INFRAESTRUTURA PARA SISTEMAS DE SOFTWARE

Firewalls e Web Proxies
Parte 2

ROTEIRO

- Web Proxy - Squid
- Outros Tipos de Firewalls
- Arquiteturas de Firewalls
- Sistemas de Detecção de Intrusão

FUNCIONAMENTO

- Filtragem de pacotes via ACL – Access Control
  - O método mais usado para configurar filtros de pacotes é conhecido como listas de controle de acesso (ACLs)
  - Dividem-se em dois tipos de padrão:
    - ACLs padrão – filtram baseadas no endereço IP
    - ACLs estendidas – procuram ‘mais dentro’ do cabeçalho do pacote

FUNCIONAMENTO

- Filtragem de pacotes via ACL – Access Control
  - Implementando um servidor proxy com o Squid
  - Squid permite compartilhar a conexão entre vários nós, servi como intermediário entre eles e a Internet

WEB PROXY SQUID

- Filtragem de pacotes via ACL – Access Control
  - Implementando um servidor proxy com o Squid
    - Para colocar em funcionamento:
      - #apt-get install squid
      - # mv /etc/squid/squid.conf /etc/squid/squid.conf.backup
    - Arquivo /etc/squid/squid.conf contendo as seguintes linhas
      - http_port 3128
      - visible_hostname servidor
      - acl all src 0.0.0.0/0.0.0.0
      - http_access allow all

WEB PROXY SQUID

- Filtragem de pacotes via ACL – Access Control
  - Implementando um servidor proxy com o Squid
    - Ex.: permissões

```
http_port 3128
visible_hostname gdh

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 901 # swat
acl Safe_ports port 1025-65535 # portas altas
acl purge method PURGE
acl CONNECT method CONNECT

http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

acl redelocal src 192.168.1.0/24
http_access allow localhost
http_access allow redelocal

http_access deny all
```

WEB PROXY SQUID

- **Filtragem de pacotes via ACL – Access Control**
  - **Bloqueando por domínios ou palavras**
    - acl bloqueados dstdomain playboy.abril.com.br
    - http_access deny bloqueados
  - **Bloqueando por domínios ou palavras (com ou sem www**
    - acl bloqueados dstdomain www.xvideos.com playboy.abril.c
    - http_access deny bloqueados
  - E se a regra ficar muito grande?

WEB PROXY SQUID

- **Filtragem de pacotes via ACL – Access Control**
  - É possível, nestes casos, criar um arquivo externo, inserir os domínios, linha a linha e posteriormente fazer uma ‘chamada’ este arquivo.
    - Ex: acl bloqueados url_regex –i “/etc/squid/bloqueados”
      - http_access deny bloqueados

- **Problema:**
  - Cada novo endereço descoberto deve ser inserido na lista
- **Solução:**
  - O Sarg pode ajudar bastante

WEB PROXY SQUID

- **Filtragem de pacotes via ACL – Access Control**
  - É possível também inverter a regra, de forma que eu possa bloquear tudo e ir liberando acesso a determinados sites
    - **Ex: acl permitidos url_regex –i "/etc/squid/permitidos"**
      - **http_access allow permitidos**
      - **http_access deny all**
  - Nos proxies mais atuais têm-se o bloqueio de domínios asso aos respectivos IPs, evitando assim que o usuário digite diretamente o IP de um site

WEB PROXY SQUID

- **Filtragem de pacotes via ACL – Access Control**
  - É possível bloquear também por endereços IP
    - Ex: acl ips-bloqueados dst 200.234.21.23 200.212.15.45
      - http_access deny ips-bloqueados

WEB PROXY SQUID

- **Filtragem de pacotes via ACL – Access Control**
  - **Bloqueando por palavras (incluídas na URL de acesso)**
    - Criar um arquivo de texto com as palavras a serem bloquea
      - Ex: facebook, xxx, sexo, teens…
  - **Adicionar a regra contendo a localização do arquivo**
    - acl palavrasproibidas dstdom_regex “/etc/squid/palavraspro
    - http_access deny palavrasproibidas
  - **Problemas?**
    - Falsos positivos

WEB PROXY SQUID

- **Filtragem de pacotes via ACL – Access Control**
  - **Mensagens de erro**
    - Adicionar a seguinte linha no squid
    - **"error_directory /usr/share/squid/errors/Portuguese/ "**

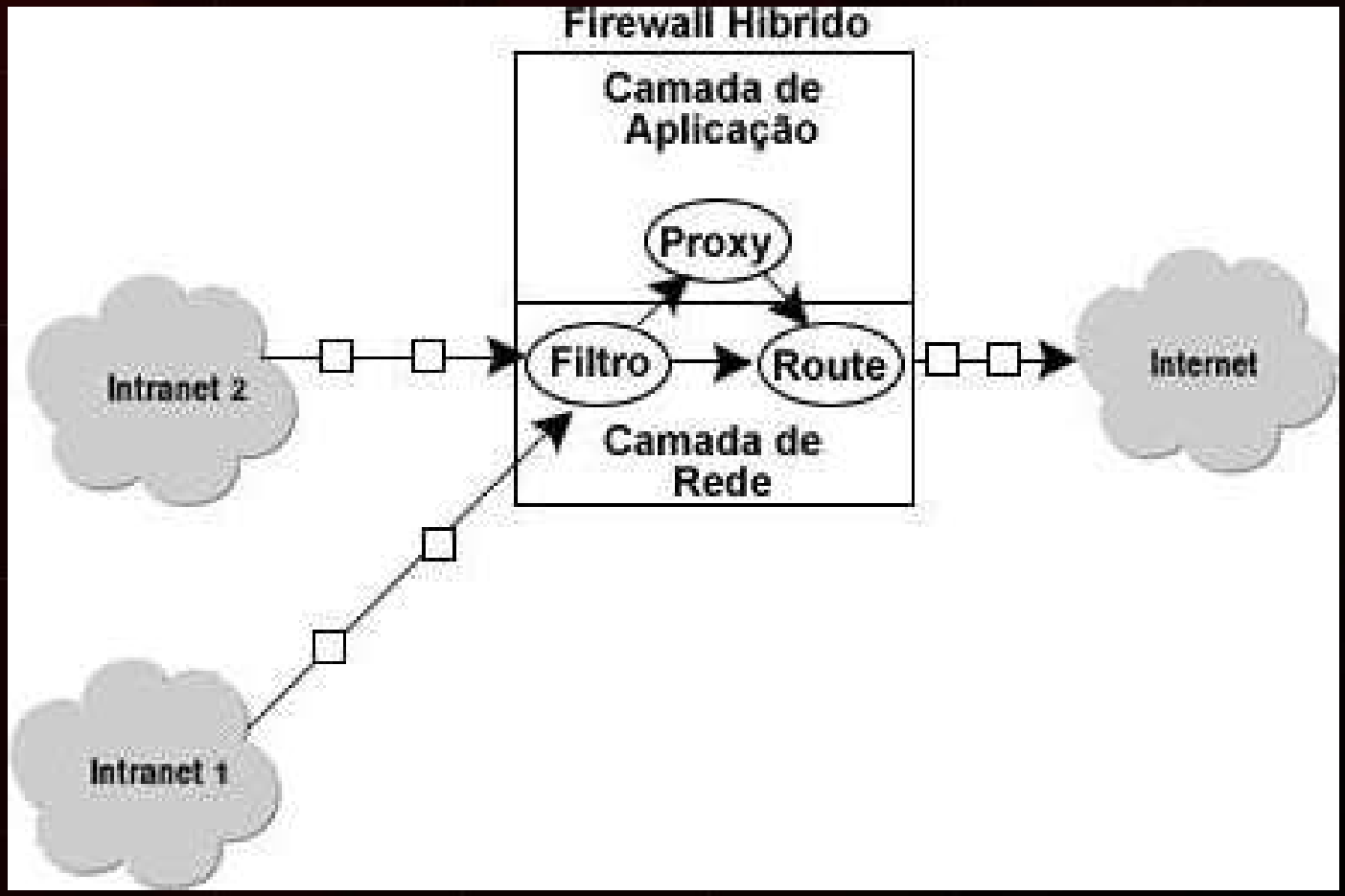
- **É possível alterar os arquivos HTML de cada mensagem d forma personalizada**

OUTROS TIPOS DE FIREWALLS

- **Firewalls Híbridos**
  - A maioria dos *firewalls* podem ser classificados como Filtro d Pacotes ou Servidores *Proxy*
  - Outros tipos de *firewalls* oferecem uma combinação entre es dois

OUTROS TIPOS DE FIREWALLS

- **Firewalls Híbridos**

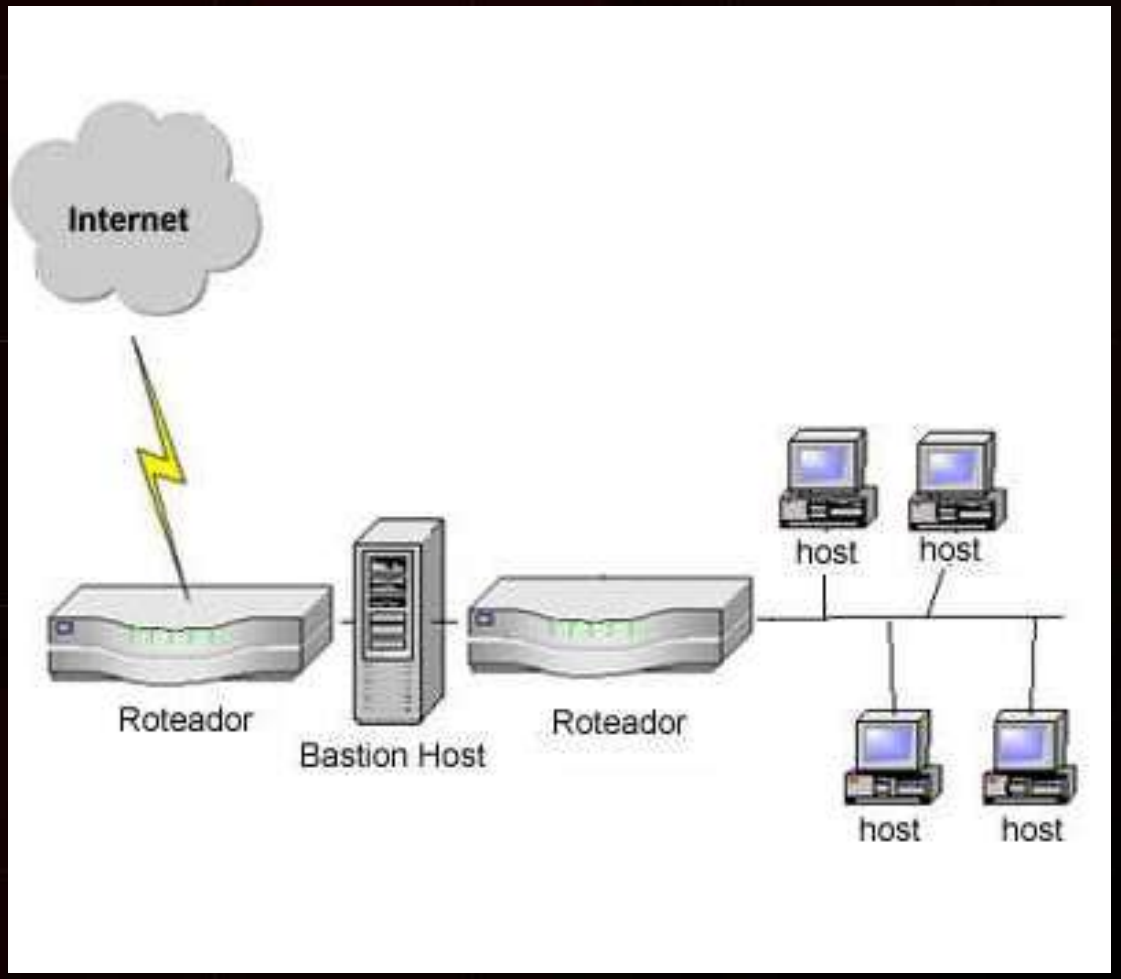


OUTROS TIPOS DE FIREWALLS

- **Firewalls Bastion Hosts**
  - Hosts fortemente protegidos
  - Único computador da rede que pode ser acessado pelo lado fora do firewall
  - Pode ser projetado para ser um servidor Web, servidor FTP, dentre outros

OUTROS TIPOS DE FIREWALLS

- **Firewalls Bastion Hosts**



OUTROS TIPOS DE FIREWALLS

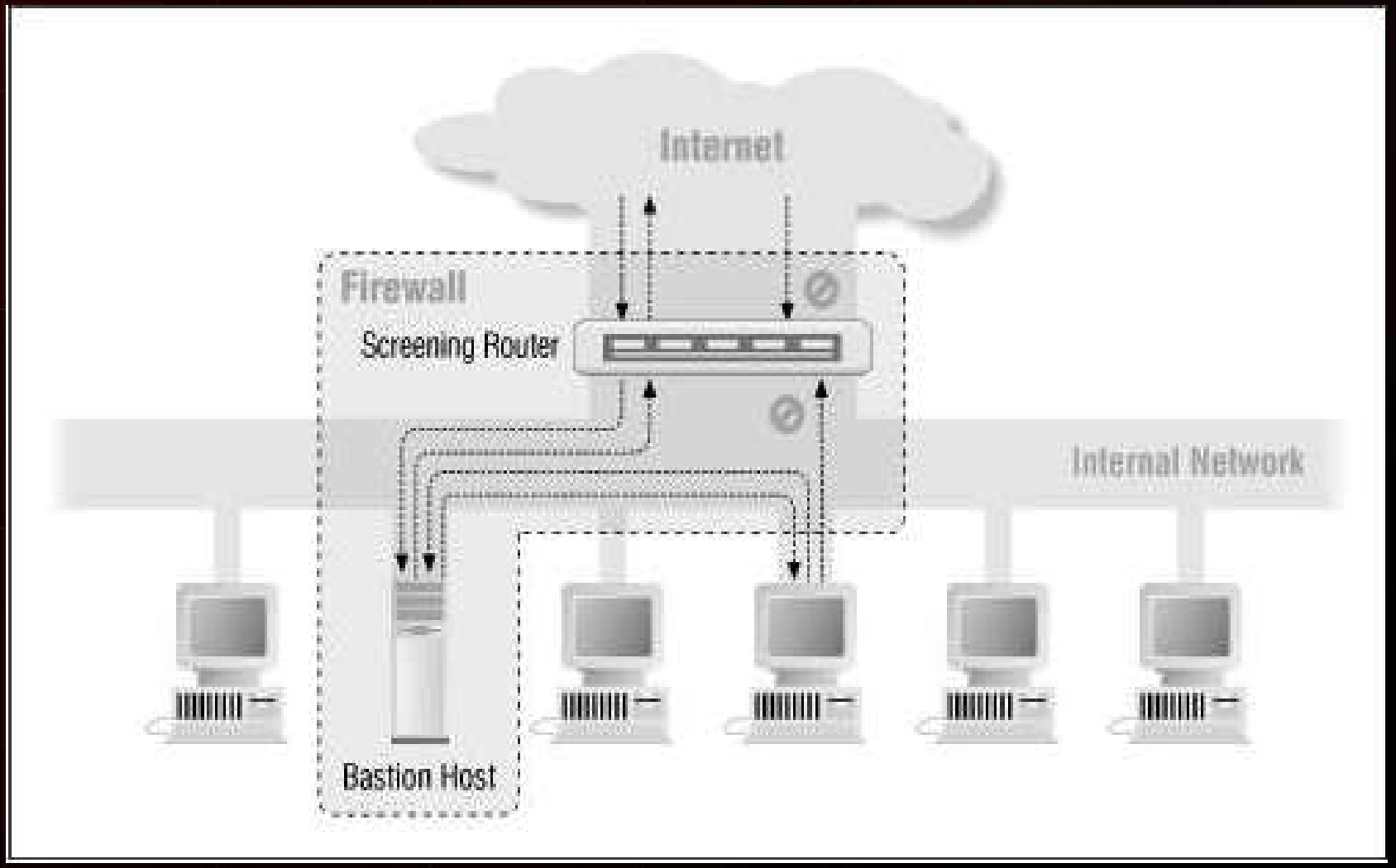
- **Firewalls Bastion Hosts**
  - **Honey Pot**
    - Chamariz para crackers
    - Função de coletar dados de tentativas de invasão
    - Ferramentas de registros de logs são mantidas o mais segu possível

ARQUITETURAS DE FIREWALLS

- **Principais:**
  - ***Screened host***
    - **Sem sub-rede de proteção**
    - **Elementos = 1 roteador e 1 *bastion host***
    - **Rede protegida sem acesso direto ao "mundo"**
    - ***Bastion host* realiza o papel de procurador – só ele passa p roteador**

ARQUITETURAS DE FIREWALLS

- **Screened Host**



ARQUITETURAS DE FIREWALLS

- ***Screened subnet***
  - *Screened* = proteger, peneirar, investigar
  - Apresenta múltiplos níveis de redundância
  - É a mais segura

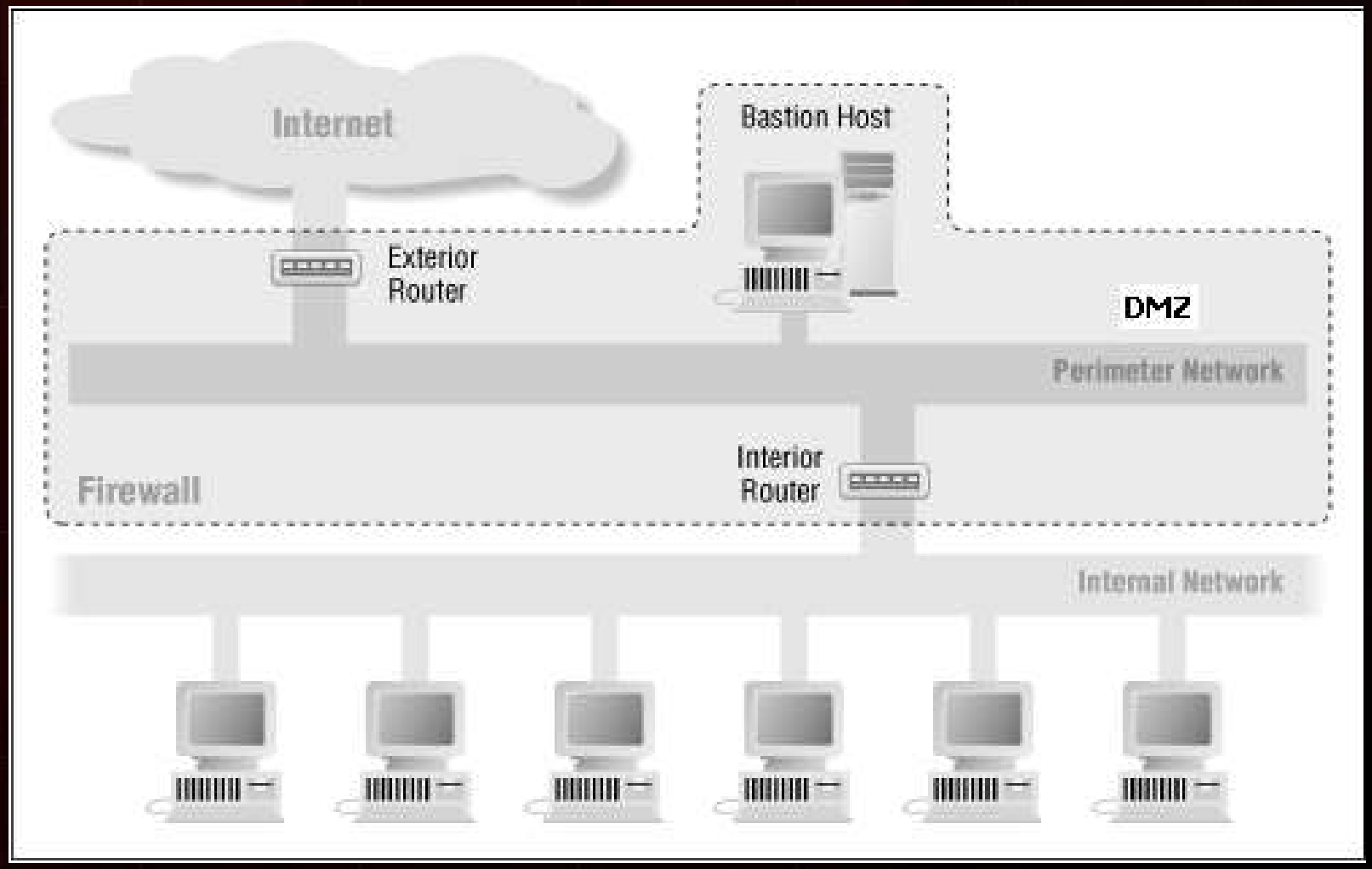
  - **Componentes:**
    - Roteador externo
    - Sub-rede intermediária (DMZ)
    - Bastion Host
    - Roteador Interno

ARQUITETURAS DE FIREWALLS

- ***Screened subnet***
- **O que é a DMZ (De Militarized Zone)?**
  - Sub-rede entre a rede externa e a protegida. Proporciona segurança.
    - Rede interna somente tem acesso ao *Bastion Host*
    - Somente a sub-rede DMZ é conhecida pela Internet

ARQUITETURAS DE FIREWALLS

- ***Screened subnet***

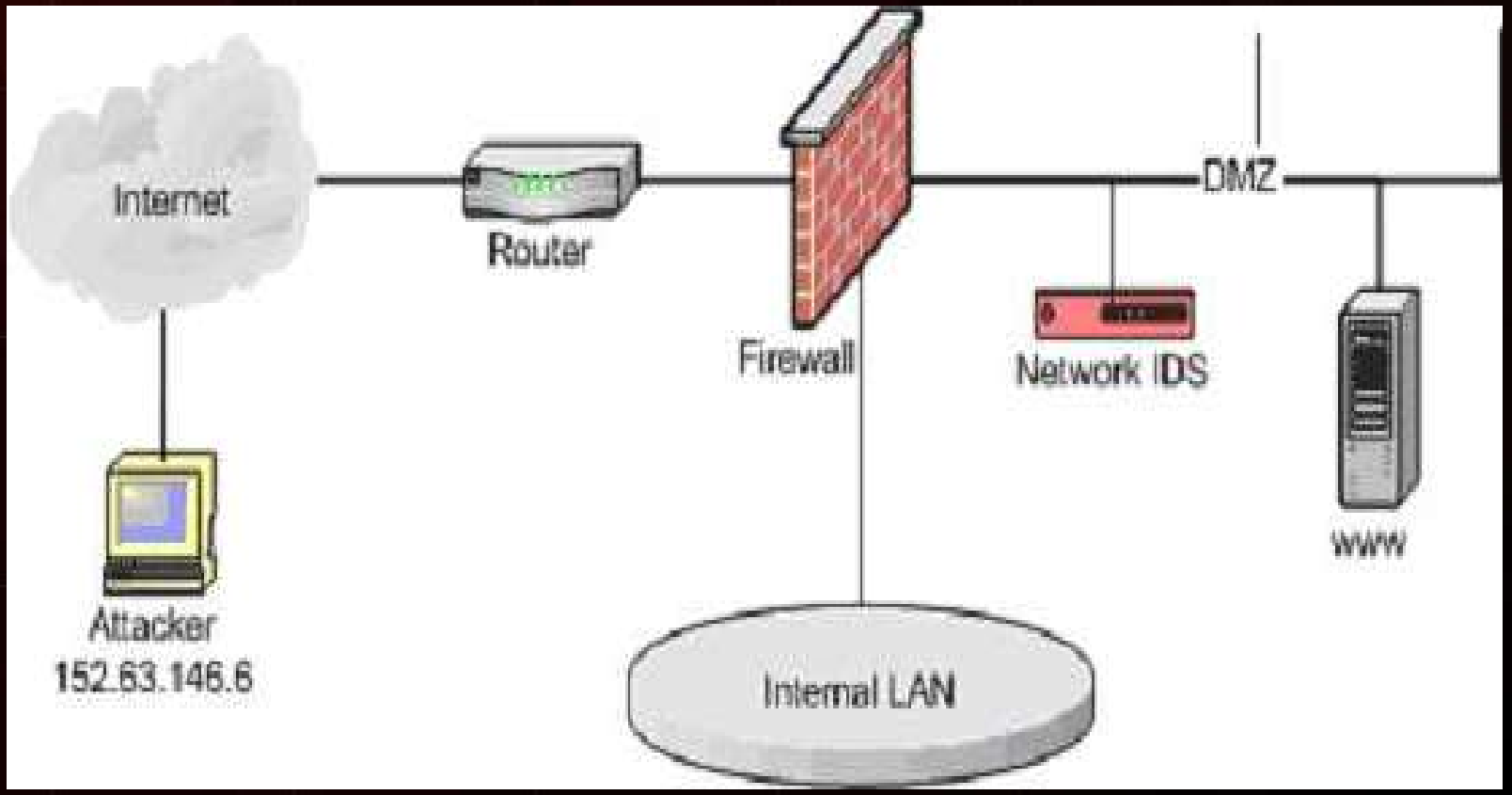


SISTEMAS DE DETECÇÃO DE INTRUSÃO

- **Solução complementar ao firewall**
  - Softwares capazes de detectar atividades suspeitas
  - Utiliza-se de padrões conhecidos de comportamento de intru
  - Podem analisar o tráfego interno, externo e entre eles

- **Tipos de análise de tráfego**
  - Detecção de assinaturas
  - Detecção de comportamento
  - Detecção de anomalias de protocolo

SISTEMAS DE DETECÇÃO DE INTRUSÃO



SISTEMAS DE DETECÇÃO DE INTRUSÃO

- **Detecção de assinaturas**
  - procura de padrões específicos
    - desvantagem : necessidade de conhecimento prévio do pa

- **Detecção Comportamento**
  - Cada rede tem determinada característica (estatística)
  - Procura alterações nestas característica (pico)
    - Desvantagem - método não muito eficaz

- **Detecção de anomalias de protocolo**
  - Análise do pacote com seu padrão

REFERÊNCIAS

Zwicky, E; Cooper, Simon – Construindo Firewalls para a Inter
O´Reilly, 2000

Internet Firewalls – UFRGS
http://penta.ufrgs.br/redes296/firewall/fire.html

INFRAESTRUTURA PARA SISTEMAS DE SOFTWARE

Firewalls e Web Proxies
Parte 2