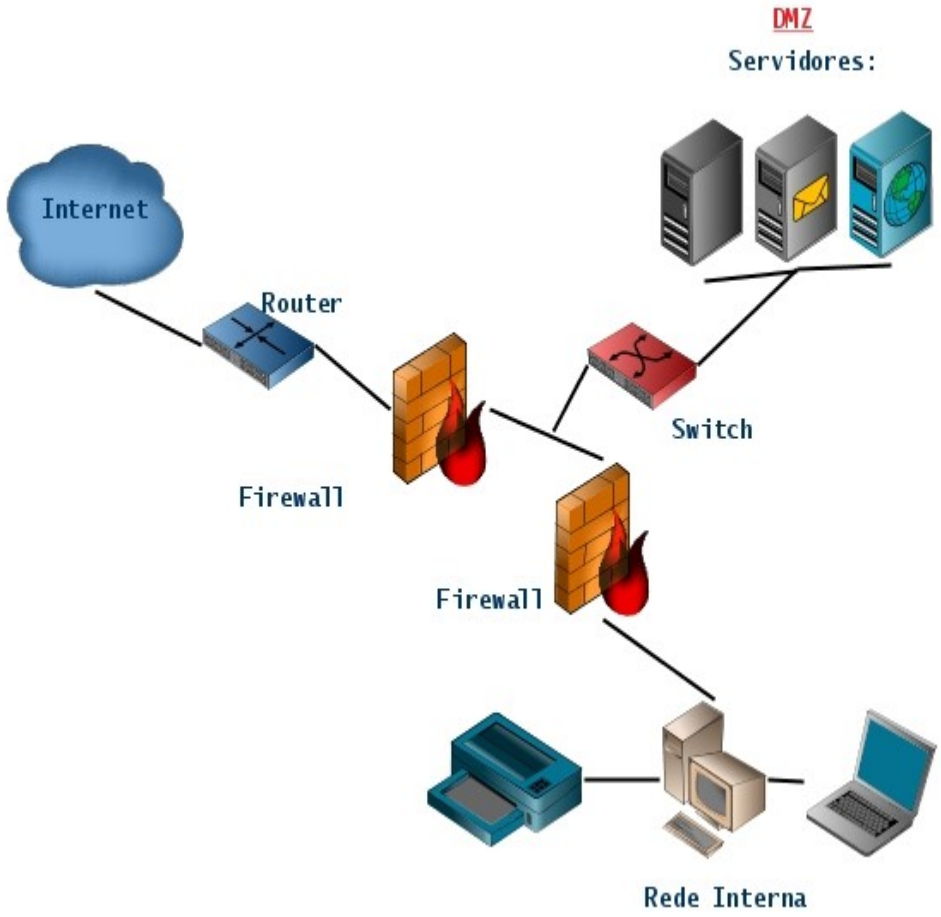
- Firewalls (“Gateways”, Dispositivos de Perímetro)

· Controle rígido do fluxo de tráfego

· Passagens seguras entre rede interna e internet

Por que Parcialmente Segura?

- Acesso Público – Risco de Atividade Maliciosa



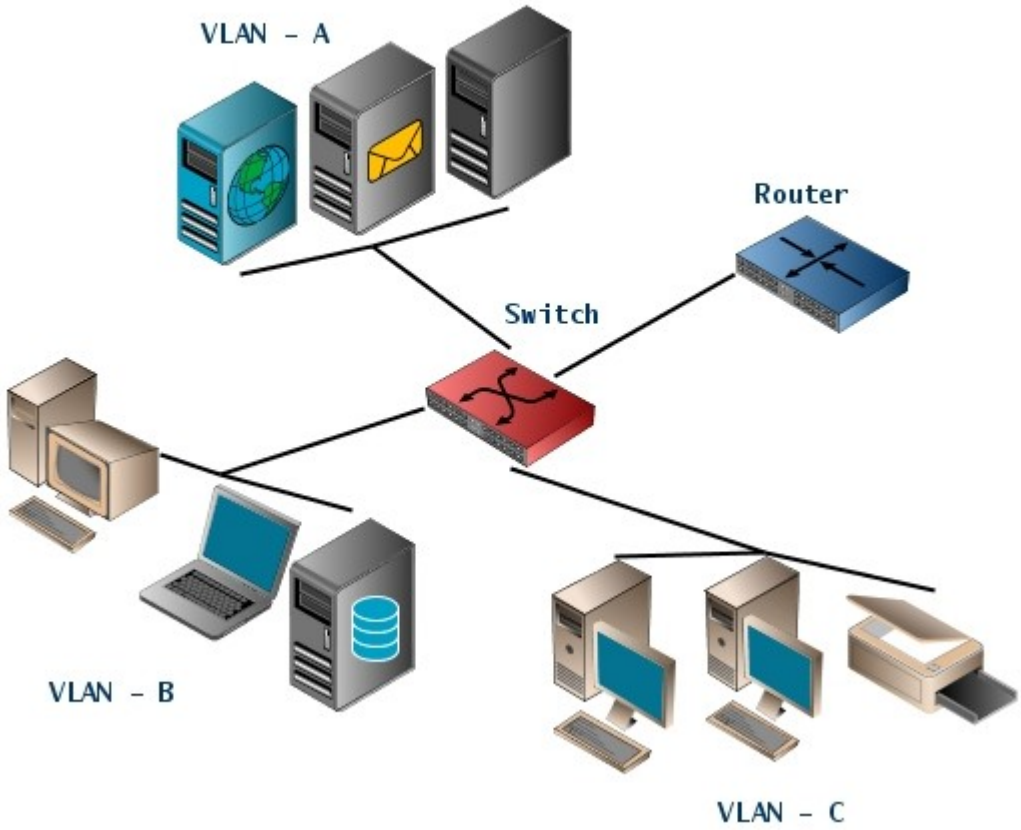
Esquema de Endereçamento IP

Política de Segurança:

- IP Público
- IP Privado – NAT

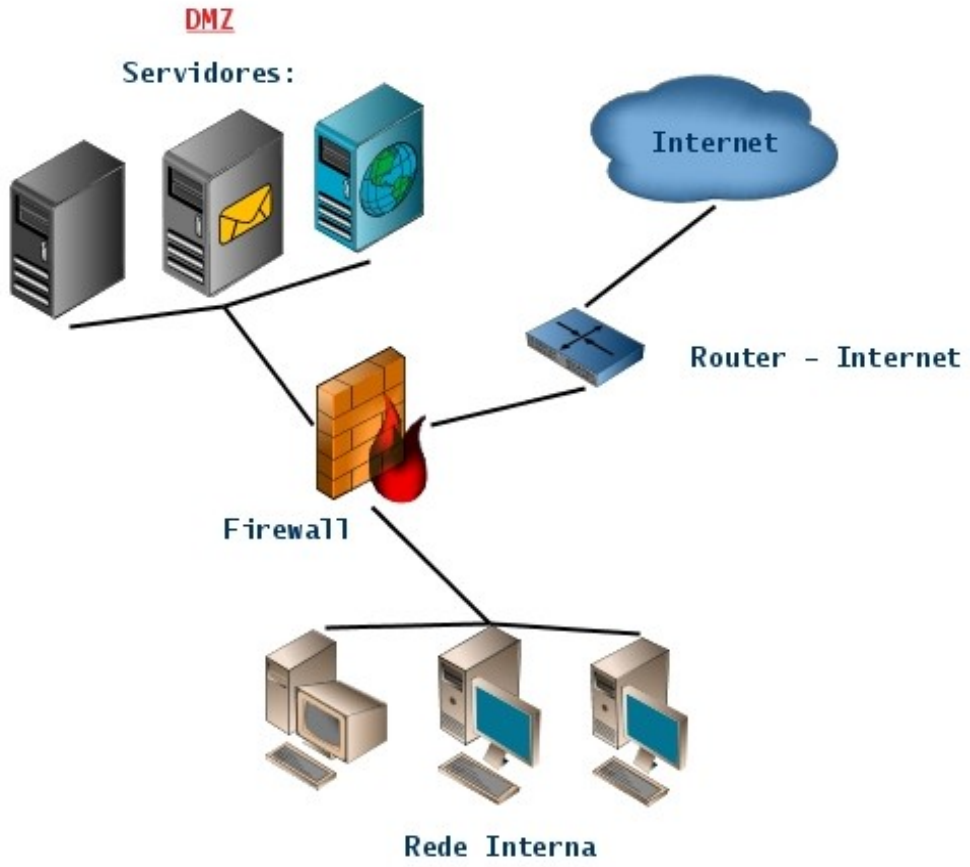
· VLANs (Redes Virtuais Distinas que não se falam entre si)

- Maior Segurança – Separar dados sigilosos
- Desempenho e Largura de Banda
- Segregação de departamentos



Um firewall com três interfaces

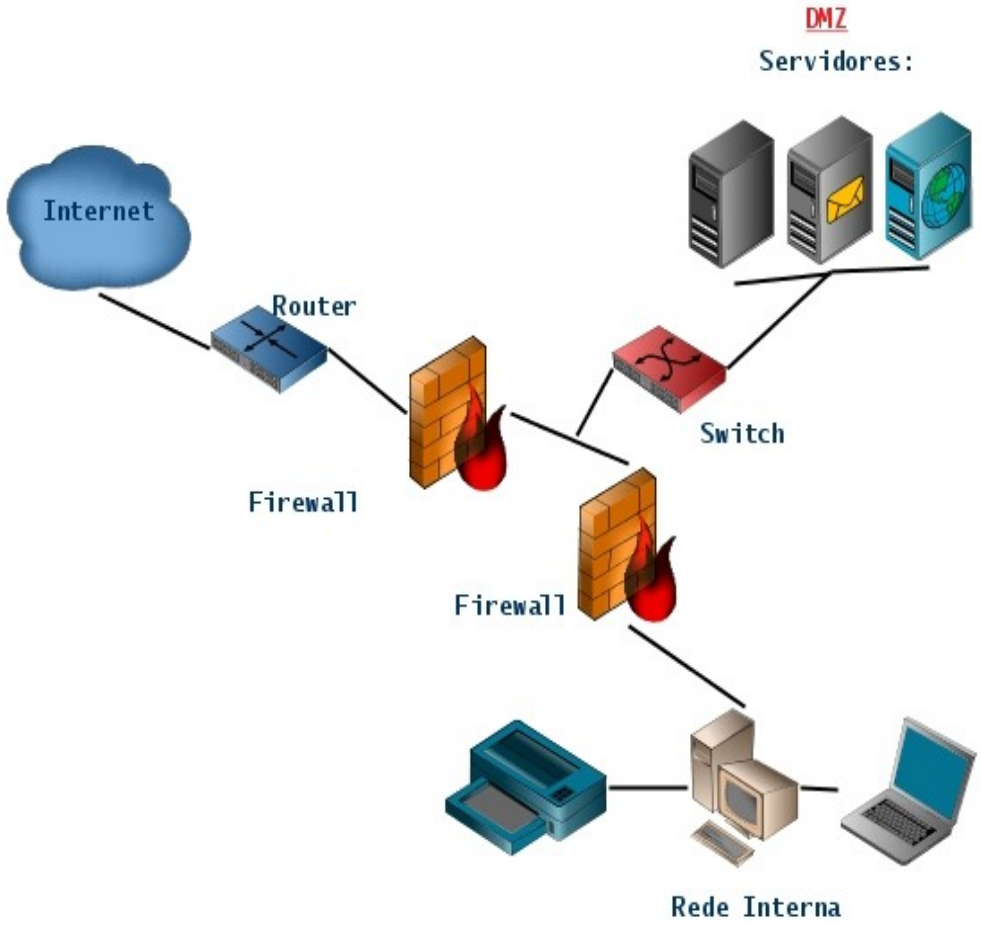
- Rede Interna (Confiável)
- Rede Externa (Não Confiável)
- DMZ (Semi-segura)



Dois Firewalls com duas interfaces cada

- Recebe tráfego da Internet

- Filtro de Pacotes na entrada da DMZ melhora o desempenho no acesso aos servidores



Regras de Firewall

- Para uma boa política de segurança a ser implementada no Firewall é importante que se estabeleçam algumas regras, como:

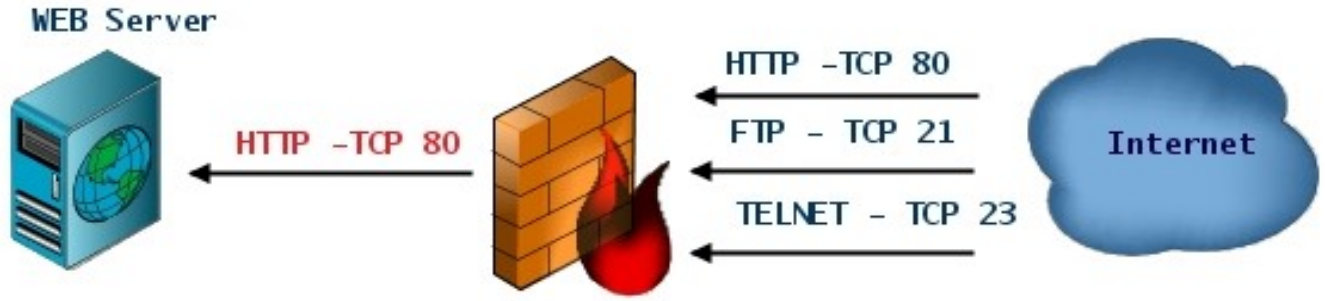
- Habilitar aplicações estritamente necessários de acordo os serviços disponibilizados aos usuários (quais portas e seus respectivos serviços)

- Regras rígidas de acordo com que tipos de endereços IP´s podem acessar quais serviços

- Gerenciamento de Log´s de portas proibidas

- Redirecionamento de Portas

- Regras de acordo com ataques específicos



Ataques e Defesas em DMZ

Mais comuns:

- DoS (Denial of Service)

- Tentativa de tornar recursos de um sistema indisponíveis

- Mais comum em servidores HTTP

- Objetivo de Tornar o serviço indisponível

- DDoS (Distributed Denial of Service)

- Maquinas infectadas controladas (zumbis) por uma máquina Mestre

- Servidor recebe número limitado de requisições, no ataque todos os “zumbis” efetuam a requisição de uma só vez

- Servidor pode reiniciar ou ficar travado

Proteção:

- Regras de Firewall com ataques específicos (mais comuns)

- Ferramentas de Hardening (IDS, IPS e etc.)

Honeypot e Ferramentas de hardening

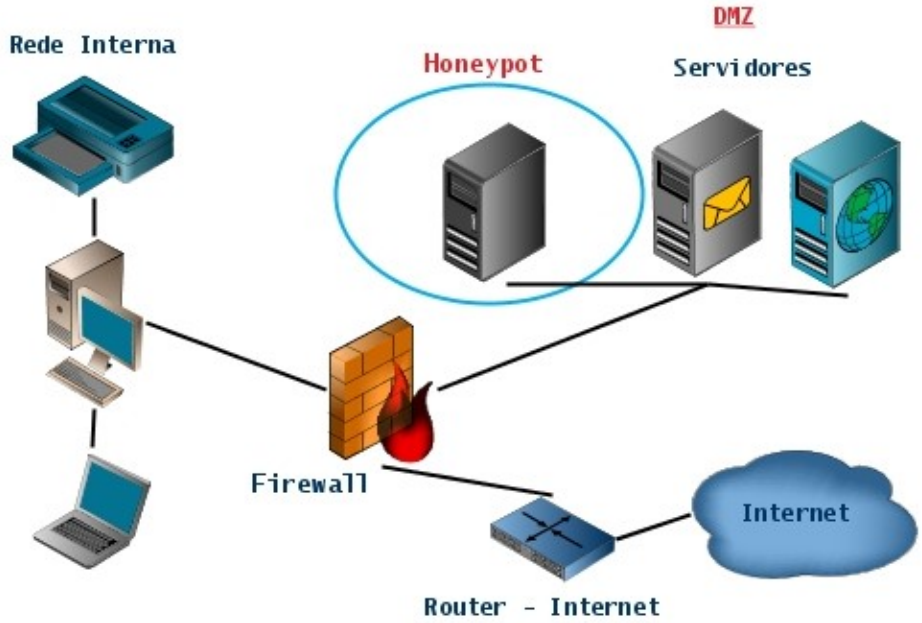
Honeypots - Opção Pró Ativa que atrai atenção dos invasores

- IDS (Intrusion Detection System)

-Detecta e Registra ações maliciosas e tráfego anôma nas rede de computadores (NIDS) e em hosts (HIDS). São Passivos.

- IPS (intrusion Prevention System)

- Detecta, Registra e trata ações maliciosas e tráfego anômalo nas rede de computadores. São Ativos



http://www.easyvmx.com/blog/?q=security_vmware_honeypots

http://www.jrcontrole.com.br/alarme.htm

Dúvidas?

Nome: Augusto Cesar da F. dos Santos

Grupo de Respostas a Incidentes de Segurança

Departamento de Ciência da Computação

Instituto de Matemática

Universidade Federal do Rio de Janeiro

augusto@gris.dcc.ufrj.br

Bibliografias:

SolutionBase Strengthen network defenses by using a DMZ:
http://articles.techrepublic.com/5100-22 11-5756029.html

Disigning a DMZ:
http://sans.org/reading room/whitepapers/firewalls/950.php

Sample DMZ Exemple:
http://www.ciberciti.biz/faq/linux-demilitarized-zone-howto/

http://www.honeynet.org

Curso Tecnologico de Redes de Computadores (Apostila em PDF)
Professores: José Maurício S. Pinheiro/ José Ricardo F. de Almeida

Firewall Suas características e Vulnerabilidades (Apostila em PDF)
Faculdade de Tecnologia do SENAI de Florianópolis – Departamento de Pós Graduação (CTAI – Florianópolis)
Vanderso C. Siewert