Anteparas de Segurança (Firewalls)

Nuno Ferreira Neves

Departamento de Informática
Faculdade de Ciências da Universidade de Lisboa

Firewalls, porquê?

Basicamente as organizações não conseguem operar sem estar ligadas às Internet!

- **Exemplos de ataques:**

1. ***Recolha de Informação:*** tem como objectivo a construção de uma base dados com informação sobre a organização da rede da instituição e das máquinas que lá residem

   FERRAMENTAS : emprego de programas como Ping e TraceRoute para determinar endereços de redes e nomes de máquinas

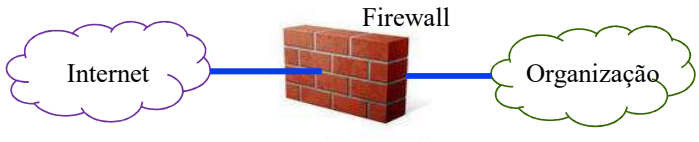
2. ***Testar (Probing) os Sistemas:*** determinar os problemas (falhas) de segurança de cada máquina

   FERRAMENTAS : 1) determinar que máquinas suportam serviços com problemas conhecidos; 2) uso de ferramentas disponíveis na Internet para testar vulnerabilidades comuns

3. ***Acesso aos Sistemas Internos:*** executar ataques que exploram as vulnerabilidades

   FERRAMENTAS : explorar os problemas de segurança de cada máquina

Princípios



- ***Localização*** **:** a antepara deve ser inserida entre a rede interna da organização e a Internet de forma a que seja possível controlar e segurar a ligação
- ***Objectivo*** **:** proporciona o ponto único de acesso à rede interna, permitindo definir regras de controle de acesso a máquinas/serviços da rede interna e protegendo-a de várias classes de ataques provenientes da Internet
  - define um ponto privilegiado na rede para se fazer monitorização, gerando-se informação de auditoria e alarmes
  - local onde se podem colocar outros serviços, como tradução de endereços locais para endereços globais
  - local onde se pode proteger o tráfego colocando-o num túnel (IPsec)

Princípios (cont)

- ***Objectivos de desenho***
  - **Todo o tráfego** do exterior para o interior, e vice versa, deve passar pela antepara ⇒ a localização física permite a interposição entre todo o tráfego
  - Só o **tráfego autorizado** (definido pela política de segurança) pode passar
  - A antepara deve ser **imune a penetrações** ⇒ implementada num sistema seguro com um sistema operativo de confiança

Controlo de Acesso com uma Firewall

- ***Controlo dos Serviços***
  - Determina que serviços podem ser acedidos

    EXEMPLO: filtrar tráfico baseando-se no endereço IP e porto TCP
- ***Controlo da Direcção***
  - Determina a direcção (de fora para dentro, e de dentro para fora) que um pedido para um serviço particular pode ser executado, e ao qual é permitida a passagem pela antepara
- ***Controlo do Utilizador***
  - Determina que utilizadores podem aceder ao serviço
  - Tipicamente os utilizadores locais não têm qualquer restrição, e os externos necessitam de uma autenticação extra
- ***Controlo de Comportamento***
  - Controla a forma como são usados determinados serviços

    EXEMPLO: limita o acesso a só algumas das directorias do servidor FTP

Limitações das Anteparas

- Não protege contra ataques que contornam a (i.e., não passam pela) antepara

  Exemplo : *sistemas na rede interna com capacidade de se ligarem a um ISP; ou a rede interna fornece um serviço de WI-FI ao exterior*
- Não protege contra ataques provenientes de máquinas internas

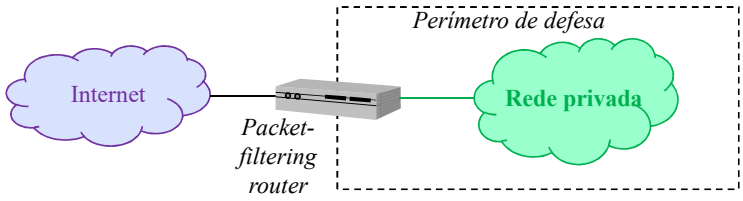
  Exemplo : *empregado que coopera com hacker externo ou que ele próprio ataca os sistemas computacionais da organização*
- Não protege (em muitos casos) contra programas ou ficheiros infectados com vírus/worms, i.e., contra ataques baseados em dados maliciosos ao nível aplicacional

  Exemplo : *vírus inserido num email; um programa aparentemente correcto é copiado para uma máquina interna, e quando é executado inicia um ataque*

Decisões Básicas na Construção da Antepara

- ***Arquitectura de Segurança da Organização*:** qual é o papel da antepara na arquitectura (completa) de segurança da organização
- ***Política de Segurança*:** define fundamentalmente a filosofia básica de segurança da organização
  - PRUDENTE: tudo o que **não** é explicitamente permitido não passa
  - PERMISIVA: tudo o que **não** é explicitamente negado é permitido
- ***Custo da Antepara*:** quanta segurança pode pagar a organização? A organização tem funcionários qualificados para construírem uma antepara a partir do software em domínio público ou é necessária a aquisição de uma antepara comercial? Quanto é que se pretende gastar na manutenção e actualização da antepara? ...
- ***Componentes do Sistema de Antepara*:** que componentes devem ser incluídos no sistema de antepara (e.g., *packet level filtering; application-level gateway; circuit-level gateway*) e como devem ser organizados

Packet-Filtering Router



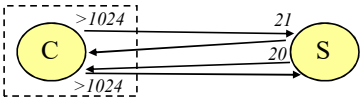
- Aplica um conjunto de regras aos pacotes que chegam **e depois** re-envia ou descarta os pacotes
- As regras de filtragem normalmente são baseadas nos cabeçalhos IP e do protocolo nível transporte (e.g., TCP ou UDP)
  - endereço IP do emissor e destinatário
  - campo protocolo do cabeçalho IP ⇒ define o protocolo nível transporte
  - portos dos cabeçalhos UDP e TCP ⇒ usualmente definem os serviços
- Caso não exista nenhuma regra associada ao pacote
  ⇒ aplica-se a **política de omissão**, descartar ou passar

Exemplos de Regras de Filtragem

Regras para o envio de emails

action	*their host*	*port*	*ourhost*	*port*	*comment*
block	Spam-com	*	*	*	we do not trust these people
allow	*	*	OUR-GW	25	connection to our SMTP port

Regras para uma ligação FTP



Servidor de FTP exterior à nossa rede

action	*src*	*port*	*dest*	*port*	*flags*	*comment*
allow	{our hosts}	*	*	*	*	our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024	*	traffic to nonservers

NOTA: assumir que política de omissão é descartar

Exemplos de Regras de Filtragem

Rule	Direction	Src addr	Dst addr	Prtocol	Dest port	Action	
1	In	External	Internal	TCP	25	Permit	Ligação ao meu servidor de SMTP
2	Out	Internal	External	TCP	>1023	Permit	
3	Out	Internal	External	TCP	25	Permit	Ligação a um servidor de SMTP
4	In	External	Internal	TCP	>1023	Permit	
5	Either	Any	Any	Any	Any	Deny	Política de omissão é descartar

Problemas com estas regras?

Exemplo para melhorar regra 4:

Rule	Direction	Src addr	Src Port	Dst addr	Prtocol	Dest port	Flag	Action
4	In	External	25	Internal	TCP	>1023	ACK	Permit

Benefícios vs. Limitações

- ***Principais Benefícios***
  - simplicidade
  - transparência para com os utilizadores
  - muito rápidos

- ***Principais Limitações***
  - não evitam ataques nível aplicacional porque não inspeccionam o conteúdo das mensagens da aplicação
  - não suportam mecanismos avançados de autenticação
  - não conseguem detectar muitos dos ataques que usam *spoofing* dos endereços IP (e.g., uso endereços de outra organização)
  - é relativamente fácil introduzir erros nas regras do filtro
  - dificuldade na definição correcta das regras para alguns serviços (e.g., FTP)

Alguns Ataques a Packet-Filtering Routers

- **IP address spoofing :** o intruso transmite pacotes em que coloca como endereço IP do emissor um endereço da rede interna.
  SOLUÇÃO: descartar pacotes provenientes da placa de rede externa com endereços de emissão internos

- **Ataques source routing :** o emissor especifica no pacote a opção de *source route* que indica a caminho a tomar na Internet, com a esperança que a antepara deixe passar o pacote por não analisar este tipo de informação.
  SOLUÇÃO: descartar todos os pacotes com esta opção

- **Ataques com fragmentos pequenos:** usa-se a fragmentação IP com o objectivo de se criarem fragmentos muito pequenos, de modo a forçar que os cabeçalhos (e.g., TCP) apareçam em fragmentos distintos.
  SOLUÇÃO: descartar todos os pacotes em que o protocolo é TCP e o tamanho dos fragmentos é pequeno (1 byte)

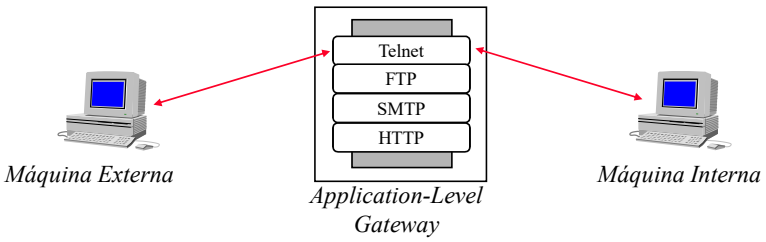
PFR com Stateful Inspection

- São PFR que mantêm contexto (i.e., estado) sobre a ligações que foram permitidas no passado
- Funcionamento
  - o PFR inspecciona o pacote que inicia a ligação
  - se a passagem do pacote é permitida pelas regras da antepara, então adiciona-se uma entrada a uma tabela que descreve esta ligação
  - a partir desse momento, os pacotes desta ligação podem passar livremente, i.e., sem mais inspecções, porque a sua passagem é permitida pela **tabela de estado**
- Vantagem
  - melhora a segurança porque, por exemplo, só deixa passar pacotes exteriores que correspondam a ligações iniciadas pelas máquinas internas
  - este método potencialmente aumenta o desempenho da antepara porque faz-se apenas uma comparação com as entradas na tabela de estado

Exemplo de Tabela de Estado

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

Application-Level Gateway (Application Proxy)



- A gateway só suporta aplicações para as quais existe um servidor de proxy, que funciona como representante do servidor interno
- Basicamente limita-se a passar o tráfego nível aplicação, e
  - os utilizadores apenas podem aceder aos servidores proxy, mas ***nunca*** se podem ligar directamente à gateway ou aos servidores da rede interna
  - o servidor de proxy pode ser configurado de forma a suportar ***apenas*** o subconjunto de serviços fornecidos pela aplicação que são considerados aceitáveis (e.g., seguros), e o resto dos serviços são negados

Como construir a Application Proxy?

- ***Conceito Base***

  TCB - Trusted Computing Base (ou Base de Computação Segura)
  - subconjunto do sistema que é inerentemente seguro (imune a intrusões)
  - geralmente é usada para executar mecanismos críticos de segurança
    - » Ex. controlo de acesso, firewall
  - composto por hardware, firmware, e software

- Propriedades desejáveis para uma TCB:
  - **Interposição**: a TCB deve estar localizada de forma a que não seja possível aceder aos recursos protegidos sem passar por ela

    Não se pode contornar a TCB
  - **Blindagem**: a TCB é construída de maneira a que esteja protegida contra acessos não autorizados

    Não se pode causar uma intrusão na TCB
  - **Validação**: a funcionalidade da TCB deve ser verificável

    A TCB deve ser simples e pequena

Como construir a Application Proxy (cont)?

- **Bastion host**: uma máquina crítica do ponto de vista de segurança (application proxy ou um circuit-level gateway)
  - executa uma versão mais segura do sistema operativo
  - apenas os serviços considerados essenciais estão instalados
  - pode requerer formas adicionais de autenticação antes que seja permitido o acesso aos serviços (ex. tecnologia de passwords descartáveis com smart cards)
- O **Proxy** é configurado: 1) para suportar um subconjunto dos comandos; 2) para permitir o acesso apenas a um subconjunto das máquinas internas; 3) para manter informação de auditoria detalhada
- Cada proxy é um programa pequeno e simples especificamente desenhado com o objectivo da segurança (e.g., email = 20000 linhas -- proxy = 1000 linhas)
- Cada proxy é independente dos outros proxies existentes
- Os proxies normalmente não precisam de aceder a disco
- Os proxies correm como utilizadores não-privilegiados e numa directoria segura

Exemplo: Proxy para o Telnet

- O cliente exterior necessita de se autenticar no bastion host
- O cliente ganha acesso à interface do proxy
- O proxy permite apenas um subconjunto dos comandos e determina quais as máquinas que estão disponíveis para ligação
- O cliente especifica a máquina de destino e o proxy faz a ligação para o servidor interno
- O proxy re-envia os comandos do cliente
- O cliente é autenticado pelo servidor na rede interna

Outside-Client > **telnet bastion_host**
Username: **Nuno Neves**
Challenge Number "123456"
Challenge Response: **768954**
Trying 198.23.45.67

HostOS UNIX (bastion_host)

bh-telnet-proxy > **help**
Valid commands are:

connect hostname
help/?
quit/exit

bh-telnet-proxy > **connect inside_server**

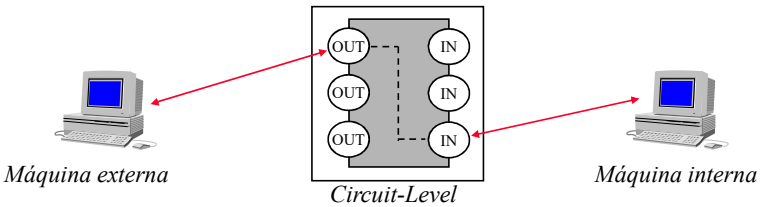
HostOS UNIX (inside_server)

login: **Nuno Neves**
Password: #########
Last login: Friday October 13 12:34:56

Benefícios vs. Limitações

- ***Principais Benefícios***
  - controlo completo sobre cada serviço: é possível especificar quais os serviços suportados e com que opções (ou comandos)
  - possibilita formas mais seguras de autenticação e de colecção de informação de auditoria
  - mais fácil de configurar e de testar que um packet-filtering router
- ***Principais Limitações***
  - Requer que os utilizadores se habituem à nova forma de funcionar dos serviços ou a existência e instalação nas máquinas clientes de software especializado para acederem a serviços proxy
  - Processamento adicional (overheads) em cada ligação

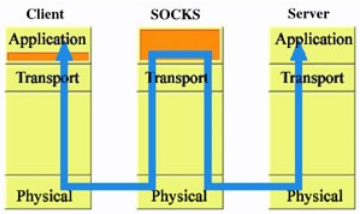
Circuit-Level Gateway (ou Circuit-Level Proxy)



- A gateway cria duas ligações (TCP), uma entre ela e a máquina interna e outra entre ela e a máquina externa
- A gateway passa o tráfego pela ligação sem fazer qualquer outro processamento
- A função de segurança consiste em determinar quais ligações é que são permitidas
- Usada quando os utilizadores internos são de confiança ⇒ a gateway é configurada como application proxy para ligações do exterior e como circuit-level para ligações do interior

Exemplo: SOCKS (RFC 1928)

- Framework para aplicações cliente-servidor que usem os protocolos TCP ou UDP, e que queiram fornecer serviços numa antepara
- Conceptualmente, o SOCKS é uma camada (fina) entre a aplicação e os protocolos nível transporte
- Componentes
  - servidor SOCKS
  - biblioteca SOCKS
  - versões SOCK-ificadas dos programas cliente standard



- Funcionamento
  - o programa cliente contacta o servidor SOCKS no porto TCP 1080
  - existe uma negociação da forma de autenticação
  - estabelece a ligação ou nega a utilização do serviço

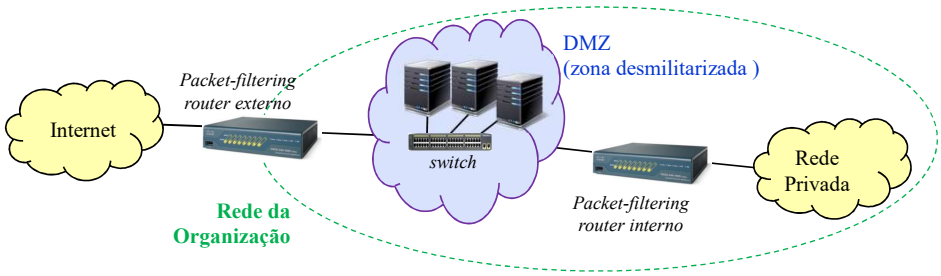
Outros formatos de Firewalls

- Firewall na máquina
  - parte do sistema operativo *ou* como um pacote adicional
  - restringem os pacotes que chegam à máquina
  - usadas em servidores ou máquinas pessoais

Vantagens
- regras de filtragem podem ser adequadas às necessidades locais
- proteção é feita independentemente da topologia de rede
- funcionam como um extra nível de proteção, que vai além do oferecido pelas firewalls de rede

Arquitecturas de Anteparas

Inline Firewalls

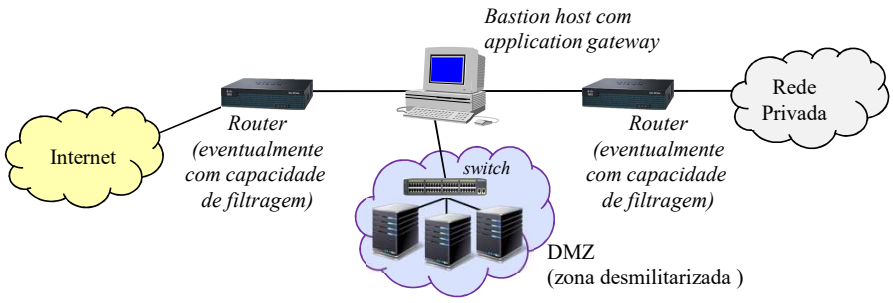


- Os computadores são distribuídos por duas (ou mais) ***zonas de segurança***
- Na exterior (DMZ) são colocados os computadores que necessitam de ser acedidos pela Internet (e.g., servidor Web, email gateway, servidor de DNS)
- Na interior são colocados os computadores privados da organização
- VANTAGEM: um adversário para conseguir corromper os computadores privados tem de passar por duas anteparas; o PFR interno pode ter regras mais estritas
- DESVANTAGEM: atraso no acesso à Internet por parte dos computadores internos

Rede de Interligação

- Rede de interligação – zona desmilitarizada (DMZ)
  - Servidores com serviços públicos (p.ex., email, http, ftp) e que por isso necessitam necessariamente de estar acessíveis do exterior
  - Máquinas sacrificáveis
    - » máquinas que podem ser comprometidas, mas por isso podem comprometer outras
    - » solução
      - isolar máquinas sacrificáveis em DMZs separadas
      - Como?
        - várias LANs ligadas a várias gateways da firewall
        - VLANs diferentes ligadas a uma gateway

Gateway simples (dual home gateway)



- Constituição da firewall: 1 máquina com duas ou mais interfaces, uma para o exterior e uma ou mais para redes interiores
- Os encaminhadores são opcionais, embora permitam reforçar a segurança uma vez que podem operar como filtros de pacotes
- Gateway-bastião diretamente exposta a ataques do exterior e do interior

Gateway simples (dual home gateway)

- Vantagens
  - simplicidade
  - economia de recursos
  - os computadores continuam a ser divididos por duas zonas de segurança, mas evitamos os atrasos extra nos computadores da rede privada

- Desvantagens
  - comprometimento da gateway-bastião
  - carga de processamento na gateway-bastião
  - limitações à localização dos serviços públicos
    - » outras redes interiores – sobrecarrega a gateway ☹

Intrusion Prevention Systems (IPS)

- Extensão aos sistemas de deteção de intrusões (IDS), adicionando-lhes a capacidade de bloquear o tráfego considerado malicioso
- IPS baseados na rede
  - atua como um IDS de rede, recebendo tráfego numa porta e reenviando-o por outra
  - pode descartar ou alterar pacotes em tempo real, ou interromper ligações
  - suportam regras mais complicadas para a deteção de intrusões, como baseadas em padrões de bytes, assinaturas que utilizam sequências de pacotes, descobrem anomalias no tráfego

Bibliografia

- Stallings & Brown, Computer Security: Principles and Practice, Third Edition, 2014
  - Leitura obrigatória: cap 9
  - Leitura opcional: