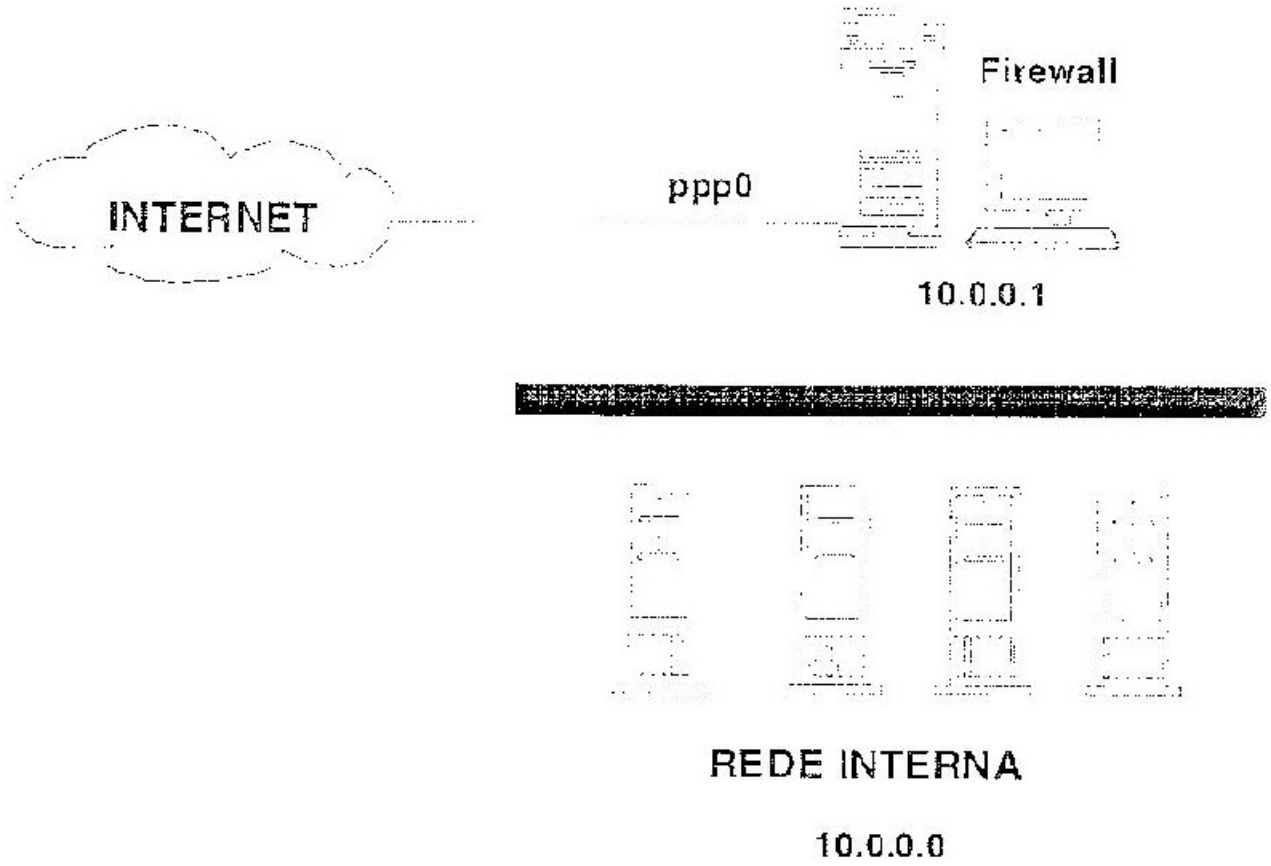
Segurança de Perímetro

Roteador de Perímetro
DMZ
Hosts de Segurança
Gateway de Aplicativo

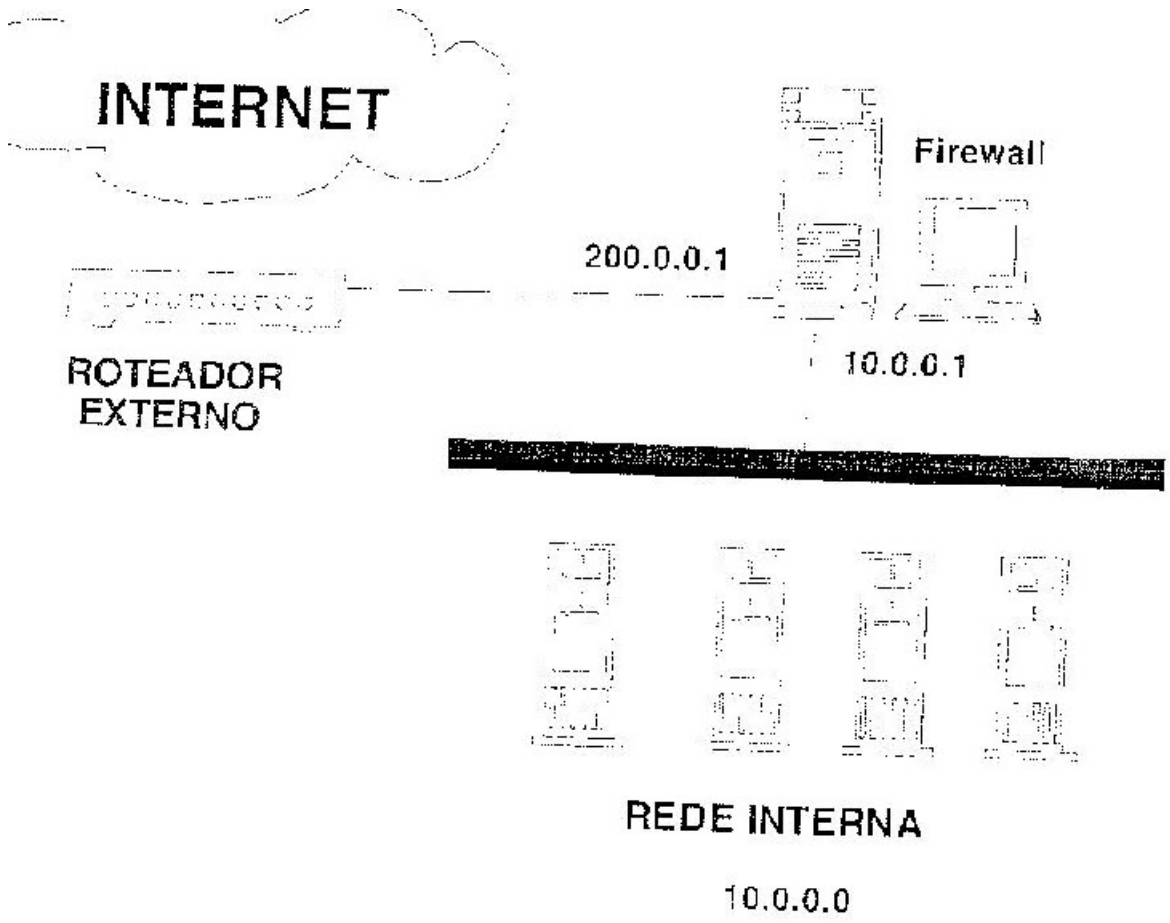
Conectando-se à Internet com Segurança

- Soluções mais simples.
- Sistemas de Segurança de Perímetro
- Zona Desmilitarizada (DMZ)
- Roteador de Perímetro
- Tipos de Firewalls
- Hosts de Segurança
- Gateways de Aplicativo

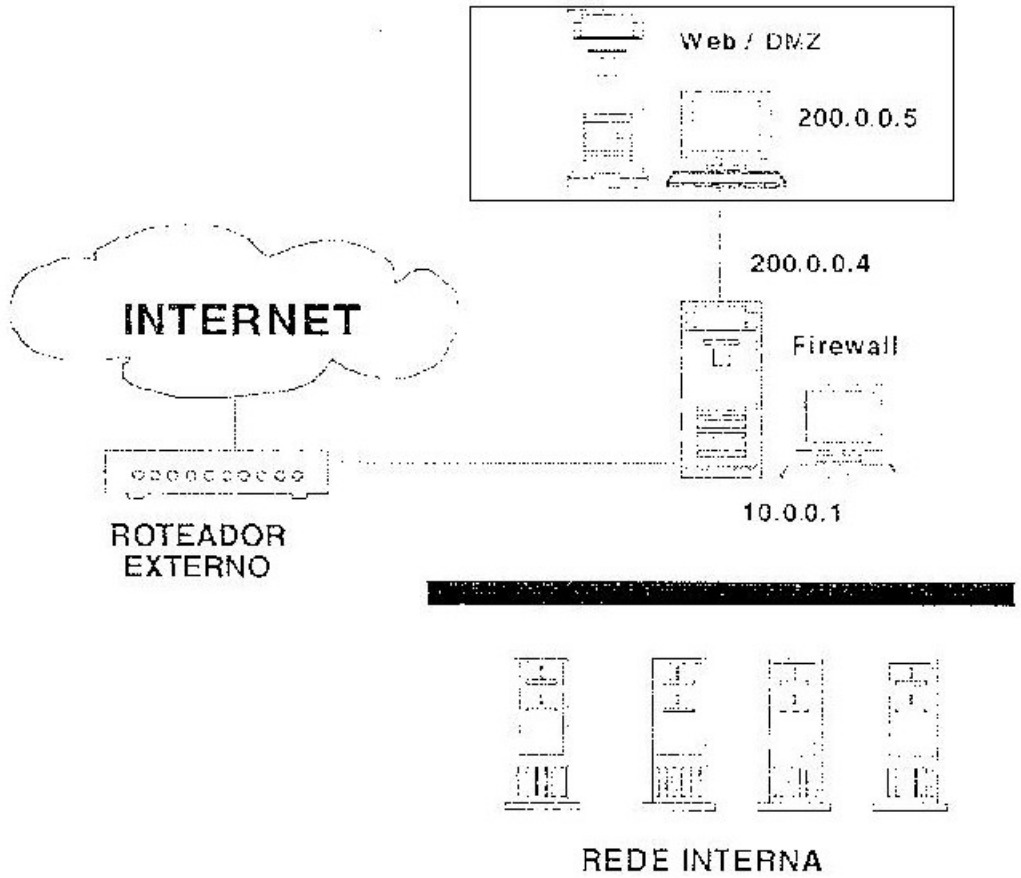
Soluções simples - Para um usuário doméstico de ADSL



Soluções simples - Firewall Corporativo



DMZ – Exemplo para uma empresa real



Segurança de Perímetro

- Implantação de tecnologias de rede para resguardar uma rede contra invasores (intrusos).
- Usada para resguardar a conexão de uma rede corporativa com a Internet.
- Mesmas tecnologias e técnicas usadas para proteger uma parte de uma rede.

Segurança de Perímetro

- A ausência ou insuficiência da segurança de perímetro abre uma brecha na segurança da rede corporativa por onde invasores podem explorar.

- É estabelecida com um roteador de perímetro, o ponto de demarcação entre uma rede desprotegida (Internet) e uma rede protegida.

Segurança de Perímetro

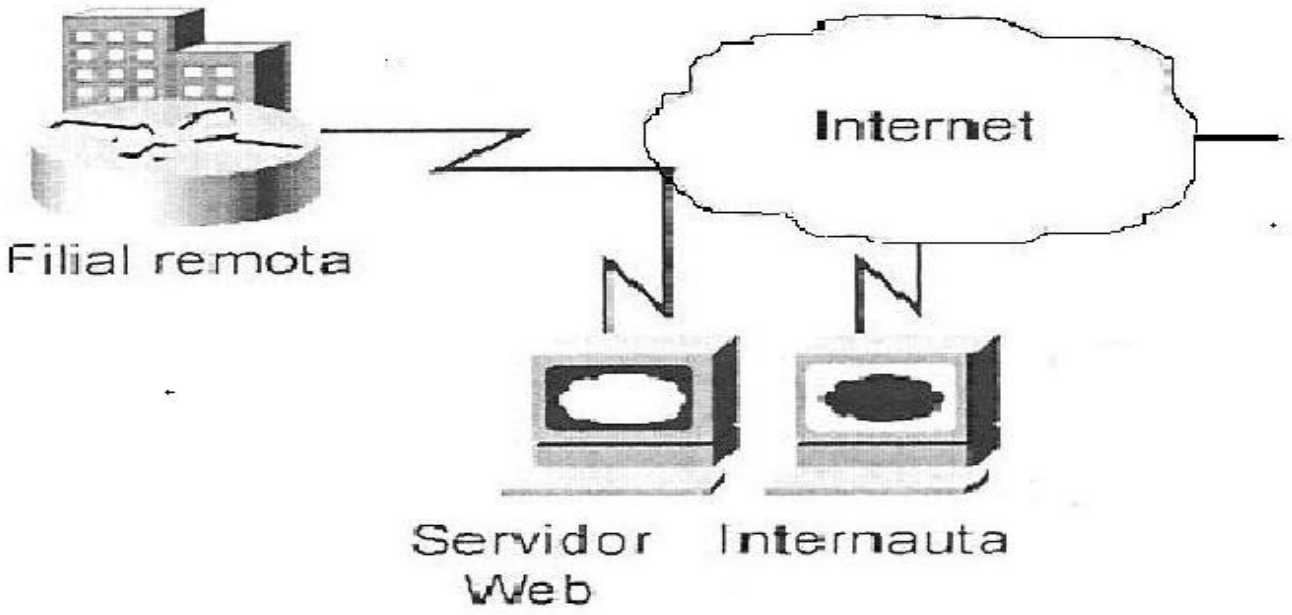
- Um roteador de perímetro pode ser usado para criar uma demarcação entre a Internet desprotegida e uma zona desmilitarizada (DMZ) semi-protegida (DMZ suja).

Segurança de Perímetro

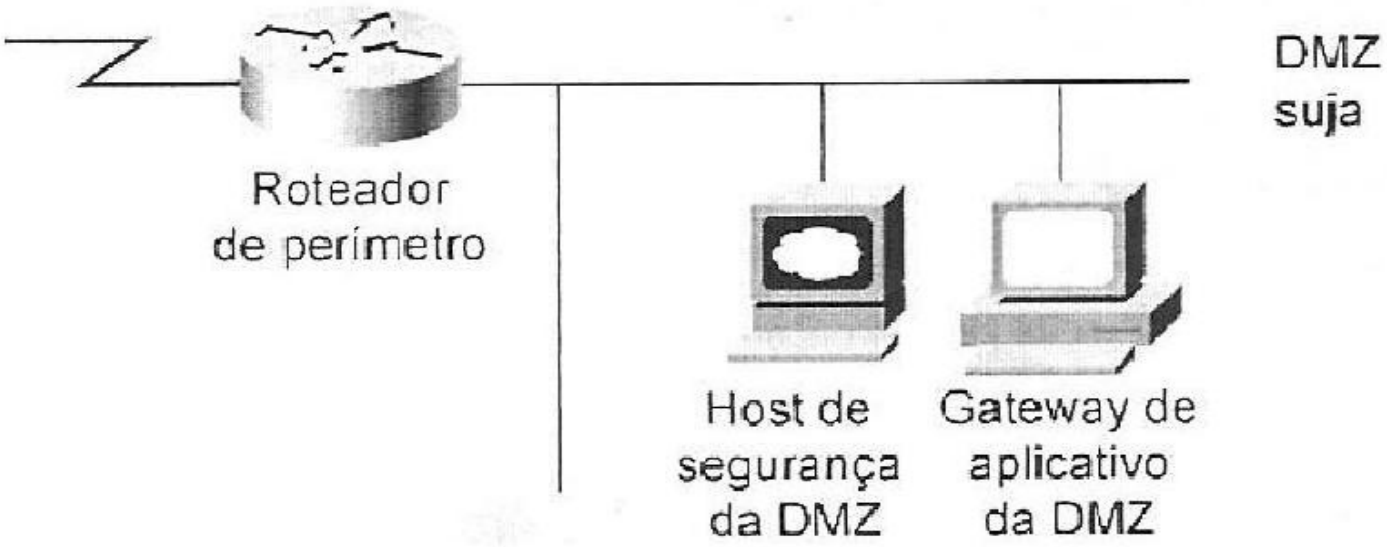
- Uma parte importante é identificar:

  - o **domínio interno** (rede corporativa abaixo do Firewall);
  - o **domínio intermediário**
  - o **domínio externo** (Internet ou um enlace com um fornecedor ou parceiro comercial).

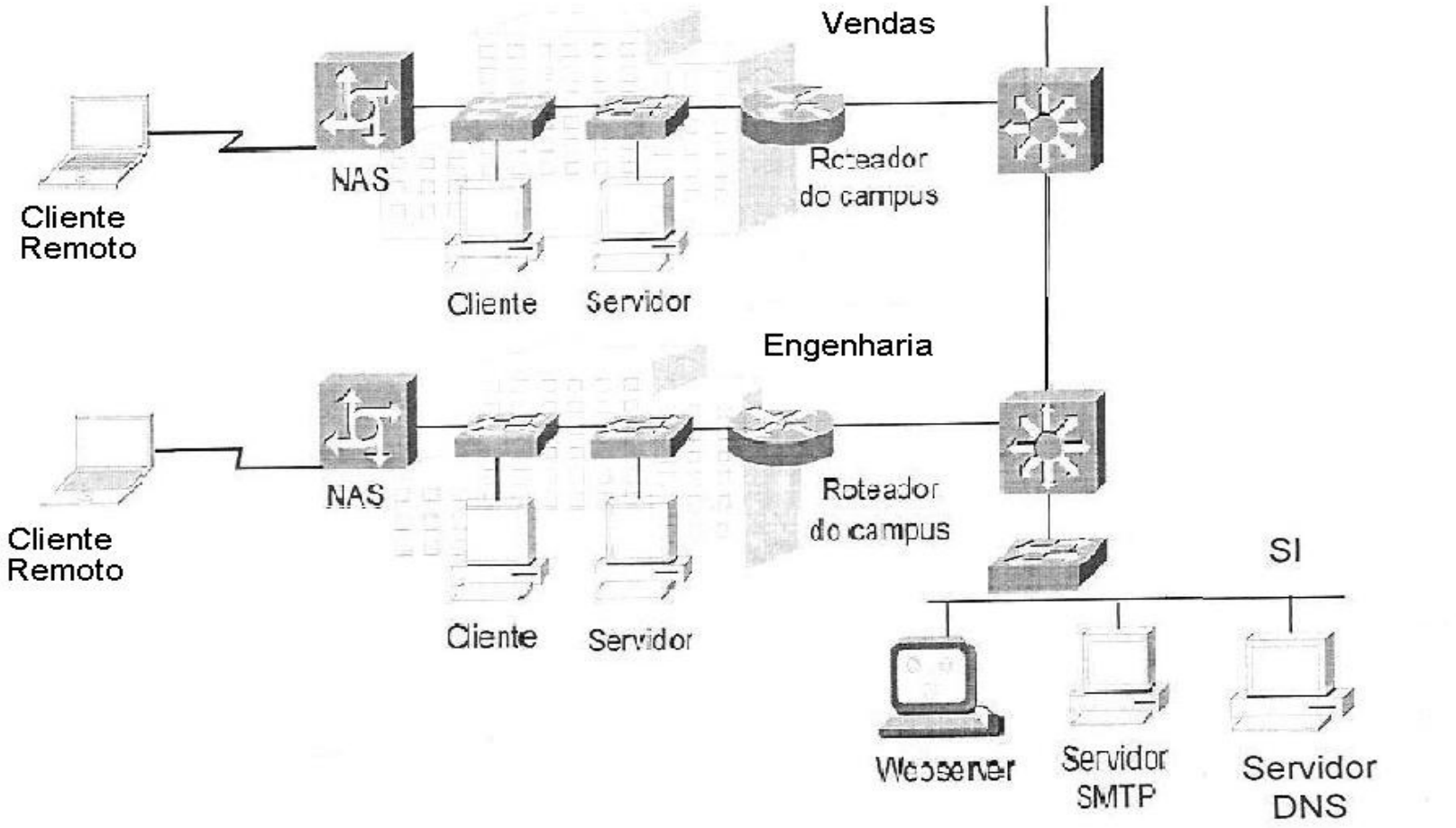
Domínio externo - Internet



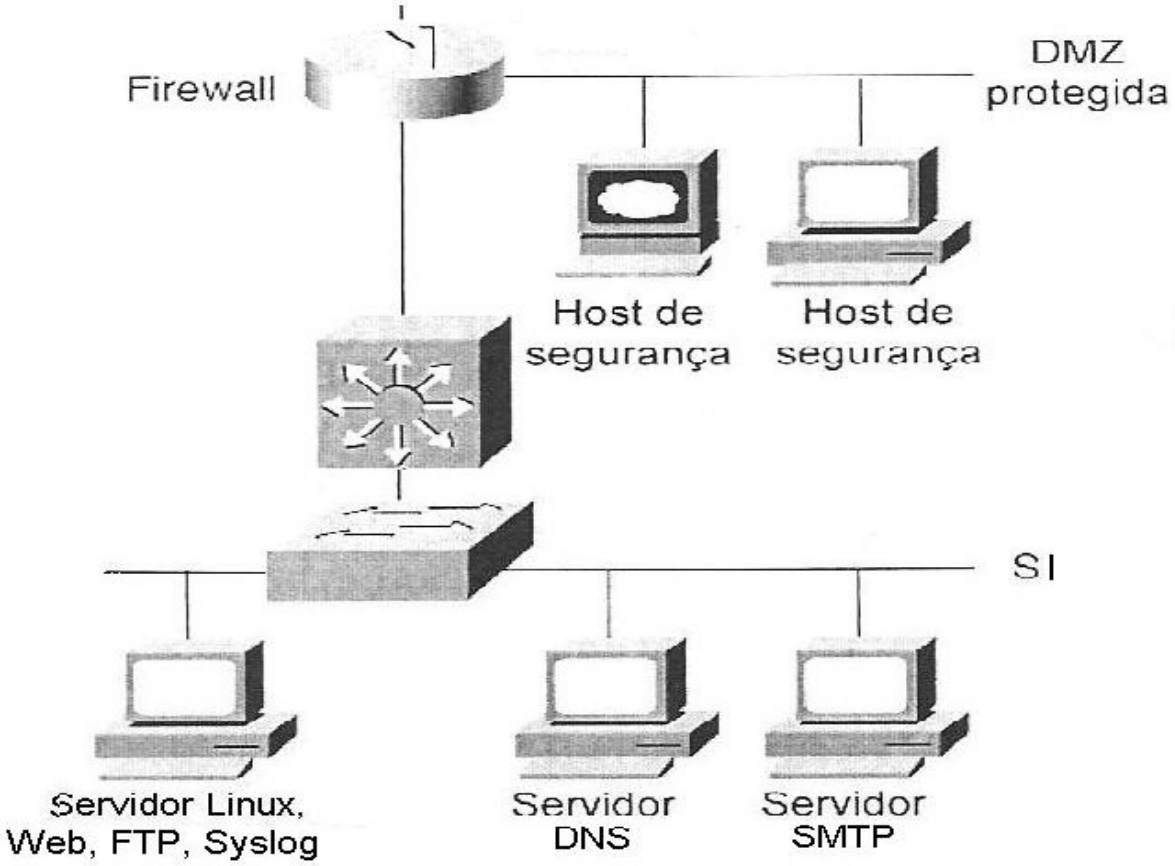
Domínio intermediário

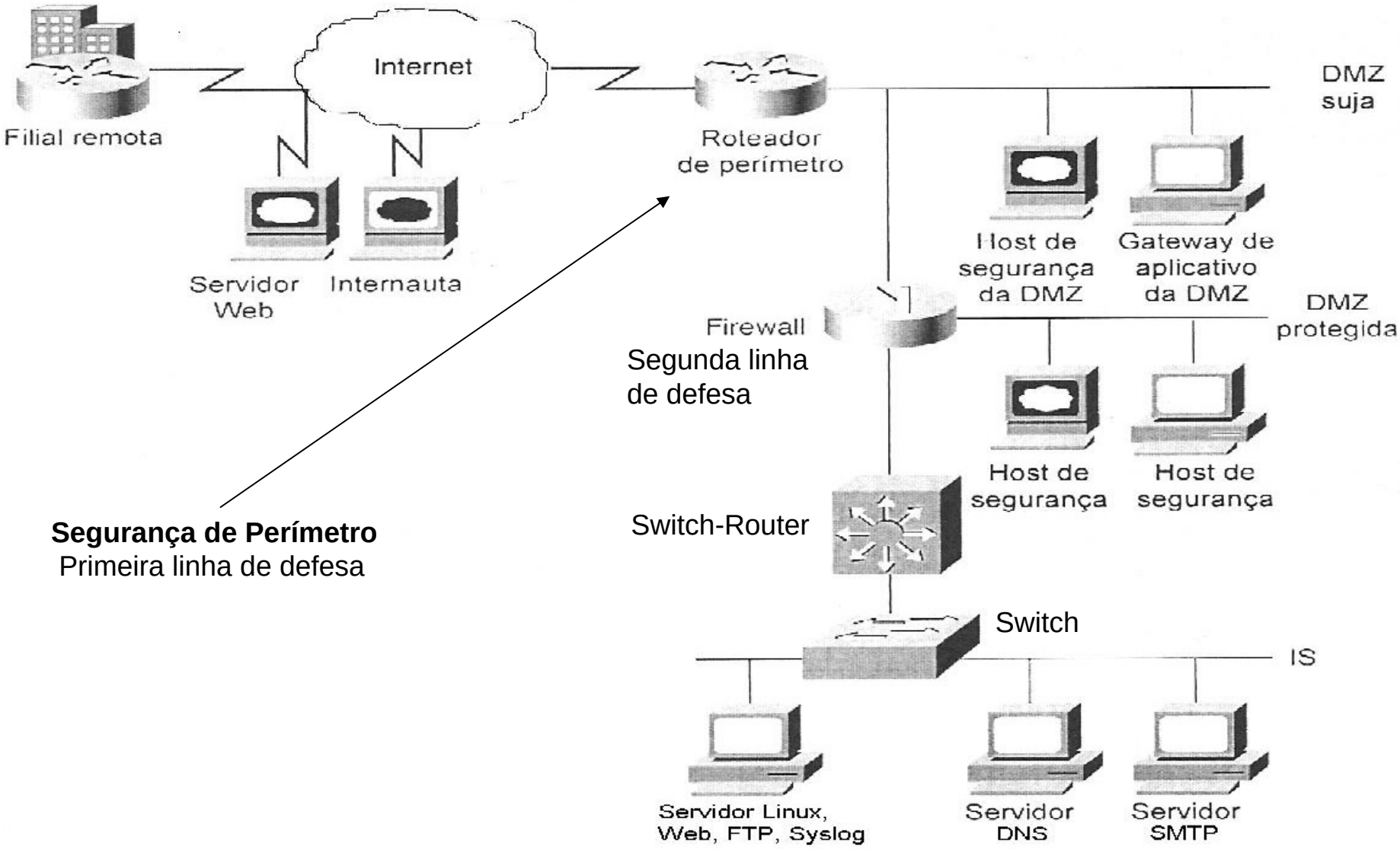


Domínio interno sem segurança de perímetro



Parte do domínio interno com segurança de perímetro





Segurança de Perímetro
Primeira linha de defesa

Segurança de Perímetro

- Pode ser implementada de maneiras diferentes de acordo com:

  - a Política de Segurança;
  - o que precisa ser protegido;
  - o nível de segurança necessário;
  - o orçamento de segurança;
  - outros fatores.

Segurança de Perímetro

- Realizada com elementos de rede, que podem ser combinados de várias maneiras para proteger a rede interna.
- Um **único roteador** poderia ser usado.

Segurança de Perímetro

- Implementada segundo uma topologia, na qual um **roteador de perímetro** é a primeira linha de defesa e um **Firewall** é a segunda linha de defesa.

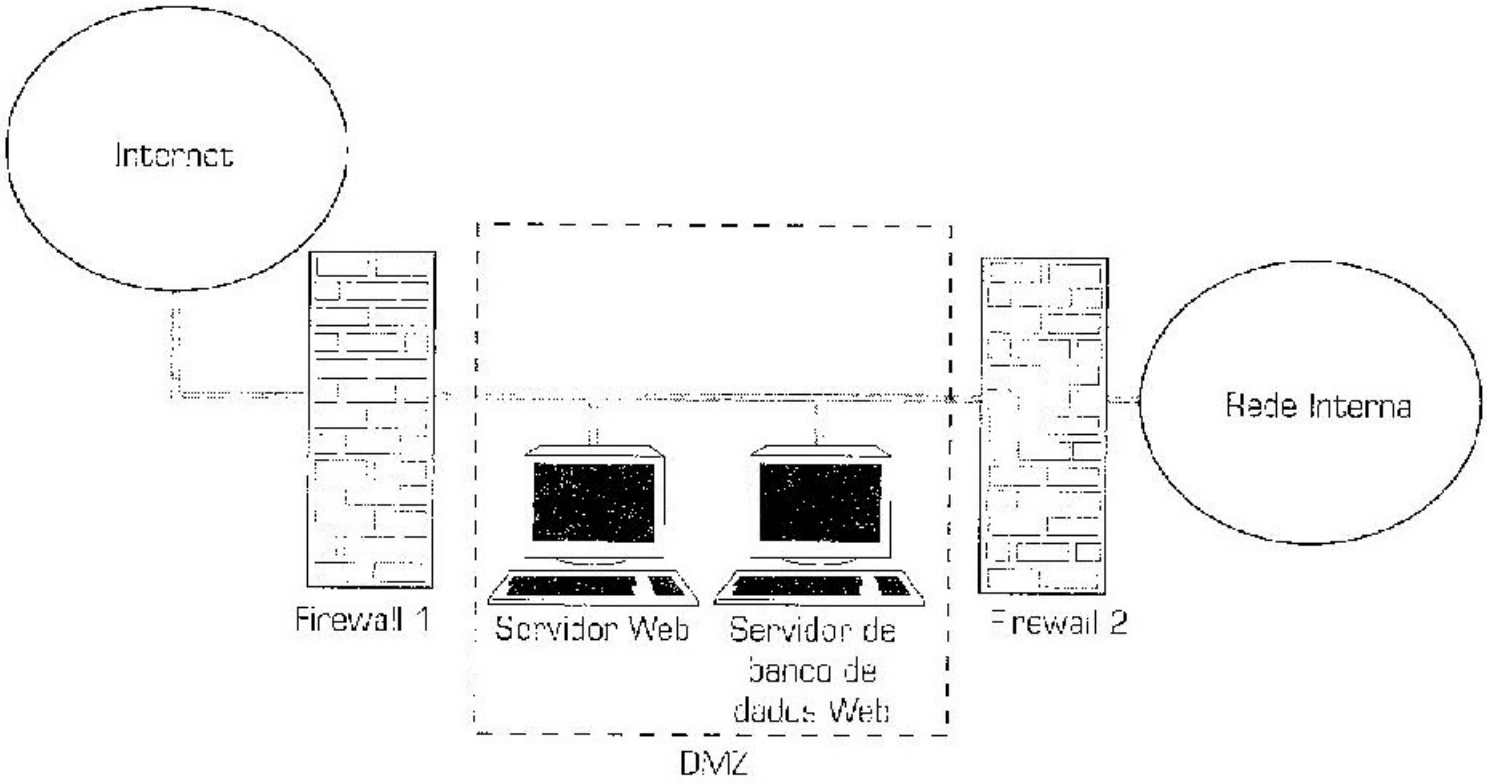
Segurança de Perímetro

- Roteadores de perímetro são usados para **implementar a parte da política de segurança de rede** que especifica **como a rede interna será conectada à rede externa**.

Conceito de DMZ – DeMilitarized Zone

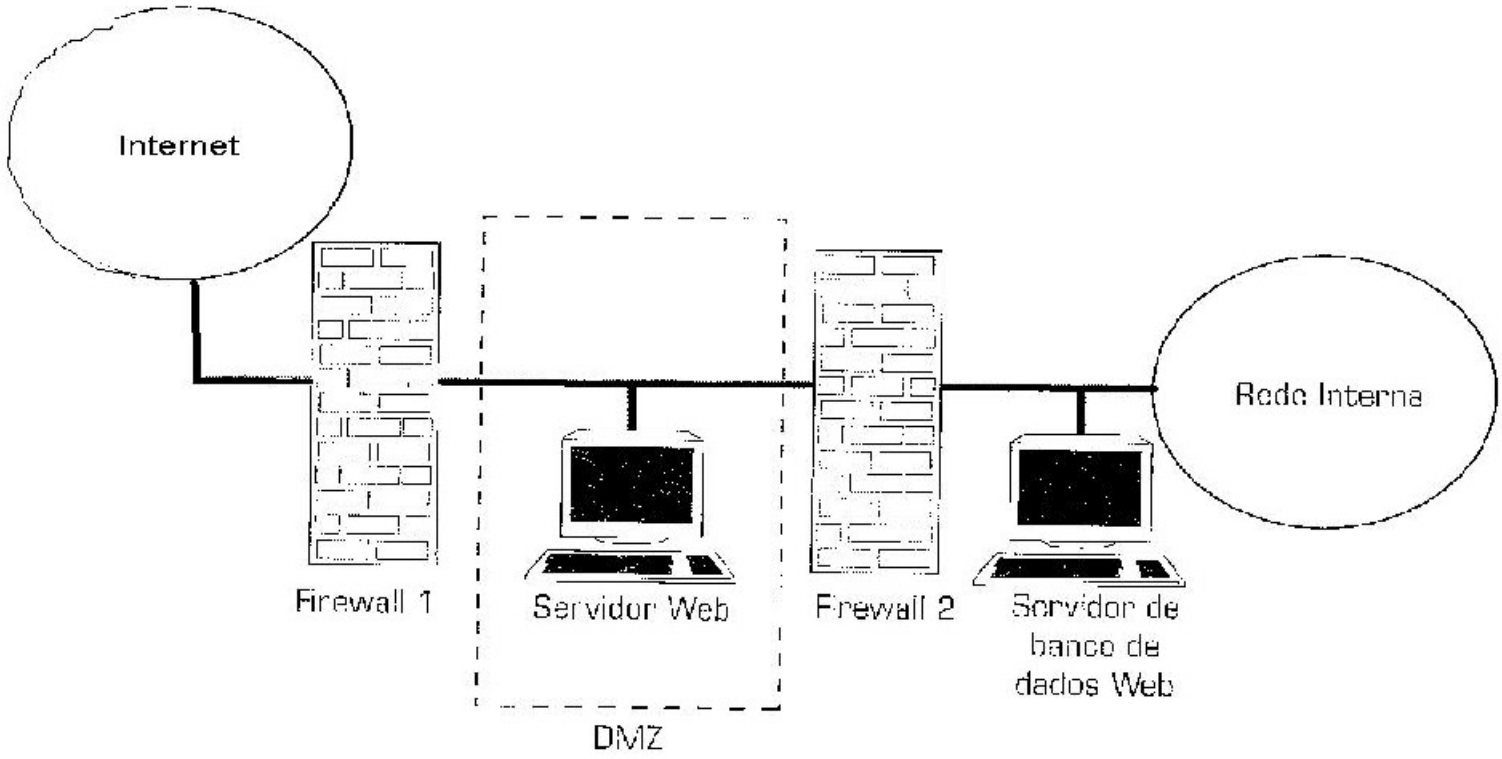
- Rede intermediária entre a rede externa (Internet) e a rede corporativa interna.
- Requer **dois firewalls** para ser implementada.

DMZ – Conceito Inicial



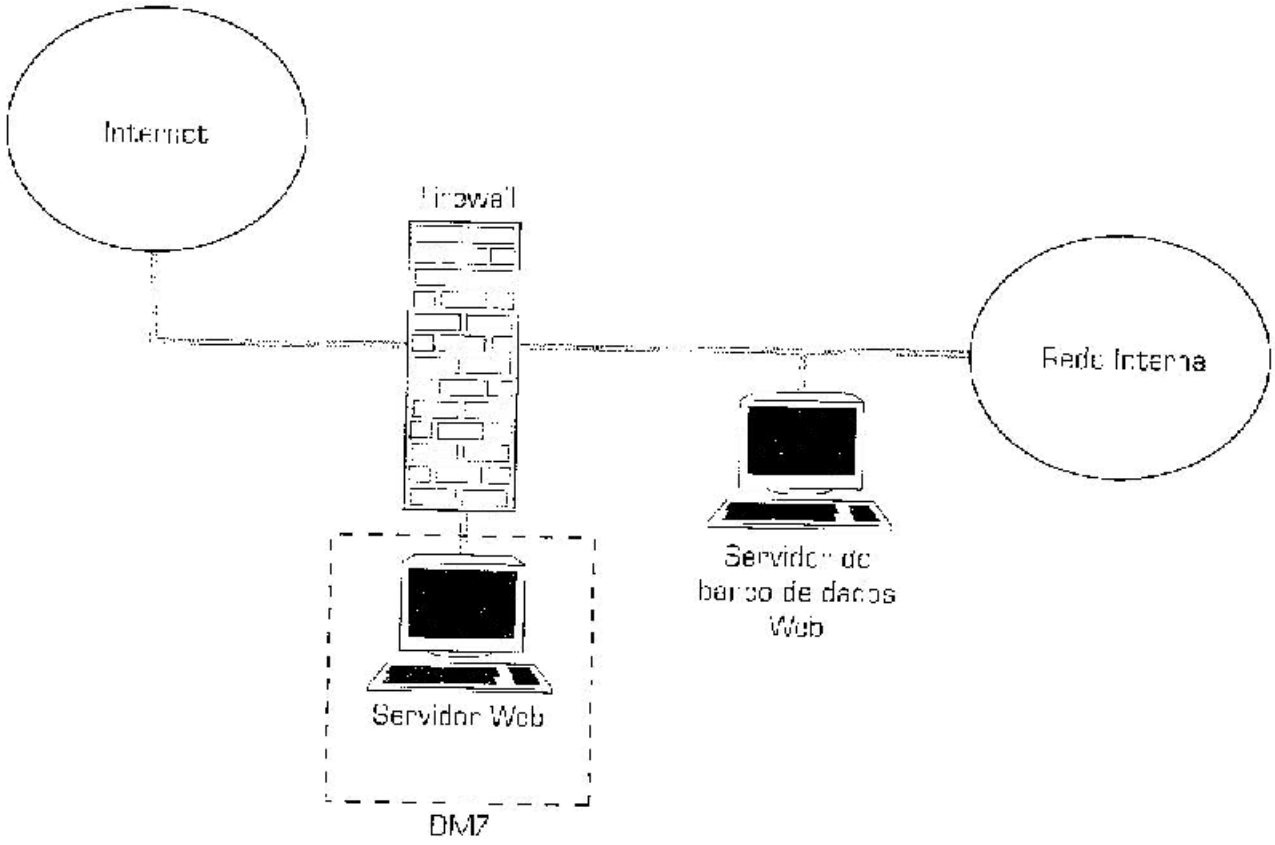
Conceito inicial de DMZ.

DMZ - Solução para falha de segurança



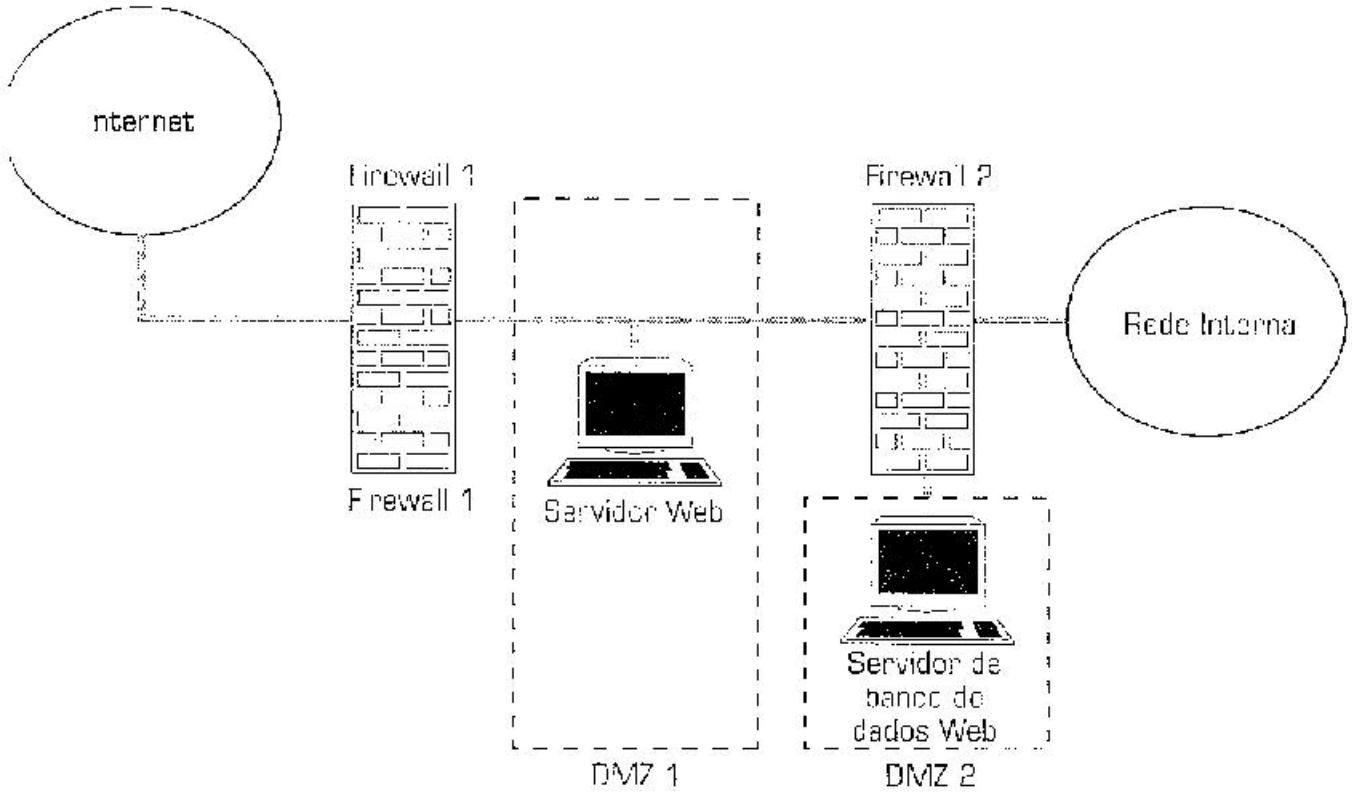
Solução para a falha de segurança apresentada pela arquitetura DMZ tradicional.

DMZ – Solução mais barata



Solução mais barata de DMZ, usando apenas um firewall.

DMZ – Solução de segurança ideal



Solução de segurança ideal usando a arquitetura DMZ.

DMZ Semi-Protegida (suja)

- Constitui a sub-rede, chamada de **LAN de Isolamento**, criada pelos elementos de rede de segurança de perímetro em conjunto, para compor um **sistema de defesa semi-protegido por um host de segurança**.

- Um Roteador de Perímetro (contém um firewall);
- Um host de segurança;
- Um Firewall.

DMZ Semi-Protegida (suja)

- Fornece **serviços** a usuários externos e internos através de um **Gateway de Aplicativo** e do **Host de Segurança**.
- Possui **um número de rede exclusivo,** diferente do número da rede corporativa.
- É a **única que pode ser vista de fora**.

Roteador de Perímetro

- A primeira linha de defesa.
- Um roteador de uso geral com uma interface serial com a Internet e conexão Ethernet com uma DMZ.
- Cria uma DMZ (semi-protegida).
- Protege os Hosts de Segurança na DMZ suja.

Roteador de Perímetro

- Protege o Firewall.
- Funciona como alarme, se ele próprio ou um Host de Segurança for invadido.
- O Firewall é usado para criar uma **DMZ protegida**, colocando **Hosts de Segurança em uma outra interface do Firewall**.

Roteador de Perímetro

- Pode utilizar **regras de filtragem de pacotes** para **restringir o acesso a serviços TCP/IP e aplicativos**.

- **Listas de Controle de Acesso (ACL)** são usadas para implementar as **regras de filtragem**.

Roteador de Perímetro

- Ponto principal do controle de acesso a redes internas.
- Recursos de segurança:
  - autenticação de usuário,
  - autorização de usuário,
  - proteção contra endereços de origem/destino desconhecidos,
  - oculta endereços IP internos,
  - rastreiam atividade dentro e fora do roteador,
  - administradores podem implementar política de segurança no perímetro.

Host de Segurança

- É um servidor protegido.
- Normalmente com base em LINUX ou Windows.

- Reside na DMZ suja.

- Serviços essenciais ao mundo exterior:
  - servidor FTP anônimo,
  - servidor Web,
  - servidor DNS
  - servidor SMTP de entrega de emails à empresa,
  - servidor de Proxy da Internet para hosts internos.

Host de Segurança

- Precisa ser muito resguardado. É vulnerável a ataques por ser exposto à Internet.
- Pode ser acessado por usuários internos.

- Fornecendo serviço de Proxy, por enviar solicitações de serviços de Internet, ele monitora suas portas para HTTP, POP, SMTP, FTP, NTP, NNTP, SSH, ... dos usuários internos para os serviços reais, com base na política de segurança da rede.

Host de Segurança

- Também pode ser configurado como um host de base dual, se possuir duas interfaces de rede – uma na rede interna e outra na rede externa.
- Desta forma, podem / devem fornecer recursos de Firewall, pois é bastante vulnerável, sujeito a ser comprometido em um ataque.
- Um Firewall que forneça segurança mais resistente que um host de base dual é uma solução mais recomendada.

Firewall

- Elemento de rede especialmente projetado para proteger uma rede interna de uma externa.

- Usa vários recursos que, em conjunto, possuem as seguintes **propriedades**:

Firewall - Propriedades

- Todo tráfego de dentro para fora e de fora para dentro, passa pelo Firewall.
- Somente o tráfego autorizado, conforme a política de segurança adotada, tem permissão para passar.
- É configurado em si, para ser imune a invasões.
- Torna a rede interna invisível ao exterior.

Firewall:
Como são implementados

- Filtro de Pacotes
- Gateway de Aplicativo
- Gateway de Conexões TCP e UDP
- Servidor de Proxy

Firewall – Filtro de Pacotes

- Inspeciona em cada pacote os parâmetros específicos de usuário, com endereços IP ou portas TCP e UDP.
- **Não controla sessões TCP ou UDP** antes de abrir uma conexão pelo Firewall.

Firewall –

Gateway de Aplicativo

- Examina mensagens no nível de aplicativo, em todos os pacotes que passam por ele antes de permitir uma conexão.
- Somente mensagens válidas são permitidas através do Firewall.
- Um gateway de aplicativo FTP, examina pacotes no aplicativo FTP e permite somente acesso válido para FTP.

Firewalls:

características de produtos

- Um conjunto de **recursos de software** apropriados para **configurar um firewall em um roteador**:
  - Cisco IOS Firewall dentro do Software Cisco IOS.

- Um firewall especializado de **hadware e software,** com um **sistema operacional protegido**:
  - Cisco PIX Firewall

Configurando segurança em roteador de perímetro

- Considere-se um roteador de perímetro.
- Com serviços TCP/IP.
- Controle desses serviços.
- Para reduzir ataques de espionagem, DoS e ataques de acesso não autorizado.
- Existem os serviços TCP/IP ativados por *default* que devem ser desativados manualmente através de comandos.
- Se um serviço é necessário, comandos específicos devem ser inseridos na configuração do roteador.

Configurando segurança em um roteador de perímetro

- Comandos para controlar serviços TCP/IP:

  - modo **configuração de interface administrativa** do roteador;
    Exemplo: controle do serviço SNMP bloqueando o acesso através do console (protegendo o console).

  - oferecidos pelo **roteador**.

Evitando ataques de reencaminhamento

- Roteadores de perímetro são suscetíveis à **tentativa de examinar atualizações de roteamento** para aprenderem a **composição de uma DMZ** ou uma **rede interna** (ataques de reconhecimento e acesso remoto).

Evitando ataques de reencaminhamento

- Como **proteger o roteamento** por roteador de perímetro ?
- Rotas estáticas
- Controlando o anúncio de rotas
- Autenticação de rota
- Controlando o acesso
- Filtragem na entrada de pacotes
- Filtragem na saída de pacotes
- Segurança de trava e chave

Proteção contra DoS

- Impedindo DDoS
- Usando interceptação TCP para controlar ataques SYN

Usando criptografia da camada de rede

- Pode ser usada em roteadores de perímetro para oferecer proteção entre os sistemas de perímetros.
- Criptografa o tráfego entre pares de aplicativos específicos.
- Criptografa somente os dados do usuário, deixando livres os cabeçalhos dos pacotes da camada de rede.

Usando criptografia da camada de rede

- É específica ao protocolo da camada de rede.

- Como pode ser obtida ?

  - CET (Cisco Encryption Technology)
  - IPSec (IP Security)

- Entre um roteador de perímetro e outro.

Usando criptografia da camada de rede

- Com CET (Cisco Encrytion Technology),
  - solução patenteada da Cisco;
  - criptografia simétrica com o DES (Data Encryption Standard);
  - algoritmo de chave pública com DH (Diffie-Hellman);
  - assinatura digital com DSS (Digital Signature Standard);
  - resumo de mensagem com MD5.

Usando criptografia da camada de rede

- Entre roteadores de perímetro, mas criando uma VPN com IPSec.
- IPSec é um conjunto de padrões abertos para assegurar comunicações privadas seguras em redes IP.
- Garante confidencialidade, integridade e autenticidade em uma rede IP pública (Internet).

Usando criptografia da camada de rede

- Resguarda o tráfego entre dois roteadores de perímetro, criando uma VPN entre um local corporativo central e um local corporativo remoto.
- Todo o tráfego entre dois roteadores de perímetro pode ser criptografado.
- Ou somente fluxos selecionados entre hosts por trás dos roteadores.

Usando criptografia da camada de rede

- Embora VPN com IPSec possa ser feita usando uma rede pública, as empresas fazem uso das mesmas políticas como numa rede privada.
- Garantem: segurança, QoS, confiabilidade e gerenciamento.
- IPSec dispõe de mais algoritmos de criptografia que CET.

Classes de Endereços IP

Classe	Nº de IP	Indicador da rede	Máscara de Sub-rede	Nº de redes disponíveis	Nº de hosts disponíveis
A	1 a 126	w	255.0.0.0	126	16,777,214
B	128 a 191	w.x	255.255.0.0	16,384	65,534
C	192 a 223	w.x.y	255.255.255.0	2,097,151	254

Existem ainda endereços reservados muito utilizados para a construção de Intra-nets. São eles:

Classe	Nº de IP	Máscara de Sub-rede
A	10.0.0.0	255.0.0.0
B	172.16.0.0	255.255.0.0
C	192.168.0.0	255.255.255.0

Para maiores detalhes recomendamos a leitura da RFC1597.

Gerenciando endereços IP

- Roteadores de perímetro:

  - usam NAT (Network Address Translation)
    RFC 1631

  - usam PAT (Port Address Translation).

Gerenciando endereços IP

- **Usando NAT** (**N**etwork **A**ddress **T**ranslation)

  NAT é um recurso de roteadores de perímetro e firewalls de filtragem de pacotes, que convertem endereços IP internos em externos (atribuídos pelo NIC – Network Information Center).

NAT

- NAT é usada no perímetro para:

  - atenuar o esgotamento de endereços IP;
  - ocultar endereços IP internos para o exterior;
  - converter endereços IP não roteáveis (inválidos) para endereços IP roteáveis.

Terminologia NAT

- **IP não válido**, não legítimo, não roteável, é um IP não atribuído pelo NIC ou um ISP.

- **endereço local interno**: endereço IP, não válido, atribuído a um host na rede interna.

- **endereço global interno**: endereço IP legítimo, que representa um ou mais endereços IP locais internos para o mundo exterior.

Terminologia NAT

- **endereço local externo**: endereço IP de um host externo como aparece para a rede interna; não necessariamente um IP válido, mas alocado no espaço de endereços roteáveis no interior.

Terminologia NAT

- **endereço global externo**: endereço IP de um host na rede externa, alocado nos endereços globalmente roteáveis ou do espaço da rede.

Formas de NAT

- **NAT Estática**
- **NAT Dinâmica**
- **NAT Oculta** (Hide)
- **NAT de Porta** (**PAT**)

NAT Estático

- Traduz um para um.
- Endereço inválido para um válido.
- Ou vice-versa: endereço válido para um inválido.
- É gerado um novo cabeçalho no pacote IP, colocando o endereço de origem como um IP válido, para trafegar na Internet.
- A troca é feita no roteador ou no firewall.

NAT Estático

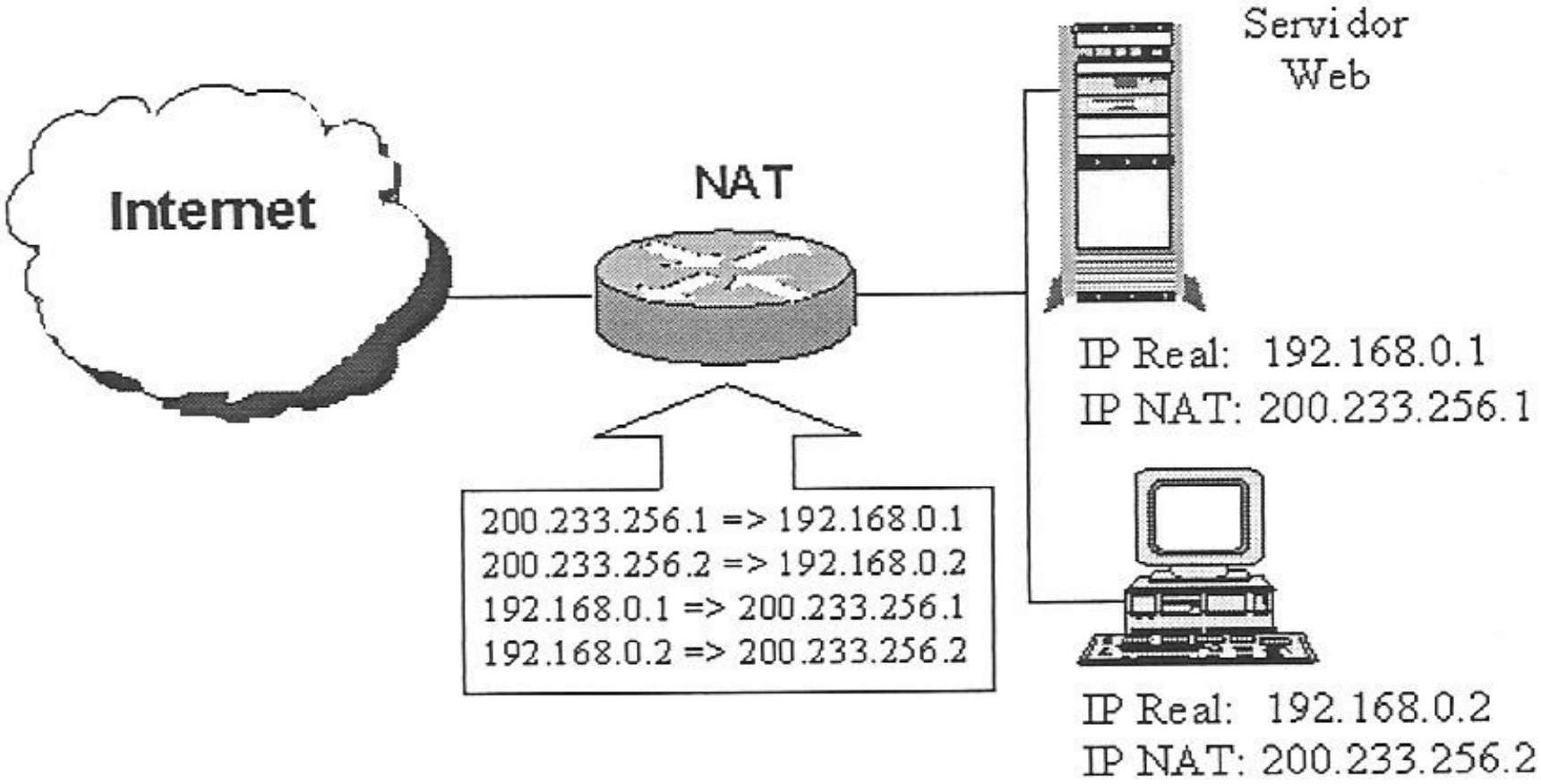
- Pacotes de retorno (da externa para interna), os endereços de destino são trocados pelo NAT.

- Para um servidor Web interno, não acessível ao mundo exterior, é feito um NAT estático com um endereço válido na Internet para o endereço real do servidor na rede interna.

Exemplo de NAT estático

- Pedidos externos (entrada) para o servidor 200.244.256.1 serão redirecionados para o endereço real do servidor Web 192.168.0.1
- Na saída do servidor Web 192.168.0.1 (retorno), todos os pacotes serão redirecionados para 200.244.256.1 .

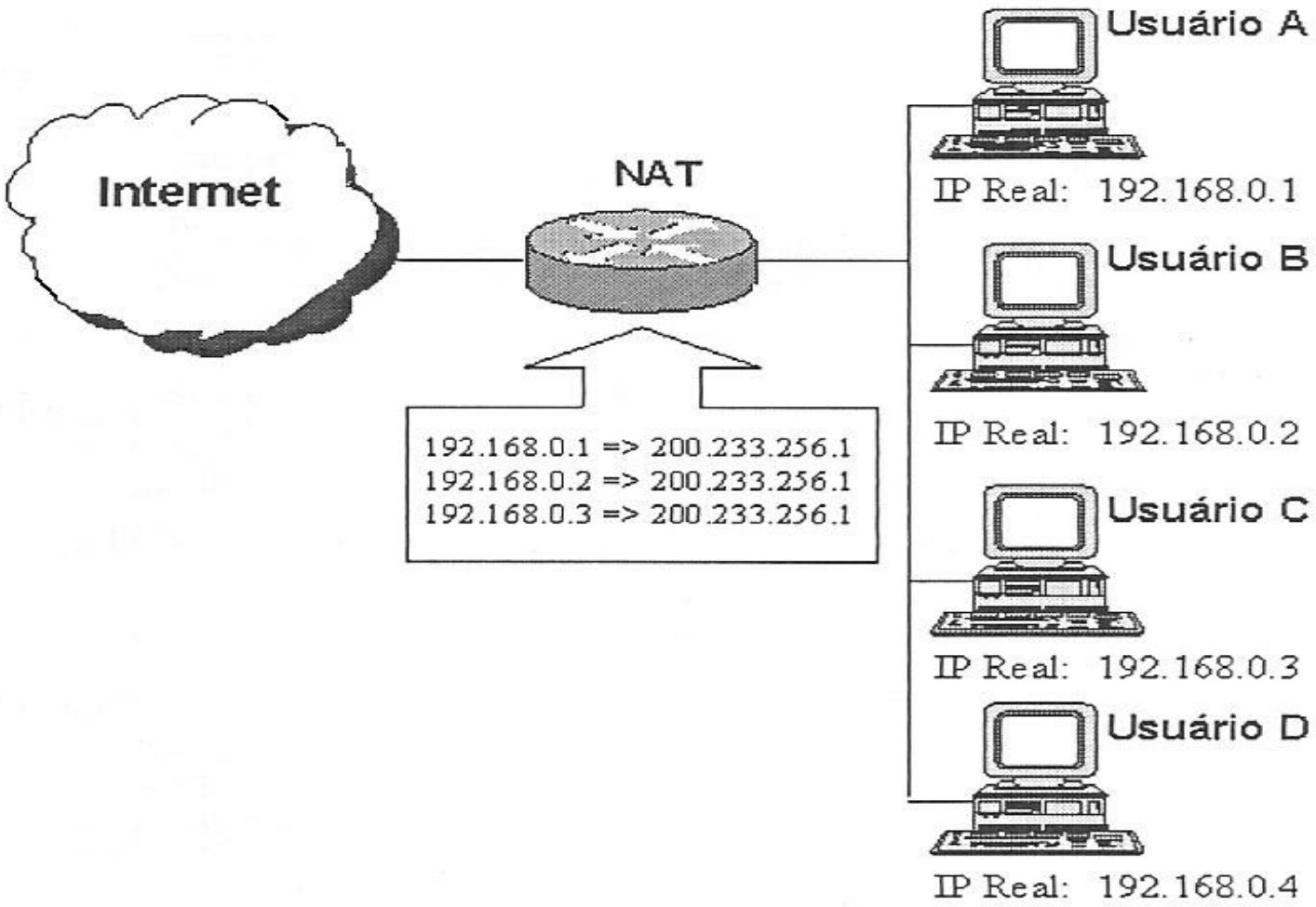
Exemplo de NAT Estático



NAT Oculto (Hide)

- Traduz de muitos IP inválidos para um IP válido (endereço local interno).
- Permite que vários usuários trafeguem na Internet.
- Um grupo de usuários com a acesso à Internet é definido.
- Todos no grupo têm o seu endereço IP inválido (real e interno), trocado por um IP válido na Internet, onde o NAT é executado.

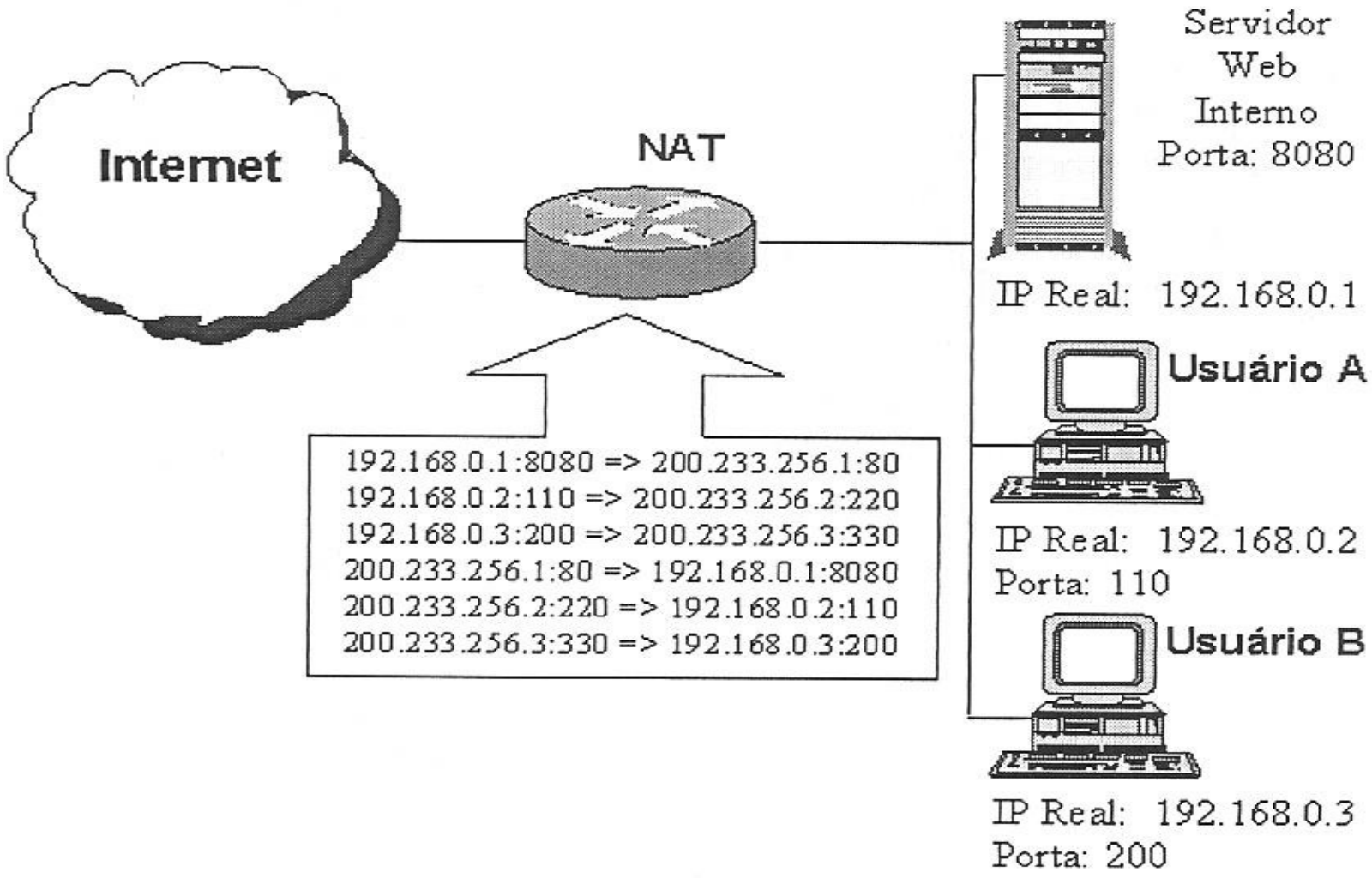
Exemplo de NAT oculto



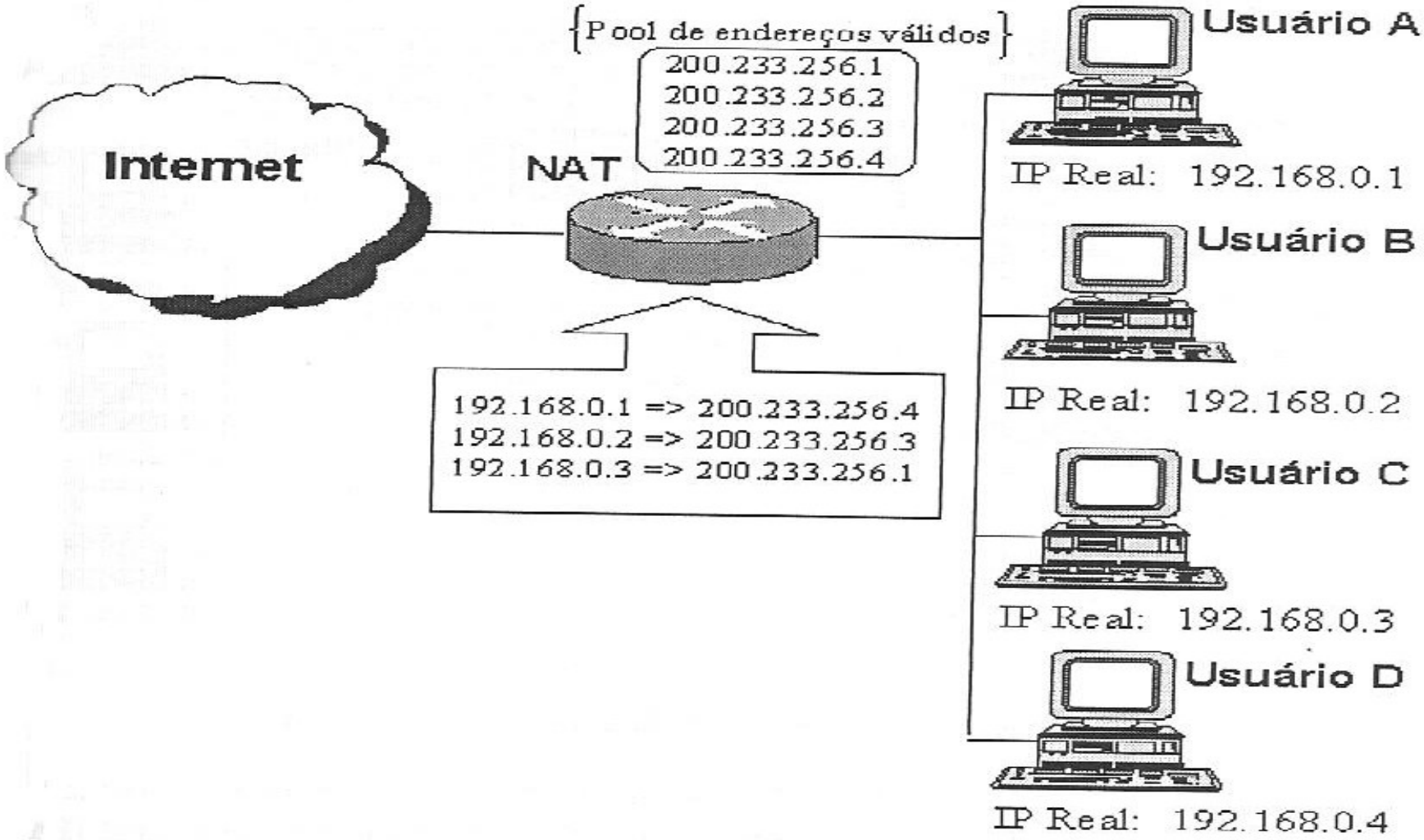
NAT de Porta - PAT

- Troca os endereços de origem e destino e também o número de porta de origem e destino.
- Serve para ocultar um número de porta estabelecido, usando-se um outro número.

Exemplo de NAT de porta



Exemplo de NAT Dinâmico



Registrando eventos do roteador de perímetro

- Configurar o ***logging*** de eventos do roteador de perímetro.
- Usar um Servidor de ***syslog*** na rede interna (IP 10.1.1.4)

Estudo de Caso: configurando um roteador de perímetro

- Cenário da Empresa XYZ
- Topologia da rede
- Política de segurança:
  - controlar serviços TCP/IP;
  - controlar o acesso de administrador;
  - Impedir o ***spoofing*** de endereço de origem.

Perguntas de Revisão

1. Cite três objetivos de um sistema de segurança de roteador de perímetro.

2. Cite os componentes que compõem um sistema de segurança de perímetro e identifique suas funções de forma concisa.

3. Qual o objetivo de um roteador de perímetro ?

Perguntas de Revisão

4. Qual a importância de se registrar eventos do roteador de perímetro em um servidor *syslog* ?

5. Que tipos de *spoofing* de endereços IP podem ser filtrados no tráfego recebido de um roteador de perímetro ?

Perguntas de Revisão

6. Para que serve o NAT estático em um roteador de perímetro ?

7. Para que serve o NAT dinâmico em um roteador de perímetro ?

8. Para que serve o PAT em um roteador de perímetro ?

Perguntas de Revisão

10. O que é uma lista de acesso ?

11. Como se pode evitar que um roteador de perímetro se transforme em um amplificador de broadcast em ataque DDoS ?

12. Como se pode controlar serviços TCP/IP em um roteador de perímetro para bloquear consultas de *echo* e *finger* da Internet ?

Listas de Firewalls

- Firewalls acadêmicos:
  assinaturas em majordomo@net.tamu.edu
- Lista compilada de firewalls:
  assinaturas em www.gnac.net/firewalls

Referências de segurança de perímetro

- Chapman and Zwicky, **Building Internet Firewalls**, O'Reilly Publishing, 1995.

  Ampla abordagem da criação de um firewall de perímetro.

- Simson, Garfinkel and Spafford, **Practical UNIX and Internet Security**, O'Reilly & Associates, 1996.