Implantação de Firewalls: Teoria e Prática

Vinícius Serafim

serafim@inf.ufrgs.br

GSeg UFRGS

Programação

- O que é um Firewall?
- Tecnologias
- Arquiteturas
- Implementação

1. Firewalls usando Linux
2. Burlando um firewall

- Aulas práticas

A Referência Bibliográfica!

- Building Internet Firewalls, 2nd Edition
  - Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman
  - O'REILLY
  - ISBN: 1-56592-871-7
  - US $44.95

O que é um Firewall?

Vinícius Serafim

serafim@inf.ufrgs.br

GSeg UFRGS

Tópicos

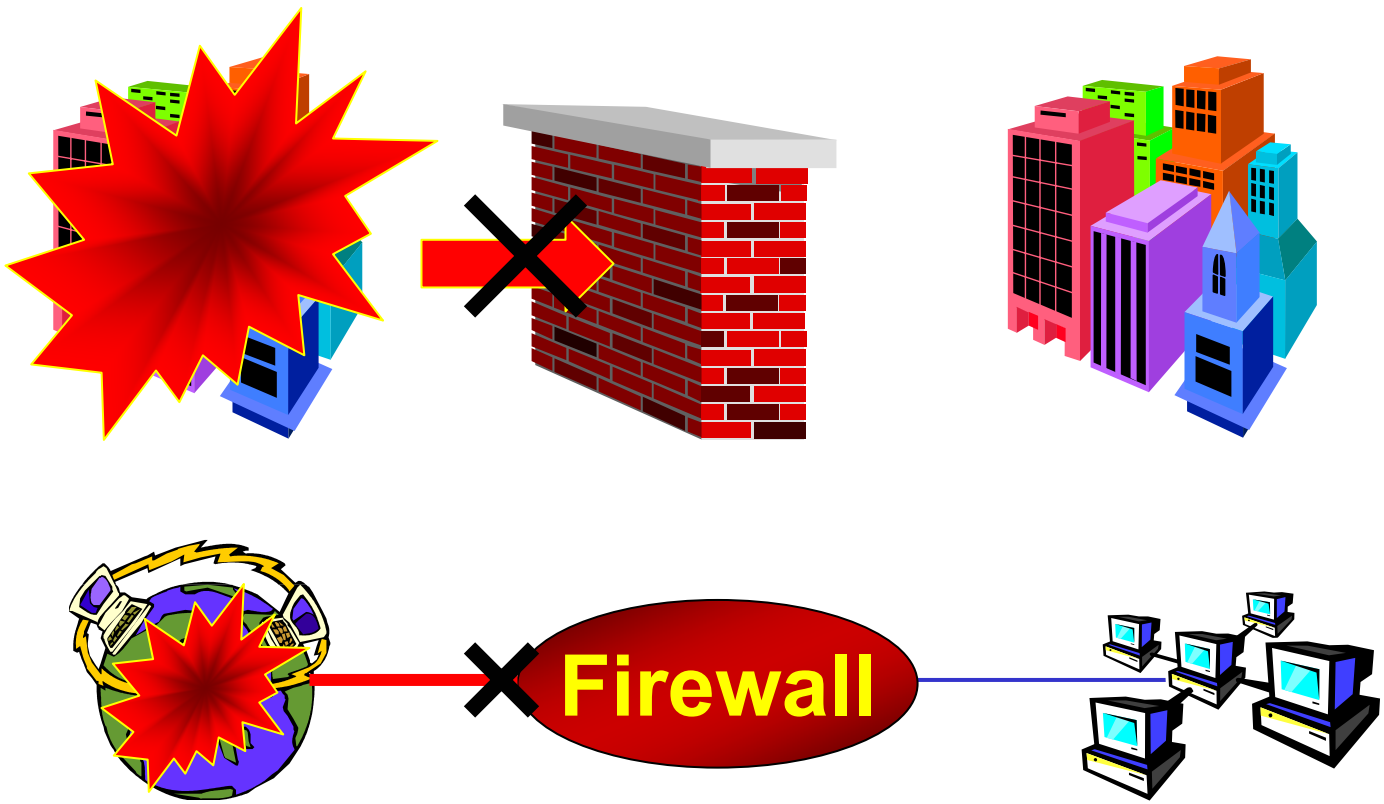
- Introdução
- O que é um Firewall?
- O que um Firewall pode fazer?
- O que um Firewall NÃO pode fazer?
- Problemas com Firewalls
- Pré-requisitos para seguirmos adiante
- Objetos tratados pelo Firewall

Introdução

- Host Security
  - varia de acordo com cada plataforma de SO
  - varia de acordo com o papel do host
  - indicada apenas para pequenos sites

- Network Security
  - pode proteger dezenas e até centenas de máquinas, ...
  - evita inúmeros ataques
  - independente da plataforma dos hosts
  - controle de pontos de acesso

O que é um Firewall?



O que é um Firewall?

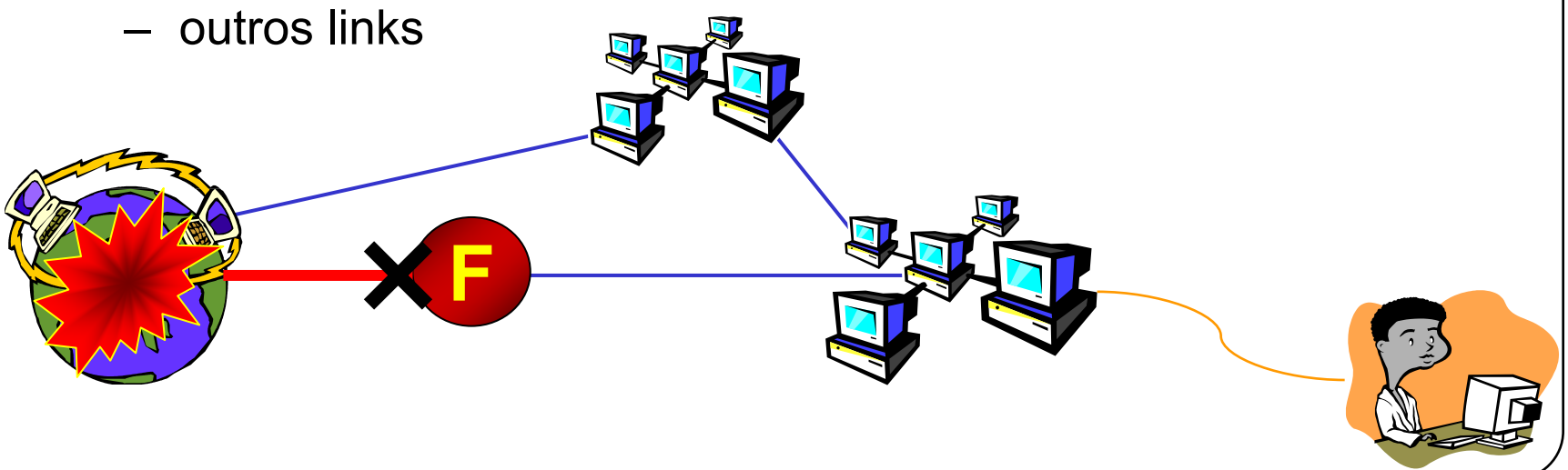
- Mecanismo bastante efetivo para segurança de rede
- Ponto de controle
  - controla entrada e saída de tráfego
  - mantém os atacantes longe das defesas internas
- Implementado de acordo com a política de segurança
- Barreira adicional de segurança
- Não é 100% seguro e efetivo
  - implementação
  - configuração
  - usuários internos

O que um Firewall pode fazer?

- Foco para decisões referentes à segurança
- Aplicar a Política de Segurança
- Registrar eficientemente as atividades da rede
- Limitar a exposição da rede interna

O que um Firewall NÃO pode fazer?

- Evitar a ação maliciosa de usuários internos
  - levar/trazer dados usando disquetes e outras mídias
- Proteger a rede de pacotes que não passam por ele
  - modems em máquinas internas
  - outros links



O que um Firewall NÃO pode fazer?

- Proteger contra ameaças completamente novas
- Não fornecem boa proteção contra vírus
  - tarefa complicada
    - muitos formatos existentes de arquivos executáveis
    - muitas maneiras de transmitir um desses arquivos
  - melhor proteção é utilizar um antivírus em cada máquina
- Auto-configuração (não é *plug & play*)
  - qualquer firewall exige algum nível de configuração

Problemas com Firewalls

- Interferem no funcionamento da internet
  - internet é baseada em comunicação fim-a-fim
  - muitos detalhes da comunicação são ocultados
  - dificultam a implantação de novos serviços
  - normalmente os usuários não gostam e até se revoltam

- Firewalls NÃO resolvem o problema da segurança
  - outros mecanismos precisam ser utilizados (ex.: host security)

Pré-requisitos para seguirmos adiante

- Saber o que é um pacote e um protocolo
  - endereçamentos (máscaras de rede)
  - portas
  - características de funcionamento

- Conhecer as camadas da pilha TCP/IP
  - aplicação
  - transporte
  - rede
  - físico

Objetos tratados pelo Firewall

- A unidade básica e essencial é o

- Trata protocolo do nível de rede
  - inspeciona:
    - endereços
    - e possivelmente os flags
  - suportam IP
  - outros protocolos não são normalmente suportados (ex.: Apple Talk, IPX)

Objetos tratados pelo Firewall

- Pode tratar protocolos do nível de transporte (portas)
  - TCP
  - UDP
- Pode tratar protocolos auxiliares
  - ICMP
  - ARP
- Pode tratar protocolos do nível de aplicação
  - HTTP
  - SMTP
  - FTP

Tecnologias

Vinícius Serafim

serafim@inf.ufrgs.br

GSeg UFRGS

Tópicos

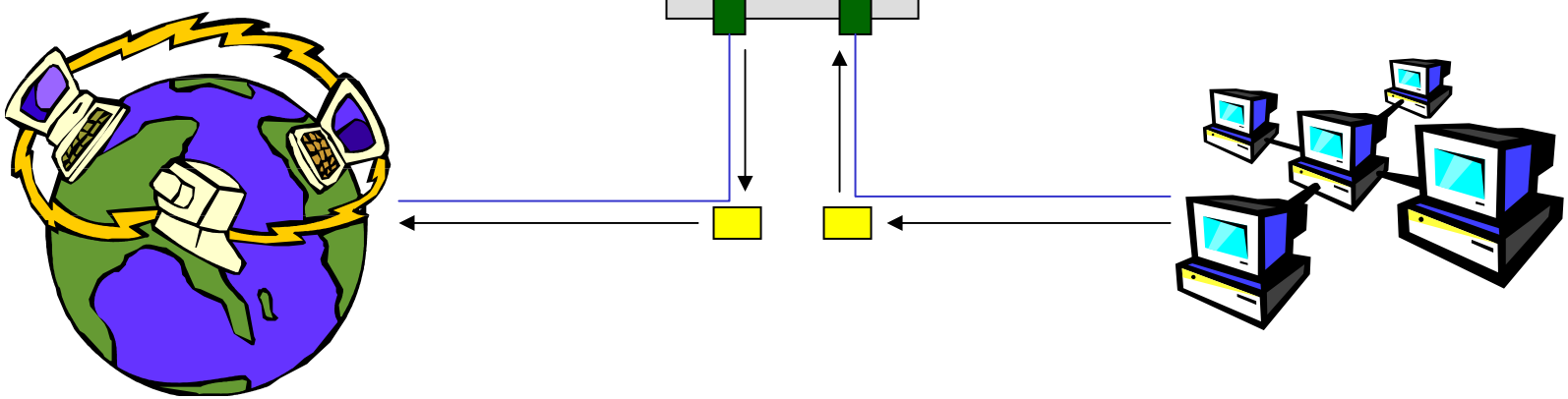
- Filtragem de Pacotes
- Proxy Services
- Network Address Translation (NAT)
- Virtual Private Network (VPN) ?

Filtragem de Pacotes

- caso o pacote não seja permitido, ele é destruído
- caso seja permitido, ele é roteado para o destino

- endereços origem/destino
- protocolo (TCP, UDP, ICMP)
- porta origem/destino
- tamanho do pacote
- tipo de mensagem ICMP

Além das informações contidas nos pacotes o filtro sabe em que interface o pacote chegou e para qual interface deve ir.



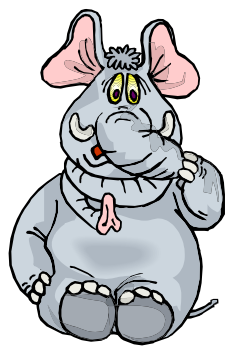
Filtragem de Pacotes

- Ações tomadas depois de um pacote ser verificado
  - Encaminhar o pacote para o destino (Allow)
  - Eliminar o pacote (Drop, Deny)
  - Rejeitar o pacote, enviando um erro para o emissor do pacote (Reject)
  - Registrar os dados do pacote (Log)
  - inúmeras outras

Filtragem de Pacotes

- Stateless Packet Inspection
  - cada pacote é analisado isoladamente, sem nenhum tipo de correlação com outros pacotes
  - mais comumente implementado

- Stateful Packet Inspection
  - o filtro leva em conta o histórico da conexão
  - bem mais eficiente
  - exige manter lista de conexões
  - vem se tornando um “padrão”



Filtragem de Pacotes

- Exemplo de regras de filtragem

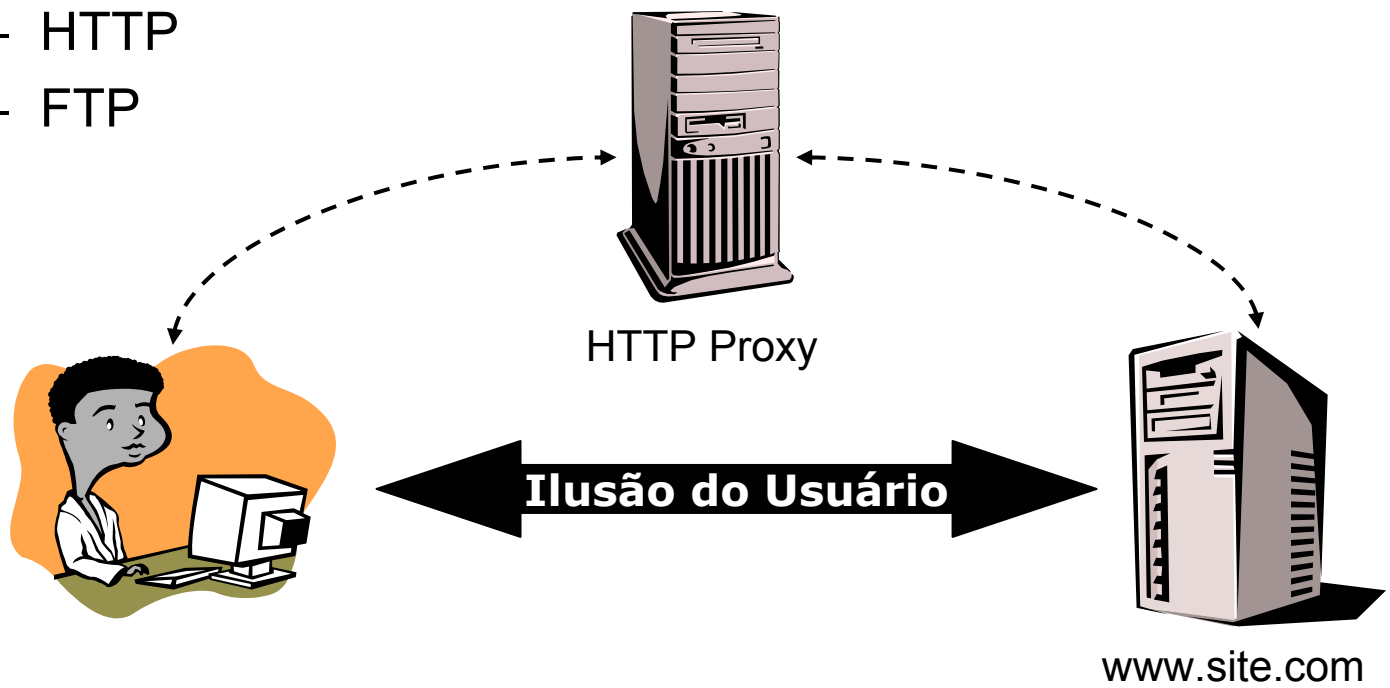
Allow **prot** tcp **src** 10.0.0.0/8 **port** any **dst** 0.0.0.0/0 **port** 23
Allow **prot** tcp **src** 10.0.0.0/8 **port** any **dst** 0.0.0.0/0 **port** 110
Allow **prot** tcp **src** 10.0.0.0/8 **port** any **dst** 0.0.0.0/0 **port** 25
Allow **prot** udp **src** 10.0.0.0/8 **port** any **dst** 0.0.0.0/0 **port** 53
Drop **prot** any **src** 0.0.0.0/0 **port** any **dst** 0.0.0.0/0 **port** any

Filtragem de Pacotes

- Vantagens
  - um roteador com filtragem pode proteger toda uma rede
  - é extremamente eficiente, principalmente *stateless*
  - é largamente disponível, pode ser encontrado em roteadores, embutido em SOs, softwares específicos, ...
- Desvantagens
  - é complicado configurar um filtro de pacotes
  - é difícil de testar
  - reduz a performance do roteamento
  - algumas vezes faltam recursos para implementar algumas regras desejadas

Proxy Services

- Proxy = Procurador
- Funcionam a nível de aplicação
  - Aplication Level Gateways
  - HTTP
  - FTP

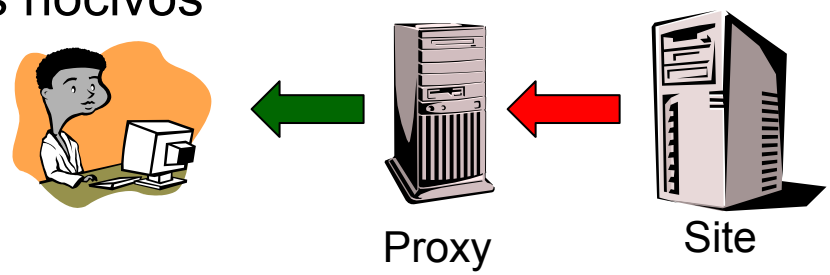


Proxy Services

- Podem realizar filtragens baseados nos dados do protocolo de aplicação
  - ex.: HTTP
    - nome do site
    - conteúdo da página
    - tipo de acesso GET/POST
    - etc.
  - ex.: SMTP
    - e-mail do remetente
    - e-mail do destinatário
    - comandos SMTP
    - conteúdo de um e-mail

Proxy Services

- Vantagens
  - nível mais apurado de registro (log)
  - filtragem mais inteligente
  - pode realizar autenticação de usuário
  - protege clientes de “pacotes nocivos”
  - pode realizar *caching*



- Desvantagens
  - cada serviço requer um proxy específico
  - alguns serviços, principalmente os novos, não tem proxy disponível
  - nem sempre é transparente para o usuário

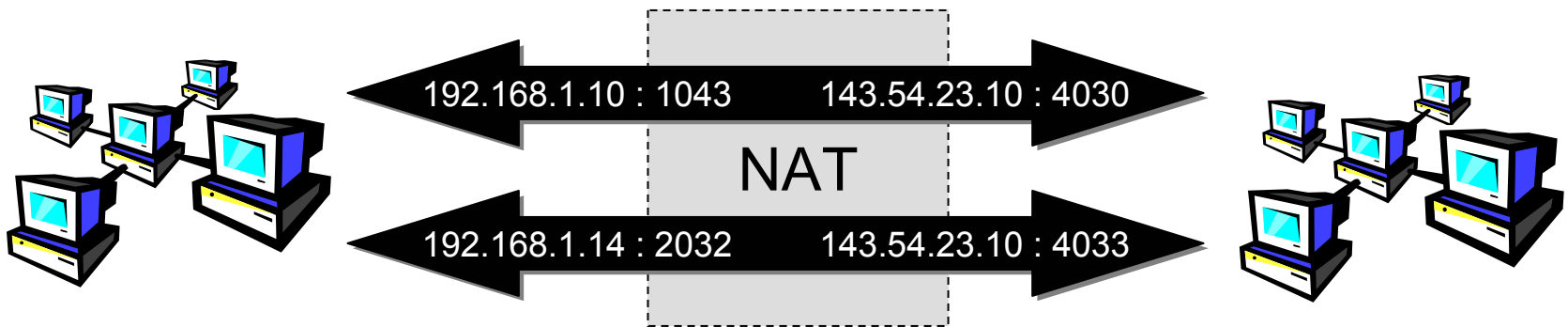
Network Address Translation (NAT)

- Endereços externamente visíveis
  - são endereços válidos na Internet
  - NÃO podem ser utilizados sem que sejam devidamente reservados (Registro.br)

- Endereços de uso interno
  - são endereços inválidos na Internet
  - RFC1918
    - 10.0.0.0 / 8
    - 172.16.0.0 / 12
      - netmask 255.240.0.0
      - faixa: 172.16.0.0 até 172.31.0.0
    - 192.168.0.0 / 16

Network Address Translation (NAT)

- Operação
  - altera dados do pacote
    - normalmente endereço e porta de origem
    - em alguns casos endereço e porta de destino (Destination NAT)



Network Address Translation (NAT)

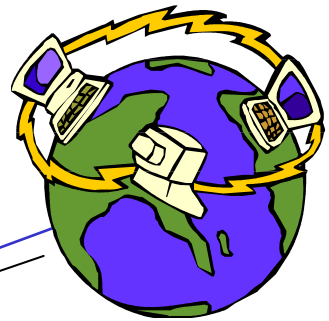
- Vantagens
  - ajuda a reforçar o controle do firewall
    - os endereços internos não funcionam na rede externa, assim, qualquer conexão de dentro para fora depende de auxílio do firewall
    - somente pacotes relativos às conexões iniciadas internamente conseguem vir da rede externa
  - oculta a estrutura (configuração) da rede interna

Network Address Translation (NAT)

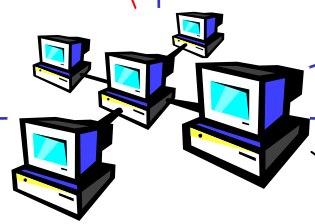
- Sem uso do NAT

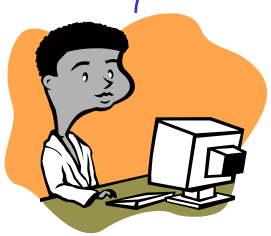
Usuários internos podem instalar serviços que poderão ser acessados de fora da rede. ex.: VNC, PCAnyWhere.

143.54.23.36

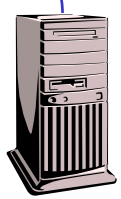


143.54.23.254





143.54.23.15

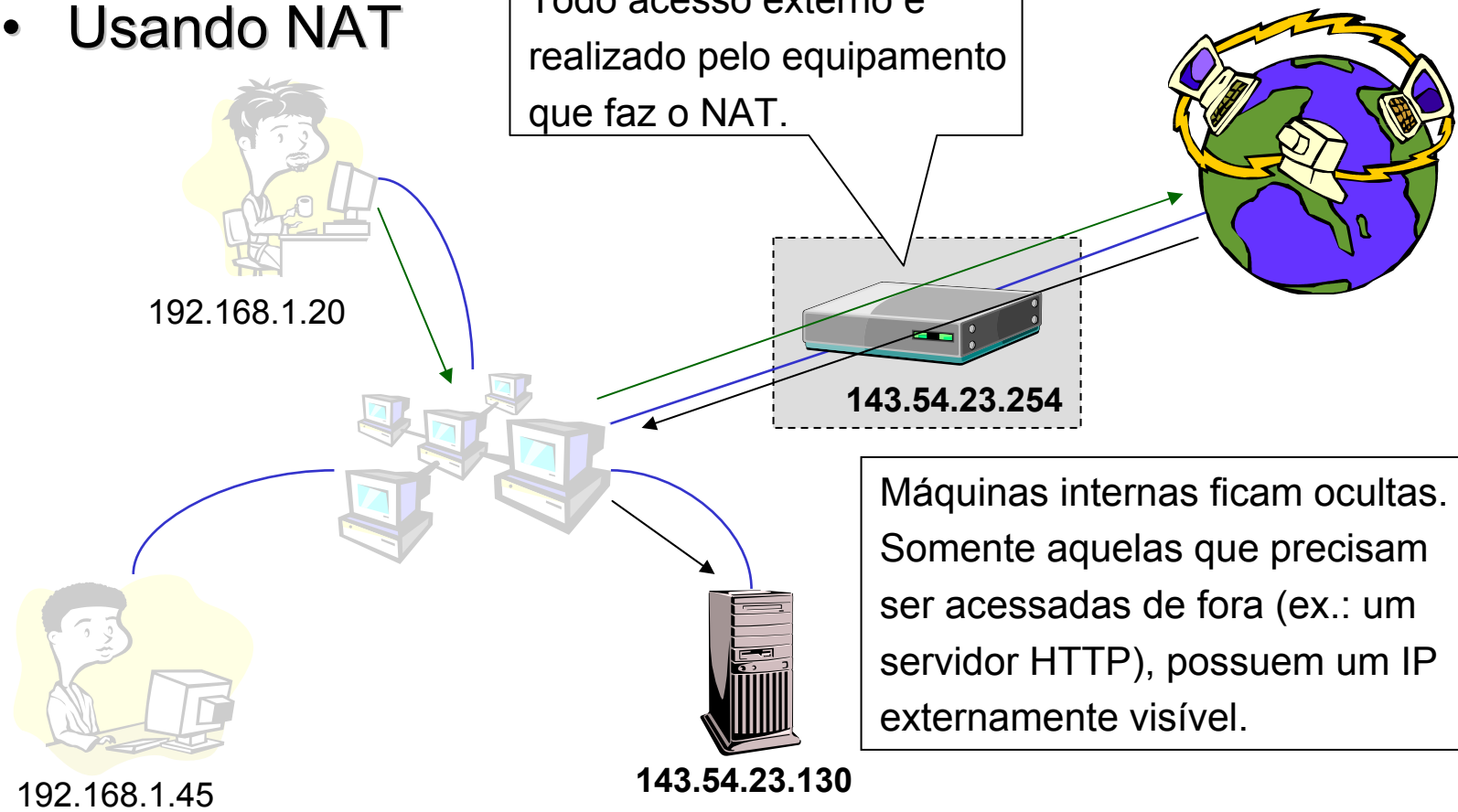


143.54.23.130

As máquinas internas podem ficar expostas, assim um atacante pode conectar-se diretamente a uma máquina interna sem maiores problemas.

Network Address Translation (NAT)

- Usando NAT



Network Address Translation (NAT)

- Desvantagens
  - o NAT altera dados do pacote, isso pode interferir em alguns protocolos, pode dificultar o registro (log) de atividades e pode ainda interferir na filtragem de pacotes
  - maior carga no equipamento

Virtual Private Network (VPN) ?

- Não é propriamente uma tecnologia de firewall
- Mas o firewall é um bom lugar para a criação de uma VPN
  - controla todo o tráfego de entrada/saída
  - um firewall não consegue controlar tráfego já cifrado

Arquiteturas

Vinícius Serafim

serafim@inf.ufrgs.br

GSeg UFRGS

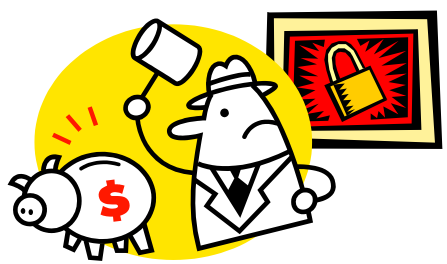
Tópicos

- Tipos de Arquiteturas
- Exemplos de Arquiteturas
- Bastion Hosts
- Exemplos de Arquiteturas
- Algumas Considerações

Tipos de Arquiteturas

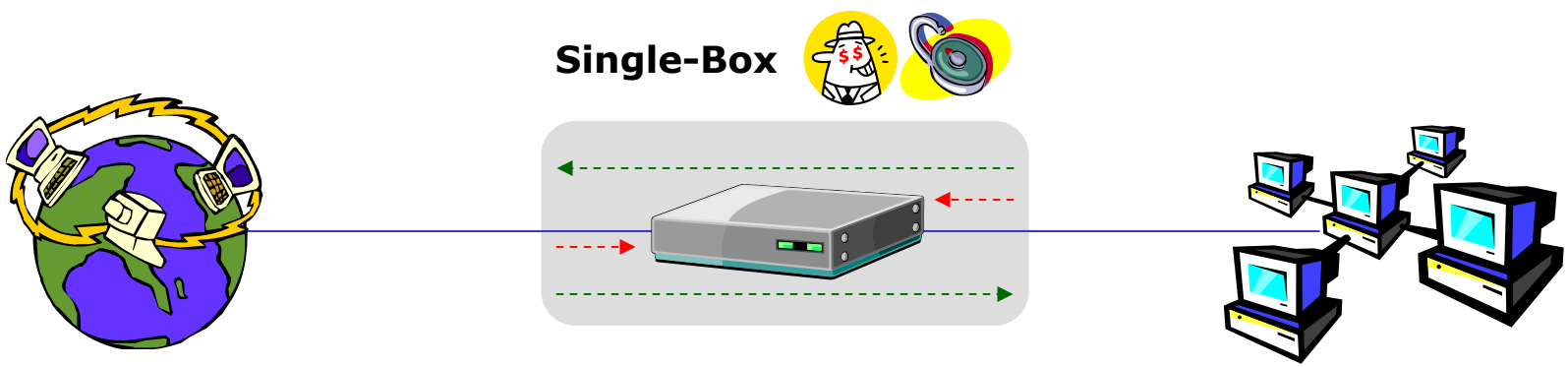
- Single-Box
  - baseados em apenas um equipamento
  - arquitetura bastante comum
  - mais barata, mais simples, menos segura
  - ponto único de falha

- Multiple-Boxes
  - é composta por um conjunto de equipamentos
  - custo pode ser muito maior dependendo da solução adotada
  - mais complexa, bem mais segura
  - fornece vários níveis de defesa
  - são inúmeros os arranjos possíveis



Exemplos de Arquiteturas

- Screening Router
  - tudo que é preciso é um roteador com filtragem, normalmente precisamos de um para a conexão com a Internet
  - normalmente só filtra pacotes, mas pode fazer NAT
  - limitado, não trata nível de aplicação

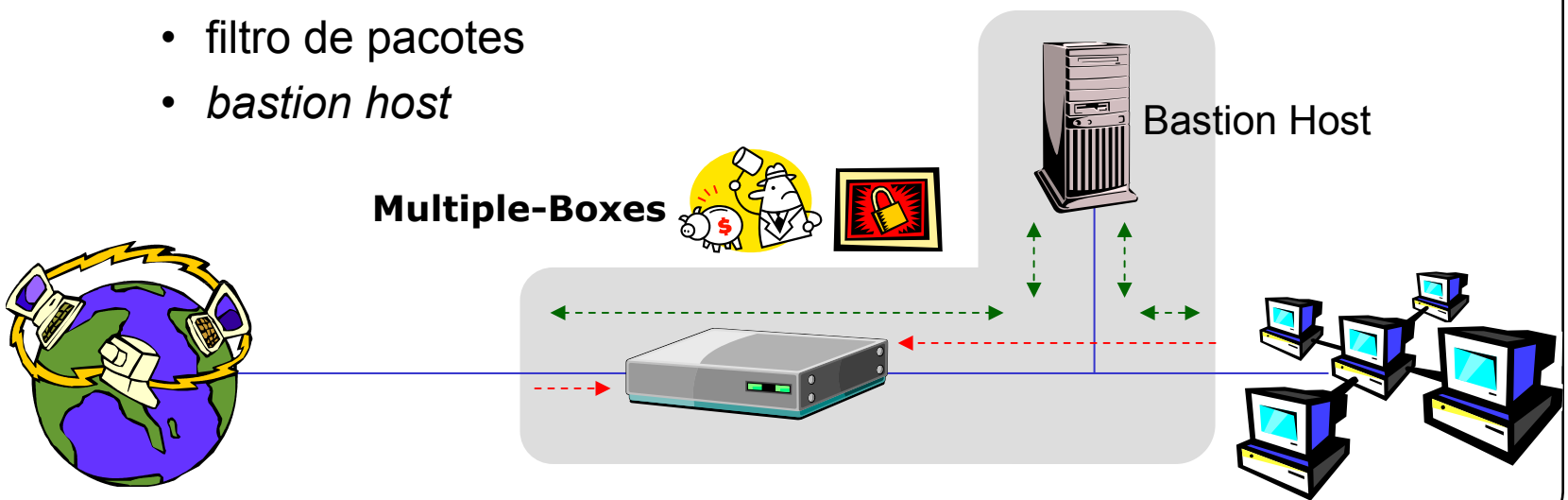


Exemplos de Arquiteturas

- Screening Router
  - Quando usar?
    - quando a rede protegida tem um alto grau de Host Security
    - número reduzido de protocolos
    - protocolos simples
    - quando o desempenho é vital
  - Onde utilizar?
    - entre redes internas (firewall interno)

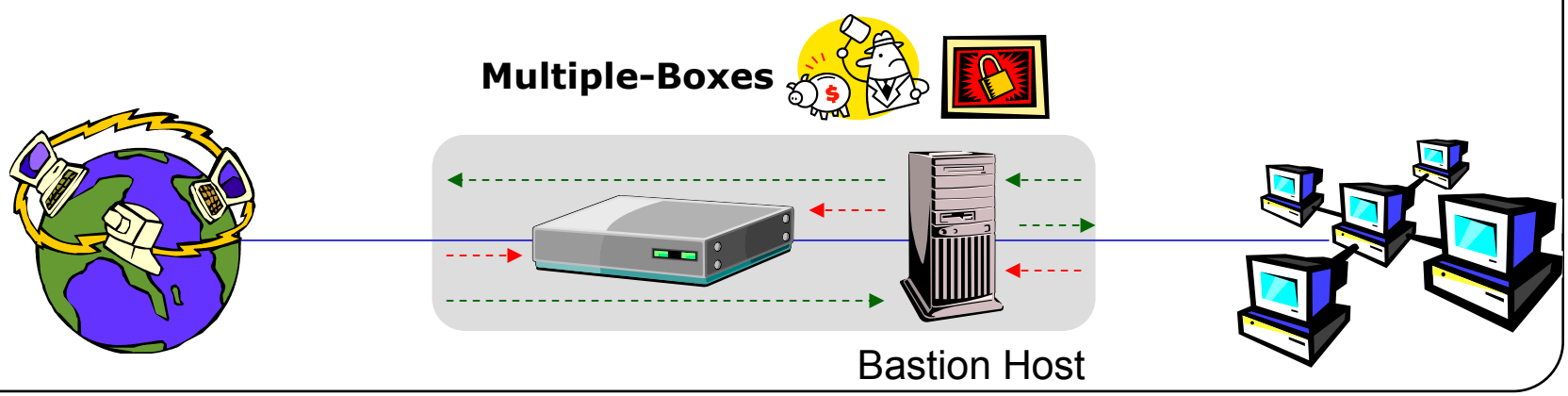
Exemplos de Arquiteturas

- Screened Host
  - filtro garante que
    - somente pacotes destinados ao bastion host podem entrar
    - somente pacotes criados pelo bastion host podem sair
  - dois níveis de segurança
    - filtro de pacotes
    - *bastion host*



Exemplos de Arquiteturas

- Screened Host
  - não dispensa host security
  - trata nível de aplicação
  - Quando utilizar?
    - quando o bastion host não for um servidor para usuários externos (servidor público)



Bastion Hosts

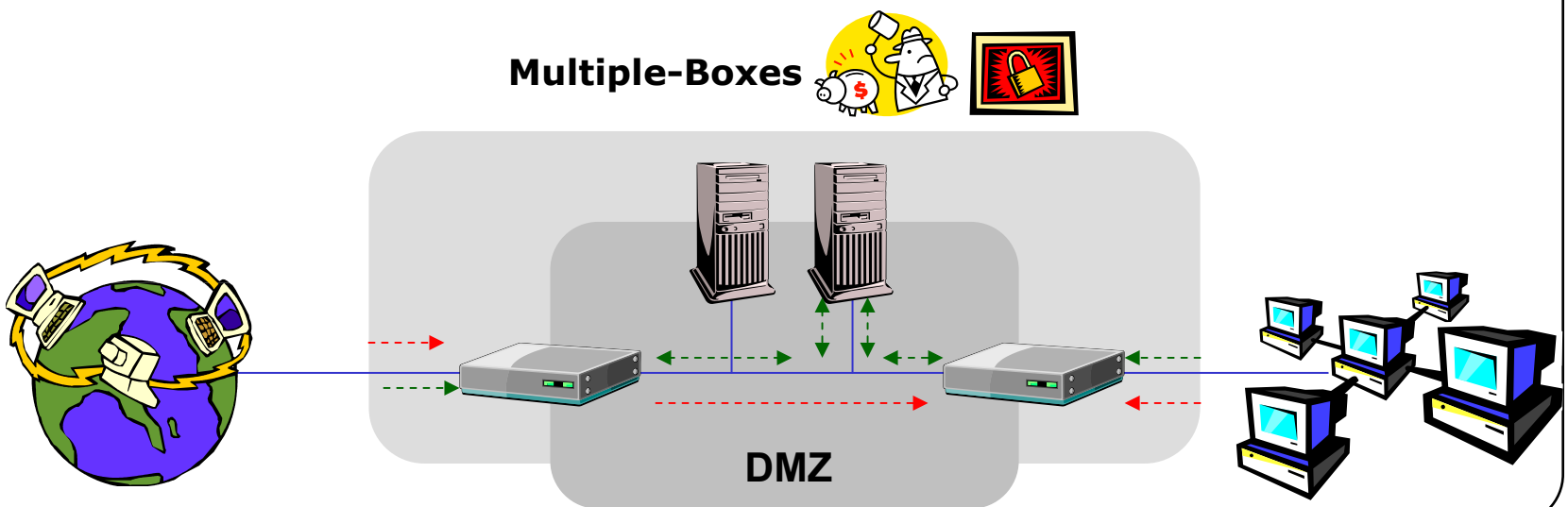
- Bastion Host
  - é como o saguão de um prédio, qualquer um pode entrar nele, mas talvez não possa seguir adiante
  - constitui a presença pública na Internet, é externamente visível e acessível
  - são máquinas potencialmente vulneráveis e portanto críticas para a segurança
  - exigem um alto nível de host security
  - serão o primeiro alvo de um atacante
  - **mais cedo ou mais tarde serão invadidos**

Bastion Hosts

- Alguns tipos
  - internos: fornecem serviços para a rede interna (proxy)
  - externos: servidores públicos HTTP, FTP, SMTP, etc.
  - Dual-Homed: máquinas com duas (ou mais) placas de rede. Interconecta duas redes ao nível de aplicação.

Exemplos de Arquiteturas

- Screened Subnet
  - filtros garantem que:
    - somente pacotes destinados ao bastion host podem entrar na DMZ
    - somente pacotes criados pelo bastion host podem sair da DMZ

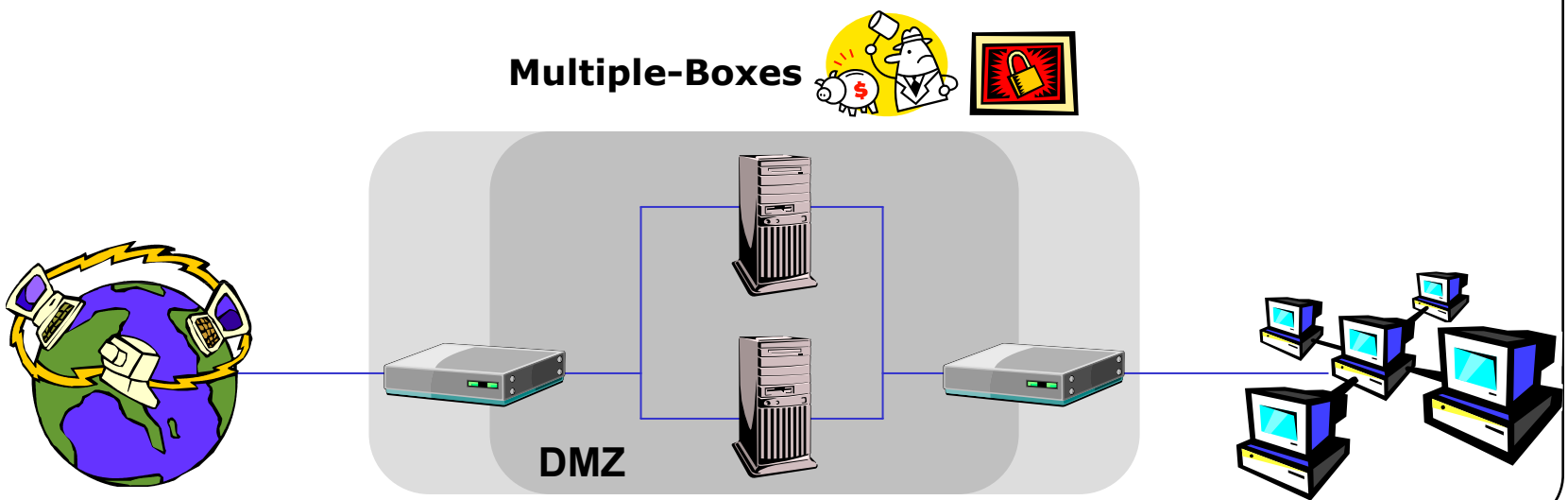


Exemplos de Arquiteturas

- Screened Subnet
  - múltiplos níveis de segurança
  - não existe um ponto único de falha
  - o atacante tem que passar pelos dois roteadores para chegar na rede interna
  - criação de uma rede perimetral
  - arquitetura apropriada para a maioria dos casos

Exemplos de Arquiteturas

- Split-Screened Subnet
  - filtros são semelhantes aos da Screened Subnet
  - filtragem e controle maximizados
  - mais complexo, mais difícil de criar e manter
  - múltiplos níveis de defesa



Algumas Considerações

- Não existem somente as aqui citadas
- Não existe um padrão
- Cada ambiente exige um firewall especialmente projetado
- Leve em conta
  - necessidade dos seus usuários internos
  - necessidade dos seus usuários externos (ex.: clientes)
  - o quanto crítica é a segurança dos seus sistemas
  - capacidade de investimento
- Não é preciso fazer tudo de uma vez, nem se deve

Implementação

Vinícius Serafim

serafim@inf.ufrgs.br

GSeg UFRGS

Tópicos

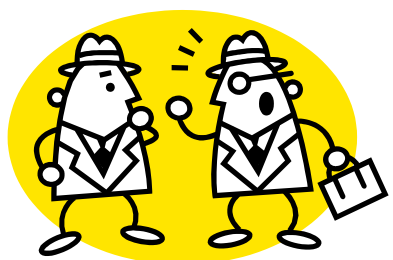
- Software Livre ou Comercial?
- Unix, Windows e outras “seitas”
- Projetando um Firewall
- Mantendo um Firewall
- Um caso para não ser seguido
- Bastion Hosts

Software Livre ou Comercial?

- Qualquer solução exige pelo menos os seguintes conhecimentos
  - como funciona a solução empregada
  - funcionamento dos protocolos a serem filtrados
- A escolha depende:
  - dos recursos disponíveis (humanos e financeiros)
  - das suas necessidades
- Os extremos são perniciosos
  - por que não combinar as melhores de cada um?

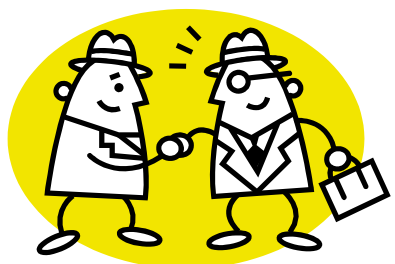
Unix, Windows e outras “seitas”

- Unix foi um dos primeiros (o primeiro) a fornecer os serviços necessários
- Hoje temos inúmeras variações do Unix e outros sistemas operacionais que também fornecem esses serviços
- Dizer que o Windows NT não serve...
  - é um pouco de preconceito
  - e de ignorância



Unix, Windows e outras “seitas”

- Usar o NT para construir um firewall é apenas mais difícil
  - Unix foi um dos primeiros a implementar o TCP/IP, o que resulta em cerca de 20 anos de uso e correções
  - Já o NT implementou o TCP/IP do zero, erros já corrigidos no Unix e que não existiam apareceram
  - O Windows NT é uma caixa preta, as coisas foram feitas para funcionarem sem que os administradores saibam como
- A máxima: use o que você já conhece



Projetando um Firewall

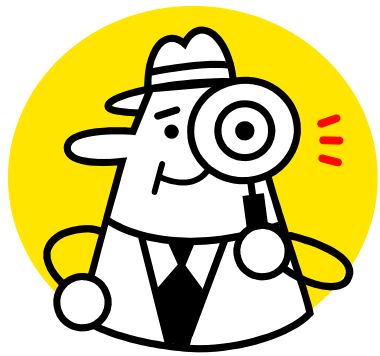
- Etapas
  - Definir suas necessidades
  - Avaliar os produtos disponíveis
  - Estudar como juntar os produtos

Projetando um Firewall

- Definir suas necessidades
  - escolher os produtos a partir das necessidades e não o contrário
  - política de segurança, não continue sem ter uma
  - que serviços serão oferecidos
  - qual o nível de segurança necessário
  - qual o tráfego esperado
    - canais disponíveis
    - quantos usuários
    - o que eles irão fazer
  - quanto é possível investir
  - recursos humanos disponíveis

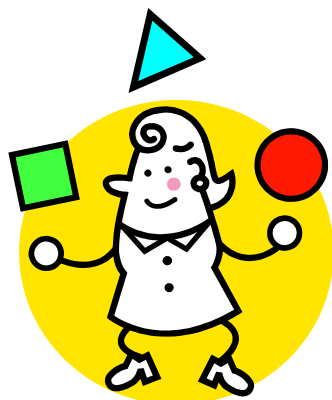
Projetando um Firewall

- Avaliar os produtos disponíveis
  - escalabilidade
  - disponibilidade e redundância
  - recursos para auditoria
  - custo
    - hardware
    - software
    - suporte e atualizações
    - administração e instalação
  - não procure uma solução perfeita, mas a que melhor atende o seu caso em particular



Projetando um Firewall

- Estudar como juntar os produtos
  - onde serão armazenados os logs
  - sincronização de relógios
  - como fazer backup
  - como será o acesso para manutenção
  - alguma possível incompatibilidade?



Mantendo um Firewall

- Backup
  - proxy
  - filtros de pacotes (seja roteador ou PC)
- Gerenciamento de senhas
  - devem ser bem escolhidas
  - usar uma diferente para cada equipamento
  - altera-las regularmente
  - controlar o tráfego

Mantendo um Firewall

- Monitoramento
  - de recursos do sistema (disco, memória, cpu)
  - de logs
    - alguém tentou varrer as portas de um servidor
    - alguém tentou algum tipo de ataque
    - mensagens de erro
    - pacotes rejeitados
  - um *Sistema de Detecção de Intrusão* (IDS) pode ser utilizado
  - verificar se o sistema foi comprometido

Mantendo um Firewall

- Atualização
  - Você
    - componente mais importante a ser atualizado
    - novos bugs
    - novos ataques
    - melhoramento de tecnologias
    - novas tecnologias
    - Onde? Na INTERNET (ex.: www.securityfocus.org)
  - Firewall
    - se você já está atualizado o resto é fácil
    - nem sempre a atualização é necessária
    - teste antes de atualizar o firewall em uso
    - todos os testes devem ser feitos off-line

Um caso para não ser seguido

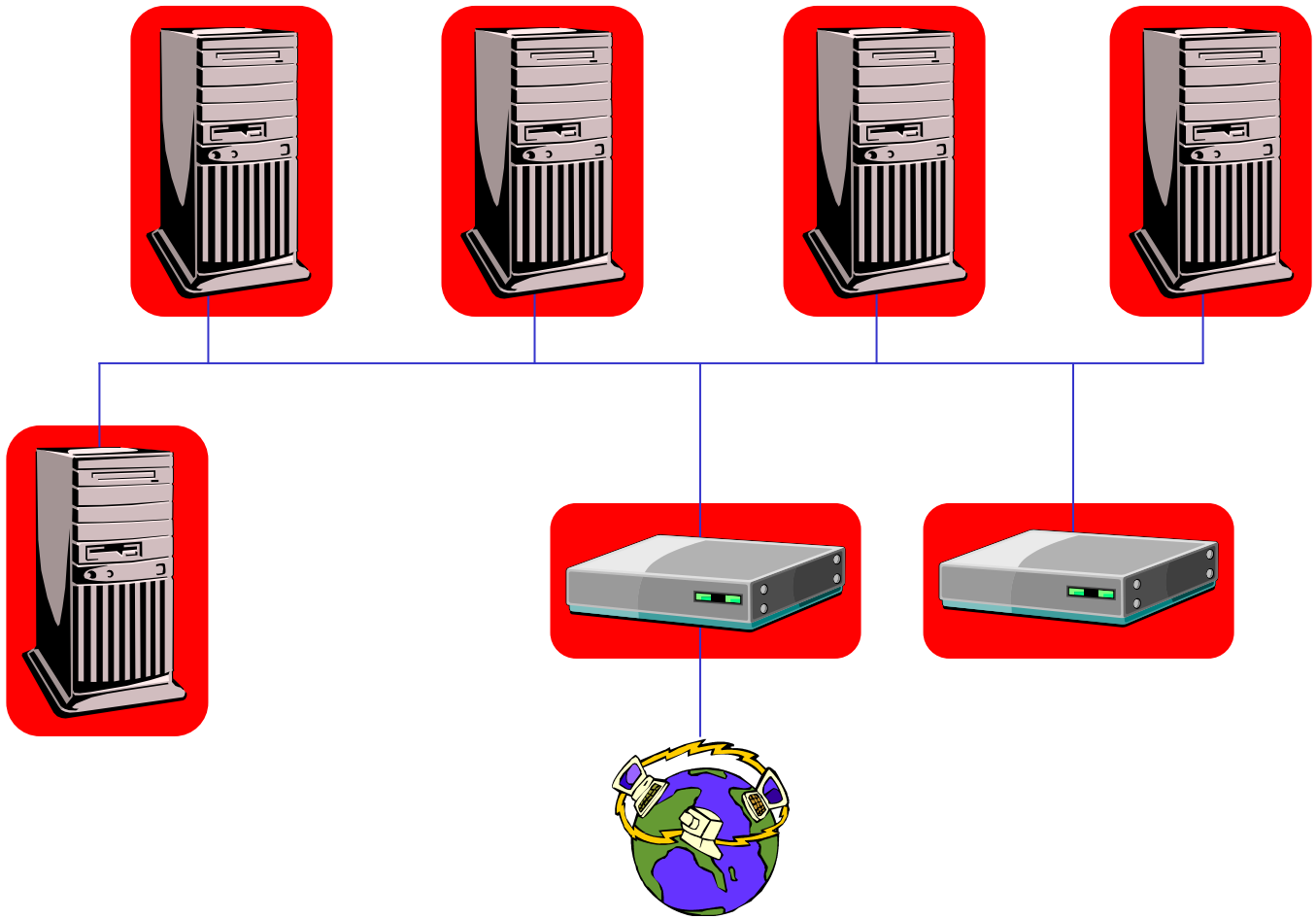
- Atacante com conhecimento zero sobre o alvo
  - dados coletados no DNS
  - portas dos servidores expostos foram varridas sem nenhuma preocupação com detecção, e de fato nada foi detectado
- Encontrado serviço POP vulnerável em um FreeBSD
  - exploração da falha resultou em acesso à conta root
  - instalação de backdoor operando em portas acima de 1023, roteador não filtrava acima disso

Um caso para não ser seguido

- Kernel teve que ser recompilado para habilitar a captura de pacotes da rede por um sniffing
  - novo kernel instalado e ninguém notou a diferença
  - senhas capturadas
    - SURPRESA!!! Todas as contas root dos servidores vizinhos e dos roteadores tinham a mesma senha, e usavam telnet para gerenciamento remoto

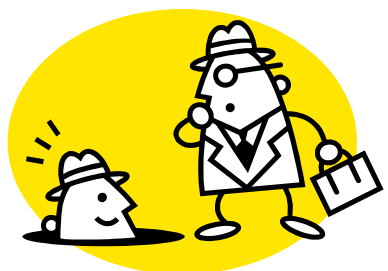
- Resultados
  - invasão durou mais de 1 ano sem qualquer detecção
  - 5 servidores e 2 roteadores completamente comprometidos
  - poderia ter ocorrido uma mudança drástica na vida dos administradores

Um caso para não ser seguido



Um caso para não ser seguido

- Erros cometidos
  - serviços não foram atualizados (POP)
  - filtro de pacotes mal configurado, possibilitando o backdoor
  - falha no monitoramento
    - varredura de portas
    - logs com o resultado da exploração da vulnerabilidade do POP
    - portas abertas pelo backdoor
    - kernel recompilado
    - instalação e uso do sniffer
  - backup comprometido
  - falha no gerenciamento de senhas
    - uso do telnet, possibilitando a captura de senhas
    - todas as senhas eram iguais



Bastion Hosts

- Recomendações gerais
  - o SO deve ser instalado a partir de mídias confiáveis (cd original do fabricante/distribuidor)
  - serviços que não serão utilizados não devem ser instalados
  - aplicar todos os patches conhecidos
  - configurar mecanismos de segurança (ex.: filtragem local de pacotes)
  - todas as configurações devem ser feitas off-line (sem contato com a Internet ou qualquer outra rede não confiável)
  - conheça os serviços a serem fornecidos
    - configuração
    - histórico de vulnerabilidades

Bastion Hosts

- UNIX Like
  - Qual UNIX?
    - familiarização *versus* ferramentas disponíveis
    - distribuições (BSD, Linux)? Somente as mais conhecidas
  - Sistema de Log (syslog)
    - organização dos arquivos de log
    - segurança (integridade dos arquivos de log)
    - log local e remoto
  - Desabilitando serviços
    - /etc/inittab
    - /etc/rc
    - inetd ou xinetd

Bastion Hosts

- UNIX Like
  - Controlando acesso
    - /etc/pam.d
    - TCP Wrapper (/etc/hosts.deny, /etc/hosts.allow)
    - filtragem local de pacotes (ipf, ipchains, netfilter, etc.)

Bastion Hosts

- Windows
  - Qual versão do Windows?
    - 3.0, 3.11, 95, 98, *workstation, release candidates: **NÃO, NUNCA, JAMAIS**
    - versões recentes, estáveis e especificamente para servidores, ex.: Windows NT Server, Windows 2000 Server
  - Sistema de Log
    - não suporta log remoto
    - perder os últimos registros ou não registrar mais?

Bastion Hosts

- Windows
  - Sistema de Log
    - recomenda-se o uso de programas auxiliares

Para não perder os últimos logs: vá no menu de configuração do Visualizador de eventos (Event Viewe) e selecione a opção "Do Not Overwrite Events"

Para a máquina desligar quando o log encher, basta colocar o valor 1 nesta chave: \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail

Para trocar a localização dos três arquivos de log (application, system e security): \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog

Bastion Hosts

- Windows
  - Desabilitando serviços
    - Services control panel
    - Devices control panel (alguns serviços são implementados desta maneira)
    - remover o executável? Nem sempre

Lista de todos os serviços em ordem alfabética:
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

Bastion Hosts

- Windows
  - Desabilitando serviços
    - O que desabilitar?
      - DNS
      - TCP/IP Printing
      - NetBIOS interface
      - Remote Access Service (só ser for utilizar VPN)
      - Server
      - Simple TCP/IP services (echo, chargen, discard, daytime, quotd)
      - SNMP service (se for utilizar use no mínimo NT4 SP4)
      - Routing (Protocols > TCP/IP > Routing > Enable IP Forwarding)
  - Recomendação: Compre o Resource Kit!!!

Firewalls usando Linux

Vinícius Serafim

serafim@inf.ufrgs.br

GSeg UFRGS

Tópicos

- IPChains
- NetFilter

IPChains

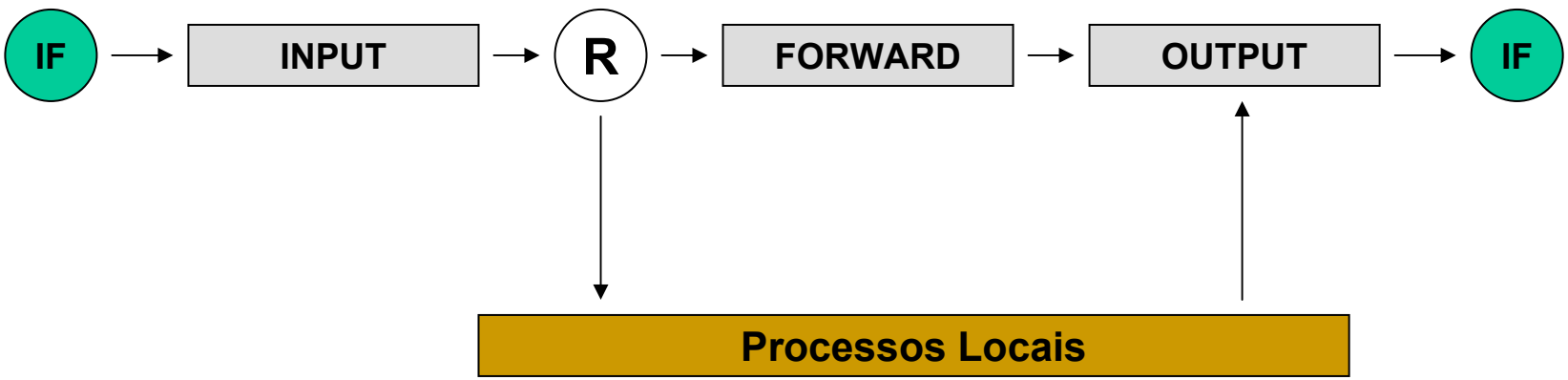
- Sucessor do **ipfwadm**
- Presente no Linux a partir do kernel 2.1.102
- Estável e seguro
- Não faz *statefull packet inspection*

IPChains

- Listas de regras (chains)
- Cada lista tem uma política default
  - ACCEPT
  - REJECT
  - DENY
- Listas podem ser criadas para melhor organizar as regras
- Cada regra tem um dos seguintes alvos
  - ACCEPT, REJECT, DENY
  - MASQ

IPChains

- Como os pacotes passam pelos filtros...



IPChains

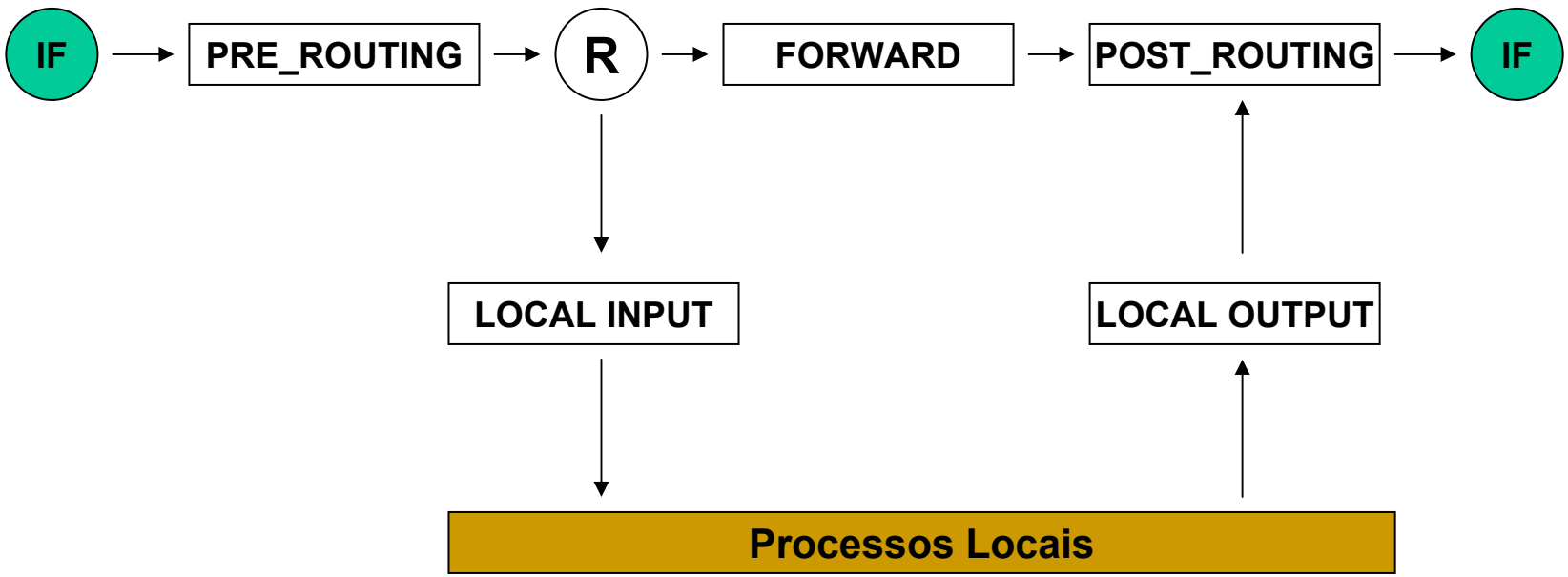
- Referências
  - Firewall and Proxy Server HOWTO
  - Linux IPCHAINS-HOWTO
  - Linux IP Masquerade HOWTO
  - todos podem ser encontrados em **http://www.linuxdoc.org**

NetFilter

- Sucessor do IPChains
- Presente no Linux a partir do kernel série 2.4.x
  - em desenvolvimento, mas já em uso
  - compatível com ipchains e ipfwadm
- Statefull Packet Inspection
- Tabelas (tables)
- Listas (chains) de Regras

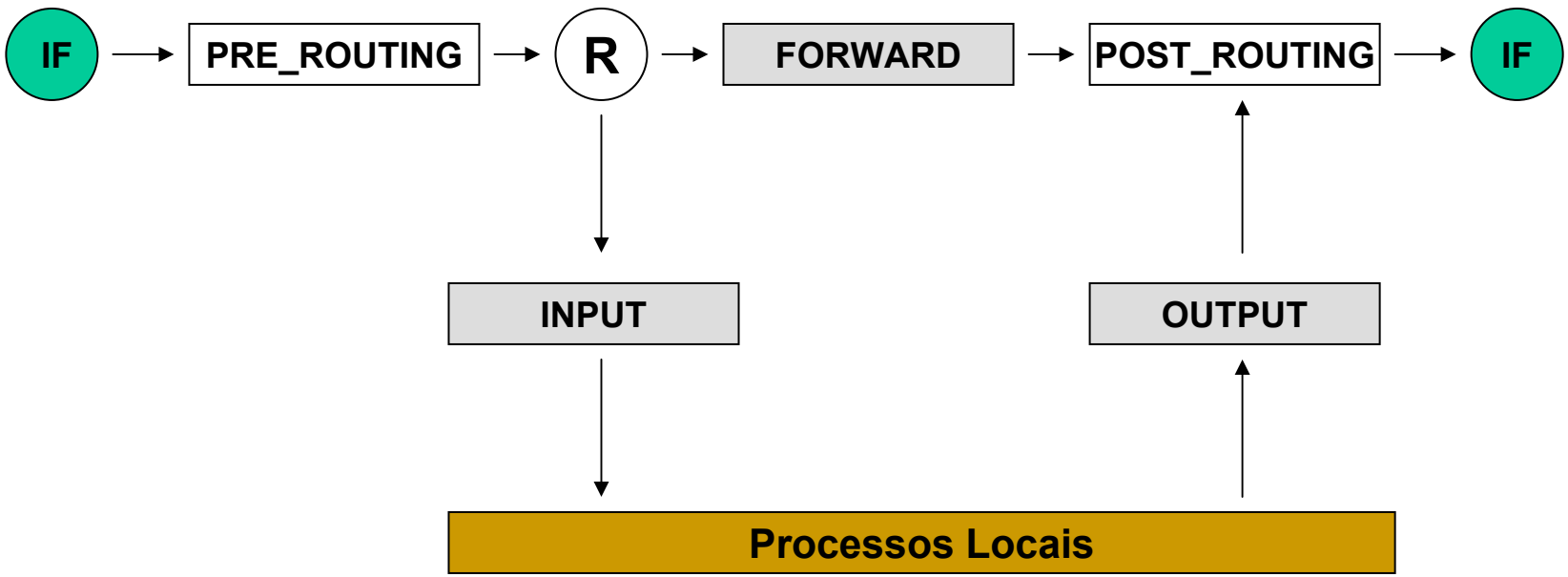
NetFilter

- NetFilter Framework



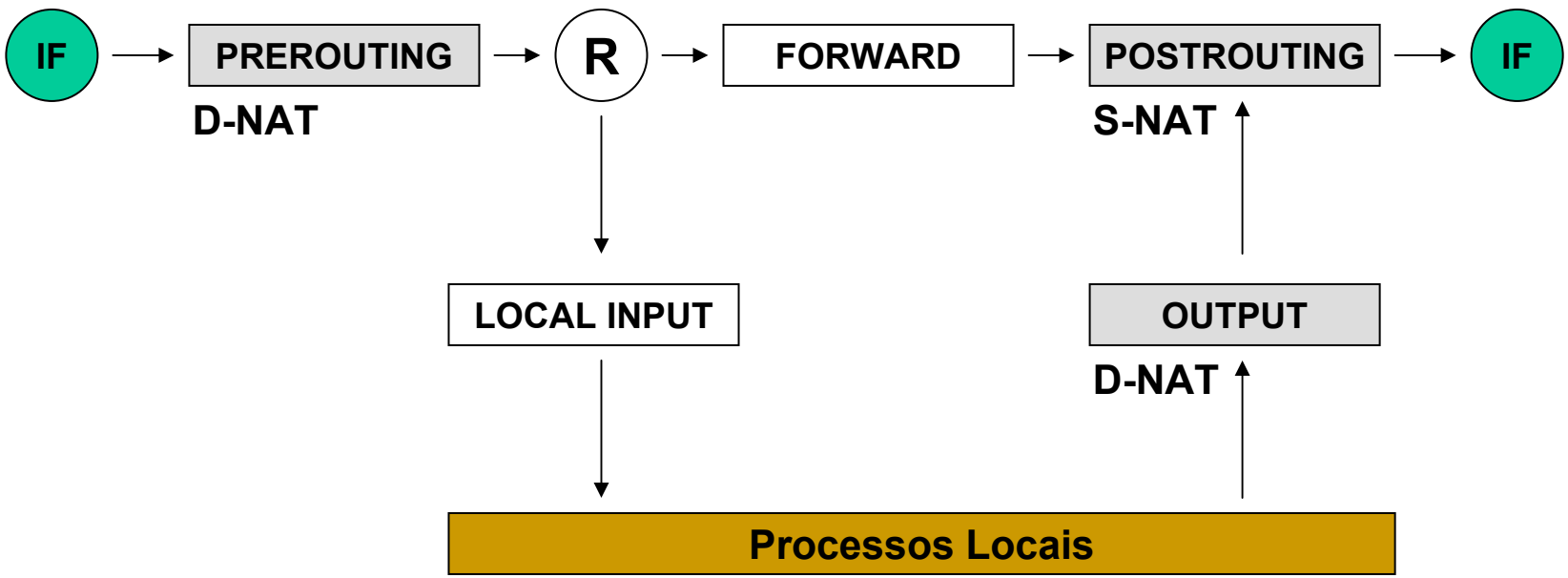
NetFilter

- Filter Table



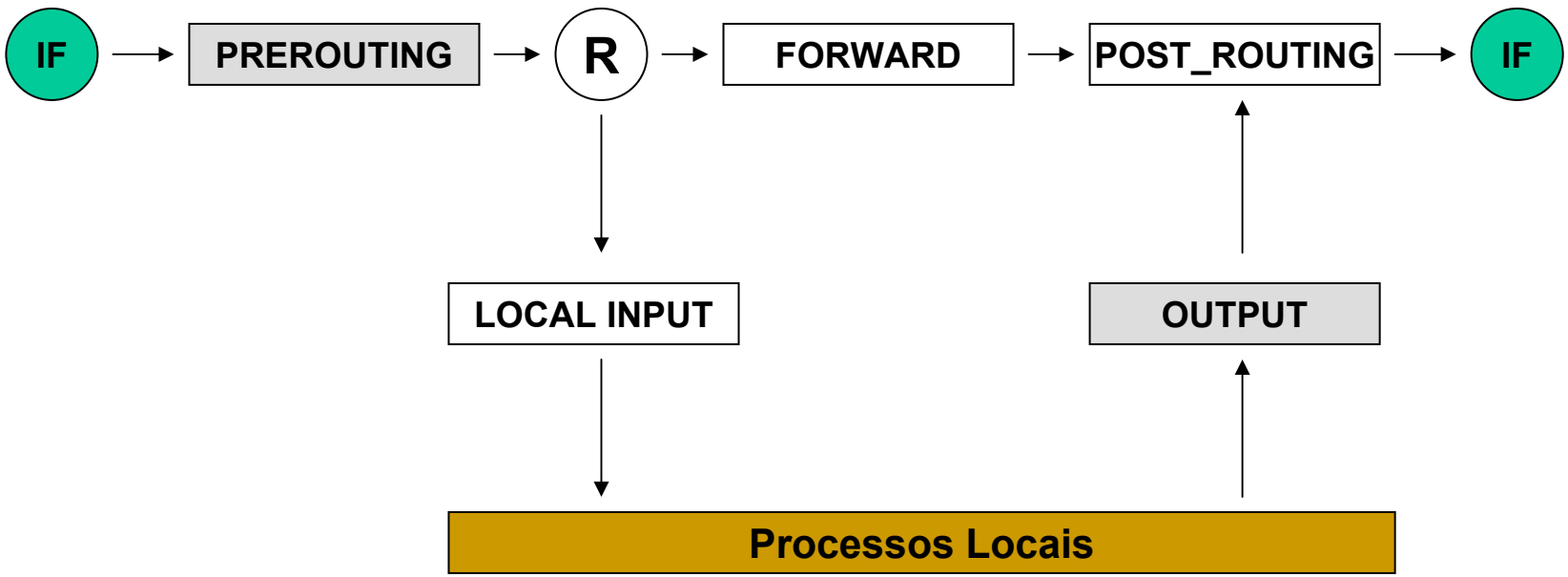
NetFilter

- NAT Table
  - Source NAT (S-NAT): Masquerading
  - Destination NAT (D-NAT): balanceamento, transparent proxy



NetFilter

- Mangle Table



NetFilter

- Onde buscar mais informações (HOW-TOs)
  - http://netfilter.samba.org

Burlando um firewall

Vinícius Serafim

serafim@inf.ufrgs.br

GSeg UFRGS

Tópicos

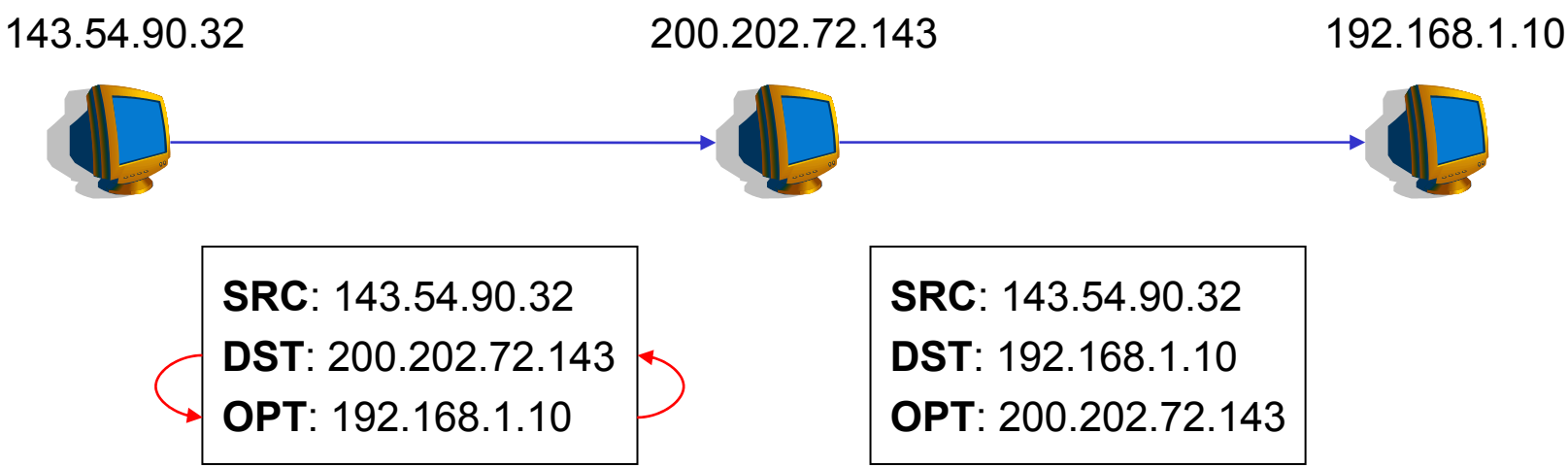
- Uso de portas altas
- Manipulação de portas e endereços
- Conexões iniciadas internamente
- Tunneling

Uso de portas altas

- Portas acima de 1023 são utilizadas para disponibilização de serviços
- São possíveis devido à falha de configuração ou à um modelo de política permissiva

Manipulação de portas e endereços

- Uso de uma porta privilegiada como porta de origem
- Opção *Source Routing* do IP



Conexões iniciadas internamente

- Normalmente são permitidas (ex.: HTTP, FTP, POP)
- Exemplo
  - pode-se instalar um “servidor” que tenta conectar-se com um determinado “cliente” em alguns horários pré-definidos.

Tunneling

- Consiste em utilizar um protocolo permitido para abrir conexões não permitidas
- Protocolos como ICMP e HTTP podem ser utilizados
- Ex.:
  - httptunnel
  - icmp file transfer