Segurança de Redes

Aula 3 – Elementos de Segurança de Redes

Prof. Fred Sauer, D.Sc.
fsauer@gmail.com

Sumário

- Conceitos básicos de Segurança (proteção, contramedidas)
- Firewall
  - Filtros de Pacotes
    - Stateful e stateless (com ou sem controle de estado)
  - Filtros de conexões
  - Firewall Proxy (Proxy de conteúdo)
- IDS e IPS
- Honeypots

Conceitos Básicos de Segurança

- Privilégio mínimo de usuários
  - Restrições de permissão de acesso de acordo com a necessidade de conhecer
- Defesa em Profundidade
  - Diversos controles que se complementam
  - Evita ponto único de falha
  - Também chamada “Defesa em Camadas”, usada na *deepweb (onion router)*

Conceitos de Segurança

- Segurança dos elementos de redes
  - Hardening dos dispositivos : switch, roteadores, etc
  - Retirar telnet, uso de senhas robustas para acesso ao SO, desabilitar serviços desnecessários, patches de correção de vulnerabilidades
- Segurança de hosts
  - Retirada de serviços desnecessários e *hardening* dos demais
  - Manutenção dos SO atualizados com patches de correção
- Segurança por obscuridade
  - Ocultar ou disfarçar informações que possam facilitar invasões (Ex.: divulgação SSID de redes sem fio)

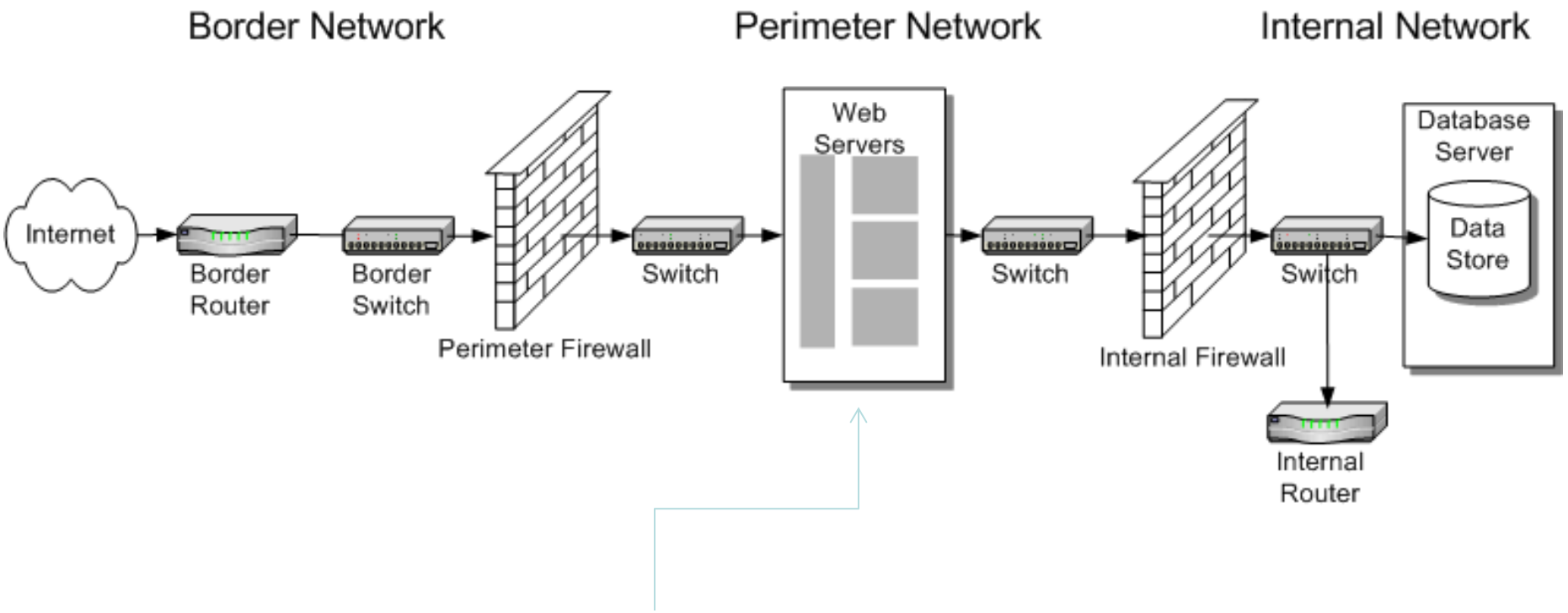
Conceitos de Segurança

- Segurança do Perímetro: Conceito importante da segurança física
  - Faixa de limites do território a proteger.
  - Segurança no perímetro da rede significa implantar mecanismos de controle nas interfaces do perímetro
- Conceito de Segregação
  - Física: não há contato físico entre redes
  - Lógica: apesar de haver contato físico, há barreiras lógicas, como por exemplo ACLs

Segurança do Perímetro

- Fazem parte da segurança do perímetro da rede:
  - Roteadores
  - Firewall/Proxy
  - IDS/IPS
  - VPN, dentre outros mecanismos

Segurança do Perímetro



Configuração típica
de uma DMZ

Roteador

- Dispositivo de rede tem como função principal conectar redes heterogêneas
  - Todo pacote, para sair de uma rede e ingressar em outra, DEVE passar por um roteador
- Por possuir SO e interfaces acessíveis, é vulnerável a ataques
- Protocolos de Roteamento Dinâmicos (RIP, OSPF, EIGRP, etc.)
  - Simplificam a configuração e operação para os administradores, mas...
    - Possibilita “envenenamentos“ das suas tabelas
    - Apenas roteadores com rotas alternativas devem usar protocolos dinâmicos
- Roteamento Estático
  - Maneira mais trabalhosa de se configurar, porém mais segura
  - A maioria das redes não precisa de um protocolo dinâmico, por estarem ligadas a um único provedor

Firewall

- Dispositivos de controle de acesso posicionados entre duas redes ou mais com níveis de segurança distintos

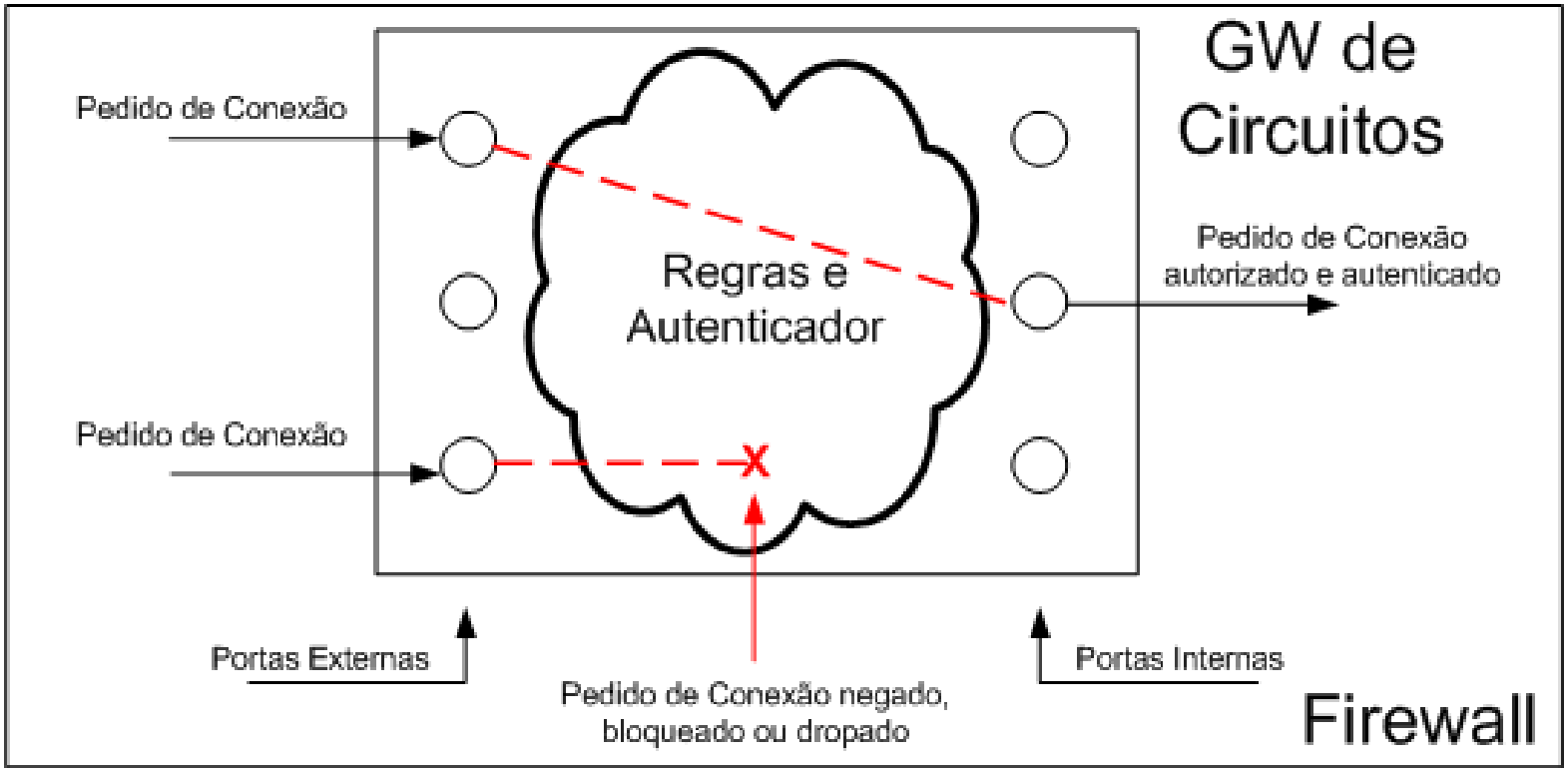
- Opera um conjunto de regras específicas que permitem ou bloqueiam o tráfego
- Podem ser implementados em um roteador ou gateway

- Funcionalidades:
  - Filtros, proxies, bastion hosts, zona desmilitarizada
  - Pode incluir outras funcionalidades, como tradução de endereços (NAT), utilização de Redes Privadas Virtuais (VPN) e serviços de AAA

Firewall

- Termo genérico que significa uma barreira ao tráfego não autorizado
- Algumas referências não incluem os proxies na categoria “Firewall”, outras usam o termo “Firewall Proxy” quando vai até a aplicação e apenas Firewall quando se trata de um filtro
- Tipos de Firewall:
  - Filtro de pacotes: Estático ou sem controle de estado (stateless)
    - Contras: Não consegue saber, por exemplo, se um SYN/ACK recebido foi precedido de um SYN enviado
    - Prós: É rápido e consome poucos recursos
  - Filtro de pacotes baseado em estado: (stateful) – mantém uma tabela com fluxos TCP, UDP e ICMP para uma melhor análise
    - Prós e contras inversos ao stateless
  - Proxy: Controla o conteúdo de uma aplicação específica
    - Pode ser para conteúdo de navegação web ou email, mas nunca é genérico para qualquer conteúdo de aplicações diversas
  - Gateway de Circuitos (Proxy de Circuito)
    - Normalmente usado apenas para forçar autenticação no acesso autorizado por regras, mas não faz filtragem de conteúdo

Gateway de Circuitos



Firewall

- Filtro de Pacotes:
  - Camada de rede e de transporte (sockets)
  - Informações básicas para permitir ou bloquear pacotes, baseados em Listas de controle de acesso (ACL – Access Control Lists)
  - Filtragem com base nos cabeçalhos IP, TCP, UDP ou ICMP. Regras podem usar:
    - Endereço IP de origem
    - Endereço IP de destino
    - Porta de origem TCP/UDP
    - Porta de destino TCP/UDP
    - Flags do TCP (sentido das conexões)
    - Mensagens ICMP (tipos e códigos das msg)
  - Pacotes podem ser aceitos, rejeitados ou dropados

Firewall

- Filtro de Pacotes:
  - Limitações de segurança
    - Não conseguem barrar ataques de fragmentação
    - Não verificam *payload*, apenas os cabeçalhos
    - Não guardam o estado das conexões quando são do tipo stateless (se o enunciado não disser o tipo, é stateless)
    - **Vulnerável ao IP SPOOFING**
    - Não oferece autenticação do usuário

Firewall

- Proxy
  - Servem para intermediar a comunicação entre cliente e servidores
  - Pode trabalhar na camada de:
    - Sessão ou de transporte: ***circuit level***
      - Relay – não verifica serviços
      - Ex.: outro serviço que utiliza porta 80 pode passar pelo proxy
    - Aplicação: ***application level***
      - O Payload é filtrado. Ex.: tags HTML filtradas em proxy HTTP
  - Fazem com que o tráfego pareça ter origem no proxy, o que mascara o endereço host interno – maior segurança da rede interna com o uso do NAT

Vantagem: Permite uso de autenticação !

Desvantagem: não filtra conteúdo

Desvantagem: depende da aplicação

Firewall

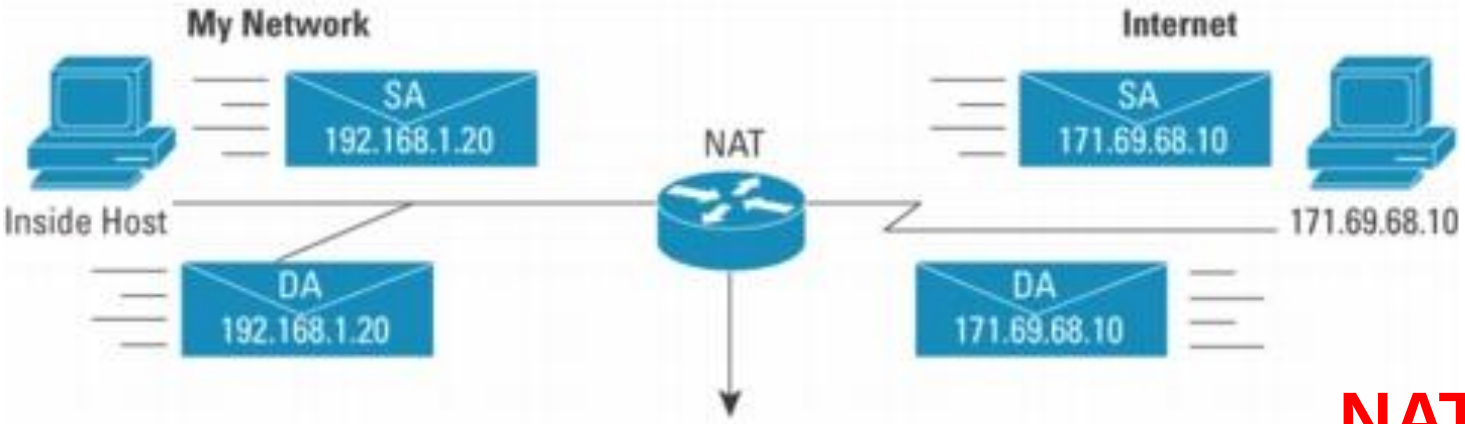
- Proxy
  - NAT – Network Address Translation
    - Converte endereços privados da rede interna em um ou mais endereços públicos
    - Oculta endereços internos
    - RFC 1631
    - Único host faz solicitação para toda a rede
    - Implementada na camada de transporte/rede (sockets)

Firewall

- NAT
  - Conversão estática
    - Encaminhamento de portas **PAT, NAT-PT ou NAPT**
    - Usada quando se tem recurso dentro da rede interna que se quer colocar disponível de forma pública
  - Conversão dinâmica
    - Automática, de modo oculto ou mascaramento de IP
    - Um endereço IP visível para fora
    - Cada IP público suporta 65536 conexões (máximo teórico)

NAT x PAT

- RFC's 1631, 2663 e 3022 não citam PAT, e sim NAPT
- A ideia do PAT é poder suportar "overloading" de conexões (ex.: servidor Web na rede privada), usando também a troca de portas



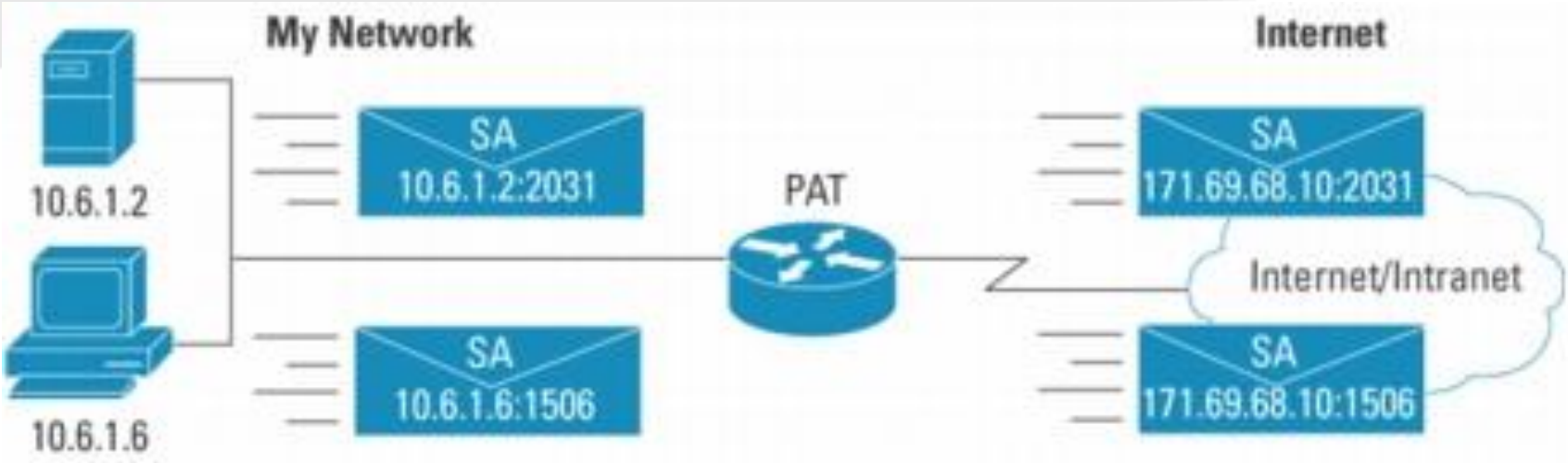
Pro	Inside Global	Inside Local	Outside Local	Outside Global
—	—	—	192.168.1.20	171.69.68.10

192.168.1.20 is inside local address

171.69.68.10 is inside global address

NAT NORMAL

NAPT (PAT)



Port Address Translation (PAT) extends NAT from "1 to 1" to "many-to-1" by associating the source port with each flow

Pro	Inside Global	Inside Local	Outside Local	Outside Global
tcp	171.69.68.5:1405	10.6.15.2:1405	204.71.200.69:80	204.71.200.69:80

PAT (Port Address Translation) includes ports in addition to IP addresses

- Many-to-one translation
- Maps multiple IP addresses to 1 or a few IP addresses
- Unique source port number identifies each session
- Conserves registered IP addresses
- Also called NAPT in IETF documents

Firewall

- Proxy nível aplicativo (Aplicação)
  - Operam como Firewall (barreira de proteção)
  - Podem ser usados para armazenar caches de páginas web
  - Ocultam os clientes privados (NAT)
  - Podem bloquear URLs suspeitas (blacklists)
  - Podem filtrar payload antes de passá-lo ao cliente
  - **Previne contra ataques de fragmentação, roteamento de origem, DoS**
- Mas...
  - Criam um ponto único de falha
  - Um proxy para cada tipo de serviço

Proxy de Aplicação

- Vantagens
  - Não permite conexões diretas entre hosts internos e externos
  - Pode implementar autenticação do usuário
  - Analisa comandos da aplicação no payload dos pacotes
  - Permite criar logs de tráfego e atividades específicas
- Desvantagens
  - É MUITO mais lento que o filtro de pacotes
  - Requer um proxy específico para cada aplicação
  - Não trata pacotes ICMP ← **Permite a ação de Rootkits, Botnets, etc**
  - Não aceita os serviços para os quais não foi projetado
  - Requer que os clientes internos saibam sobre ele
    - **Exceto proxies transparentes – que redirecionam as sessões que passam pelo firewall para um serviço de proxy local de modo transparente**

Firewall

- **Filtro de Pacotes Dinâmico (*Stateful Inspection*)**
  - Permitem abrir regras dinâmicas que valem para aquele momento, naquelas portas, entre aqueles endereços IP, obedecendo a sequência TCP.
  - Filtragem de pacotes → feita com base nas regras do firewall **E** na tabela de estados
  - Maior segurança que filtros estáticos
  - Em vez de trabalhar apenas com um conjunto de critérios estáticos (ACL) , coletam informações sobre os pacotes trafegados, armazenando em tabela de estados
  - Também trabalha na camada de rede = filtro de pacotes
  - Principal diferença do filtro de pacotes = estado de conexões monitorado a todo instante
    - Ex. Checkpoint Firewall

Filtro de pacotes baseado em estado

- Vantagens
  - Menor overhead que os Proxies, porém maior que o filtro stateless
  - Independe da Aplicação
  - Mais poderoso que os filtros stateless
- Desvantagens
  - Permite conexão direta para hosts internos a partir de redes externas
  - Não oferece autenticação do usuário, a não ser via gateway de aplicação
  - Mesmas vulnerabilidades do stateless (IP spoofing, teardrop, etc.)

Firewall

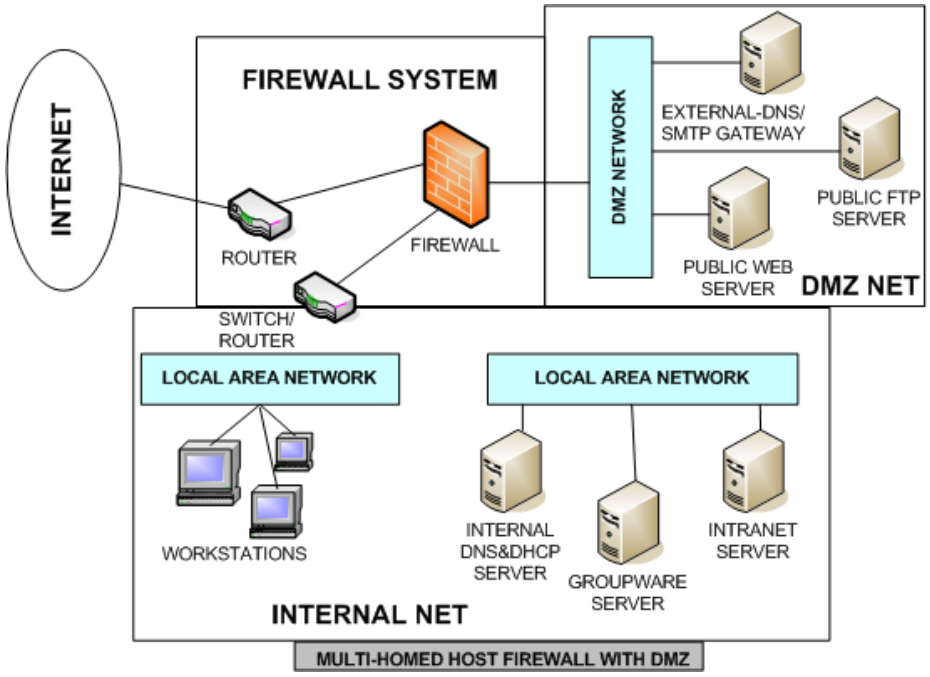
Tecnologia	Performance	Segurança	Facilidade de uso
Filtro Estático	3	1	2
Proxy	1	3	2
Filtro Dinâmico	2	2	3

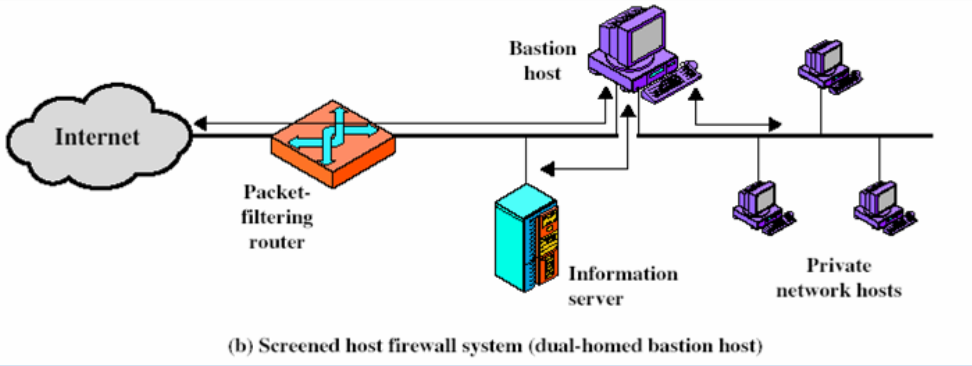
Tabela comparativa entre os tipos de firewall com notas de 1 a 3.
Fonte: Guia oficial para Formação de Gestores em Segurança da Informação – Security Officer – Volume 2 - Módulo Education Center

Obs.: Quanto maior a nota, melhor...

Arquiteturas de Segurança

- DMZ – zona desmilitarizada
  - Permite que serviços sejam prestados a usuários externos (bastion hosts) ao mesmo tempo que protegem a rede interna dos acessos externos
- Bastion Host
  - Elemento que concentra todas as soluções de segurança





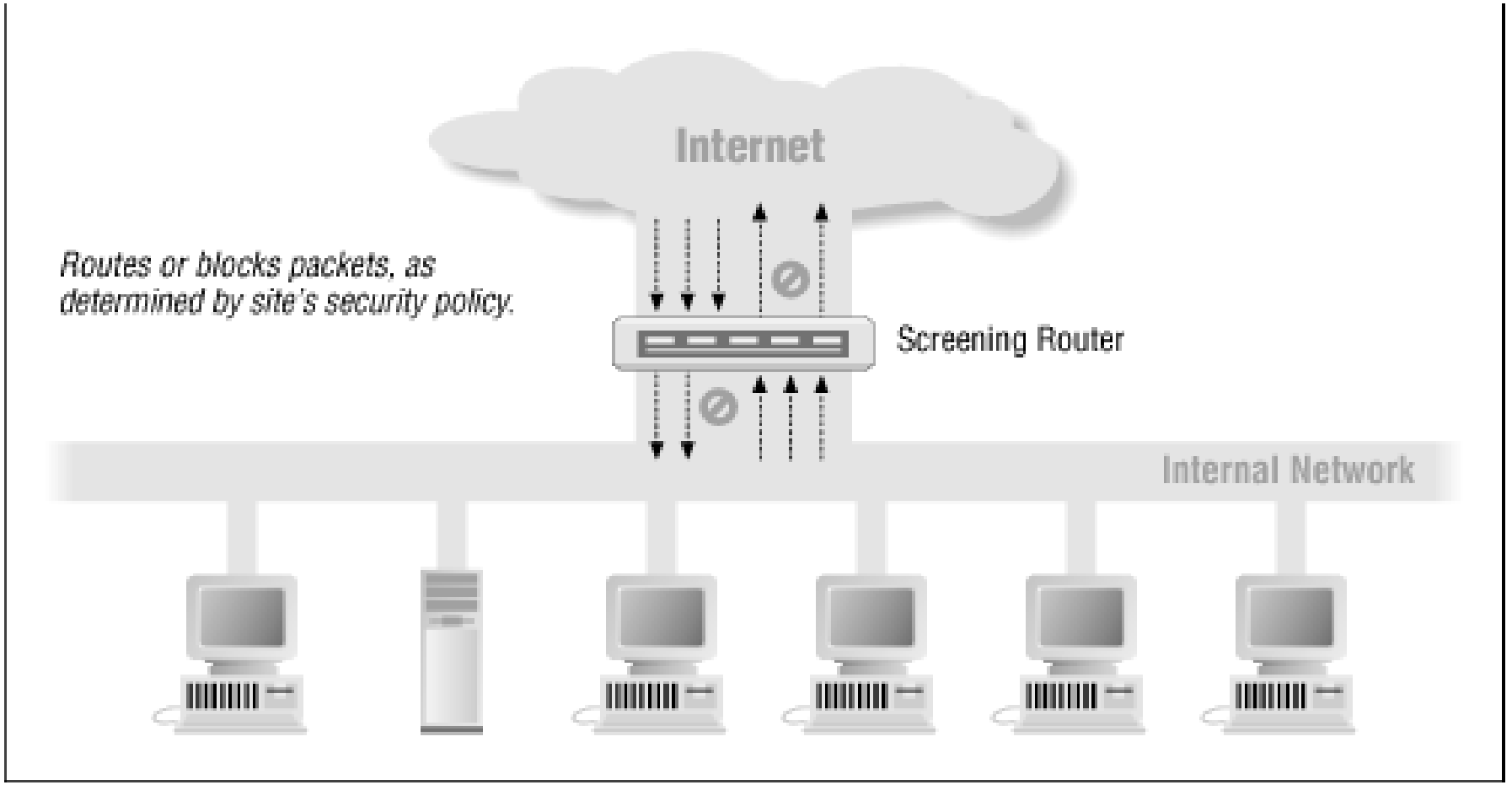
(b) Screened host firewall system (dual-homed bastion host)

Arquiteturas de Segurança

- Single Box – único dispositivo sendo o firewall da rede
  - Roteador com ACL
  - Dual-Homed-Host
- Screened Host
- Screened Subnet

Arquiteturas de Segurança

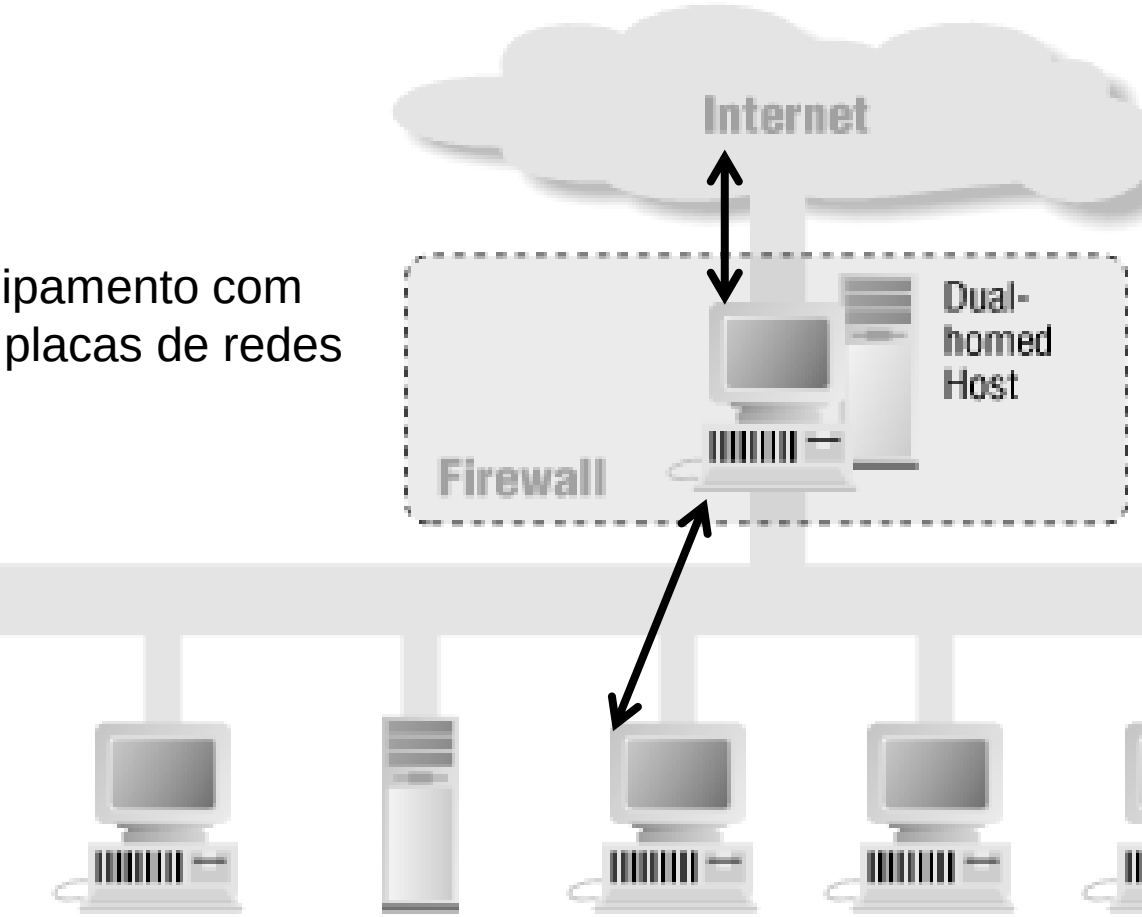
- Roteador com ACL



Arquiteturas de Segurança

- Dual-Homed-Host

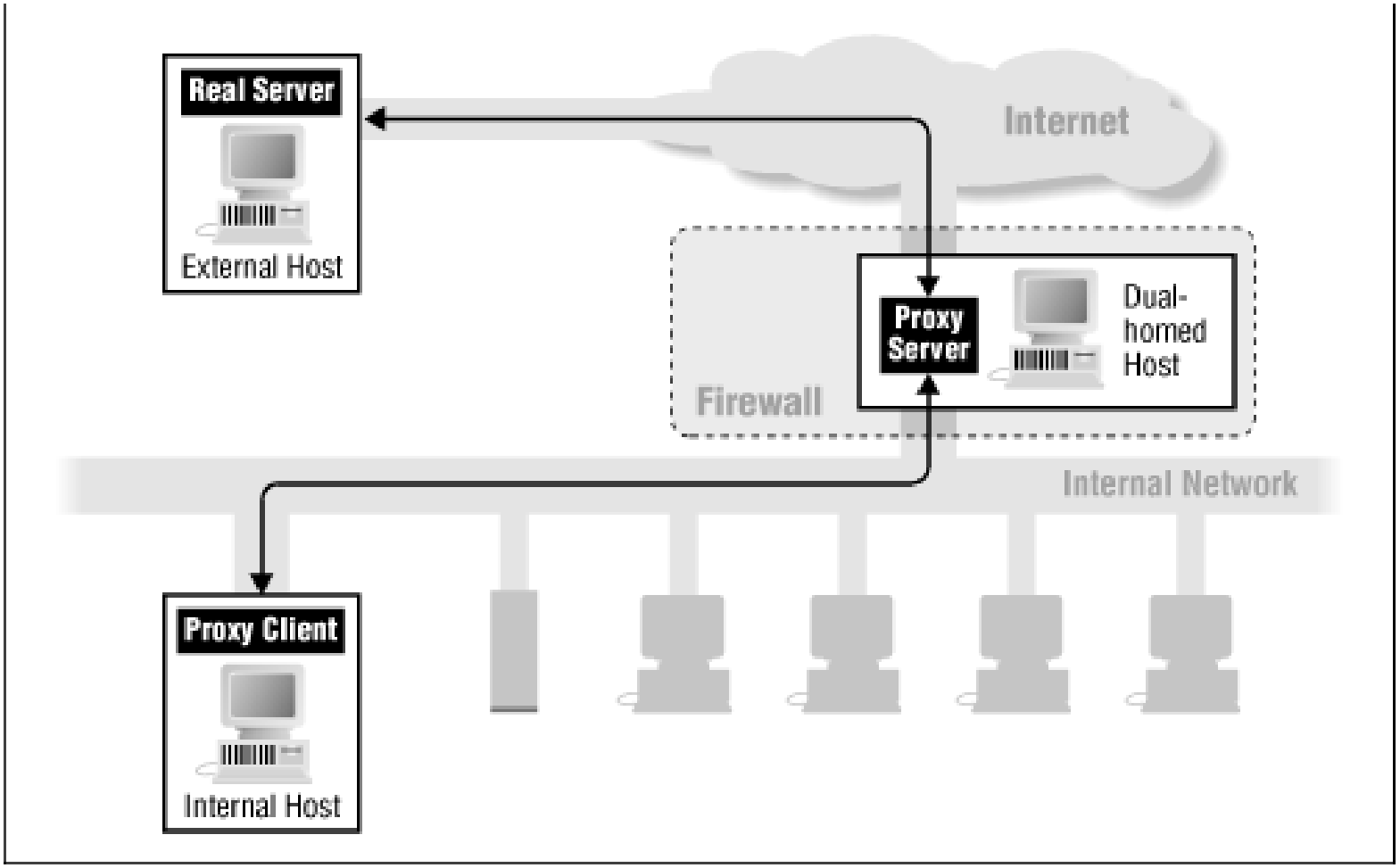
- Equipamento com duas placas de redes



-Conexão em duas etapas
-Roteamento tem que ser desabilitado no FW

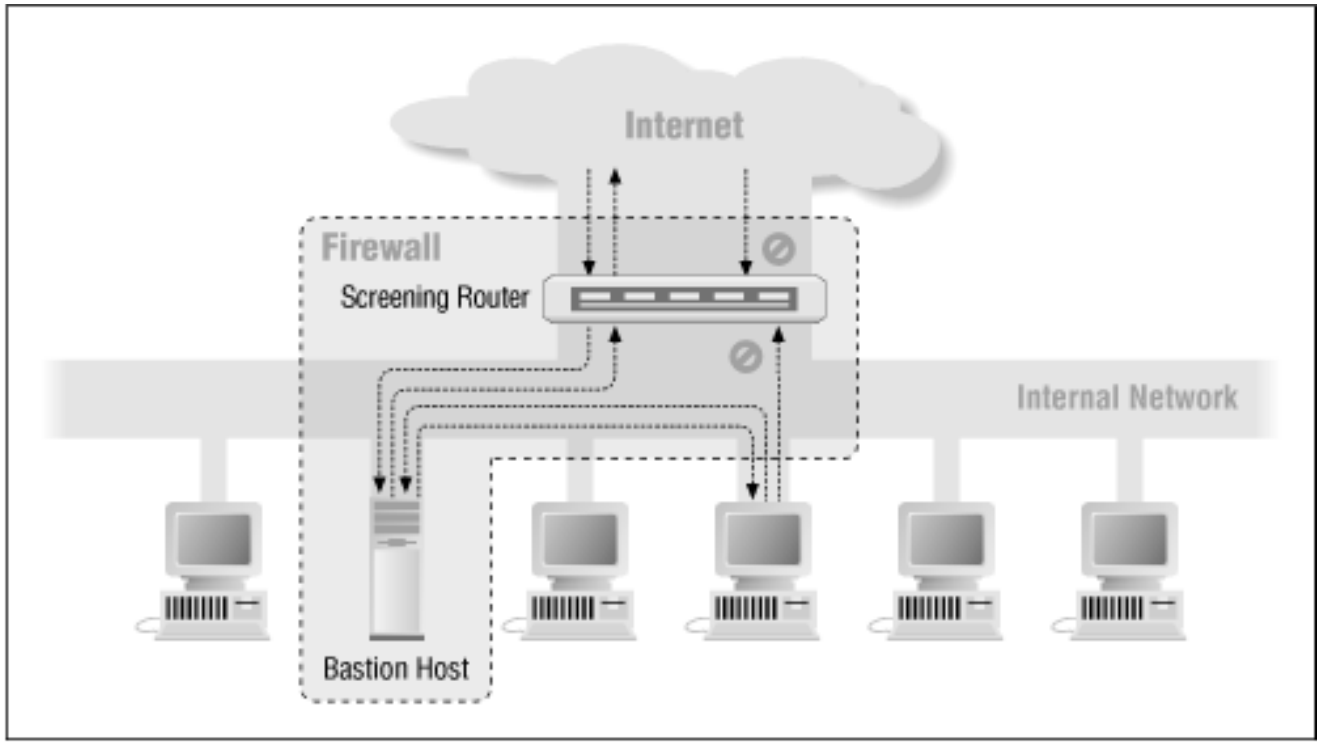
Arquiteturas de Segurança

- Serviço de Proxy com Dual-Homed-Host



Arquiteturas de Segurança

- Screened Host
  - Bastion Host – recebe acessos externos por trás de um firewall, dentro da rede interna, junto com outros recursos



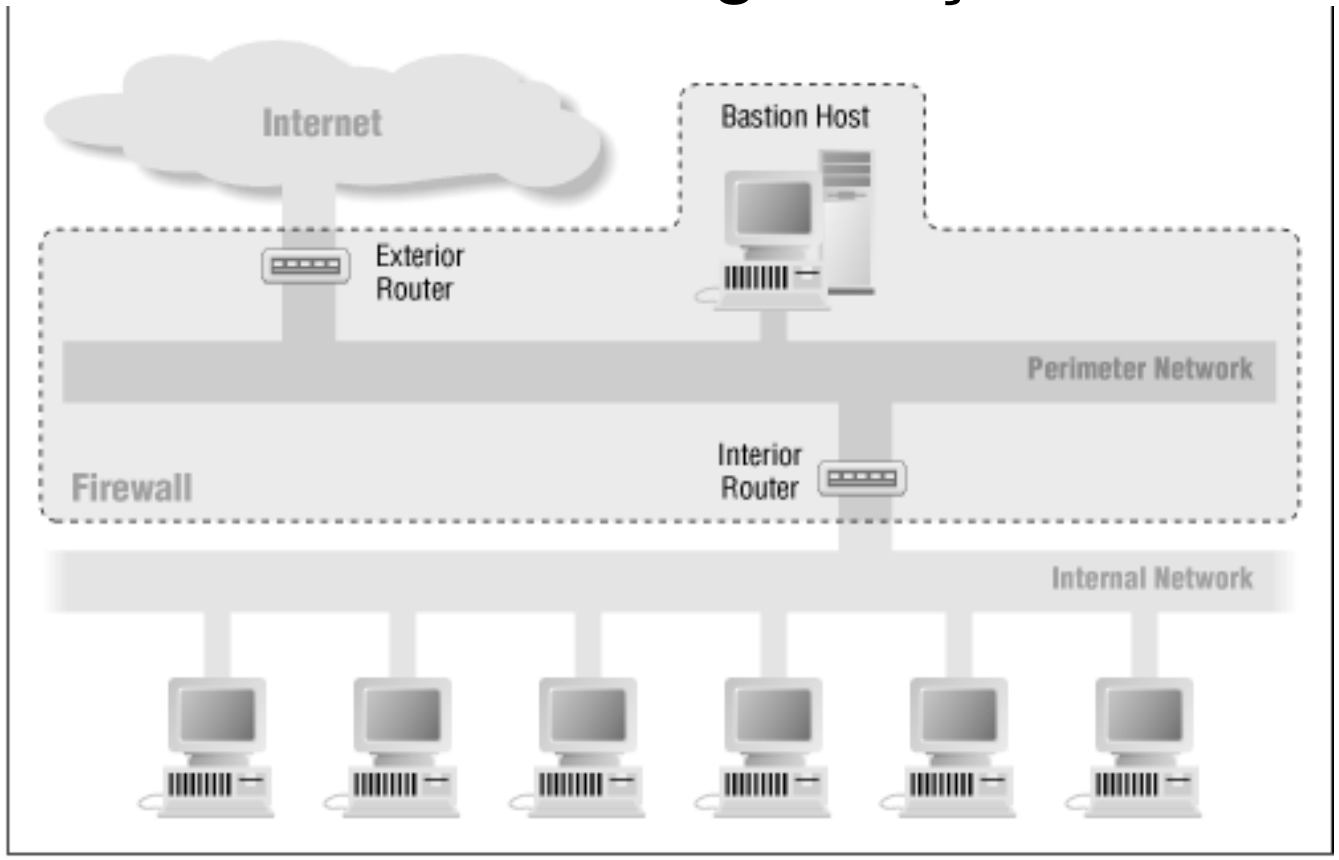
- formada por um filtro de pacotes + bastion host

-Tráfego de fora para dentro somente pelo bastion host

- Se o Bastion host for comprometido, o invasor estará dentro da rede interna

Arquiteturas de Segurança

- Screened subnet – com uso de dois roteadores/Firewall e um bastion host. Perímetro de Segurança chamado DMZ



- se o Bastion host for comprometido, o invasor NÃO estará dentro da rede interna e sim na DMZ

-Filtros internos e externos devem ter configurações compatíveis (interno mais robusto)

-Variação: FW com 3 placas de rede

IDS – Intrusion Detection System

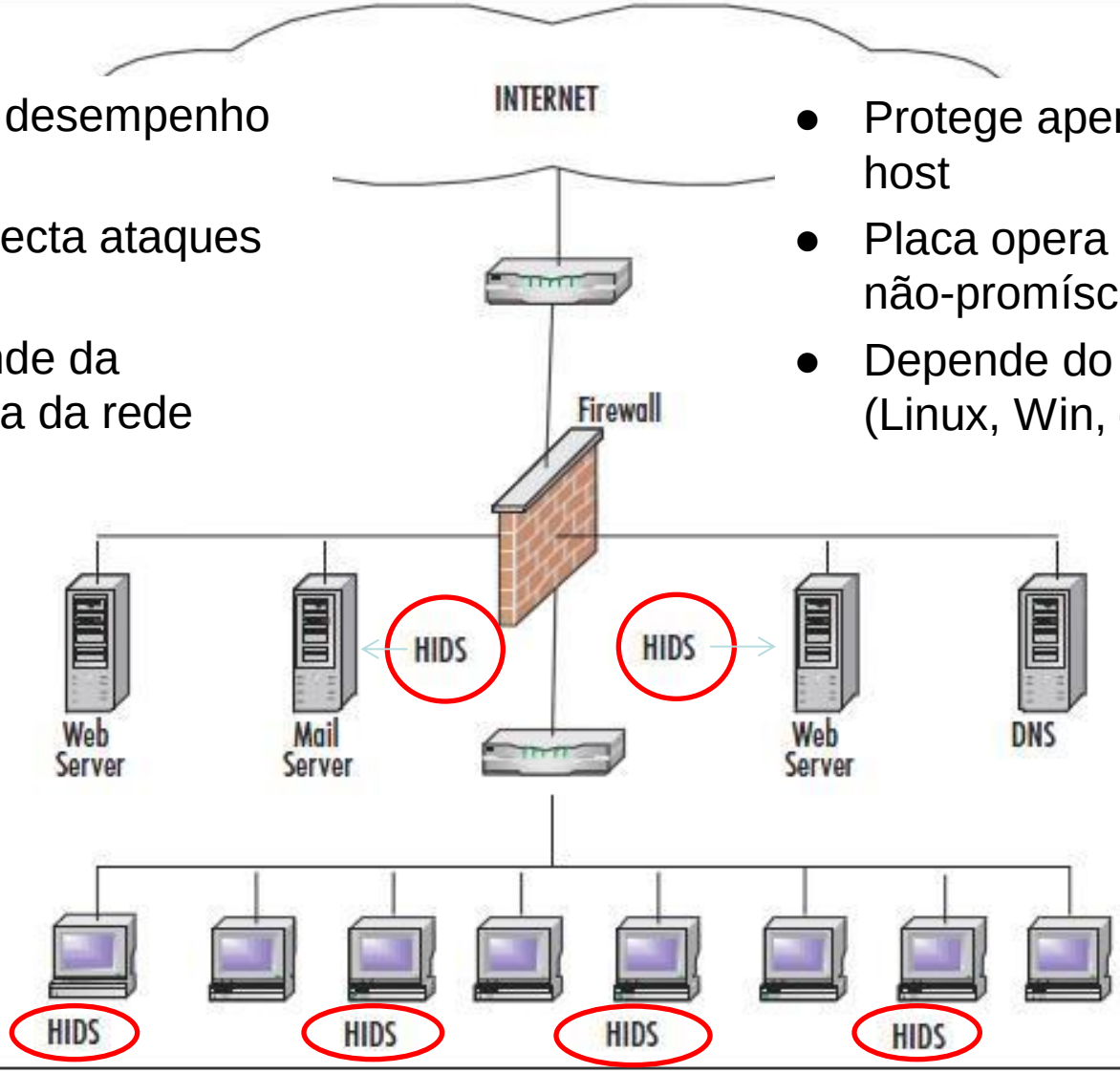
- IDS - Sistemas de **<u>Detecção</u>** de Intrusão
  - Detectar ataques e intrusões (*store and forward*)
  - Ferramenta especializada que sabe ler e interpretar o conteúdo de arquivos de log de roteadores, firewalls, servidores e outros dispositivos de redes
  - Utilizam banco de dados de assinaturas de ataque conhecidas mas podem também usar heurísticas
  - Pode comparar padrões de atividade, tráfego ou comportamento no tráfego monitorado, comparando com as assinaturas
  - Pode emitir alerta, adotar ações automáticas (desativação de links, serviços, ativação de rastreadores, reunir evidência, etc)

SDI (IDS) - Sistemas de Detecção de Intrusão

- O SDI (IDS) tem que ter a capacidade de manter o "estado" dos pacotes, remontar os fragmentos e depois fazer a análise.
- De acordo com sua localização:
  - de hosts (SDIH) (inglês: HIDS) – no host
  - de rede (SDIR) (inglês: NIDS) – em um segmento
- Dois métodos de detecção ou estratégias de análise de evento:
  - Detecção de assinaturas
    - Banco de dados com assinaturas de ataques
  - Detecção de anomalia
    - Regras e conceitos pré-definidos sobre atividades "normais" e "anormais" chamadas *heurísticas.*

SDIH (HIDS) – Sistema de Detecção de Intrusão de Hosts

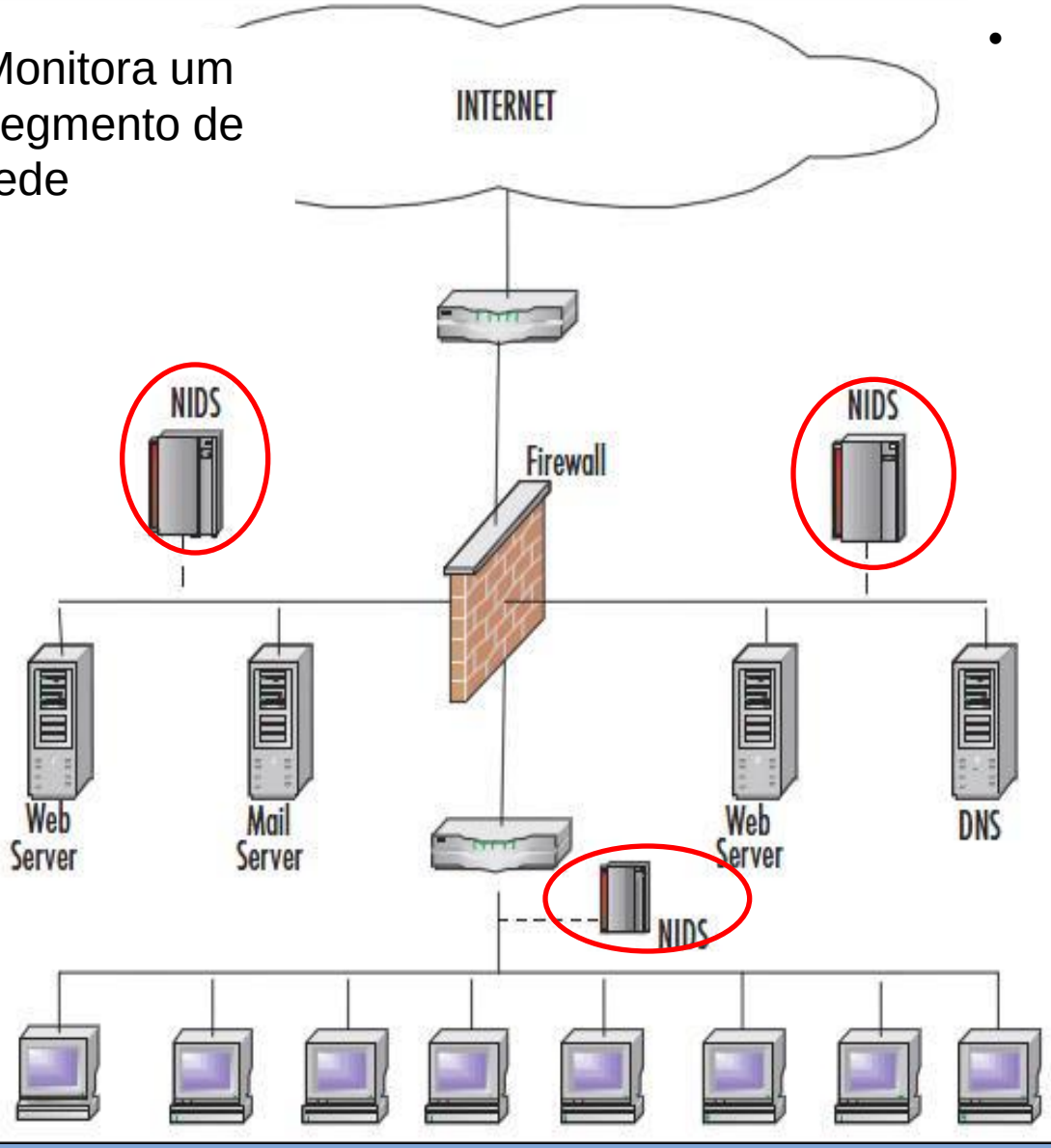
- Diminui desempenho do host
- Não detecta ataques de rede
- Independe da topologia da rede



- Protege apenas o host
- Placa opera no modo não-promíscuo
- Depende do SO (Linux, Win, etc.)

SDIR (NIDS) – Sistema de Detecção de Intrusão de Rede

- Monitora um segmento de rede



- Deve operar em modo promíscuo para captar todas as comunicações no segmento de rede
- Port scanning, ip spoofing, teardrop, podem ser detectados, pois há a análise do cabeçalho e payload

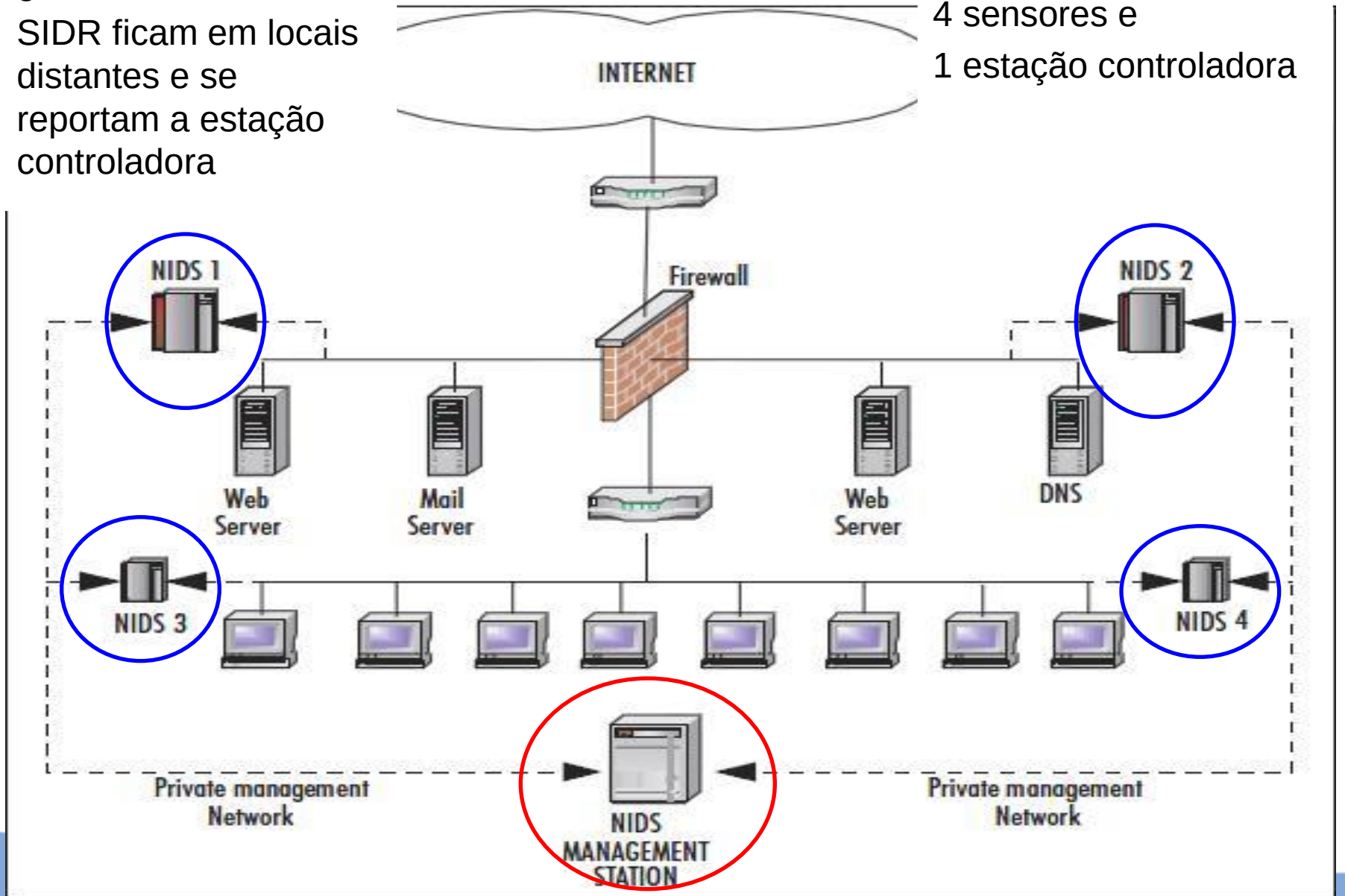
SDID – Sistema de Detecção de Intrusão Distribuídos

- Possui estação de gerenciamento
- SIDR ficam em locais distantes e se reportam a estação controladora

- Na fig. Temos:

4 sensores e

1 estação controladora



SDI (IDS) – Resultados possíveis da detecção

- Comportamento Normal
  - Tráfego suspeito detectado
  - Tráfego legítimo que o IDS analisa como legítimo
- Falso Positivo
  - Tráfego legítimo que o IDS analisa como suspeito
- Falso Negativo
  - Tráfego suspeito não detectado
  - Ataque não detectado

IPS – Intrusion Prevention System

- SPI (IPS) - Sistema de Prevenção de Intrusão
- Operação *in line*
  - Capaz de detectar os ataques e preveni-los
  - Todos os pacotes passam pelo sistema que faz a verificação de todo o fluxo
  - É intrinsecamente ativo, ou seja, havendo a detecção de um ataque, uma ação de proteção é executada

Honeypot x Honeynet

- Honeypot é um recurso preparado especificamente para ser sondado, atacado ou comprometido e para registrar essas atividades. Tipos:
  - **De produção** – adiciona segurança para organização; usado para ajudar a mitigar riscos
  - **De pesquisa** – não protege a rede, é usado para aprender como os atacantes estão operando

- Honeynet é uma rede projetada especificamente para ser comprometida e utilizada para observar os invasores. Essa rede normalmente é composta por sistemas reais e necessita de mecanismos de contenção eficientes e transparentes, para que não seja usada como origem de ataques e também não alertar o invasor do fato dele estar em uma honeynet

Honeypots em uma Honeynet