EN-3611

Segurança de Redes

Firewalls

Prof. João Henrique Kleinschmidt

Middleboxes

- RFC 3234: Middleboxes: Taxonomy and Issues
- Middlebox
  - Dispositivo (box) intermediário que está no meio do caminho dos pacotes entre sua origem e destino
  - Realiza funções não convencionais a um roteador IP
    - Roteadores são totalmente necessários
- Objetivo
  - Utilizar uma menor quantidade de endereços IP, melhorar o desempenho e aumentar a segurança
- Middleboxes trazem alguns problemas
- Tipos de middleboxes: NAT, firewall, proxy, cache, balanceador de carga, etc.

Firewall - definição

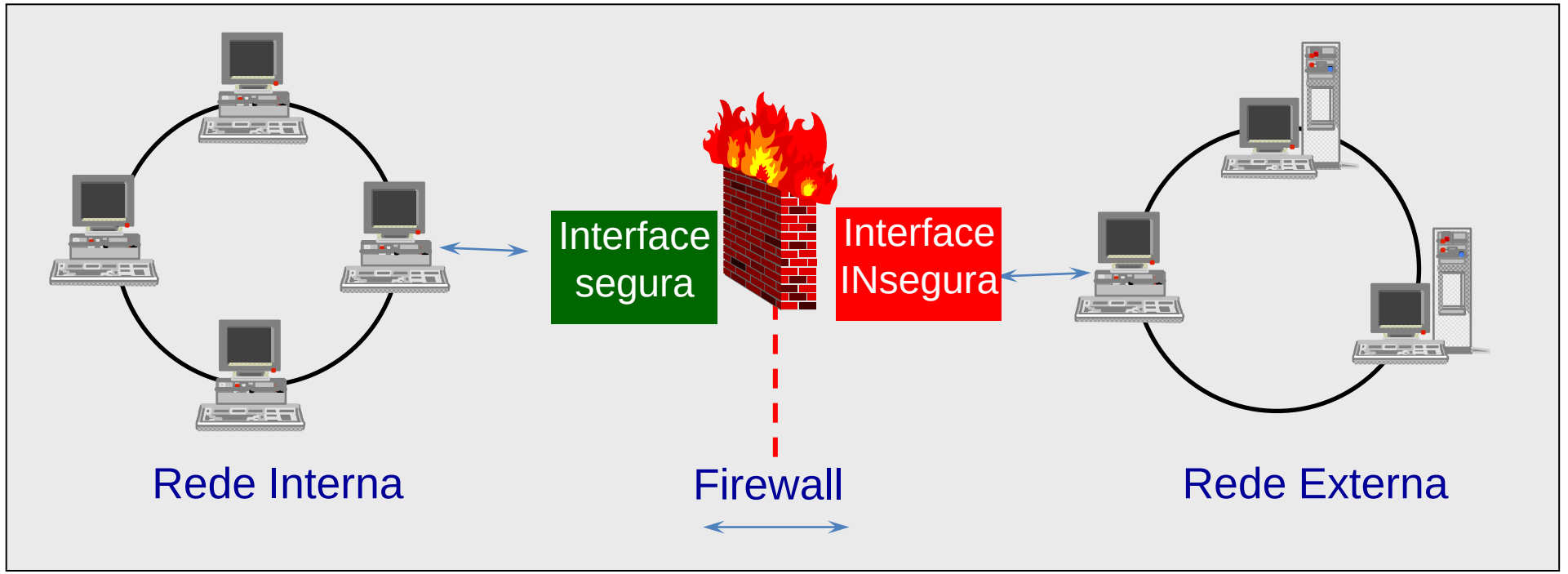
- “Ponto entre duas ou mais redes, no qual circula todo o tráfego. A partir desse ponto é possível controlar e autenticar todo o tráfego, além de registrar, por meio de logs, todo o tráfego da rede, facilitando sua auditoria.” (Cheswick e Bellovin)

- “Componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet, ou entre conjunto de redes.” (Chapman)

Firewall - Motivação

- Motivação:
  - Proteger uma rede privada contra “intrusos”
  - Impedir acessos a recursos computacionais por usuários não autorizados
  - Impedir exportação de informações não autorizadas
- Outros Propósitos:
  - Bloquear acesso a sites particulares
  - Prevenir que certos usuários/máquinas acessem certos servidores/serviços

O Sistema Firewall



O Sistema Firewall

- É um mecanismo de segurança
- Consiste em uma máquina interceptando todo o tráfego de entrada e saída da rede
- Pode ser configurado para filtrar acesso da Internet para a rede interna e vice-versa
  - De acordo com um **conjunto de regras**
- Controla quais dados saem e entram na sua rede
- Quando bem configurado é difícil de quebrar

O que é um Firewall?

- Logicamente é um separador, analisador ou filtro de pacotes
- Fisicamente pode ser um roteador, um computador ou uma combinação de roteadores e computadores com o software apropriado
- Pode ser comparado com um fosso de um castelo, e como um fosso, não é invulnerável
- Pode trabalhar em conjunto com um Intrusion Detection System (IDS)

Firewall: Funções

- O que um firewall faz?
  - Serve como foco das decisões de segurança
  - Reforça a política de segurança
  - Registra a atividade de internet com eficiência
  - Limita a exposição
- O que um firewall não faz?
  - Não protege contra atacantes internos
  - Não protege contra conexões que não passam através dele
  - Não protege contra novas vulnerabilidades
  - Não protege completamente contra vírus
  - Não se auto configura corretamente

Funcionalidades

- Componentes clássicos:
  - Filtros
  - Proxies
  - Bastion hosts
  - Zonas desmilitarizadas (DMZ)
- Outros componentes:
  - Network Address Translation (NAT)
  - Rede privada virtual (VPN)
  - Autenticação/certificação
  - Balanceamento de cargas e alta disponibilidade

Evolução técnica

- Tecnologia antiga (final da década de 80) na indústria de segurança, mas em constante evolução. Existe uma tendência de adicionar cada vez mais funcionalidades que podem não estar relacionadas necessariamente à segurança. Porém, essa integração deve ser feita com cuidado. Quanto mais funções o firewall possuir, maiores são as chances de algo dar errado.
- Tecnologias de firewall:
  - Filtro de pacotes
  - Filtro de pacotes baseado em estados
  - Proxy
  - Híbrido
  - Adaptativo
  - Reativo
  - Individual ou pessoal

Filtro de pacotes

- Funciona na camada de rede e de transporte TCP/IP, realizando as decisões de filtragem com base nas informações do cabeçalho de pacotes.
- IP: endereço IP de origem e destino, flags
- UDP: porta origem e destino
- TCP: porta de origem e destino, flags TCP: SYN, SYN-ACK, ACK, RST, FIN (usados para observar sentido das conexões, por exemplo)

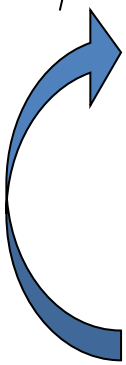
- Exemplo: permissão de usuários internos a websites

Regra	End. origem:Porta origem	End.destino:porta destino	Ação
1	IP rede interna: porta alta	Qualquer endereço:80 (HTTP)	Permitir
2	Qualquer endereço:80 (HTTP)	IP rede interna: porta alta	Permitir
3	Qualquer end:qualquer porta	Qualquer end:qualquer porta	Negar

Sequência de criação de regras

- A sequência na qual as regras são aplicadas pode alterar completamente o resultado da política de segurança. Por exemplo, as regras de aceite ou negação incondicional devem ser sempre as últimas regras da lista.

O deslocamento de uma regra genérica para cima anula as demais.



Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Out	tcp	interno	*	> 1023	23	*
permitir	In	tcp	*	interno	23	> 1023	1
permitir	In	tcp	*	interno	> 1023	23	*
permitir	Out	tcp	interno	*	23	> 1023	1
negar	*	*	*	*	*	*	*

Filtro de pacotes

- Vantagens
  - Baixo overhead/alto desempenho da rede
  - Barato, simples e flexível
  - Transparente para o usuário
- Desvantagens
  - Permite conexão direta para hosts internos de clientes externos
  - Dificuldade de filtrar serviços que utilizam portas dinâmicas
  - Deixa brechas permanentes abertas no perímetro da rede (DMZ)
  - Difícil de gerenciar em ambientes complexos

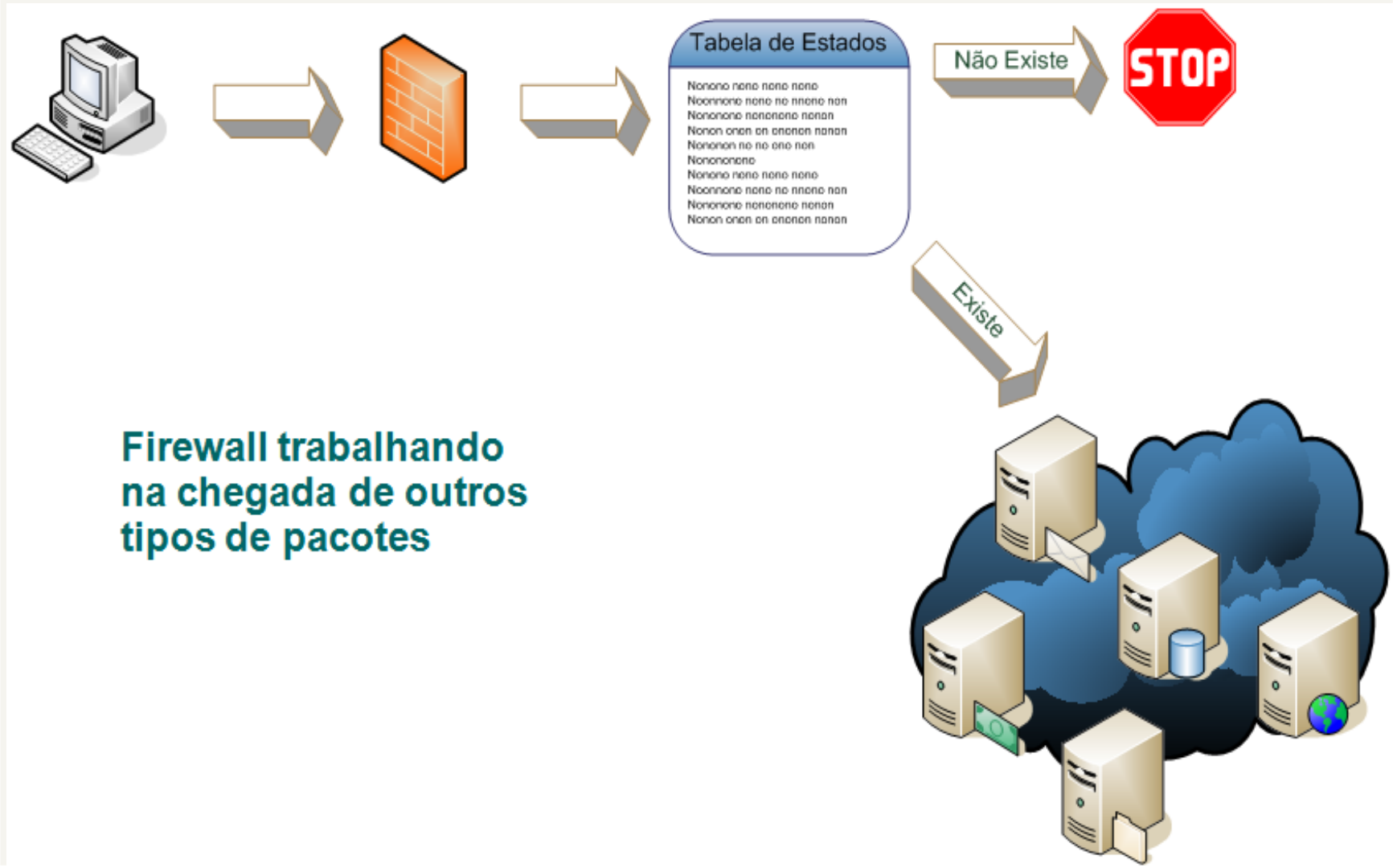
Filtro de pacotes baseado em estados

- Filtro de pacotes dinâmicos ou baseado em estados, decisões de filtragem usando
  - Informações dos cabeçalhos dos pacotes
  - Tabela de estados, que guarda os estados de todas as conexões
- O firewall trabalha verificando somente o primeiro pacote de cada conexão. Se este pacote é aceito, os demais pacotes são filtrados de acordo com as informações desta conexão na tabela de estados.

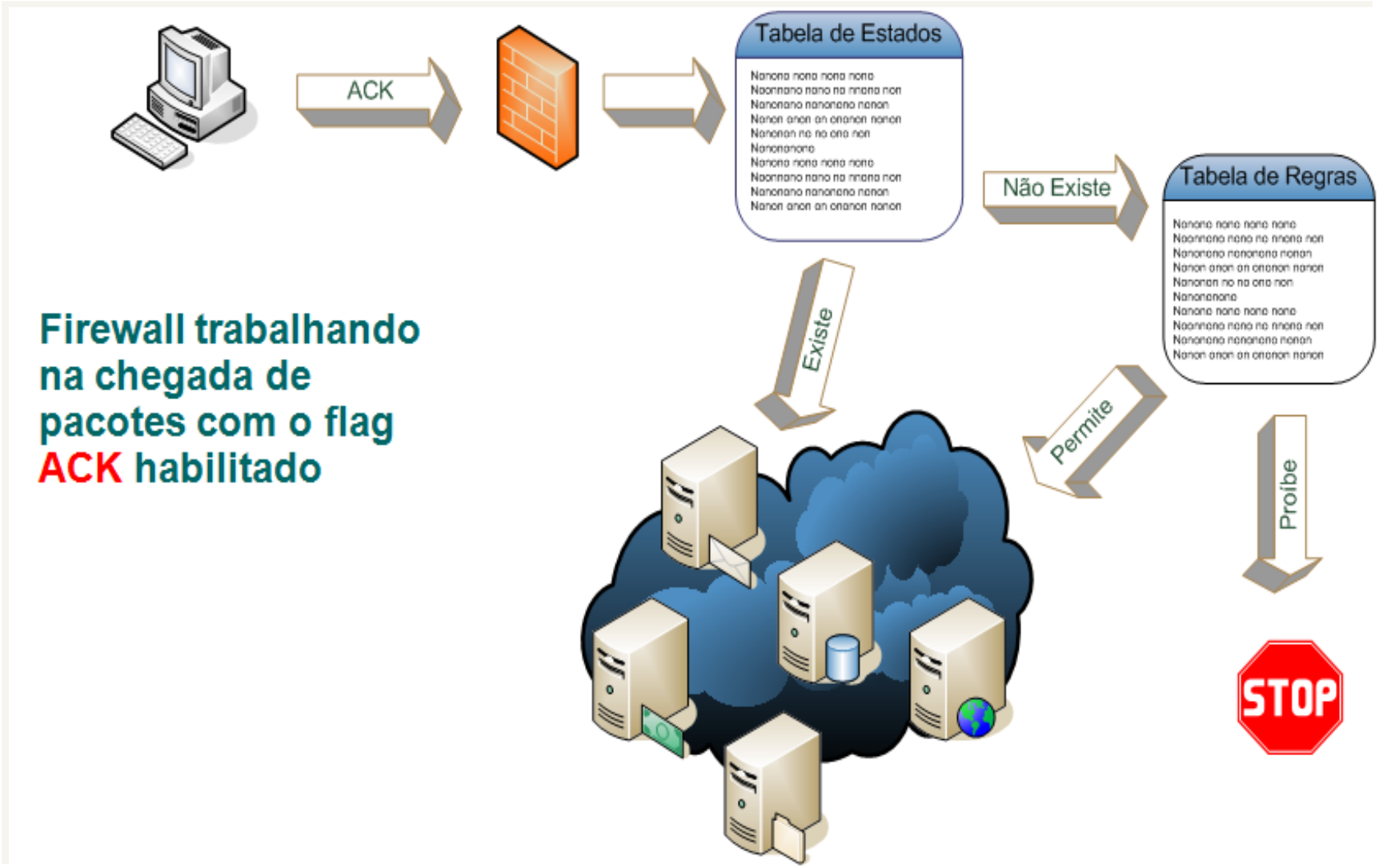
Regra	End. origem:Porta origem	End.destino:porta destino	Ação
1	IP rede interna: porta alta	Qualquer endereço:80 (HTTP)	Permitir
2	Qualquer end:qualquer porta	Qualquer end:qualquer porta	Negar

Filtro de pacotes baseado em estados

Filtro de pacotes baseado em estados



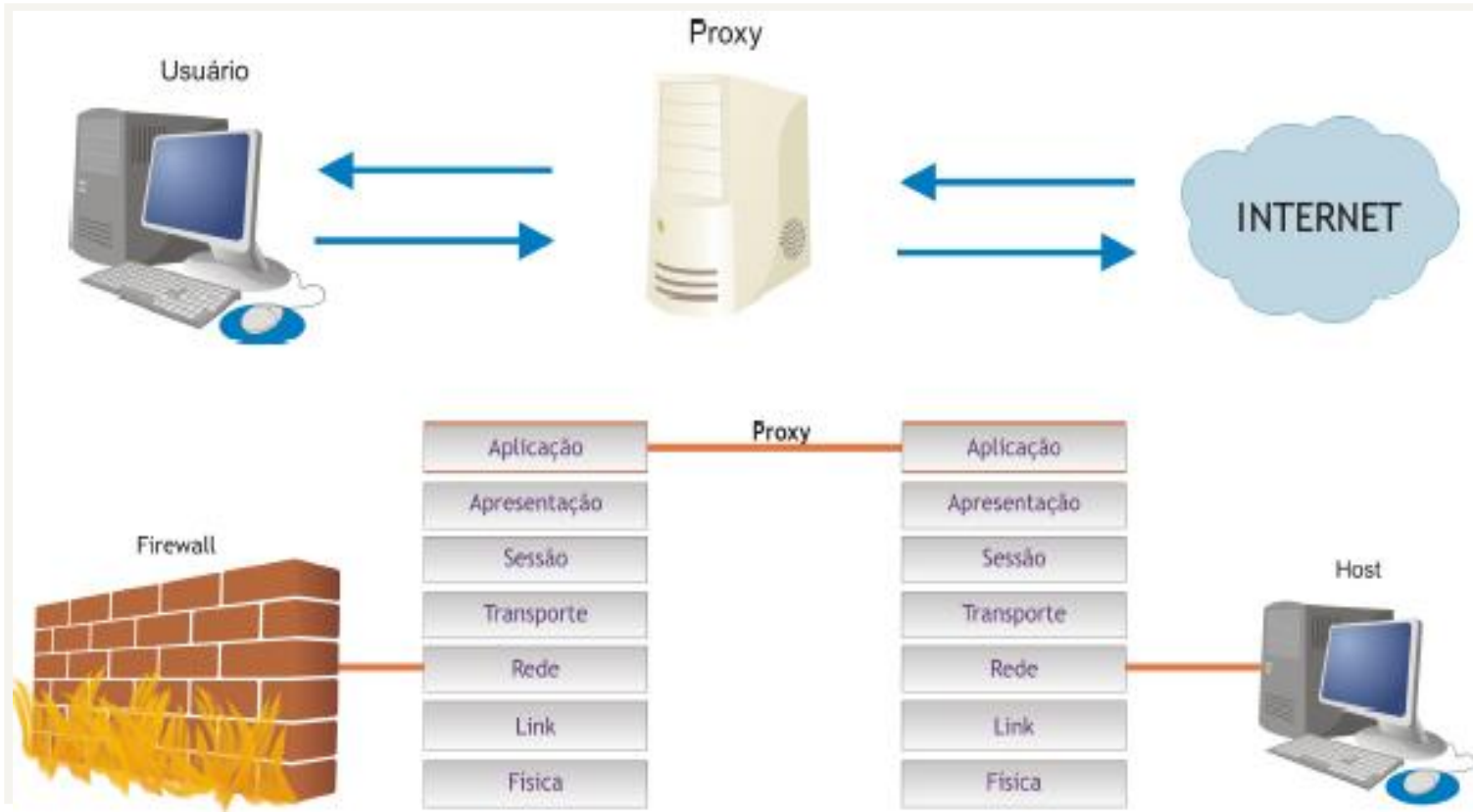
Filtro de pacotes baseado em estados



Filtro de pacotes baseado em estados

- Vantagens
  - Aberturas apenas temporárias no perímetro da rede
  - Baixo overhead/alto desempenho da rede
  - Aceita quase todos os tipos de serviços
- Desvantagens
  - Permite conexão direta para hosts internos a partir de redes externas
  - Não oferece autenticação de usuário

Proxy


Proxy
Usuário
INTERNET
Proxy
Aplicação
Apresentação
Sessão
Transporte
Rede
Link
Física
Aplicação
Apresentação
Sessão
Transporte
Rede
Link
Física
Firewall
Host

Proxy

- Usuário se conecta a uma porta TCP no firewall, que então abre outra conexão no mundo exterior.
- Faz com que o tráfego pareça ter origem no proxy, mascarando o endereço do host interno.
- Vantagens:
  - Não permite conexões diretas entre hosts internos e externos
  - Aceita autenticação de usuário
  - Analisa comandos da aplicação no payload dos pacotes de dados
  - Permite criar logs do tráfego
- Desvantagens:
  - Requer um proxy específico para cada aplicação
  - Não aceita todos os serviços
  - Requer que os clientes internos saibam da sua existência (está mudando com o uso de proxy transparente)

Proxy transparente

- Servidor proxy modificado, que exige mudanças na camada de aplicação e no núcleo do firewall
- Redireciona as sessões que passam pelo firewall para um servidor proxy local
- Isso é transparente para o usuário
  - Não necessita configurar aplicativos
- Squid pode ser usado como proxy transparente

Tecnologias de firewall

- Firewalls híbridos
  - Misturam elementos de filtros de pacotes, pacotes baseado em estados e proxies para cada serviço específico
  - Utiliza estes mecanismos de segurança em paralelo
  - Atualmente, a maioria dos firewalls comerciais é híbrida
  - Ex: telnet é manipulado por filtro de pacotes e FTP pelo proxy (filtragem no nível da aplicação)
- Proxies adaptativos
  - Utiliza mecanismos de segurança em série
  - Ex: FTP emprega duas conexões (tráfego de controle e transferência de dados). A parte de controle é processada na camada de aplicação e os dados na camada de rede pelo filtro de pacotes

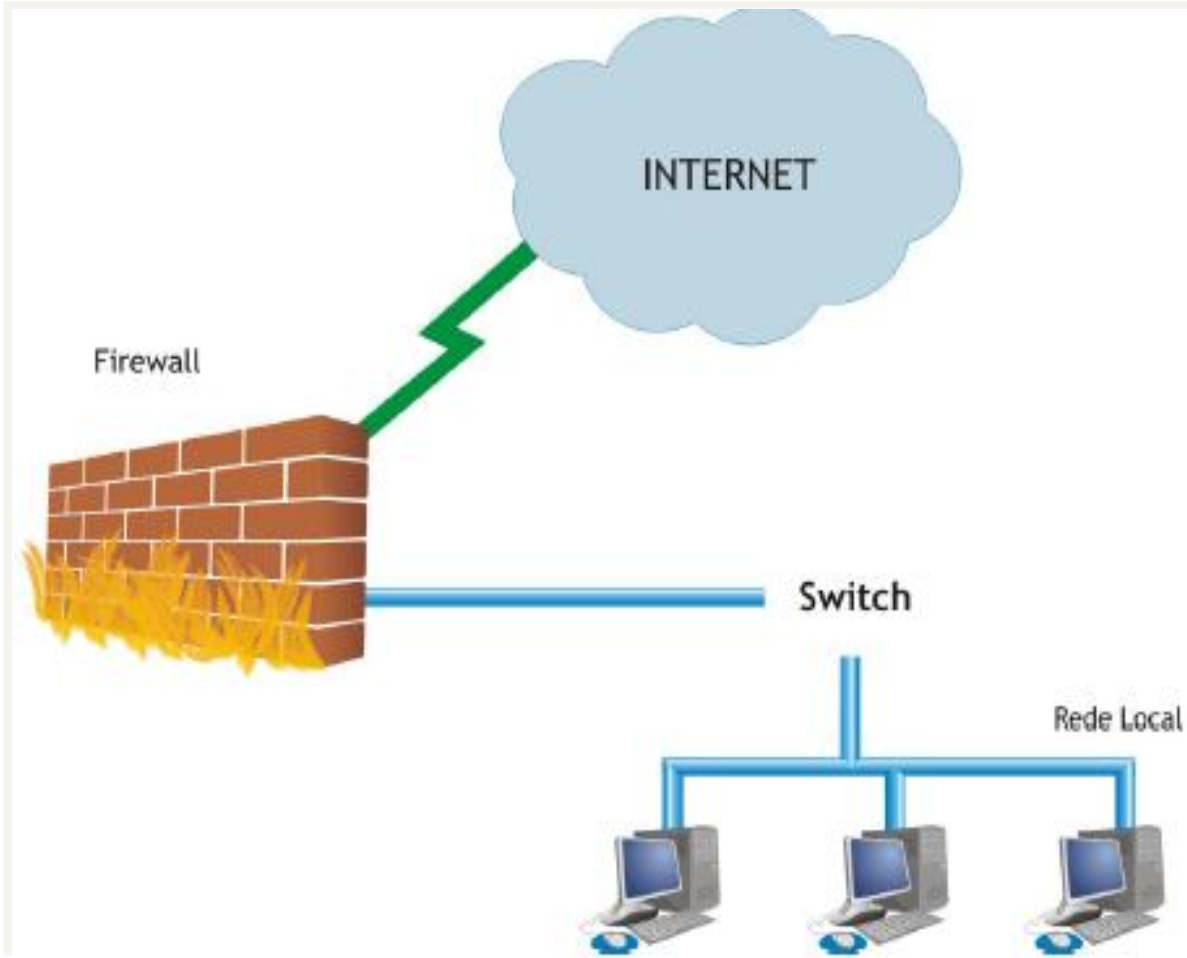
Tecnologias de firewall

- Firewalls reativos
  - Apresentam integração com sistemas de detecção de intrusão
  - É capaz de mudar a configuração de suas regras de filtragem de modo dinâmico, enviar mensagens aos usuários e ativar alarmes
  - Desvantagem: pode ser alvo de ataques de DoS (se pacotes que acionem alarmes forem enviados, por exemplo)
- Firewalls individuais
  - Atua na segurança do host individual, e não da rede
  - A conexão na rede interna cada vez mais é feita através de laptops e acessos remotos por equipamentos na cada do usuário, usando VPNs. Isso faz com que esses equipamentos necessitem de uma proteção adequada.
  - Usado por usuários domésticos, que são comumente usados como intermediários em ataques DDoS.

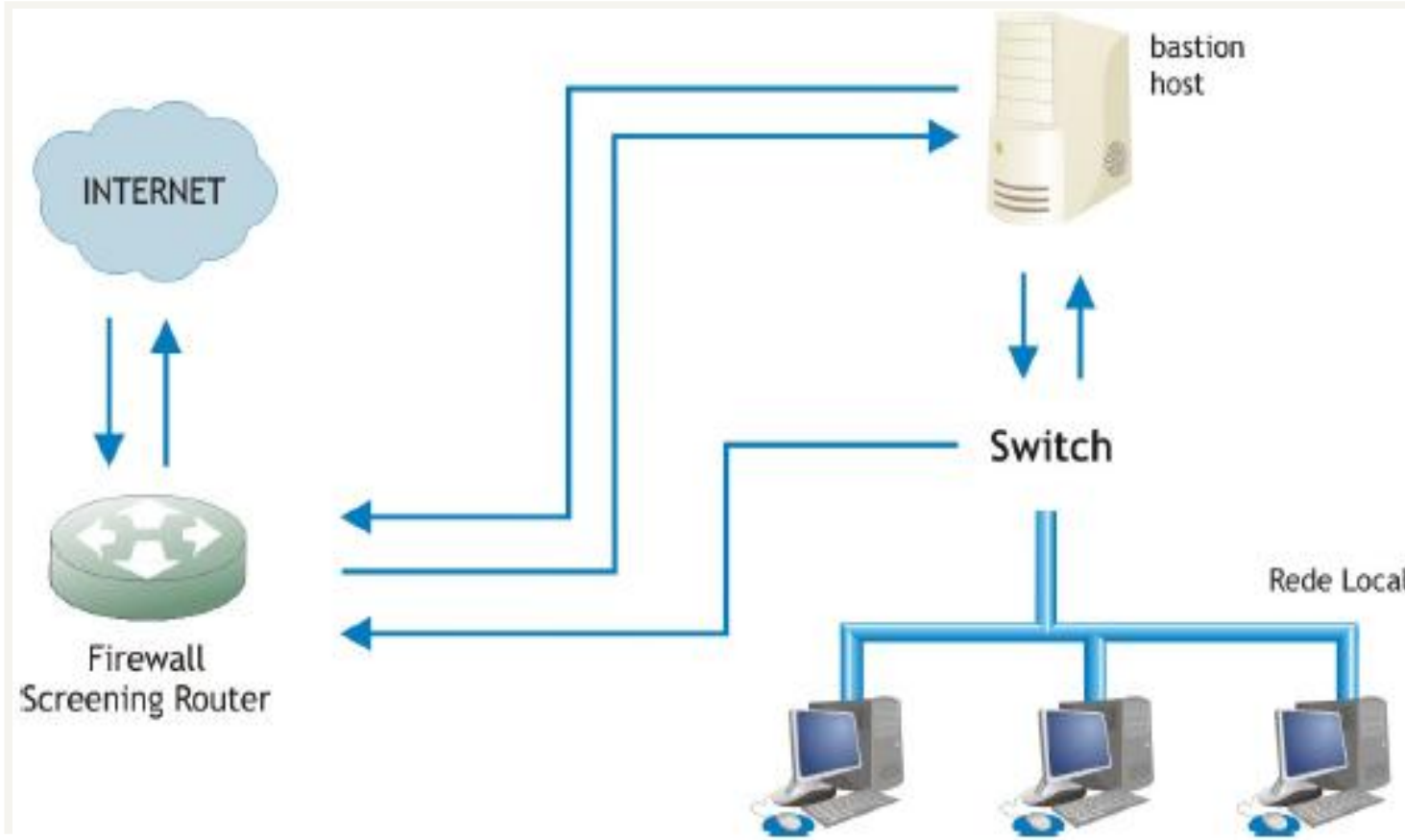
Arquiteturas de firewall

- Devem ser definidas de acordo com a necessidade da organização
- Arquiteturas clássicas
  - Dual-homed host – Formada por um equipamento que tem duas interfaces de rede e funciona como um separador entre as duas redes.
  - Screened host – Formada por um filtro de pacotes e um bastion host. Se o bastion host for comprometido, o invasor já estará dentro da rede interna.
  - Screened subnet – Aumenta a segurança ao adicionar uma DMZ (zona desmilitarizada). O bastion host fica na DMZ, o que evita que um ataque ao bastion host resulte na utilização de um sniffer para a captura de pacotes de usuários internos.
- Arquitetura firewall cooperativo

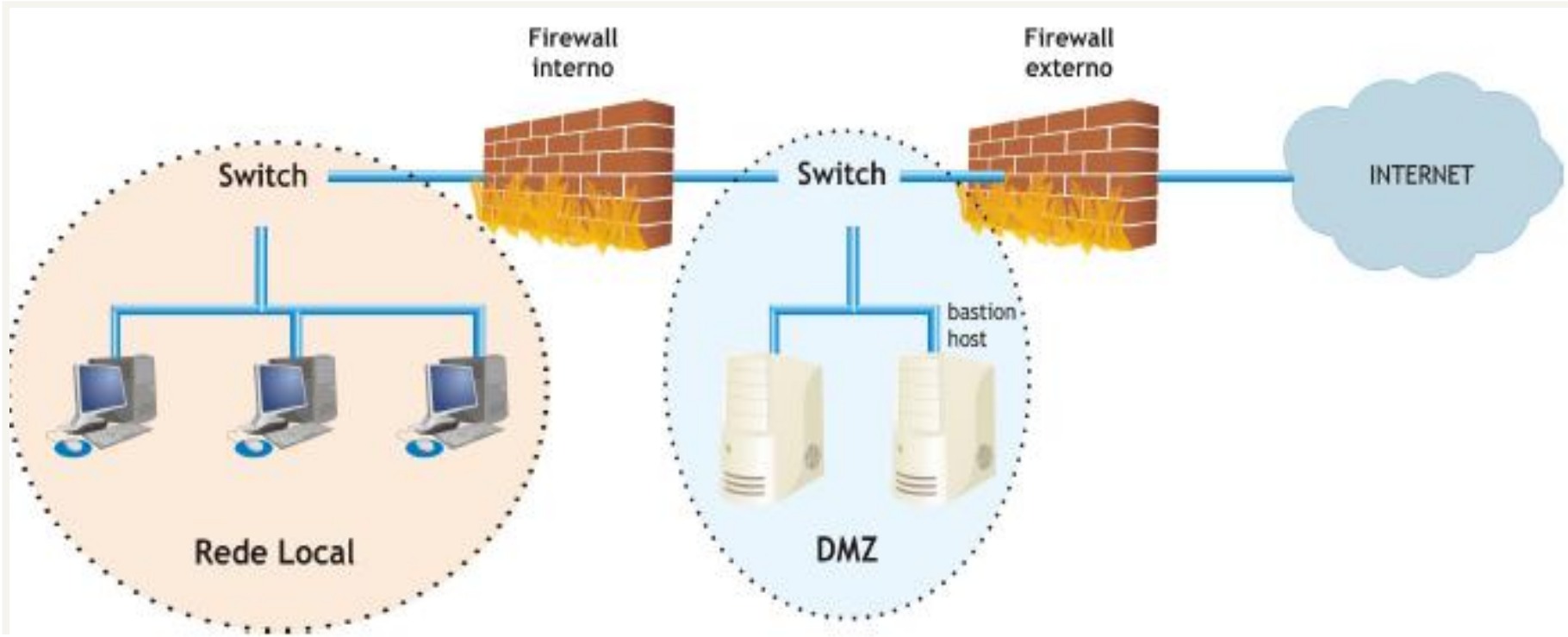
Dual homed-host



Screened host



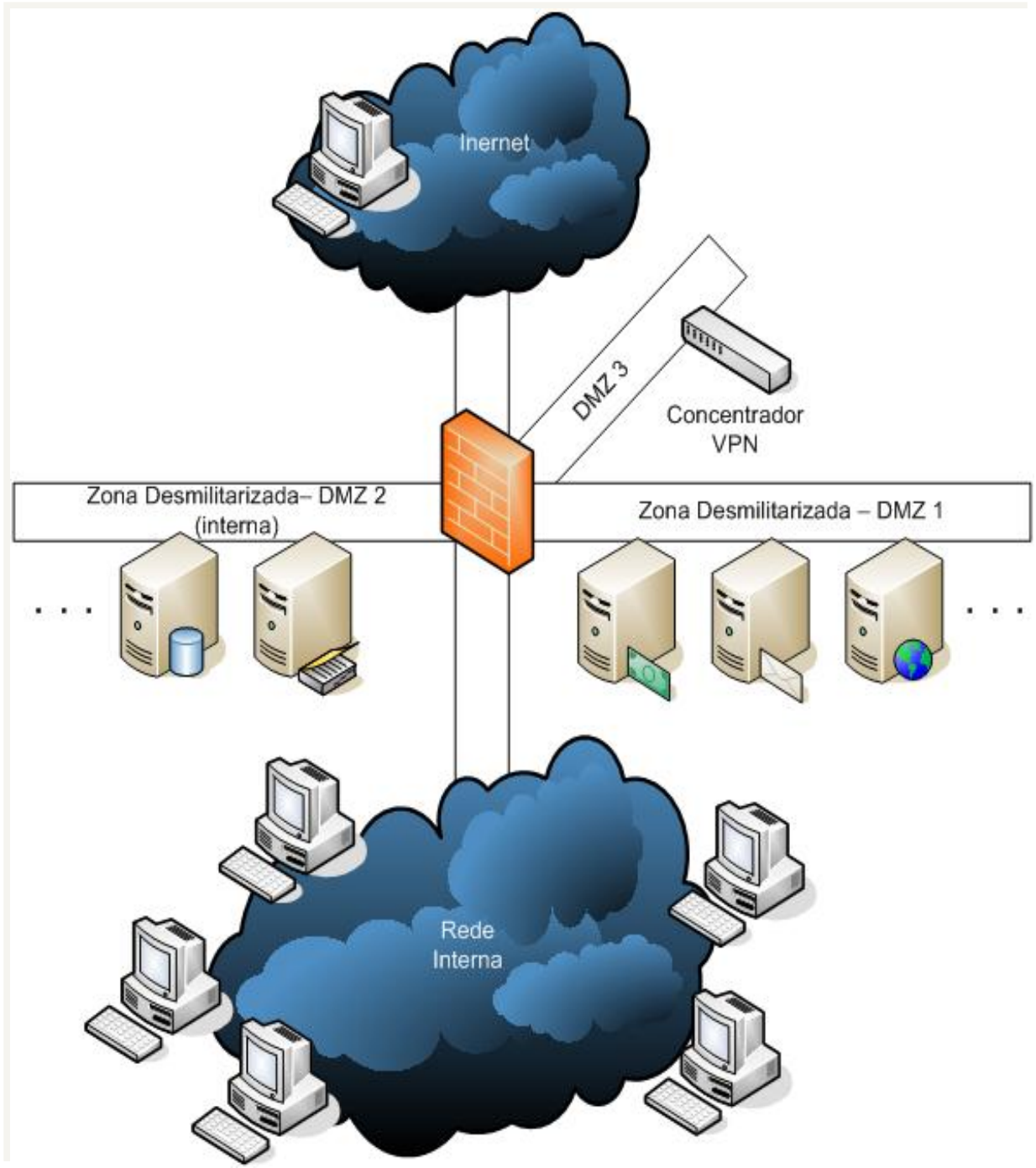
Screened subnet



Firewall cooperativo

- Arquitetura em que são inseridos novos componentes:
  - Redes privadas virtuais – VPNs
  - Sistemas de detecção de intrusão (IDS)
  - Infra-estrutura de chave pública (ICP)
- Usuários internos tratados como usuários externos (não tem acesso direto – sem firewall – a servidores e demais recursos críticos)

Firewall cooperativo



Desempenho de firewall

- Como o firewall é o responsável pela análise de todos os pacotes que passam pelas conexões da rede, deve ter um desempenho satisfatório para que não se torne um gargalo.
- Existem versões que são capazes de operar a 1 Gbps, suportando 500 mil conexões concorrentes e 25 mil túneis VPN.
- Filtros de pacotes baseados em estados tem melhor desempenho que filtros de pacotes, que tem desempenho melhor que proxies.
- Atenção: tente configurar o mínimo de regras de forma a manter o firewall seguro

Mercado

- *Firewall appliances:* produtos fornecidos pré-instalados com o hardware.
- Diversos produtos de acordo com a capacidade de tráfego e número de usuários.
- Não é o produto que vai garantir a segurança, mas sim a política de segurança definida e sua correta implementação.
- Diverso aspectos devem ser analisados na escolha do firewall: fabricante, suporte técnico, projeto, logs, desempenho, gerenciamento, testes, capacitação de pessoal.

Teste do firewall

- Testar o firewall significa verificar se uma política de segurança foi bem desenvolvida, se foi implementada de modo correto e se o firewall realiza aquilo que declara realizar.
- Devem ser feitos por quem? Funcionários, hackers, revendedores, empresas de auditoria
- Diversas etapas:
  - Coleta de informações indiretas e diretas (firewalking)
  - Ataques externos
  - Ataques internos

Problemas do firewall

- Firewall leva à falsa sensação de segurança
- Equívocos cometidos nas organizações:
  - Liberar novos serviços porque os usuários dizem que precisam deles
  - Separar a VPN do firewall
  - Concentrar os esforços no firewall, enquanto outras medidas de segurança são ignoradas
  - Ignorar os arquivos de logs
  - Permitir que diversas pessoas administrem o firewall
  - Presença de modems
  - Não ter uma política de segurança

NAT: Network Address Translation

- RFC 2663
  - IP Network Address Translator (NAT) Terminology and Considerations
- NAT é um método pelo qual endereços IP são mapeados de um domínio de endereçamento para outro
- Tradicionalmente, dispositivos NAT são usados para conectar uma rede privada que usada endereços não registrados com a Internet global, onde os endereços são únicos e registrados

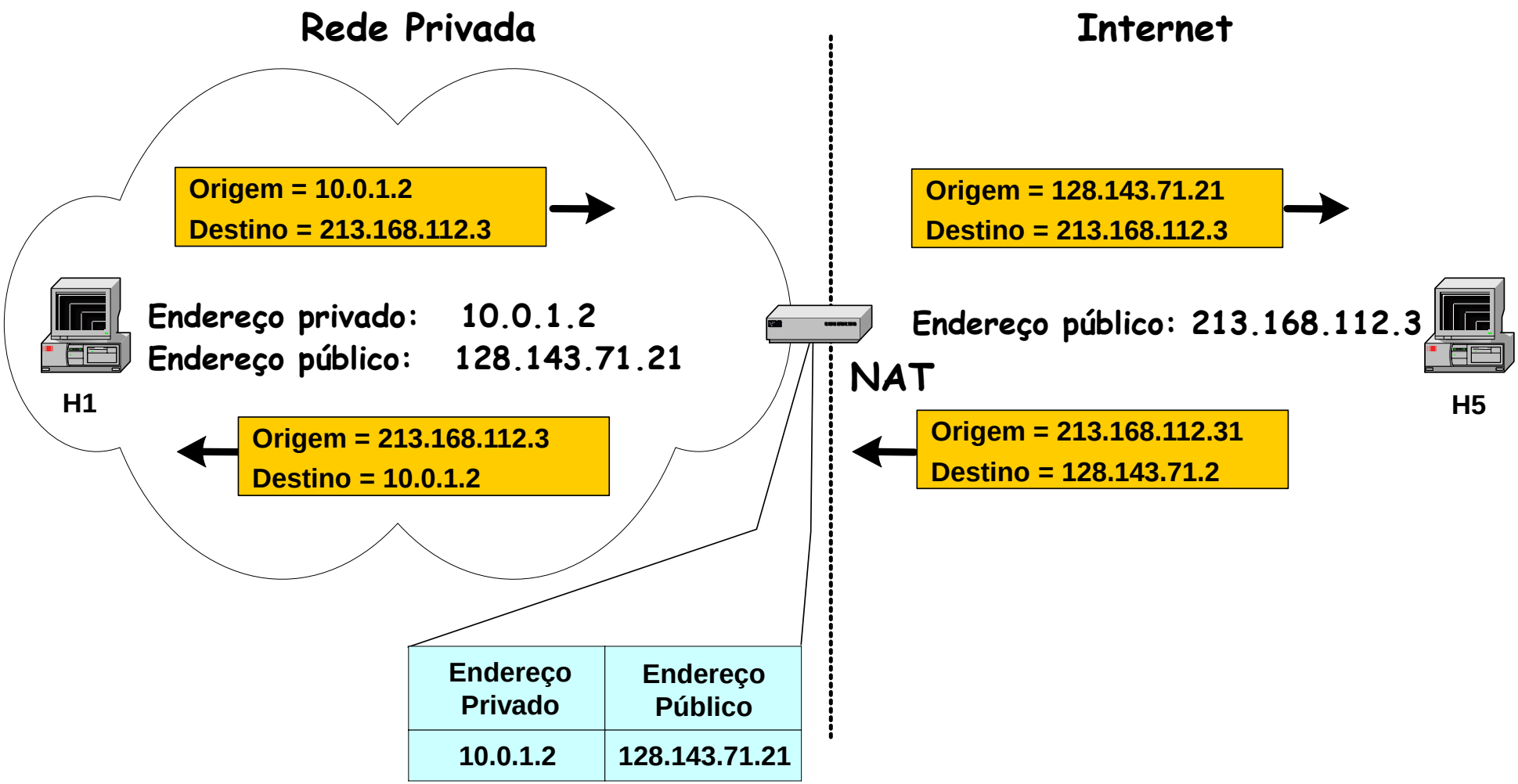
Categorias de NAT

- Tradicional, outbound, unidirecional
  - Básico (ou somente NAT)
    - Realiza apenas tradução de endereços
    - Geralmente utilizado para mapear endereços locais privados para um pool de endereços públicos
  - NAPT (Network Addresss and Port Translation)
    - Realiza o Nat básico e substitui a porta fonte do host por uma porta do dispositivo que realiza o NAT
    - Usado para mapear vários endereços privados para único endereço público

Categorias de NAT

- Bidirecional
  - Realiza Nat para tráfego inbound e outbound
  - Existe um mapeamento de um para um
  - Endereço público é um alias para endereço privado
- NAT Duplo
  - Realiza NAT nas duas direções, mas tanto o endereço fonte quanto o destino são alterados nas duas direções

NAT


Rede Privada
Internet
Origem = 10.0.1.2
Destino = 213.168.112.3
Origem = 128.143.71.21
Destino = 213.168.112.3
Endereço privado: 10.0.1.2
Endereço público: 128.143.71.21
Endereço público: 213.168.112.3
H1
NAT
H5
Origem = 213.168.112.3
Destino = 10.0.1.2
Origem = 213.168.112.31
Destino = 128.143.71.2
Endereço Privado
Endereço Público
10.0.1.2
128.143.71.21

Netfilter e Iptables

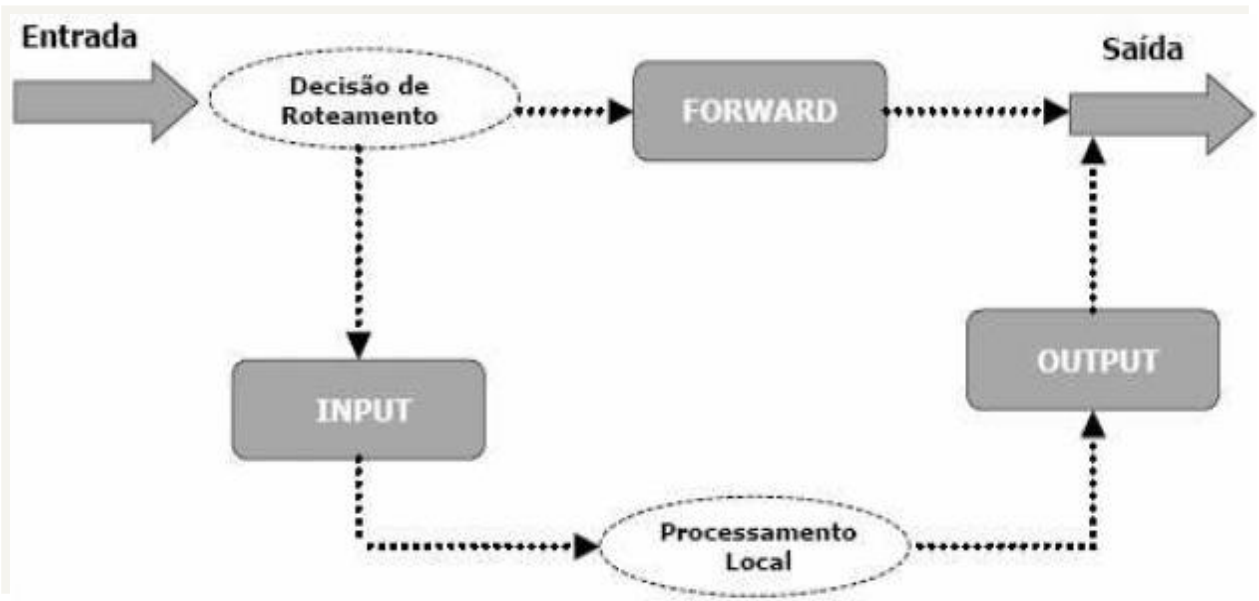
Iptables/Netfilter

- O projeto netfilter/iptables é um subsistema de firewalling para o kernel Linux 2.4 e superiores. Com o uso desta ferramenta pode-se definir regras especiais para entrada, saída e passagem de pacotes entre interfaces, podendo atuar antes ou após as ações referentes ao roteamento.

- O iptables atua sobre as tabelas presentes no Kernel, que indicam situações de roteamento, de acordo com a situação em que se encontra o pacote, a qual é referida por uma corrente de regras, ou **chain**.

Tabelas do iptables

- **filter**: é a tabela padrão, sobre a qual podemos nos referir a três correntes de regras, ou *chains*:
  - *INPUT*, pacotes que entram na interface;
  - *OUTPUT*, pacotes que saem da interface
  - *FORWARD*, tudo o que chega ao host mas deve ser redirecionado a um host secundário ou outra interface de rede



Tabelas do iptables

- **nat**: esta tabela se refere ao uso do recurso de *Network Address Translation* ou NAT, na qual podemos nos referir aos *chains*:
  - *PREROUTING*, pacotes que serão alterados antes de roteamento;
  - *OUTPUT*, pacotes locais que serão alterados antes do roteamento;
  - *POSTROUTING*, pacotes que serão alterados após a aplicação das regras de roteamento.
- **mangle**: usada para alterações especiais no pacote,
  - *PREROUTING*, para alteração antes do roteamento
  - *OUTPUT*, pacotes locais que serão alterados antes do roteamento.

Comandos do iptables

- [comando] : manipula a tabela através das regras e chains correspondentes.
  - -A anexa a regra ao fim da lista já existente.
  - -D apaga a regra especificada.
  - -L lista as regras existentes na lista.
  - -P altera a política padrão das chains.
  - -F remove todas as regras, ou remove todas as regras referentes a um determinado chain.
  - -I insere uma nova regra, mas no início da lista de regras.
  - -R substitui uma regra já adicionada por outra.
  - -N permite inserir uma nova chain na tabela especificada.
  - -E Renomeia uma nova chain criada.
  - -X apaga uma chain criada pelo administrador do firewall.

Ações no iptables

- -p: especifica o protocolo aplicado a regra (tcp, udp, icmp, etc)
- -i : especifica a interface de entrada a ser utilizada (eth0, eth+, ppp0, lo (loopback), etc)
- -o: especifica a interface de saída a ser utilizada
- -s: origem do pacote ao qual a regra deve ser aplicada
  - Ex: -s 10.0.10.0/255.255.255.0
- -d: especifica o destino do pacote ao qual a regra deve ser aplicada
- -j: define o alvo do pacote caso se encaixe em uma regra (ACCEPT, DROP, etc)
- --sport: define porta de origem (usado com tcp e udp)
- --dport: porta de destino Ex: -p tcp --dport 25
- !: significa exclusão – usado quando se deseja aplicar exclusão a uma regra Ex: -p ! icmp

Alvos - iptables

- Quando um pacote se adequa a uma regra ele deve ser direcionado a um alvo:
  - ACCEPT significa deixar o pacote passar.
  - DROP significa descartar o pacote.
  - QUEUE significa passar o pacote para um programa usuário administrar o fluxo atribuído ao mesmo.
  - RETURN significa parar de atravessar esta chain e continuar na próxima regra na chain anterior (a chain que chamou esta).
  - LOG liga o logging do kernel.
  - REJECT envia como resposta um pacote de erro e descarta o pacote.
  - SNAT altera o endereço de origem de pacote e é usado somente na chain POSTROUTING.
  - DNAT altera o endereço de destino do pacote e é usado nas chains PREROUTING e OUTPUT

Exemplos

- Listar regras da tabela NAT

  iptables –t nat -L
- Configurar o alvo padrão da chain INPUT da tabela filter como DROP

  iptables –P INPUT DROP
- Liberar tráfego de entrada da interface de loopback

  iptables –A INPUT –i lo –j ACCEPT
- Liberar pacotes do site www.suaempresa.com.br para entrar na rede interna (10.0.30.0)

  iptables –A FORWARD –s www.suaempresa.com.br –d 10.0.30.0 –j ACCEPT
- Descartar pacotes que entram por qualquer interface de rede exceto da eth0

  iptables –A FORWARD –i ! eth0 –j DROP

Exemplos

- Descartar pacotes destinados à porta 80 do host firewall

  iptables –A INPUT-p tcp --dport 80 –j DROP
- Arquivar em log pacotes destinado a porta 25 do host

  iptables –A INPUT –p tcp --dport 25 – j LOG
- Mascaramento IP: Faz com que qualquer pacote que saia da rede local (pela interface eth2) para outra rede tenha seu endereço de origem alterado para 192.168.0.33

  iptables –t nat –A POSTROUTING –o eth2 –j SNAT –to 192.168.0.33
- Inserir/criar nova chain na tabela filter

  iptables –t filter –N internet

Tabela NAT

- SNAT
  - Source NAT – quando o endereço fonte do pacote é alterado.
  - É sempre realizado no ponto POSTROUTING
  - Masquerade é um SNAT especializado
  - iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4:80
- DNAT
  - Destination NAT – quando o endereço destino do pacote é alterado
  - É sempre realizado nos pontos OUT e PREROUTING
  - Port Forwarding, balanceamento de carga e proxy transparente são formas de DNAT
  - iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 5.6.7.8:80
  - iptables -t nat -A OUTPUT -o eth0 -j DNAT --to 5.6.7.8:80

Tabela Mangle

- Utilizada para alterações especiais como modificar o **tipo de serviço** (ToS) de um pacote.
- Permite dizer ao firewall que qualquer pacote cujo “tipo de serviço” seja, por exemplo, SSH, deve possuir uma prioridade de tráfego “x”, e que outros pacotes cujo “tipo de serviço” seja, por exemplo, MSN, deve possuir prioridade “y”.
- Ao invés de criar **regras de bloqueio** de tráfego via filtragem de pacotes ou **controle de palavras chave via Proxy**, o TOS propicia o controle do tráfego, simplesmente, **definindo prioridades para os serviços**.

Tabela Mangle - exemplo

- Aplicar prioridade máxima para tráfego de saída na interface eth0 em pacotes do protocolo SSH (porta 22):

  iptables –t mangle –A OUTPUT –o eth0 –p tcp --dport 22 –j TOS –set-tos 16

BIT TOS	AJUSTE DO BIT
Espera Mínima (Minimize-Delay)	16 ou 0x10
Máximo Processamento (Maximize-Throughput)	8 ou 0x08
Máxima Confiança (Maximize-Reliability)	4 ou 0x04
Custo mínimo (Minimize-Cost)	2 ou 0x02
Prioridade Normal (Normal-Service)	0 ou 0x00

Módulos – iptables

MÓDULO (-m)	DESCRIÇÃO
limit	Limita o número de vezes que uma regra será executada antes de passar para a próxima regra
state	Observa o estado da Conexão. Estes podem ser (NEW, ESTABLISHED, RELATED e INVALID)
mac	Permite que o Iptables trabalhe com endereçamentos Mac
multiport	Permite que sejam especificadas até 15 portas a uma regra de uma só vez
string	Observa o conteúdo do pacote para somente então aplicar a regra
owner	Observa o usuário que criou o pacote

Exemplos

- limit

  -m limit –limit 1/s –j ACCEPT (intervalos de tempo: s, m, h, d)

- state

  NEW - Confere com pacotes que criam novas conexões

  ESTABLISHED - Confere com conexões já estabelecidas

  RELATED - Confere com pacotes relacionados indiretamente a uma conexão, como mensagens de erro icmp, etc.

  INVALID - Confere com pacotes que não puderam ser identificados por algum motivo. Como respostas de conexões desconhecidas.

Ex: *iptables –A INPUT –m state –state INVALID –i eth0 – j DROP*

Exemplos

- Bloquear a entrada de pacotes que contenham a palavra “torrent”

  iptables –A INPUT –m string --string “torrent” –j DROP

- Autorizar os usuários do grupo de ID 50 a acessar o site www.proibido.com.br e negar o acesso aos demais usuários:

  iptables –A OUTPUT –m owner --gid-owner 50 –d www.proibido.com.br –j ACCEPT

  iptables – A OUTPUT –d www.proibido.com.br –j DROP