INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança de Redes

Firewall

Filipe Raulino
filipe.raulino@ifrn.edu.br

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

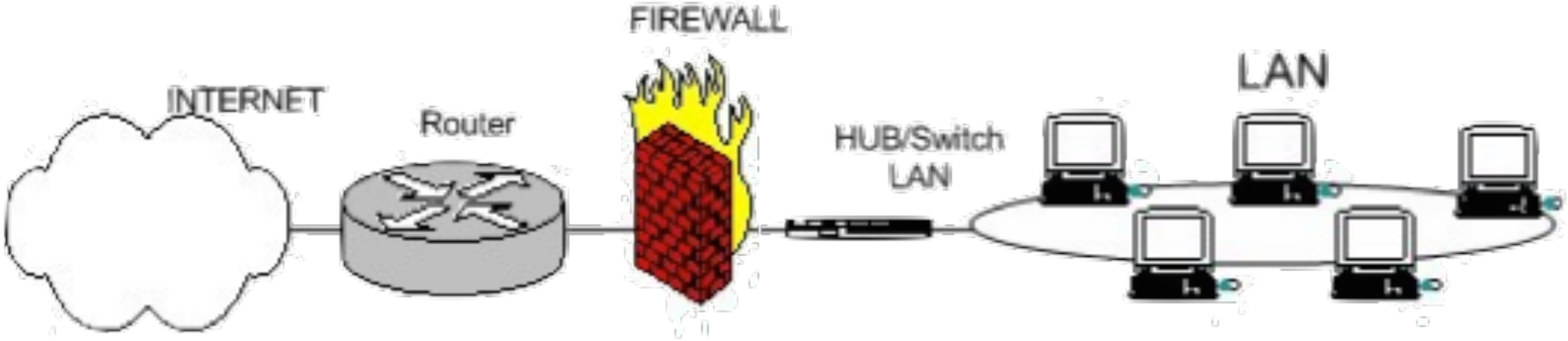
Introdução

- O firewall é uma combinação de hardware e software que isola a rede local de uma organização da internet;
- Com ele é possível implementar uma política de controle de acesso, bloqueando ou permitindo a passagem de pacotes;

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Firewalls

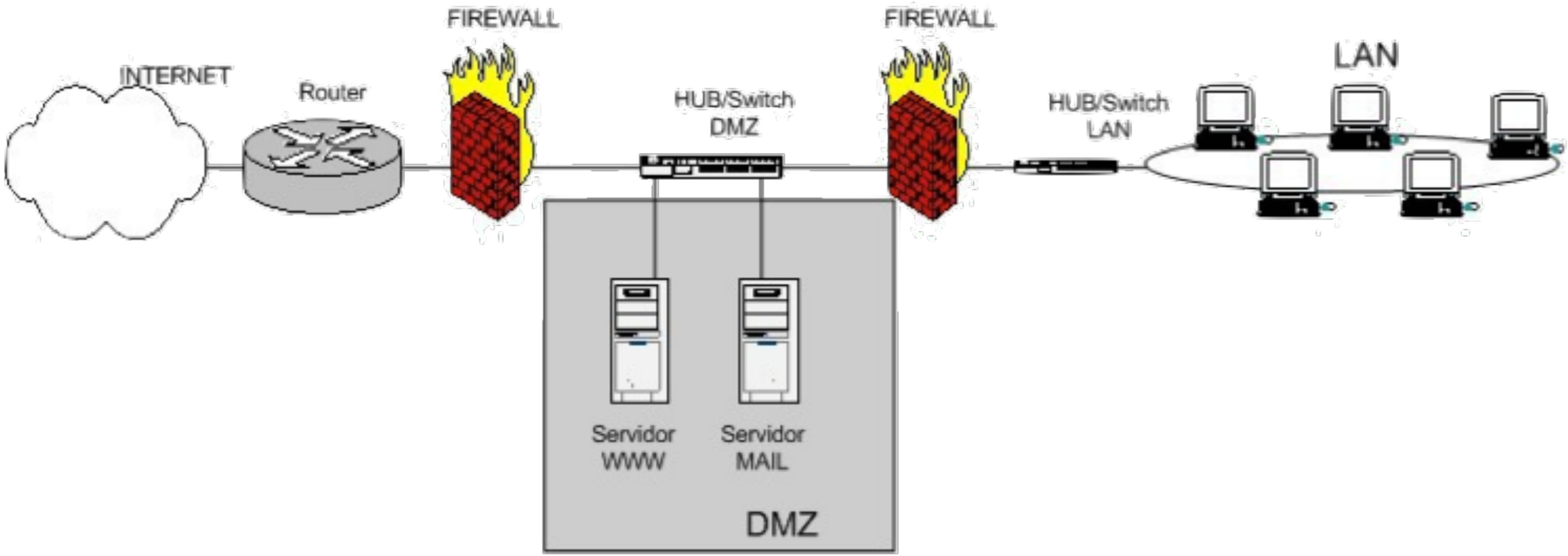
- **Topologia**



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Firewalls

- **Topologia**



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Características

- Pelo firewall devem passar todos os pacotes que chegam ou saem de uma rede.
  - Somente o tráfego autorizado na política de segurança da organização será encaminhado.

- O firewall deve prover ferramentas para registro e monitoramento do tráfego, como logs e envios de alertas.

- O firewall também é adequado para:
  - Implementação de serviços como NAT e VPN;
  - Realização de auditorias; e
  - Geração de estatísticas do uso da rede.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

NAT - Network Address Translations

- Conversão de endereços privados para endereços públicos:
  - As máquinas internas utilizam endereços privados.
- Esconde a topologia interna da rede:
  - Isola as máquinas da rede interna.
- O gateway faz a tradução de endereços.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Tipos de Firewall

- **Firewalls de filtragem de pacotes:** Este tipo de firewall toma as decisões baseadas nos parâmetros do pacote, como porta/endereço de origem/ destino, estado da conexão, e outros parâmetros do pacote. O firewall então pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT). O **iptables** é um excelente firewall que se encaixa nesta categoria.

- **Gateways de camada de aplicação:** Firewalls deste tipo são mais intrusivos e permitem um controle relacionado com o conteúdo do tráfego. Alguns firewalls em nível de aplicação combinam recursos básicos existentes em firewalls de filtragem de pacotes combinando as funcionalidade de controle de tráfego/controle de acesso em uma só ferramenta.

Os dois tipos de firewalls podem ser usados em conjunto

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtragem de Pacotes

- Aplica sequencialmente uma série de regras de filtragem aos pacotes e então encaminha ou descarta os mesmos;
- As regras são baseadas nas informações contidas nos cabeçalhos dos pacotes:
  - Endereço IP de origem;
  - Endereço IP de destino;
  - Interface de rede;
  - Protocolos (TCP, UDP, ICMP, …).

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtragem de Pacotes

- Em geral, são implementados junto com o processo de roteamento;

- Alguns tipos de firewall de filtragem de pacotes podem guardar o estado da conexão:
  - Pacotes que pertençam a uma conexão já conhecida podem ser encaminhados sem uma nova consulta às regras de filtragem;
  - Dificultam diversos tipos de ataques, e possibilitam o funcionamento de serviços problemáticos para a filtragem de pacote convencional como SIP, H323, FTP…

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtragem de Pacotes

- Ao final do conjunto de regras será aplicada uma ação (política) padrão: descartar ou encaminhar
  - Em Firewalls cuja **política padrão é descartar** as regras devem ser de liberação, pois tudo que não for permitido estará proibido.
  - Em Firewalls cuja **política padrão é encaminhar** as regras devem ser de bloqueio, pois tudo que não for proibido será permitido.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Firewall de Camada de Aplicação

- São também conhecidos como servidores **proxy**;
- Age como um intermediário das conexões em nível de aplicação;
- Apesar de poderem ser implementados para qualquer aplicação, historicamente são utilizados para os serviços de HTTP e FTP.
- Não protegem o sistema operacional da própria máquina
- Desempenho inferior ao de filtro de pacote

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Limitações de Firewalls e Gateways

- **IP spoofing:** roteador não pode saber se os dados realmente vêm da fonte declarada
- Se múltiplas aplicações requerem um tratamento especial, cada uma deve ter seu próprio gateway de aplicação
- O software cliente deve saber como contatar o gateway

  Ex., deve configurar o endereço IP do proxy no browser Web
- Filtros muitas vezes usam uma regra radical para UDP: bloqueiam tudo ou deixam passar tudo
- Compromisso: grau de comunicação com mundo exterior versus nível de segurança

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Proteger?

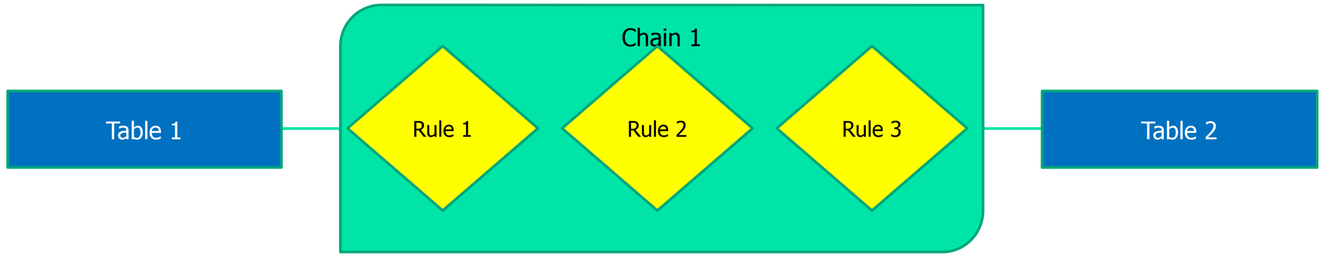
- Quais serviços precisa proteger.
- Que tipo de conexões eu posso deixar passar e quais bloquear.
- Que máquinas terão acesso livre e quais serão restritas.
- Que serviços deverão ter prioridade no processamento.
- Que máquinas/redes NUNCA deverão ter acesso a certas/todas máquinas.
- Etc…

Iptables

- O iptables, assim como a maioria (ou todos) dos filtros de pacotes, baseia-se em ACL´s (Access Control List), que servem para representar a política de segurança desejada

- As ACL´s do iptables possuem várias peculiaridades, porque vários elementos sofisticados são utilizados para formar uma regra dentro do contexto da política desejada

- O iptables utiliza os conceitos de
  - Cadeias (chains)
  - Tabelas (Tables)
  - Regras (rules)



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Regras

- As regras são como comandos passados ao iptables para que ele realize uma determinada ação (como bloquear ou deixar passar um pacote).

- As regras são armazenadas dentro dos **chains** e processadas na ordem que são inseridas.

- As regras são armazenadas no kernel, o que significa que quando o computador for reiniciado tudo o que fez será perdido. Por este motivo elas deverão ser gravadas em um arquivo para serem carregadas a cada inicialização.

Um exemplo de regra: iptables -A INPUT -s 123.123.123.1 -j DROP.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Cadeias

- É onde podemos especificar a situação do tratamento dos pacotes, seja qual tabela for;
- Podem ser classificadas como estruturas para comportar regras;
- Existem dois tipos de cadeias:
  - Cadeias padrão ; e
  - Cadeias criadas pelo usuário.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Cadeias Padrão

- **PREROUTING**
  - Tráfego ingressante na máquina (incluindo tráfego gerado localmente com destino local)
- **INPUT**
  - Tráfego que tem como destino a própria máquina
- **FORWARD**
  - Tráfego passante pela máquina
- **OUTPUT**
  - Tráfego gerado localmente (tanto com destino local como remoto)
- **POSTROUTING**
  - Todo tráfego que "sai" da máquina (incluindo tráfego gerado localmente com destino local)

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Criando uma Cadeia

- Criação de cadeias (user-chain)
  - iptables –N <OP>

    -N Create a new chain
    -X Delete an EMPTY chain
    -P Change the Policy for a built-in chain
    -L Lists the chain rules
    -F Flushes the rules of a chain
    -Z Sets the counters to zero on all the rules in a chain

  - iptables –N allow
  - iptables –L allow

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Tabelas

- Tabelas são os locais usados para armazenar os chains e conjunto de regras com uma determinada característica em comum. As tabelas podem ser referenciadas com a opção -t tabela;

- Existem 3 tabelas disponíveis no iptables:
  - **FILTER** - responsável pela filtragem de todos os pacotes que passam pelo host, não importando origem e destino;
  - **NAT** - responsável pelo controle dos pacotes que passam pelo host, mas cuja origem ou destino não é o mesmo.
  - **MANGLE** - ermite alterar características específicas do pacote, como por exemplo: o TOS (Tipo de Serviço) o que permite implementar um sistema simples de QOS (qualidade de serviço).

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Fluxos do Iptables

A tabela *FILTER* - É a tabela padrão do Netfilter e trata das situações implementadas por um Firewall filtro de pacotes. Estas situações são: **INPUT, FORWARD e OUTPUT.**

A tabela NAT - Usada para dados que gera outra conexão (masquerading, source nat, destination nat, port forwarding, proxy transparente são alguns exemplos). Possui 3 chains padrões: **PREROUTING, OUTPUT e POSTROUTING**

A tabela MANGLE - Implementa alterações especiais em pacotes em um nível mais complexo. A tabela mangle é capaz, por exemplo, de alterar a prioridade de entrada e saída de um pacote baseado no tipo de serviço (TOS) o qual o pacote se destinava. Suas situações são: **PREROUTING e OUTPUT.**

Iptables - Ações

- São os destinos dados ao pacote quando o pacote coincide com a regra

- Target padrão
  - ACCEPT
  - DROP
  - REJECT
  - LOG

- Target personalizada
  - Implementado com chains personalizadas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Política Padrão

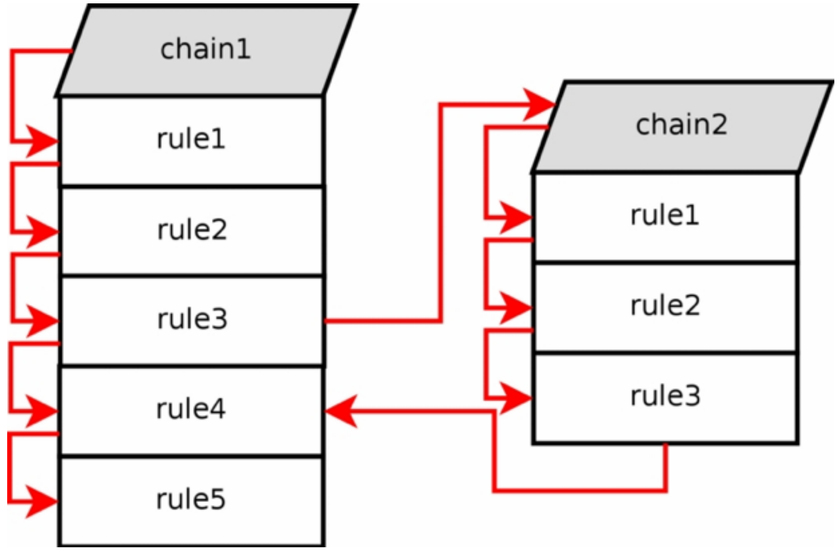
As chains INPUT, OUTPUT e FORWARD possuem também políticas

- Política ACCEPT
  - Tudo que não estiver bloqueado será permitido
  - Regras serão de bloqueio

- Política DROP
  - Tudo que não estiver liberado será bloqueado
  - Regras serão de liberação

Sintaxe: iptables -P <chain> <politica>

- Ordem de aplicação das regras
  - São avaliadas na ordem em que são inseridas, seqüencialmente



  - Após avaliadas todas as regras, sem ocorrência de ‘match’, a política padrão será aplicada

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Sintaxe básica

- Inserir uma regra no início de uma chain
  - iptables [-t <tabela>] -I <chain> <regra> -j <acao>
- Inserir uma regra no final de uma chain
  - iptables [-t <tabela>] -A <chain> <regra> -j <acao>
- Remover uma regra de uma chain
  - iptables [-t <tabela>] -D <chain> <regra> -j <acao>

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Iptables - Sintaxe básica

- Alterar a política de uma chain
  - iptables -P <chain> <politica>
- Listar as regras de uma chain
  - iptables [-t <tabela>] -L [-n] <chain>
- Remover todas as regras de uma chain
  - iptables -F <chain>