FIREWALLS

SEGURANÇA DE REDES E SISTEMAS DE INFORMAÇÃO

TECNOLOGIAS E PROGRAMAÇÃO DE SISTEMAS DE INFORMAÇÃO

NUNO TORRES | NMIGUELTORRES@ESTG.IPVC.PT

2023/2024

FIREWALLS

- As **firewalls** surgiram na década de 1990, para lidar com os riscos inerentes à ligação de redes privadas de organizações a outras redes não controladas pelas mesmas organizações, nomeadamente a Internet.

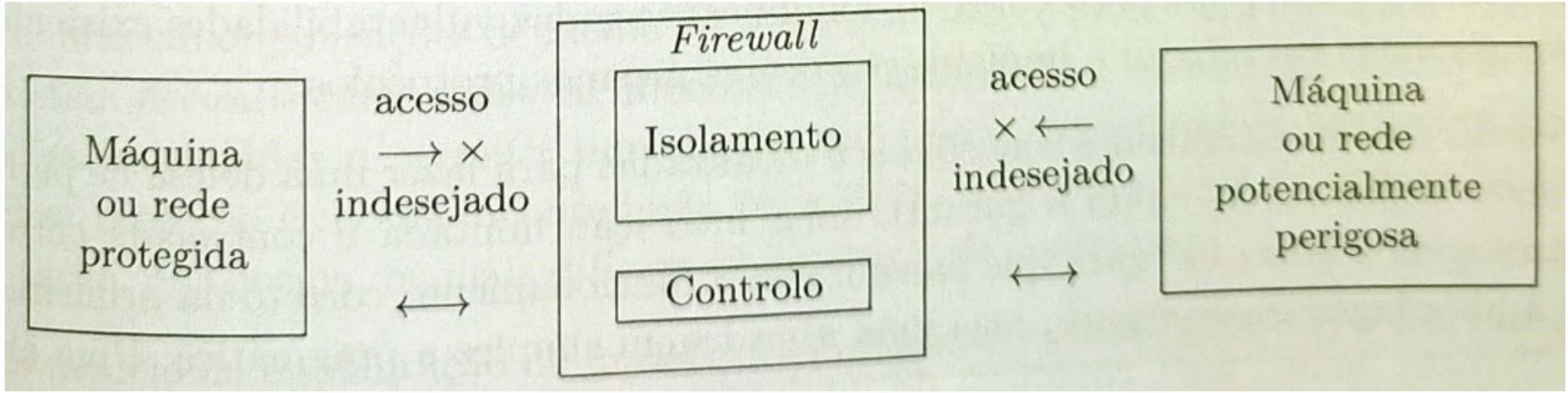
- Uma **firewall** é um equipamento computacional colocado na zona de fronteira de uma rede, cujo principal objetivo é o controlo de acesso a essa rede por parte de utilizadores sediados em outras redes.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS

- Uma firewall tem dois objetivos fundamentais, ambos relacionados com segurança: **protecão por isolamento de máquinas ligadas à rede** e **controlo de interações entre máquinas**;

- Em ambos os casos, as decisões tomadas por uma firewall são controladas por um **conjunto de regras** e **aplicações** que as interpretam e reagem em função do tráfego que chega à firewall.



PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS

- A **Proteção por isolamento** de uma máquina ligada à rede é um requisito crítico. A ligação em rede permite disponibilizar e/ou utilizar serviços de outras máquinas, mas é um risco, pois expõe vulnerabilidades da máquina que podem ser exploradas por "outros".

- **O Controlo de interações entre máquinas** permite definir e concretizar, de maneira simples e centralizada, uma política organizacional de controlo sobre as interações via rede. Essas interações podem acontecer entre um conjunto de máquinas/redes pertencentes ao domínio de segurança da firewall ou entre essas máquinas/redes e as demais da Internet.

- Uma firewall é, atualmente, um elemento indispensável na ligação de máquinas pessoais e redes privadas a redes alheias potencialmente perigosas, nomeadamente à Internet. Contudo, **conceber**, **implementar** e **manter** uma firewall **é uma tarefa complexa, que exige bons conhecimentos a nível dos protocolos de comunicação e das vulnerabilidades existentes nos diversos sistemas em relação à implantação desses mesmos protocolos.**

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – ESTRUTURA BÁSICA

- Todo o tráfego entre o perímetro protegido e as redes externas/perigosas passa pela firewall.

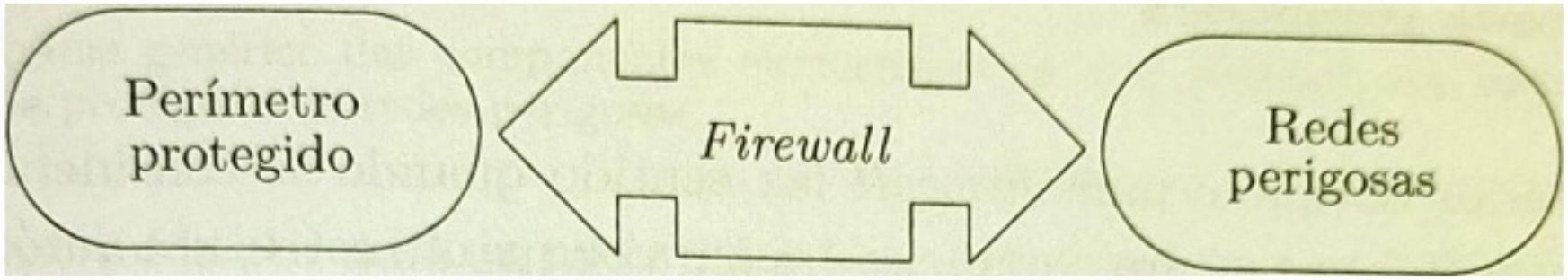
- A firewall é constituída por diversas componentes funcionais, quer de **hardware** — **máquinas**, **redes** e **equipamentos de interligação** como hubs, switches, gateways, routers, etc. — quer de **software** — aplicações específicas para **filtrar**, **controlar** e **modificar** fluxos de comunicação.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – ESTRUTURA BÁSICA

- Ou seja, uma firewall não é uma máquina mas sim uma **infraestrutura,** mais ou menos complexa, que isola um perímetro protegido de redes perigosas a que o mesmo se liga. O isolamento visa não cortar toda e qualquer interação entre as redes, mas sim limitar a mesma a tráfegos e conteúdos autorizados.

- A firewall inclui uma gestão de diversos aspetos típicos de gateways, como **gestão de encaminhamento** e **tradução de endereços de máquinas ou portos de transporte de serviços.**



PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS PESSOAIS

- O uso crescente de computadores pessoais ligados à Internet, através de ISP, e móveis que se podem ligar a qualquer ISP ou a redes organizacionais inseguras (por exemplo, redes universitárias), levou ao aparecimento das chamadas **firewalls pessoais**.

- As firewalls pessoais não são mais do que firewalls que se destinam a **proteger uma única máquina** e fazem parte do sistema da mesma. Funcionalmente, são semelhantes às demais, no entanto, alguns dos princípios de base do desenho normal de firewalls não se aplicam, isto é, uma firewall pessoal é, por norma, um sistema de software que executa na mesma máquina que se quer proteger, ou seja, a firewall e o perímetro protegido são exatamente a mesma máquina.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS PESSOAIS

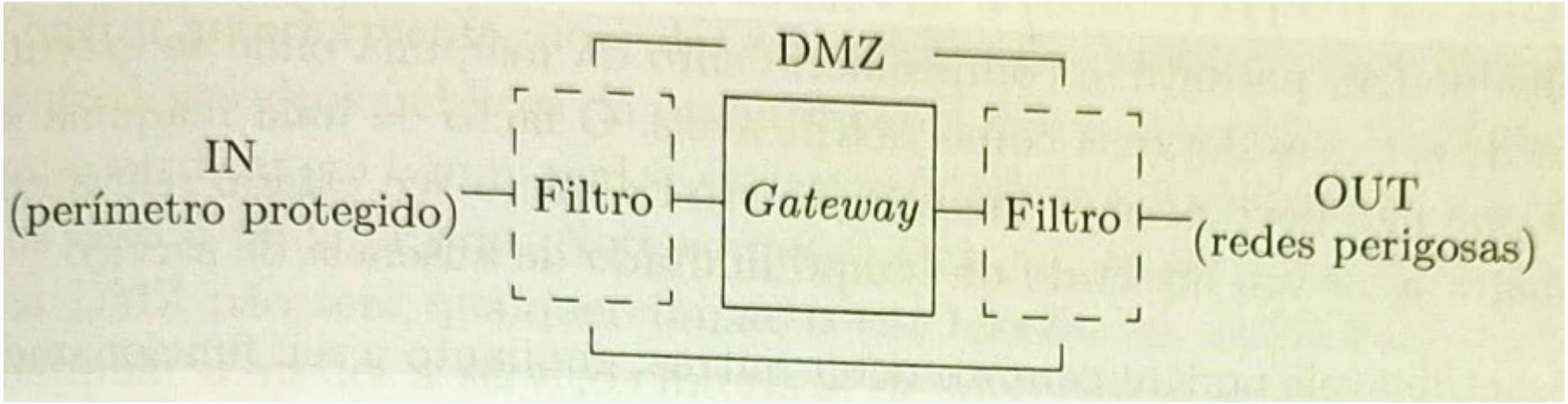
- As firewalls pessoais distinguem-se também por permitirem controlar quais as aplicações locais capazes de efetuar determinadas interações com o exterior.

- As firewalls pessoais não são componentes fáceis de configurar por um utilizador normal de um computador ligado em rede.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – ESTRUTURA SIMPLIFICADA

- Uma firewall é formada por uma **gateway**, **dois filtros** e uma rede de interligação de todas estas componentes, denominada **zona desmilitarizada - DMZ (de DeMilitarized Zone).**



PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – ESTRUTURA SIMPLIFICADA

- A gateway é constituída por uma ou mais máquinas cuja função é **controlar** e **encaminhar** corretamente a **comunicação IN-OUT**; Cumpre com **funções de encaminhamento genérico** dos níveis de rede e de transporte, e ainda dos níveis superiores (aplicação). Pode ainda atuar a nível da **tradução de endereços e portos de máquinas e serviços da rede protegida.**

- Os filtros destinam-se a fazer alguma filtragem elementar do tráfego autorizado a passar pela firewall, e também impedem que a gateway possa ser "contactada" diretamente por outras máquinas IN ou OUT.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – TRADUÇÃO DE ENDEREÇOS NAT

- Como já referido as firewalls efetuam ações de tradução de endereços de máquinas ou de portos de transporte de serviços, designada normalmente por **NAT** (Network Address Translation), por **PAT** (Port Address Translation) ou por **NAPT** (Network Address and Port Translation), e envolve duas operações elementares — **IP masquerading** e **port forwarding;**

- O NAT tem um **duplo objetivo**: **simplificar a gestão de endereços** das redes internas ligadas à Internet através da gateway; e **impedir um endereçamento ad hoc de máquinas internas** originado na rede externa. Com efeito, na rede privada podem ser usados endereços IP privados (por exemplo, a classe A 10.x.x.x, as 16 classes B 172.16-31.x.x ou as 256 classes C 192.168.0-255.x ver RFC 1918 [214]) e apenas a gateway precisa de possuir um ou mais endereços IP públicos e registados na InterNIC para comunicar com o exterior.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – TRADUÇÃO DE ENDEREÇOS NAT

- **IP masquerading:**
- A tradução de endereços IP, designada por **IP masquerading** ou DNAT (Dynamic Network Address Translation), **visa esconder uma rede privada atrás de endereços públicos da sua gateway**. Assim, **quando um datagrama IP passa pela gateway para o exterior, o seu endereço IP de origem é mudado para um IP público da gateway**. A gateway guarda um mapa de traduções de endereços IP e portos de transporte interiores para portos relativos ao IP exterior da gateway.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IP MASQUERADING E PORT FORWARDING

- A tabela de traduções é construída e mantida dinamicamente.

- Esta técnica – **IP masquerading** – é particularmente útil para a segurança fornecida por uma firewall, porque permite que **máquinas interiores estabeleçam contactos com o exterior mas impede o contrário.** Teoricamente, no exterior não se consegue sequer ter a noção de que existem máquinas para além da firewall.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IP MASQUERADING E PORT FORWARDING

- **Port forwarding:**
- É complementar ao anterior: **permite que acessos originados no exterior possam chegar até um serviço localizado numa máquina interior cujo IP não é público**. Neste caso, a tabela de tradução de endereços da gateway **não é totalmente dinâmica e mantém traduções fixas em relação a alguns portos**.

- Nomeadamente, mantém traduções fixas entre pares (IP, porto de transporte) da gateway e pares semelhantes relativos a máquinas internas. Desta forma, a rede interna pode disponibilizar serviços públicos, uma vez que os mesmos podem ser acedidos do exterior através dos mapeamentos fixos feitos através de **port forwarding.**

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IP MASQUERADING E PORT FORWARDING

- Por exemplo, para a receção de e-mail numa máquina interior via SMTP a tabela de **port forwarding** pode indicar que um porto 25 TCP público (relativo a um dos IP públicos da gateway) está associado ao porto 25 TCP da máquina interna X. Quando um cliente SMTP se ligar a esse porto público, a gateway irá redirigir essa ligação para o porto 25 TCP da máquina X.

- Esse reencaminhamento é feito transparentemente para o cliente. Em termos de segurança tal é muito vantajoso porque se impede, de forma simples, todo e qualquer acesso exterior a X que não seja o acesso aos portos exportados via port forwarding (no exemplo, ao porto 25 TCP).

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – ENCAPSULAMENTO (TUNNELING)

- O encapsulamento consiste em colocar datagramas de um protocolo como corpo de datagramas de outro protocolo, em conjunto com um cabeçalho descritivo do encapsulamento. Esta técnica permite transportar datagramas através de redes onde normalmente não circulariam.

- As firewalls, por serem o elo de ligação de uma rede organizacional à Internet, estão num local Privilegiado para efetuarem o encapsulamento de vários protocolos, quer sejam ou não suportados pela Internet. Quando o encapsulamento se mistura com a comunicação cifrada, dá origem a **redes virtualmente privadas** (VPN - Virtual Private Network). No entanto, podem existir VPN sem qualquer forma de encapsulamento de protocolos de comunicação. (tema a abordar à posteriori)

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – CARACTERIZAÇÃO

- Há autores que identificam três tipos de firewall's segundo o seu modelo de intervenção:

- **Filtro de datagramas** (packet filter)
- **Filtro de circuitos** (circuit gateway)
- **Filtro aplicacional** (application gateway).

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- É uma filtragem que atua fundamentalmente a nível da camada da rede, nomeadamente na troca de datagramas IP.

- Estes filtros, normalmente, limitam-se a aceitar ou rejeitar a passagem de um **datagrama** pela firewall, no âmbito do seu encaminhamento através da mesma.

- Por definição, **estas firewall's não lidam** com protocolos aplicacionais.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- Estrutura de um datagrama IP

Versão	(4 bits)
Internet Header Length (IHL)	(4 bits)
Tipo de serviço	(8 bits)
Comprimento Total	(16 bits)
Identificação	(16 bits)
Flags	(3 bits)
Offset de Fragmento	(13 bits)
Tempo máximo de vida	(8 bits)
Protocolo	(8 bits)
CheckSum do cabeçalho	(16 bits)
Endereço de Origem	(32 bits)
Endereço de Destino	(32 bits)
Opções	(numero de bits variável)
Padding	(assegura que o cabeçalho tem um comprimento múltiplo de 32 bits)
Dados	(variável, mas deve ser sempre um múltiplo de oito, um "datagrama" IP pode ter até 65535 bytes)

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- Estrutura de um datagrama IP (revisão):

- **Versão do protocolo IP** (IPv4 ou IPv6); A versão do protocolo condiciona a estrutura do "datagrama" e mecanismos;
- **Campo IHL** contém o número de conjuntos de 32 bits que constituem o cabeçalho;
- **Tipo de serviço** - Este campo divide-se na especificação de 8 níveis de prioridade (3 bits), dois níveis de fiabilidade, dois níveis de atraso e dois níveis de capacidade;
- O **comprimento total** do "datagrama" (cabeçalho + dados) é indicado no campo seguinte, o seu valor máximo é de 65535 bytes.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- Estrutura de um datagrama IP (revisão) continuação:

- Os 3 campos seguintes (**Identificação; Flags; Offset de Fragmento**) estão relacionados com o mecanismo de fragmentação/reagrupamento - Para que os "fragmentos" de diferentes "datagramas" não se confundam entre si, para cada "datagrama" o emissor define um valor para o campo "Identificação" de tal modo que, em conjunto com os campos "Endereço de Origem", "Endereço de Destino" e "Protocolo" defina um valor único;

- O primeiro bit do campo "**Flags**" é colocado a 1 para indicar que existem mais fragmentos a seguir, o valor zero indica que se trata do último fragmento ou que o "datagrama" não foi fragmentado. O segundo bit do campo "Flags" pode ser colocado a 1 para evitar a fragmentação, neste caso se o MTU não suporta o tamanho do "datagrama", este é ignorado. O terceiro bit do campo "Flags" não é utilizado.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- Estrutura de um datagrama IP (revisão) continuação:

- O campo "**Offset de Fragmento**" indica a posição relativa do fragmento no "datagrama" original, o valor é especificado em unidades de 64bits. No caso de se tratar de um "datagrama" não fragmentado ou o primeiro fragmento de um "datagrama" este campo possui o valor zero.
- O **tempo máximo de vida** é um contador de saltos até à auto-destruição do "datagrama". É inicializado pelo emissor e sempre que o "datagrama" é transferido entre redes por um "router" o seu valor é decrementado em uma unidade, quando chega a zero o "datagrama" é ignorado.
- O campo "**Protocolo**" contém um identificador do protocolo responsável pelos dados que são transportados, trata-se de um simples mecanismo de multiplexagem para permitir a coexistência de vários protocolos a utilizarem o IP como base.
- O **checksum** do cabeçalho é calculado por somatório de todos os conjuntos de 16 bits do cabeçalho

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- Os filtros usam listas de regras, que são aplicadas sequencialmente segundo a ordem estabelecida pelo administrador da firewall até encontrarem uma regra aplicável ao datagrama. Essa regra dita o destino do datagrama: **aceitação** ou **rejeição**.

- **Exemplos de filtragem por datagramas - packet filter:**
- **Endereços IP (de origem ou destino)** - O controlo dos endereços de origem permite autorizar ou negar fluxos de informação entre máquinas, independentemente dos protocolos de transporte usados. Pode também controlar pedidos em difusão, que muitas vezes estão na origem de ataques esmagadores à prestação de serviços - ("só respondo a quem conheço"; "não falar para estranhos";

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- **Exemplos de filtragem por datagramas - packet filter (continuação)**
- **Protocolos e portos de transporte** (de origem ou destino) - O controlo dos protocolos de transporte permite autorizar ou negar completamente certos tipos de protocolos de transporte (UDP, TCP, etc.), muito embora, por norma, não se tome este tipo de decisões.

- Com efeito, o controlo destina-se fundamentalmente a ajudar a tornar decisões a nível da autorização ou negação de interações envolvendo certos tipos de portos de transporte, normalmente indicativos de protocolos aplicacionais específicos (por exemplo, porto 53 UDP para DNS, porto 80 TCP para HTTP etc.);

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- **Exemplos de filtragem por datagramas - packet filter (continuação)**
- **Operação ICMP e dados anexos** - As operações ICMP destinam-se a auxiliar as tarefas de administração e exploração da pilha de protocolos IP, mas podem ser indesejadas ou revelar aspetos da organização que interesse esconder (por exemplo, a estrutura de rede interna).

- Nesse sentido, devem apenas ser autorizados a fluir através da firewall os datagramas ICMP cujas operações sejam consideradas úteis para os seus destinatários.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- **Exemplos de filtragem por datagramas - packet filter (continuação)**
- **<u>Sentido de criação de circuitos virtuais</u>** - O sentido de criação de circuitos virtuais é importante para controlar de que modo os circuitos virtuais podem ser estabelecidos, uma vez que a sua génese é assimétrica, ou seja, existe normalmente um agente passivo (servidor) e um ativo (cliente).

- Por exemplo, um servidor HTTP numa DMZ está geralmente autorizado a receber ligações TCP do exterior para o porto 80 TCP mas não a iniciar ligações (ou seja, a atuar como cliente). Assim, devem ser permitidas ligações do exterior para o servidor e não o contrário.

- Na prática, tal significa que a firewall não deve permitir que o servidor envie segmentos TCP SYN simples (apenas SYN/ACK), mas que possa receber esses segmentos;

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- **Limitações na implementação da firewall - packet filter:**
- **Utilização de portos de transporte dinâmicos packet filter** - Diversos protocolos aplicacionais usam portos dinâmicos para os servidores e um serviço de nomes para procurar esses portos, considerando que para o mesmo serviço, podem utilizar portos diferentes.

- Isto complica a definição de regras de filtragem, já que são normalmente definidas sobre portos fixos. (solução: aplicar firewall com filtro aplicacional)

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – PACKET FILTER

- **Limitações na implementação da firewall - packet filter:**
- **Criação bidirecional de ligações TCP** – Quando um determinado protocolo aplicacional utiliza um comunicação bidirecional pode ser problemático na gestão de regras de filtragem da firewall.

- O exemplo mais vulgar é o caso das ligações FTP. O FTP explora dois canais para troca de dados: o **canal de controlo** (porto 21) e o **canal de dados** (porto 20). (solução: aplicar firewall com filtro aplicacional)

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – FILTRO DE CIRCUITOS (CIRCUIT GATEWAY)

- Este tipo de filtragem está associado ao reencaminhamento de ligações.
- Por exemplo:

- **1)** Uma firewall deste tipo permite o acesso SMTP de fora para qualquer uma das suas máquinas internas, mas pode e deve redirigi-lo transparentemente para uma única máquina que servirá como ponto de entrada central para todo o e-mail com destino à organização.

- Desta forma, é possível efetuar de forma abrangente um conjunto de atividades de controlo e filtragem, como deteção e eliminação de vírus e spam. (O mesmo processo poderá ser aplicado a todo o trafego SMTP de saída da organização).

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – FILTRO DE CIRCUITOS (CIRCUIT GATEWAY)

- **2)** Pode também ser utilizado para balanceamento de carga e tolerância a faltas/falhas.

- Uma empresa a disponibilizar um serviço http através de um conjunto de servidores, pode a cada acesso dos clientes redirigir para um dos servidores "disponíveis" controlando desta forma velocidade de resposta, disponibilidade, endereços IP do cliente, etc;

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – FILTRO DE CIRCUITOS (CIRCUIT GATEWAY)

- **3)** Outro exemplo, é em autorizar, ou não, o estabelecimento de um circuito virtual após autenticação do requerente. Essa autenticação é feita segundo um protocolo próprio, na firewall, independentemente de qualquer outro que possa existir a nível da aplicação.

- Este tipo de filtragem não é tão usual, já que requer conhecimentos mais "avançados" – **protocolo SOCKS** (Socket Secure) e **protocolo AFT** (Authenticated Firewall Transversal).

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – FILTRO APLICACIONAL (APPLICATION GATEWAY)

- As firewall's deste tipo operam na camada da aplicação. A sua função é mediar parte ou totalidade das interações aplicacionais entre interlocutores remotos, localizados em redes interligadas pela firewall, de forma a controlar a execução desse mesmo protocolo.

- As firewall's deste tipo utilizam como complemento um conjunto de aplicações mediadoras designadas como proxies/proxy que são executados na máquina firewall.

- Contudo, não há mediadores genéricos, para cada protocolo aplicacional tem que ser implementado um mediador especifico. Este é um aspeto pelo qual as firewall's usam um filtro de datagramas para controlar grande parte dos fluxos e um conjunto reduzido para lidar com fluxos em particular.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – FILTRO APLICACIONAL (APPLICATION GATEWAY)

- A implementação de mediadores permite efetuar diversas operações que não estão ao alcance da filtragem por datagramas, nomeadamente: controlo de acessos de utilizadores, análise e alteração de conteúdos, registo (logging) pormenorizado, etc.

- O controlo de acessos de utilizadores permite introduzir uma barreira no acesso a recursos do outro lado da firewall, independentemente do controlo de acessos inerente ao serviço a que o utilizador pretende aceder.

- Por exemplo: uma firewall pode possuir um mediador de Telnet que autentique os utilizadores que pretendam aceder à rede protegida a partir do exterior, e só após uma autenticação bem sucedida permita aceder à máquina que o utilizador pretende aceder remotamente.

- O mesmo é comum ser aplicado outros mediadores a outros serviços, tais como: serviços de e-mail (POP, IMAP Web mais, etc), serviços de ficheiros distribuídos, serviços de impressão, serviços de FTP, etc.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- A **autorização** é uma das principais funções de uma firewall. Os **filtros de datagramas (packet filter)** autorizam ou negam fluxos de dados de acordo com informação disponível do nível de transporte.

- Os **filtros de circuitos (circuit gateway)** permitem autorizar ou negar o estabelecimento de circuitos para o exterior, ou internos, após uma autenticação potencialmente mais complexa do que a simples confrontação do endereço IP de origem com uma lista de endereços autorizados.

- Finalmente, **os filtros aplicacionais (application gateway)** autorizam ou negam operações específicas definidas a nível dos protocolos, através da implementação de mediadores de protocolos aplicacionais.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- **Redirecionamento/Port forwarding** - Uma firewall é um local natural para redirigir tráfego para servidores/utilizadores internos concretos os quais podem nem ser endereçáveis diretamente pelos clientes.

- O redirecionamento pode servir para diversos fins: balanceamento de carga entre diversos servidores equivalentes, tolerância a faltas de servidores e mediação explícita e transparente ou ocultação de servidores NAT.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- **Controlo de operações e conteúdos** - Uma firewall pode controlar totalmente as operações requeridas no âmbito de diversos protocolos aplicacionais e pode ainda controlar conteúdos transferidos entre o interior e o exterior da organização protegida.

- Em ambos os casos, tal controlo deverá ser feito através de filtros aplicacionais, um por cada protocolo aplicacional.

- **Comunicação Segura** - Atualmente as linhas dedicadas, em questões de segurança, foram substituídas por soluções mais económicas e flexíveis, designadas por redes virtualmente privadas (VPN's).

- Uma firewall, por ser o elo de ligação entre uma rede organizacional e a rede pública, onde é estabelecida a VPN está numa situação topológica privilegiada para gerir várias VPN para máquinas ou redes exteriores.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- **Proteção face a ataques DoS ou de reconhecimento de sistemas -** Certos tipos de ataques à prestação de serviços exploram vulnerabilidades no desenho de protocolos de comunicação ou na sua utilização.

- Uma firewall, por estar no caminho entre uma rede organizacional e a rede pública, pode **monitorizar**, **controlar** ou **contrariar** diversos tipos de ataques iniciados no exterior contra máquinas interiores ou vice-versa.

- Em particular, as firewalls são pontos excelentes para colocar sistemas de identificação de intrusões (**IDS – Intrusion Detection Systems**) para proteção de ataques vindos do exterior.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- **1)** Uma firewall pode anular quaisquer ataques que abusem dos endereços públicos da organização protegida usando IP spoofing . Assim, a firewall não deverá deixar entrar na rede organizacional datagramas IP cujo endereço de origem seja um dos da rede protegida.

- Complementarmente, a firewall não deverá deixar sair para a rede pública quais quer datagramas IP que não possuam um endereço IP de origem que seja um dos endereços públicos da organização.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- **2)** A informação do cabeçalho IP de um datagrama, bem como de outros cabeçalhos incluídos no seu corpo (cabeçalhos de transporte UDP, TCP, etc.), pode ser estrategicamente construída de modo a obter informações ou explorar vulnerabilidades.

- Logo, uma firewall pode incluir como operação profilática à deteção e ao descarte de datagramas malformados ou anormais.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- **3)** A firewall pode mudar valores em cabeçalhos de datagramas ICMP UDP ou em segmentos TCP para iludir ferramentas de identificação de sistemas operativos, como o nmap.

- Essa modificação pode ser feita na maioria dos casos sem manter qualquer estado, bastando modificar certos campos dos cabeçalhos ou reconstruindo-os, de forma fixa ou com algum grau de aleatoriedade, para evitar o reconhecimento de comportamentos típicos dos remetentes.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SERVIÇOS OFERECIDOS (RESUMO)

- **4)** Uma firewall pode também detetar e contrariar um SYN flooding attacks protegendo todo e qualquer servidor/utilizador da rede interior de ataques vindos do exterior.

- É da responsabilidade da firewall gerir a melhor maneira, eficaz e rápida, nas respostas do SYN / SYN-ACK /ACK

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IPTABLES

- O **iptables** é um módulo do núcleo Linux que recebe todos os datagramas que chegam à máquina e serão enviados a partir desta. O destino desses datagramas depende das regras programadas no módulo.

- A funcionalidade intrínseca do iptables permite realizar apenas uma firewall do tipo **filtro de datagramas**. No entanto, o iptables, através do reencaminhamento de datagramas, permite que os fluxos de informação sejam redirigidos para quaisquer aplicações locais.

- Logo, o iptables fornece também os mecanismos-base para a utilização de outros tipos de firewalls, nomeadamente filtros de circuitos ou aplicacionais. No entanto, a funcionalidade de tais filtros é completamente independente do iptables;

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IPTABLES

- O iptables possui cinco cadeias-padrão, mas podem ser criadas outras para reutilizar regras. As cadeias-padrão são **INPUT, OUTPUT, FORWARD, PREROUTING** e **POSTROUTING**.
- A **INPUT** aplica-se a datagramas recebidos pela máquina e que lhe são dirigidos;
- a **OUTPUT** aplica-se a datagramas enviados pela máquina e com origem na mesma;
- a **FORWARD** aplica-se a datagramas recebidos pela máquina mas que não lhe são dirigidos, ou seja, que passam em trânsito pela máquina, que faz o seu encaminhamento (Routing);
- a **PREROUTING** aplica-se a todos os datagramas recebidos pela máquina;
- e a **POSTROUTING** aplica-se a todos os datagramas enviados pela máquina.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IPTABLES

- O iptables usa tabelas para subdividir a aplicação de regras em cada cadeia. Há três tabelas-base: **filter**, **nat** e **mangle**. A **tabela filter** existe sempre por omissão e serve para filtrar datagramas, ou seja, para decidir apenas sobre a sua aceitação ou rejeição.

- A **tabela nat** serve para detetar e atuar em situações em que seja necessário fazer NAT. A **tabela mangle** serve para efetuar diversos tipos de alterações nos datagramas

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IPTABLES

- Para estabelecer as diversas regras são definidas determinadas decisões-base. As decisões-base são: **ACCEPT, DROP, QUEUE** e **RETURN**.

- A primeira indica o datagrama deve ser aceite, a segunda que deve ser descartado, a terceira que o datagrama deve ser enviado para uma fila de espera afeta a uma aplicação local e a quarta que cadeia atual deve ser abandonada e retomada a análise de regras na regra seguinte da cadeia anterior.

- As **principais vantagens** do iptables consistem no facto de ser: um produto comparável em eficácia às demais firewalls comerciais; relativamente estável, confiável e escalável; desenvolvido, testado e melhorado por uma grande comunidade de utentes (que é rápida a corrigir problemas); económico em termos de recursos computacionais necessários.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – IPTABLES

- As suas **principais desvantagens** consistem em: ter de se perceber bem como funciona a interação entre o núcleo Linux, o iptables e diversos outros módulos que interagem com os dois anteriores; não ser uma solução autónoma, sendo antes uma peça do imenso "Lego" que é o núcleo do Linux;

- e o facto de não haver uma ferramenta gráfica padrão adequada aos administradores menos habituados à administração de máquinas Linux (muito embora haja várias ferramentas gráficas alternativas) .

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SISTEMAS WINDOWS

- Os sistemas operativos MS Windows a partir do Windows 2000 possuem algumas facilidades que permitem acionar firewalls pessoais ou firewalls para redes locais com uma funcionalidade mínima. Estas firewalls são perfeitamente suficientes para barrar a maioria dos ataques remotos com ciberpragas a serviços vulneráveis;

- A partir do sistema Windows 7 passou a existir o conceito de **perfis de ligação à rede**. Há três perfis de rede com os quais se pretendeu agrupar políticas de proteção para ambientes similares: **Pública**, **Privada** e **Domínio** (domain). O perfil de rede Privada pode, por sua vez, ser uma rede de **Trabalho** (work) ou **Doméstica** (home). A firewall pode ser ativada ou desativada para cada tipo de perfil;

- **O perfil de rede Pública** - destina-se a classificar uma interface de rede sempre que esta se liga a uma rede pública, ou seja, a uma rede onde nada se pode afirmar sobre o seu grau de ameaça (que se deve supor elevado).

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

FIREWALLS – SISTEMAS WINDOWS

- **O perfil de rede Privada** - destina-se a redes domésticas ou de escritório, onde se assume que o grau de risco é muito reduzido e se privilegia a troca de informação mais aberta entre sistemas em detrimento da segurança inerente a um maior isolamento.

- **O perfil de rede de Domínio** - destina-se a redes de escritórios com sistemas centrais MS Windows, onde é suposto haver alguma integração com um conjunto alargado de serviços que necessitam de autorizações de comunicação especiais.

- Contudo, por defeito todos os perfis bloqueiam globalmente contactos iniciados de forma remota com o sistema local (ligações de entrada não solicitadas), exceto nos casos em que isso for explicitamente autorizado por uma regra. Tal representa uma imposição do **princípio do privilégio mínimo**, o que é aconselhável. Porém, podemos sempre alterar e criar exceções às regras.

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte

BIBLIOGRAFIA

- André Zúquete, Segurança em redes informáticas, (6ªEdição 2021, FCA)
- James F. Kurose and Keith W. Ross - "Computer Networking: A Top-Down Approach 8th Edition", (2021, AddisonWesley)

PORTUGAL 2030 Cofinanciado pela União Europeia NORTE 2030 Programa Regional do Norte