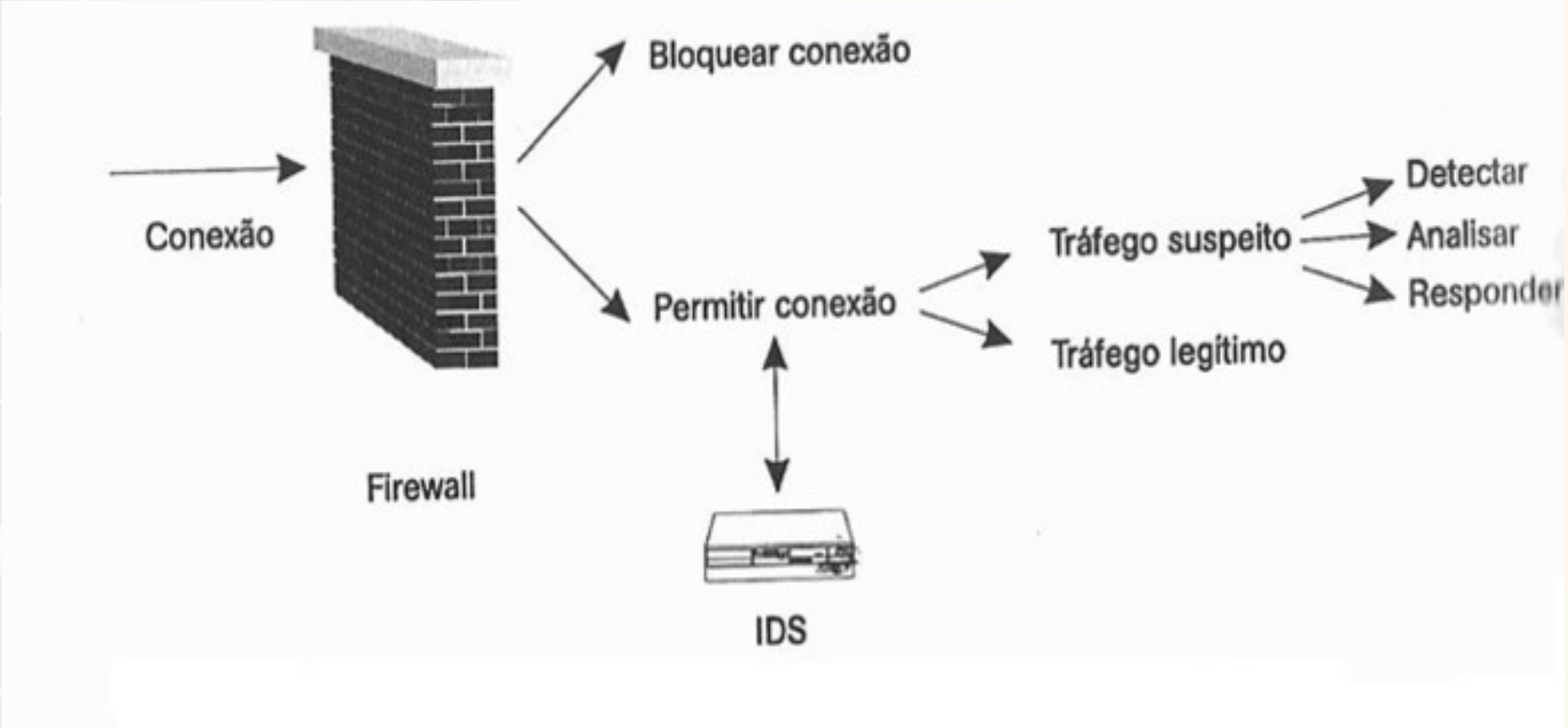
Contramedidas

- Sistemas de Detecção/Prevenção de Intrusão (IDS/IPS - Intrusion Detection/Prevention System)



Introdução

Firewall

- 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

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

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

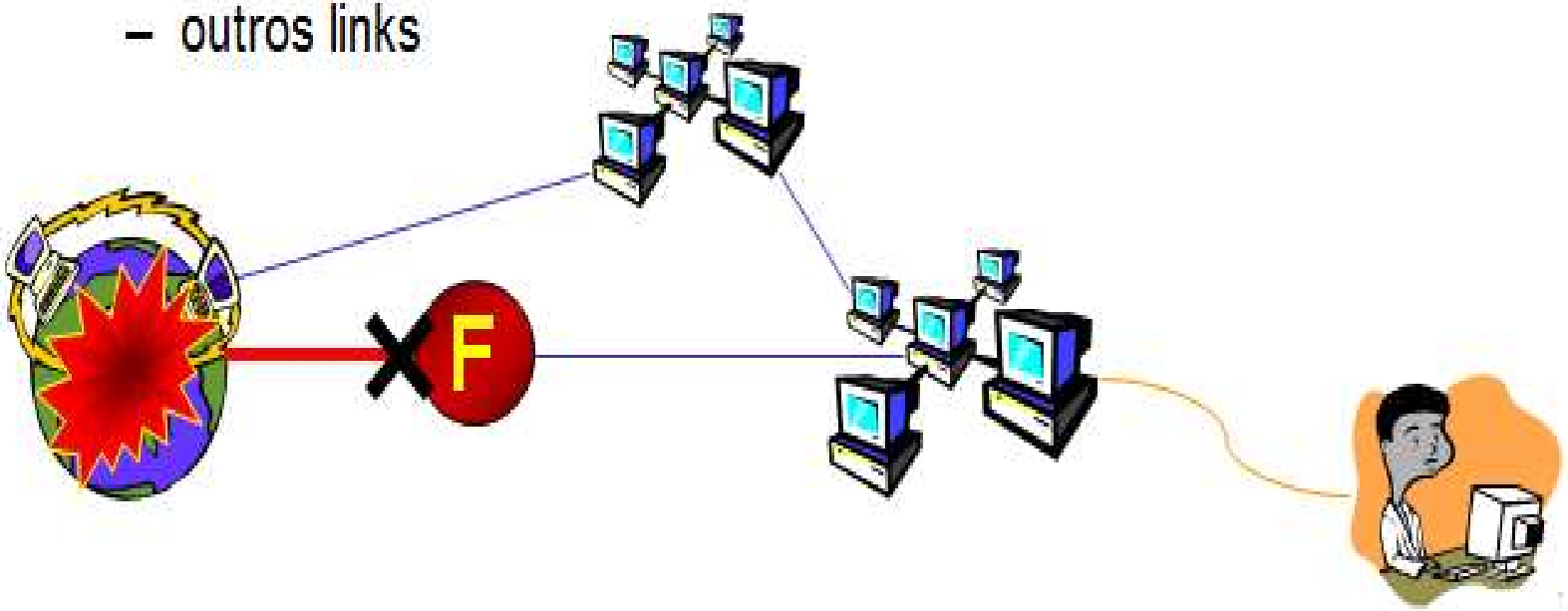
O que um Firewall pode fazer?

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Problemas com Firewall

- 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)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Objetos tratados pelo Firewall

- A unidade básica e essencial é o PACOTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Objetos tratados pelo Firewall

- Conceito de Porta
  - Tratando-se de *firewall*, porta se diz respeito a um mecanismo de entrada/saída que um determinado protocolo use para se comunicar com outro computador na rede
  - A comunicação de dois ou mais computadores pela rede se dá através dos protocolos de comunicação, o qual cada um deles, possui sua porta de comunicação específica de uso.
  - O *firewall* é o dispositivo que controla essas portas, se estão disponíveis (abertas) ou indisponíveis (fechadas) para um determinado protocolo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

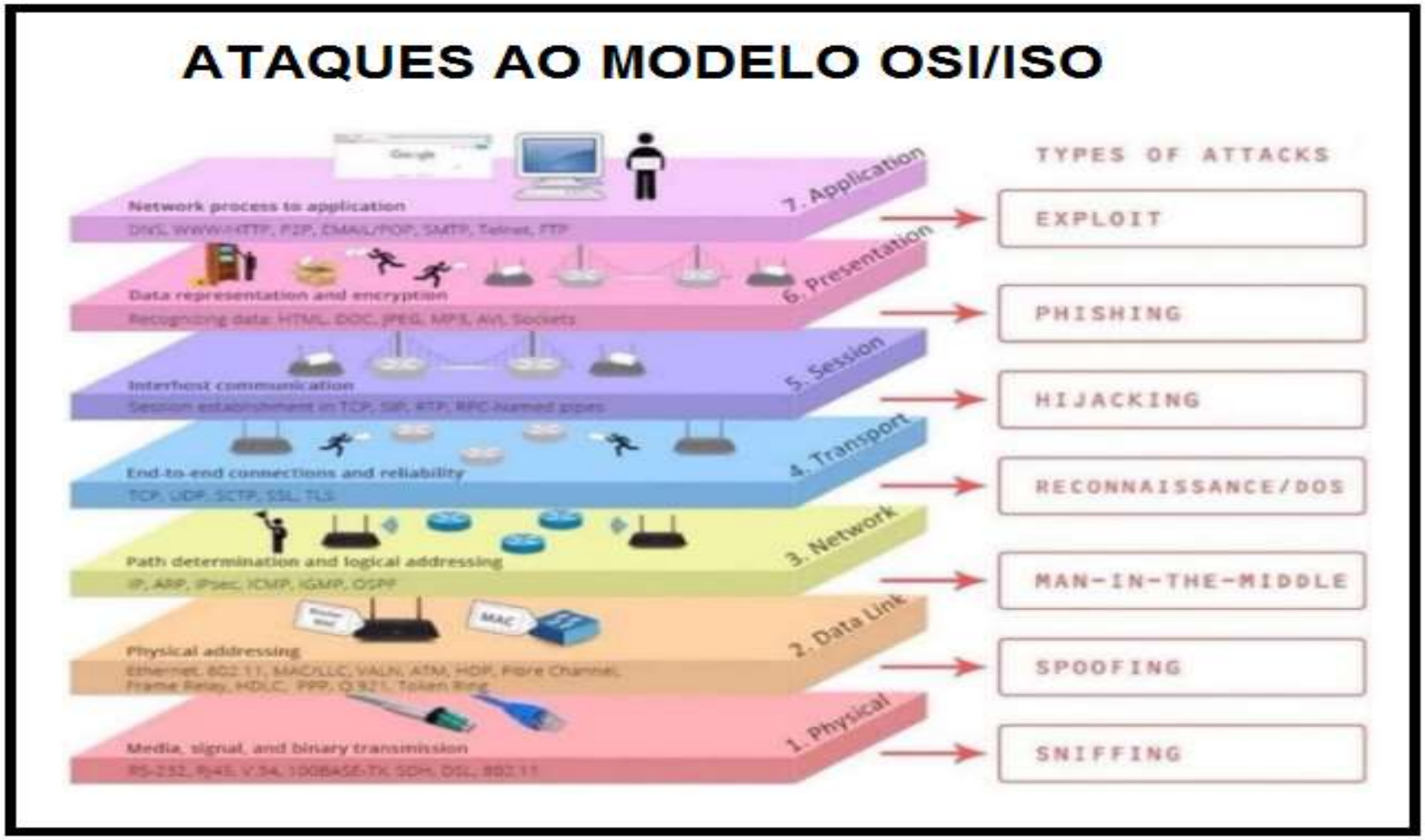
Objetos tratados pelo Firewall

Principais Portas/Protocolos

Serviço	TCP	UDP	Observações
FTP	21	21	Transferência de arquivos
SSH	22	22	Protocolo de login remoto encriptado
Telnet	23	23	Protocolo de login remoto
SMTP	25	25	Para envio de email
DNS	53	53	Resolução de nomes para IP
HTTP	80	80	Para web browser
POP3	110	110	Para recepção de email
IMAP	143	143	Para recepção/envio de email
TLS/SSL	443	443	Protocolo de camada de sockets segura
IRC	6667	6667	Para conversação/chat
Pichat	9009	9009	Protocolo de conversação/chat

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

ATAQUES E AS CAMADAS TCP/IP



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

TIPOS DE FIREWALLS

Firewalls de rede: Também conhecidos como firewalls de perímetro, são dispositivos físicos ou virtuais colocados entre a rede interna e a Internet. Eles filtram o tráfego com base em regras definidas para permitir ou bloquear o acesso a determinados serviços, portas e endereços IP.

Firewalls de aplicativos: Também chamados de firewalls de camada de aplicativo ou firewalls de aplicativos da web, são projetados para proteger aplicativos específicos, como servidores da web, contra ataques direcionados. Eles monitoram o tráfego de aplicativos em busca de atividades suspeitas ou maliciosas e aplicam políticas de segurança personalizadas.

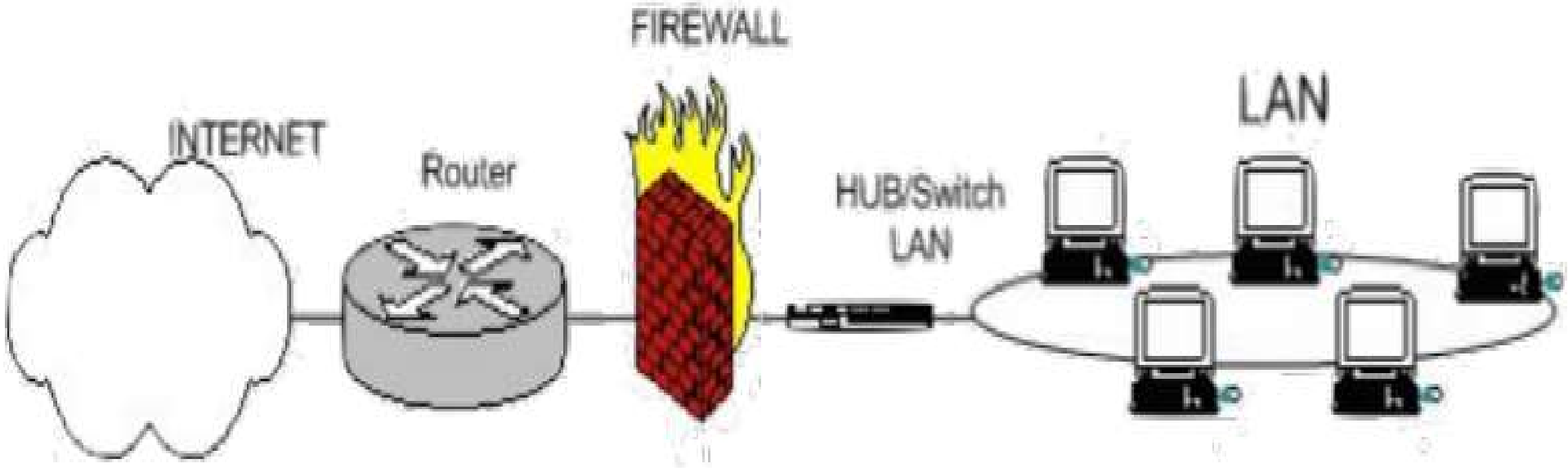
Firewalls de host: Esses firewalls são executados em um dispositivo individual, como um computador ou um servidor, e controlam o tráfego de rede para e do dispositivo específico. Eles permitem definir regras de filtragem de pacotes com base em endereços IP, portas e protocolos.

Firewalls de próxima geração (NGFW): Esses firewalls combinam as funcionalidades dos firewalls de rede tradicionais com recursos avançados de inspeção de pacotes em nível de aplicativo. Eles podem incluir recursos de prevenção de intrusões (IPS), filtragem de

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Firewalls

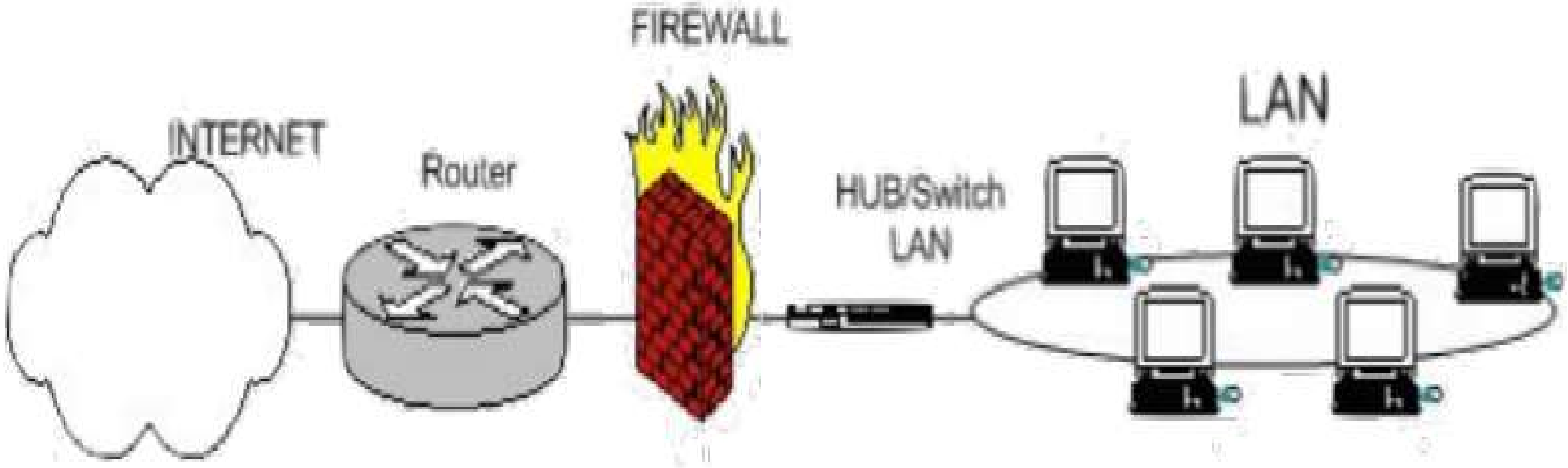
- **Topologia**



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Firewalls

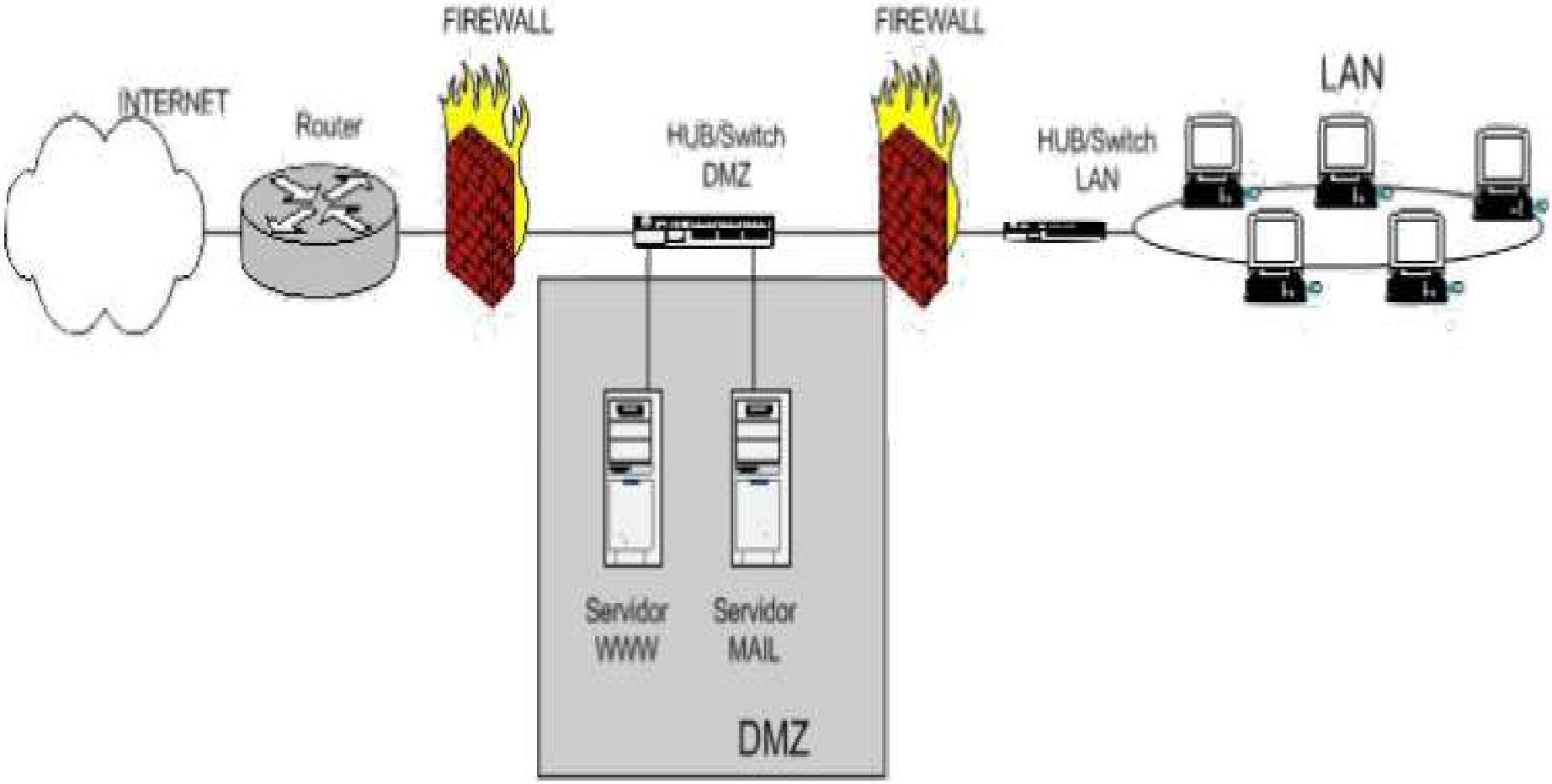
- **Topologia**



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Firewalls

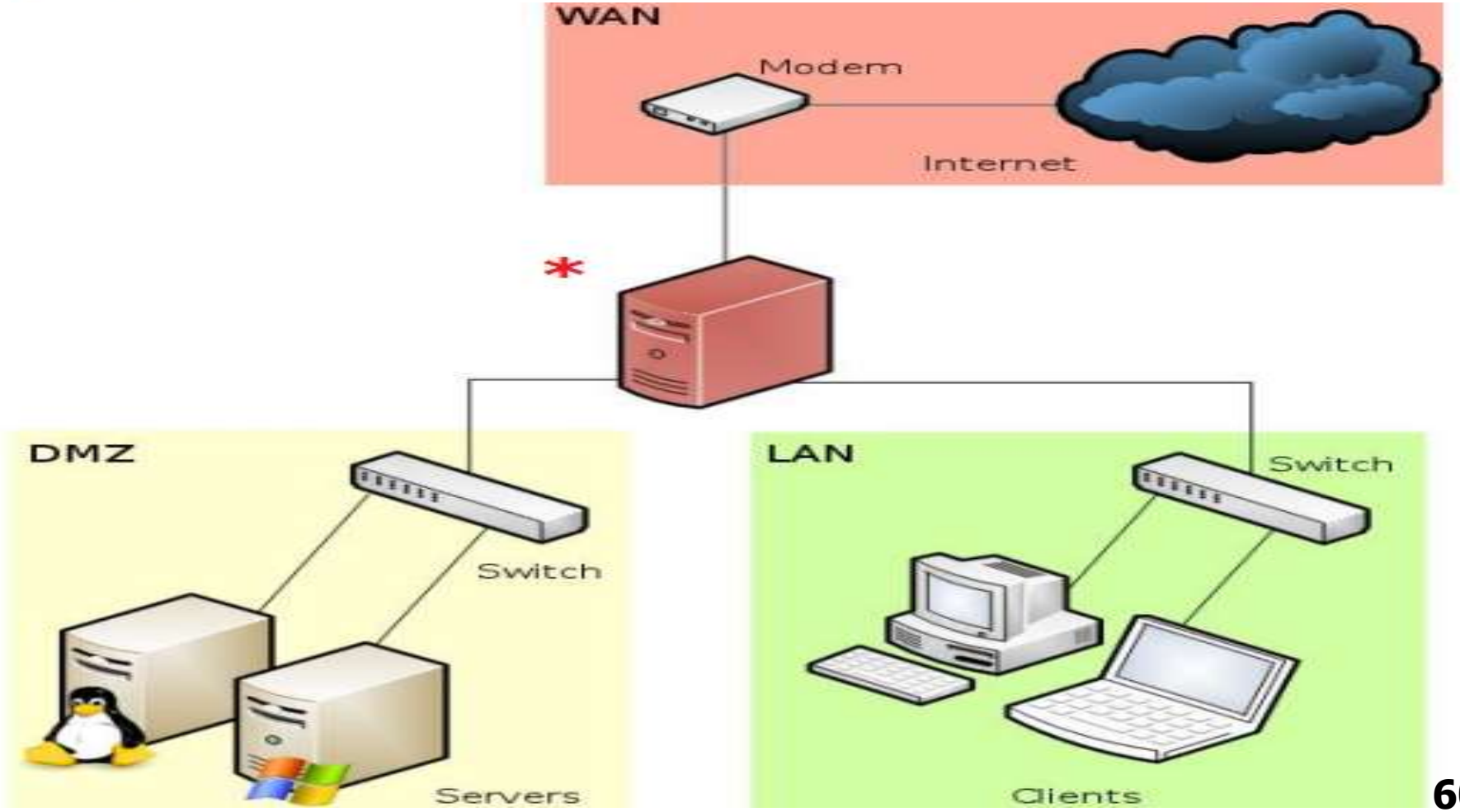
- **Topologia**



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Firewalls

- Topologia



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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...

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

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

NAT - Network Address Translations

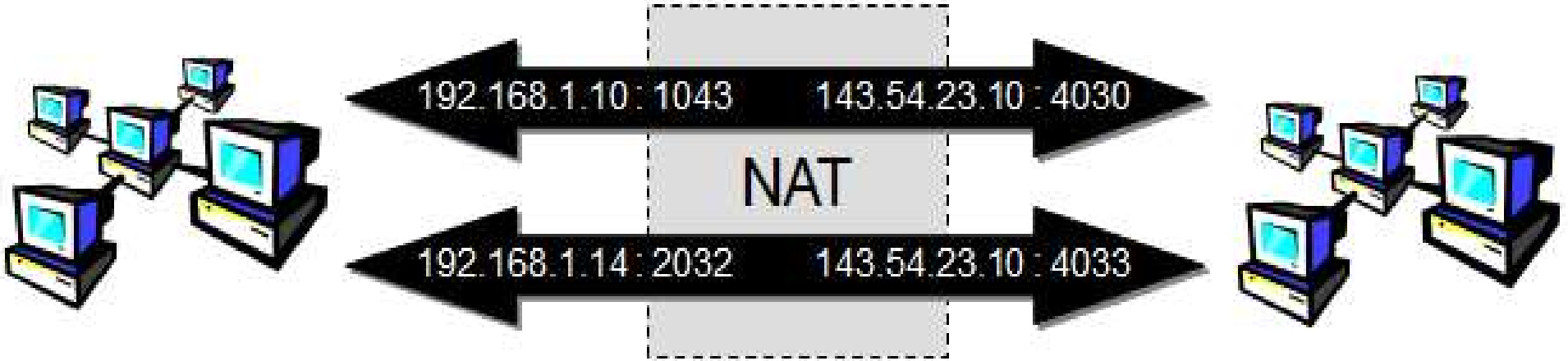
- Endereços externamente visíveis
  - são endereços válidos na Internet
  - NÃO podem ser utilizados sem que sejam devidamente reservados (Registro.br)

- 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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

NAT - Network Address Translations

- Operação
  - altera dados do pacote
    - normalmente endereço e porta de origem (Source NAT)
    - e endereço e porta de destino (para os pacotes que retornam)



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Tipos de Firewall

FIREWALLS DE REDE: Também conhecidos como firewalls de perímetro, são dispositivos físicos ou virtuais colocados entre a rede interna e a Internet. Eles filtram o tráfego com base em regras definidas para permitir ou bloquear o acesso a determinados serviços, portas e endereços IP.

FIREWALLS DE APLICATIVOS: Também chamados de firewalls de camada de aplicativo ou firewalls de aplicativos da web, são projetados para proteger aplicativos específicos, como servidores da web, contra ataques direcionados. Eles monitoram o tráfego de aplicativos em busca de atividades suspeitas ou maliciosas e aplicam políticas de segurança personalizadas.

FIREWALLS DE HOST: Esses firewalls são executados em um dispositivo individual, como um computador ou um servidor, e controlam o tráfego de rede para e do dispositivo específico. Eles permitem definir regras de filtragem de pacotes com base em endereços IP, portas e protocolos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Tipos de Firewall

FIREWALLS DE PRÓXIMA GERAÇÃO (NGFW): Esses firewalls combinam as funcionalidades dos firewalls de rede tradicionais com recursos avançados de inspeção de pacotes em nível de aplicativo. Eles podem incluir recursos de prevenção de intrusões (IPS), filtragem de conteúdo, detecção de malware e análise comportamental para fornecer uma camada adicional de segurança.

FIREWALLS DE NUVEM: Projetados para ambientes em nuvem, esses firewalls são fornecidos como serviços e são altamente escaláveis. Eles protegem as instâncias de nuvem, redes virtuais e recursos em nuvem, permitindo a definição de políticas de segurança granulares.

FIREWALLS DE SOFTWARE: São programas de software instalados em um dispositivo para fornecer proteção contra ameaças de rede. Eles podem ser instalados em computadores pessoais ou servidores e oferecem recursos de filtragem de pacotes e inspeção de tráfego.

FIREWALLS BASEADOS EM CONTÊINERES: Projetados especificamente para ambientes de contêiner, esses firewalls fornecem proteção entre os contêineres e também contra ameaças de rede externas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

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

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

Filtragem de Pacotes

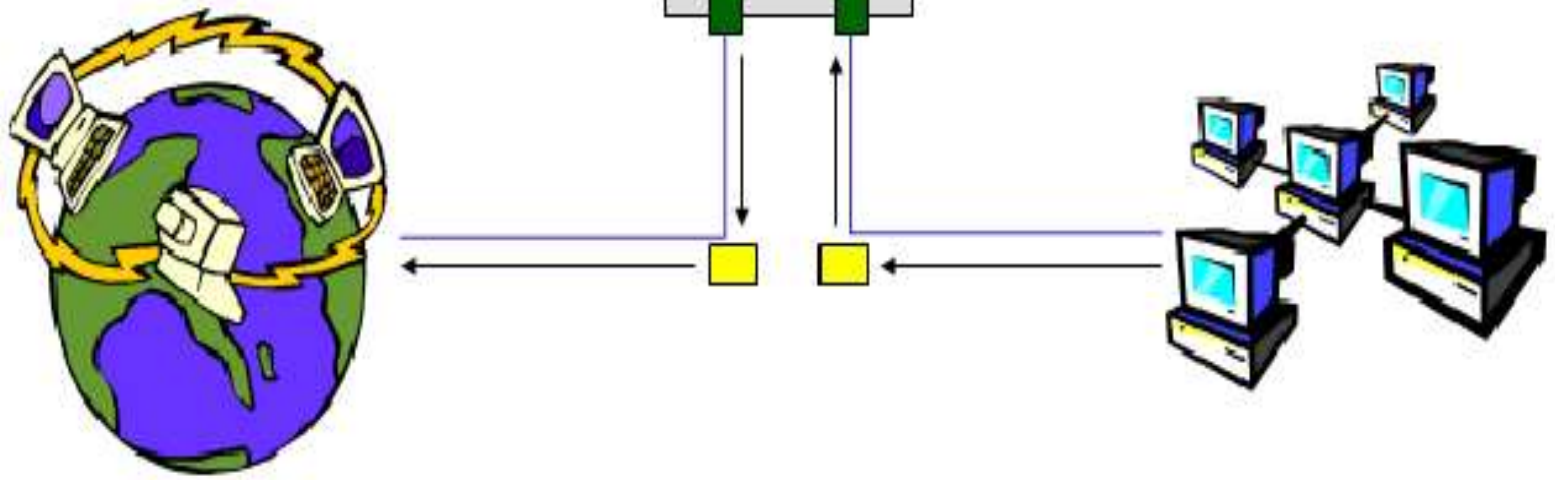
- Ao final do conjunto de regras será aplicada uma ação (política) padrão: descartar ou encaminhar
  - Em Firewalls cuja **política padrão é descartar** as regras devem ser de liberação, pois tudo que não for permitido estará proibido.
  - Em Firewalls cuja **política padrão é encaminhar** as regras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

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.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Filtragem de Pacotes

Regra	End. Origem	Porta Origem	End. Destino	Porta Destino	Ação
1	Qualquer endereço da rede interna	> 1023	Qualquer endereço	80	Permitir
2	Qualquer endereço	80	Qualquer endereço da rede interna	> 1023	Permitir
3	Qualquer endereço	Qualquer porta	Qualquer endereço	Qualquer porta	Negar

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

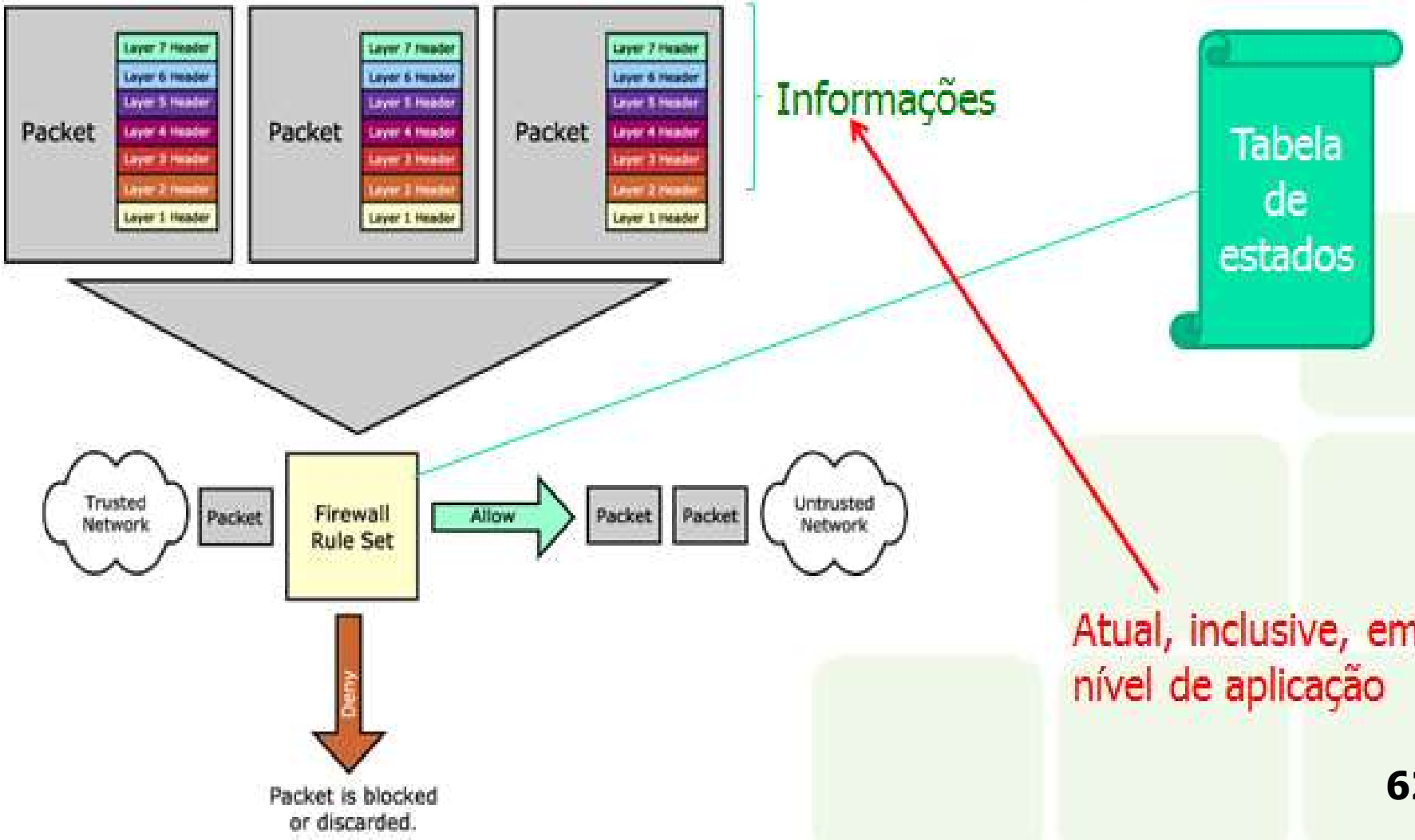
Filtragem de Pacotes

Filtro de pacotes baseado em estados - Funcionamento

- 1) Cliente inicia uma conexão;
- 2) O pacote inicial é checado da mesma forma que um filtro de pacotes;
- 3) Se o pacote não passar pelas regras do filtro de pacotes, ele é descartado;
- 4) Caso o pacote seja aceito, a sessão é inserida na tabela de estados do *firewall;*
- 5) Para os demais pacotes, se a sessão estiver na tabela e o pacote fizer parte dessa sessão, ele será aceito;
- 6) Se os pacotes não fizerem parte de nenhuma sessão presente na tabela de estados, eles serão descartados.

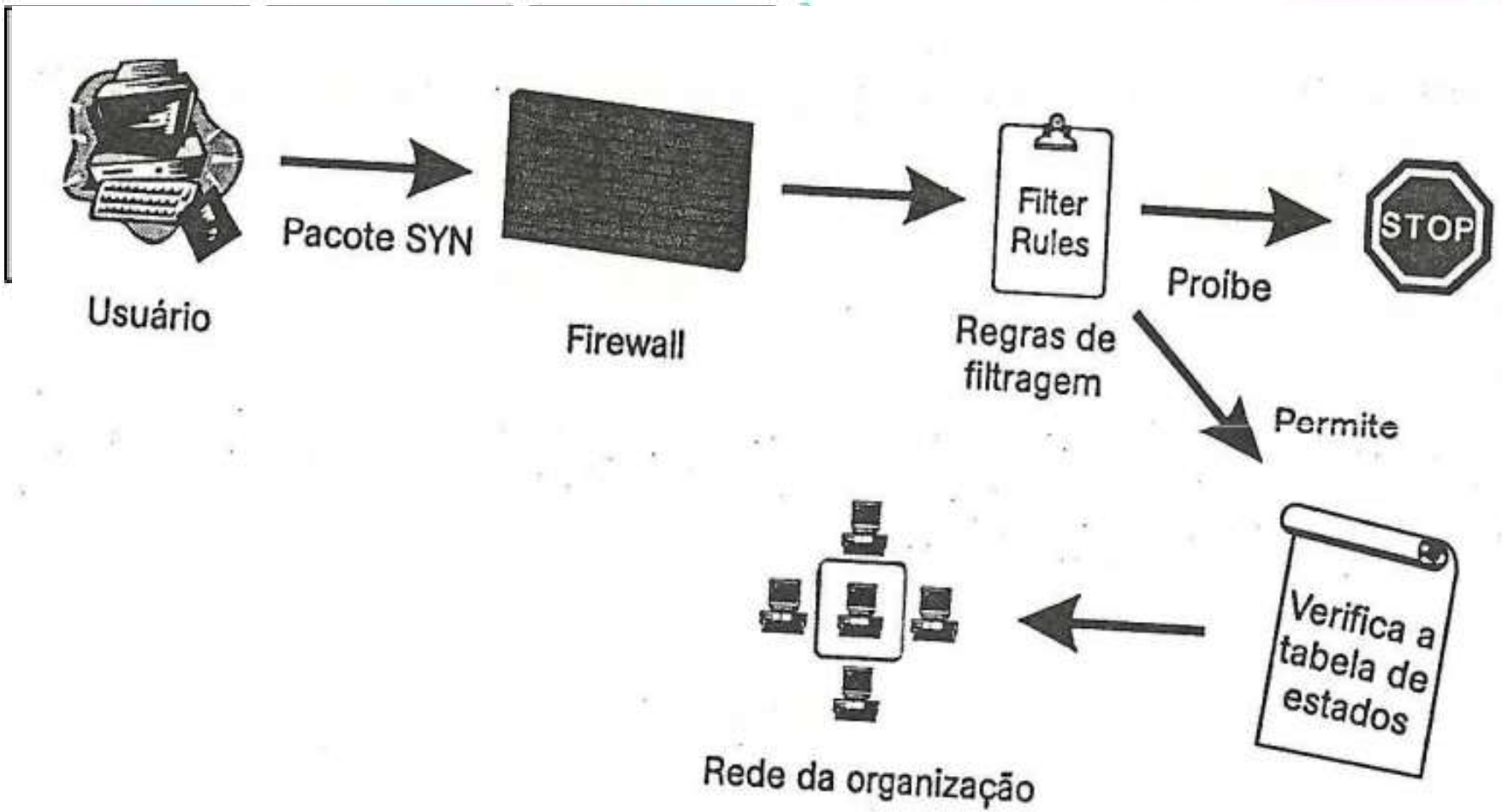
Filtragem de Pacotes

- Filtragem de pacotes com Estados



Filtragem de Pacotes

- Filtragem de pacotes com Estados



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Filtragem de Pacotes

- Filtragem de pacotes com Estados

Filtro de pacotes baseado em estados **Avaliação**

- O desempenho do sistema melhora, pois apenas os pacotes SYN são comparados com a tabela de regras do filtro de pacotes;
- Pacotes restantes são comparados com a tabela de estados;
- O conjunto de regras na tabela do filtro de pacotes é menor, pois leva em conta somente os inícios das conexões;
- O conjunto de regras fica mais enxuto e, consequentemente mais fácil de administrar.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Filtragem de Pacotes

Filtragem de pacotes com Estados

Prós dos firewalls com estado

- Os firewalls com estado podem detectar quando dados ilícitos estão sendo usados para se infiltrar na rede.
- Um firewall de inspeção com estado também tem a capacidade de registrar e armazenar aspectos importantes das conexões de rede.
- Os firewalls com estado não precisam que muitas portas estejam abertas para facilitar a comunicação tranquila.
- Um firewall de rede com estado pode registrar o comportamento dos ataques e, em seguida, usar essas informações para evitar tentativas futuras. Essa é uma das maiores vantagens do firewall com estado vs. sem estado.
- Um firewall com estado aprende enquanto opera, o que permite que ele tome decisões de proteção com base no que aconteceu no passado. Isso o torna uma solução de firewall de gerenciamento unificado de ameaças (UTM) potencialmente poderosa, que é um único dispositivo que executa várias funções de segurança.

Fonte: https://www.fortinet.com/br/resources/cyberglossary/stateful-vs-stateless-firewall

Filtragem de Pacotes

Filtragem de pacotes com Estados

Contras dos firewalls com estado

- A menos que um firewall com estado tenha as atualizações de software mais recentes, as vulnerabilidades podem permitir que ele seja comprometido por um hacker e, em seguida, controlado.
- No caso de alguns firewalls com estado, eles podem ser enganados para permitir uma conexão prejudicial à rede.
- Os firewalls com estado podem ser mais suscetíveis a ataques “man-in-the-middle” (MITM), que envolvem um invasor interceptando uma comunicação entre duas pessoas para espionar o tráfego ou fazer alterações nele.

Fonte: https://www.fortinet.com/br/resources/cyberglossary/stateful-vs-stateless-firewall

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Filtragem de Pacotes : Avaliação

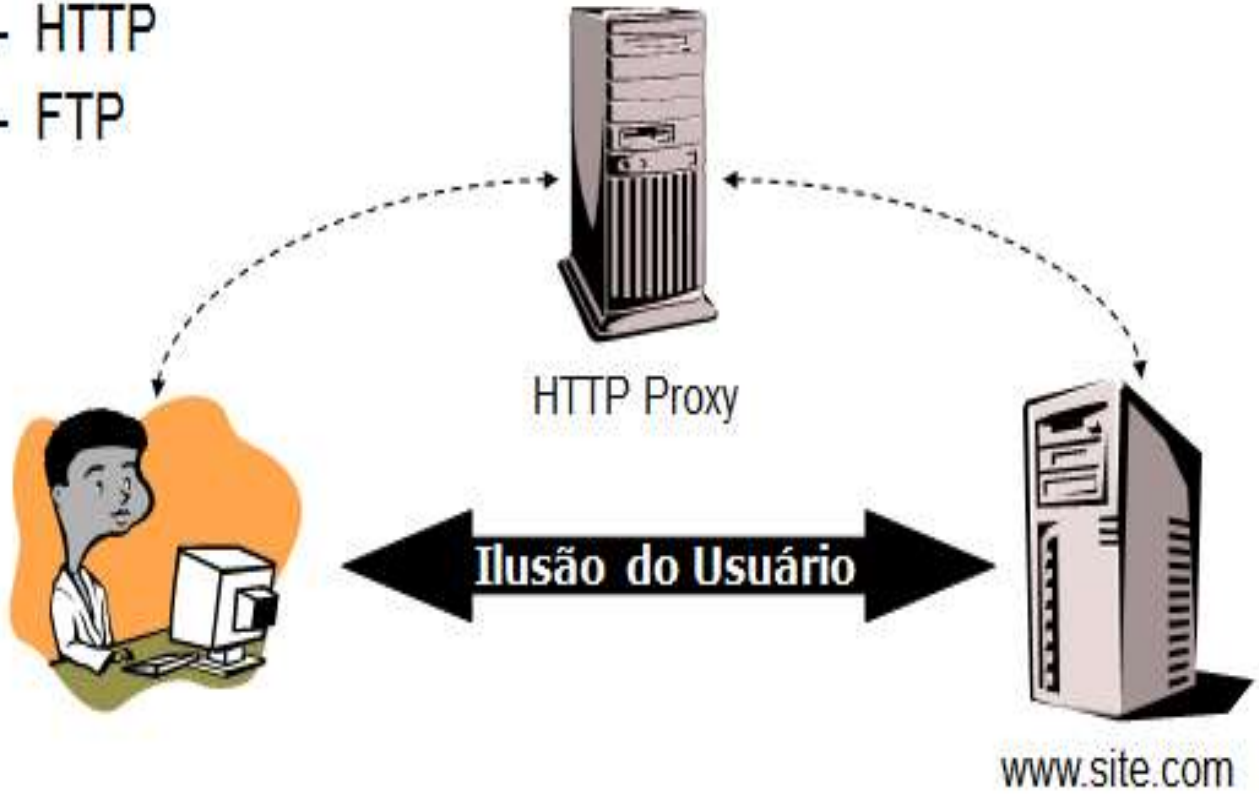
- Vantagens
  - um roteador com filtragem pode proteger toda uma rede
  - é extremamente eficiente, principalmente *stateless*
  - é largamente disponível, pode ser encontrado em roteadores, embutido em SOs, softwares específicos, ...

- 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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Proxy - Firewall da camada Aplicação

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



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

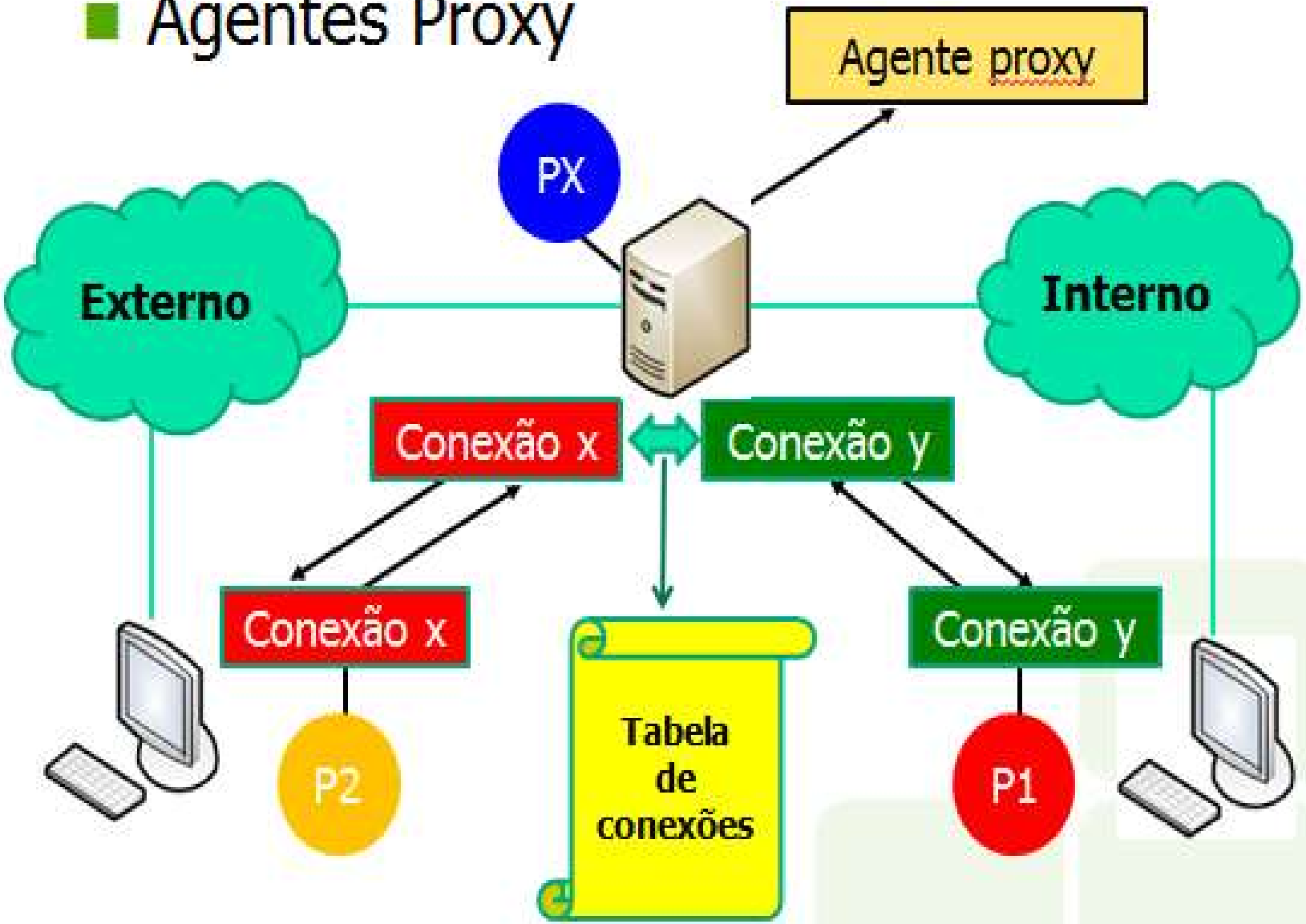
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

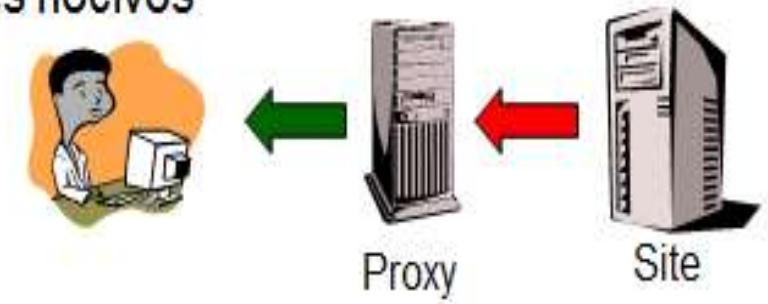
- Agentes Proxy



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

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

Limitações de Firewalls e Gateways

- spoofing:

IP Spoofing: Nesse tipo de ataque, o invasor falsifica o endereço IP de origem em um pacote IP para fazer parecer que a origem é confiável ou autorizada. Isso pode ser usado para evitar a filtragem de pacotes ou para enganar os sistemas de autenticação baseados em endereços IP.

DNS Spoofing: Também conhecido como envenenamento de cache DNS, esse ataque ocorre quando um invasor falsifica os registros DNS de um servidor DNS ou altera as informações de DNS em um cache de DNS. Levando os usuários para sites falsos ou maliciosos.

ARP Spoofing: Nesse ataque, o invasor falsifica as tabelas de resolução de endereços (ARP) em uma rede local. Isso permite que o invasor associe seu próprio endereço MAC a um endereço IP legítimo, redirecionando o tráfego destinado a esse endereço para o invasor.

Limitações de Firewalls e Gateways

- spoofing:

Spoofing de e-mail: Também conhecido como phishing, esse tipo de ataque envolve o envio de e-mails falsificados que parecem ser originados de uma fonte confiável. Os invasores podem falsificar o remetente, o nome do remetente e o endereço de e-mail para enganar os destinatários.

Spoofing de identidade: Esse tipo de ataque ocorre quando um invasor falsifica a identidade de um usuário legítimo para obter acesso não autorizado a sistemas ou recursos. Isso pode ser feito por meio de roubo de credenciais, como senhas, ou por meio de engenharia social.

Contramedidas: autenticação robusta, criptografia e monitoramento de tráfego de rede, para mitigar os riscos associados a esses tipos de ataque

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Exemplos

Firewalls Cisco ASA 5500

Característica	5505	5520	5540	5550	5580-40
Memória RAM	512 MB	1 GB	2 GB	4 GB	12 GB
Capacidade de filtragem	150 Mbit/s	450 Mbit/s	650 Mbit/s	1 Gbit/s	10 Gbit/s
Máximo de ligações simultâneas	10,000	280,000	400,000	650,000	2,000,000
Máximo de ligações por segundo	4,000	12,000	25,000	36,000	150,000
Capacidade VPN 3DES/AES	100 Mbit/s	225 Mbit/s	325 Mbit/s	425 Mbit/s	1 Gbit/s
Máximo de sessões VPN SSL	25	750	2500	5000	10,000
Capacidade de expansão	1 SSC	1 SSM	1 SSM	Não	6 IC
Prevenção de intrusão	Sim, c/ AIP SSC	Sim, c/ AIP SSM	Sim, c/ AIP SSM	Não	Não
Filtragem de conteúdos	Não	Sim, c/ CSC SSM	Sim, c/ CSC SSM	Não	Não
Tolerância a falhas	Não	Sim	Sim	Sim	Sim
Balanceamento de carga	Não	Sim	Sim	Sim	Sim
Contextos de segurança (max)	0	20	50	100	250

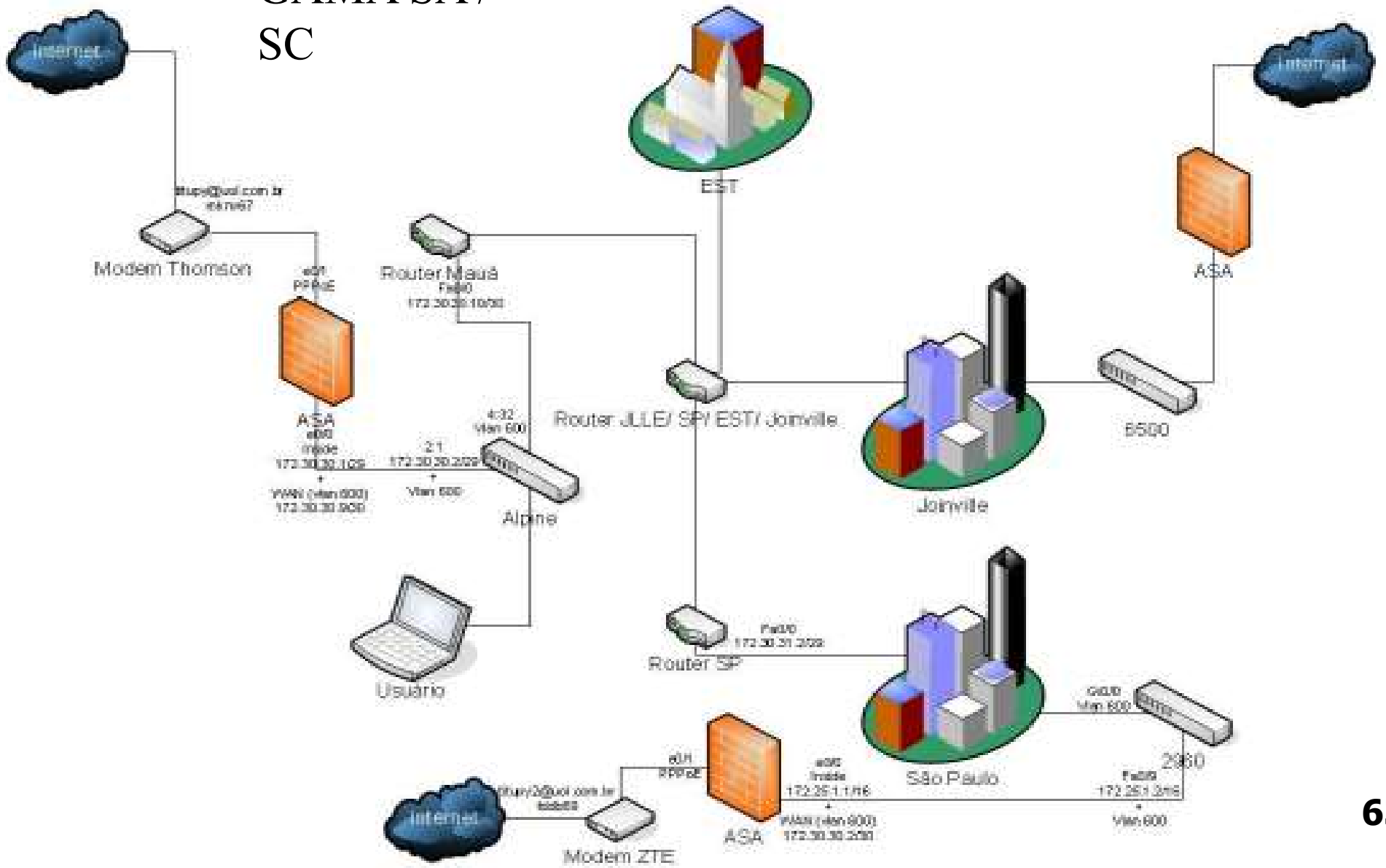
Figura 9 – Modelos da família ASA 5500
Fonte: CISCO SYSTEM, 2013

Figura 10 – ASA 5585
Fonte: CISCO SYSTEM, 2013

Exemplos

Firewalls Cisco ASA 5500

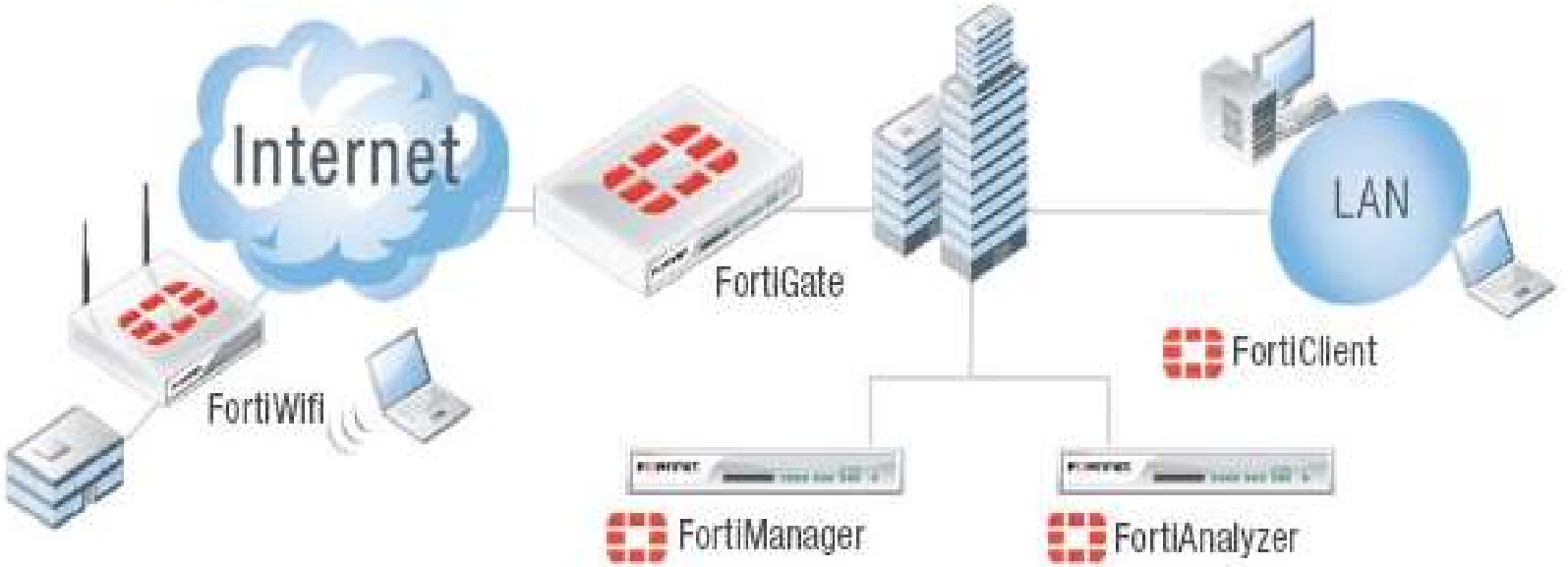
GAMA SA / SC



Exemplos

Firewalls FortiGate

IF Sertão



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Firewall - Considerações Finais

- 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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Firewall - Considerações Finais

O *firewall* não é a solução total de segurança!

- É importante ter em mente que o *firewall* é apenas uma parte de um conjunto de componentes de um sistema de segurança para a proteção das organizações;
- *Firewalls* podem ser uma "faca de dois gumes": representam uma primeira linha de defesa e são necessários em uma infra-estrutura que envolve a segurança;
- Porém, tendem a tranquilizar as organizações com uma falsa sensação de segurança;

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Firewall - Considerações Finais

O *firewall* não é a solução total de segurança!

- Serviços legítimos, como acesso ao servidor Web, devem ser permitidos pelo *firewall*;
- Ou seja, a segurança não depende somente do *firewall*, mas sim dos próprios serviços legítimos;
- Uma autenticação eficiente a um banco de dados, por exemplo, passa a ser fundamental;
- Assim, o enfoque da segurança, agora, está em selecionar os usuários que podem acessar a rede, definir os direitos que eles têm e monitorar o que eles estão fazendo;