Firewalls

Introdução

- O que é uma *firewall*?
  - É um sistema desenhado para prevenir acessos não autorizados de ou para uma rede privada.
  - As firewalls podem ser implementadas em hardware, software ou uma combinação de ambas.
  - As firewalls são usadas normalmente para prevenir acessos não autorizados a partir da Internet a redes privadas que estão ligadas à Internet.
  - Todo o tráfego que entra ou sai para a Internet tem que passar através da firewall. Esta examina todos os pacotes e bloqueia aqueles que não estão de acordo com a política de segurança.

Objectivos das *firewalls*

- Todo o tráfego que entra ou sai só pode passar através da *firewall*. Isto é feito bloqueando fisicamente todos os acessos à rede privada, excepto pela *firewall*.
- Apenas o tráfego autorizado, definido pela política de segurança, é que pode passar pela *firewall*.
- A *firewall* deve ser imune aos ataques.

Técnicas de controlo

- **Por serviço** – o tráfego é filtrado com base nos portos e nos endereços IP (de origem e/ou destino), pode ainda usar um proxy que reconhece a sintaxe dos protocolos.
- **Por direcção** – o tráfego é filtrado com base na sua direcção (entrada ou saída) e a partir de onde pode ser iniciado ou permitido.
- **Por utilizador** – controla o acesso a um serviço com base no utilizador que o tenta aceder. Esta técnica é usada principalmente dentro das redes privadas.
- **Por comportamento** – controla a forma como um serviço é usado. Por exemplo uma *firewall* pode filtrar email para eliminar SPAM e vírus.

O que as *firewalls* não protegem

- Ataques que não passem pela *firewall*, por exemplo se existir na intranet um computador ligado a um modem
- Contra ataques dentro da própria rede privada. Cerca de 70% dos ataques têm origem dentro das redes privadas.
- Vírus e outro *malware*, principalmente se a comunicação for efectuada através de canais cifrados.
- *Bugs* dos programas que fornecem os serviços autorizados a passar pela *firewall*.

Tipos de *firewall* (1)

- Existem 3 tipos de firewalls:
  - Filtragem de pacotes:
    - *Stateless*
    - *Statefull*
  - *Gateway* de aplicações (*proxys*)
  - *Gateway* de circuitos

Tipos de *firewall* (2)

- Filtragem de pacotes
  - Aplica regras de filtragem a todos os pacotes e depois reencaminha-os ou rejeita-os
  - As regras são aplicadas ao tráfego de entrada e de saída
  - As regras são baseadas na informação contida nos pacotes:
    - Endereços IP de origem e/ou destino
    - Protocolo (tcp, udp, icmp, ...)
    - Portos de origem e/destino dos protocolos de transporte
    - Interface de rede

Tipos de *firewall* (3)

- Filtragem de pacotes (cont.)
  - As regras são aplicadas pela mesma ordem com que são introduzidas
  - Quando um pacote iguala a uma regra, essa regra é evocada (para aceitar ou descartar o pacote)
  - As regras seguintes aquela que foi igualada já não são verificadas
  - Se um pacote não igualar nenhuma das regras existentes é aplicada uma acção que foi pré-definida. Existem dois tipos de acções pré-definidas:
    - Tudo o que não for explicitamente permitido é negado
    - Tudo o que não for explicitamente negado é permitido

Tipos de *firewall* (4)

- Filtragem de pacotes (cont.)
  - Vantagens
    - Desempenho
  - Desvantagens
    - Não examinam a informação nas camadas superiores à do transporte.
    - A informação contida nos logs é limitada
    - A maioria destas firewall não suportam autenticação dos utilizadores
    - É muito difícil detectar ataques por IP *spoofing*
    - É fácil cometer erros de configuração

Tipos de *firewall* (5)

- *Gateway* de aplicações
  - Também são conhecidos por proxys
  - Os utilizadores ligam-se ao proxy por telnet ou FTP e autenticam-se
  - Se a autenticação for aceite o proxy estabelece a ligação com o serviço pretendido (nunca deixa que a ligação seja feita directamente)
  - Como o proxy conhece os protocolos pode-se limitar o uso de alguns comandos desses protocolos

Tipos de *firewall* (6)

- *Gateway* de aplicações (cont.)
  - Vantagens:
    - Mais fácil de configurar sem enganos
    - Mais seguros que as firewalls de pacotes
    - Log's com mais informação
  - Desvantagens:
    - Todo o tráfego (de entrada e saída) tem de ser monitorizado ao nível da aplicação, por isso são mais lentas

Tipos de *firewall* (7)

- *Gateway* de circuitos
  - São o meio termo entre as firewalls de filtragem de pacotes e os gateways de aplicações
  - São necessárias 2 ligações (como no gateway de aplicações), uma para o gateway e outra do gateway para o serviço
  - No entanto o conteúdo não é analisado, permitindo um maior desempenho
  - A segurança reside na especificação dos circuitos que são ou não permitidos

Tipos de *firewall* (8)

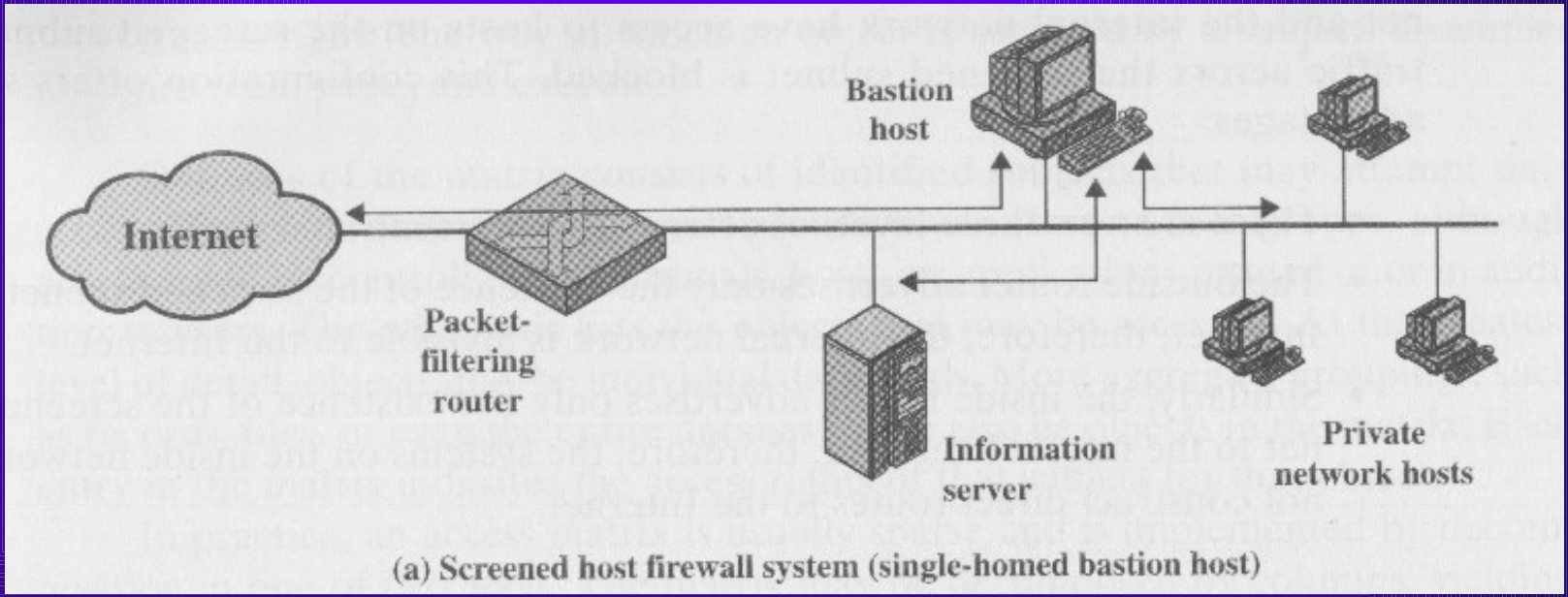
- *Gateway* de circuitos (cont.)
  - Esta solução é empregue quando existe confiança nos utilizadores da rede privada
  - Um exemplo deste tipo de firewalls é o SOCKS
  - Também é necessário efectuar autenticação dos utilizadores

Configurações típicas (1)

- Normalmente são usados mais do que um tipo de firewall numa organização para se poder tirar partido das vantagens de cada uma delas.

Configurações típicas (2)

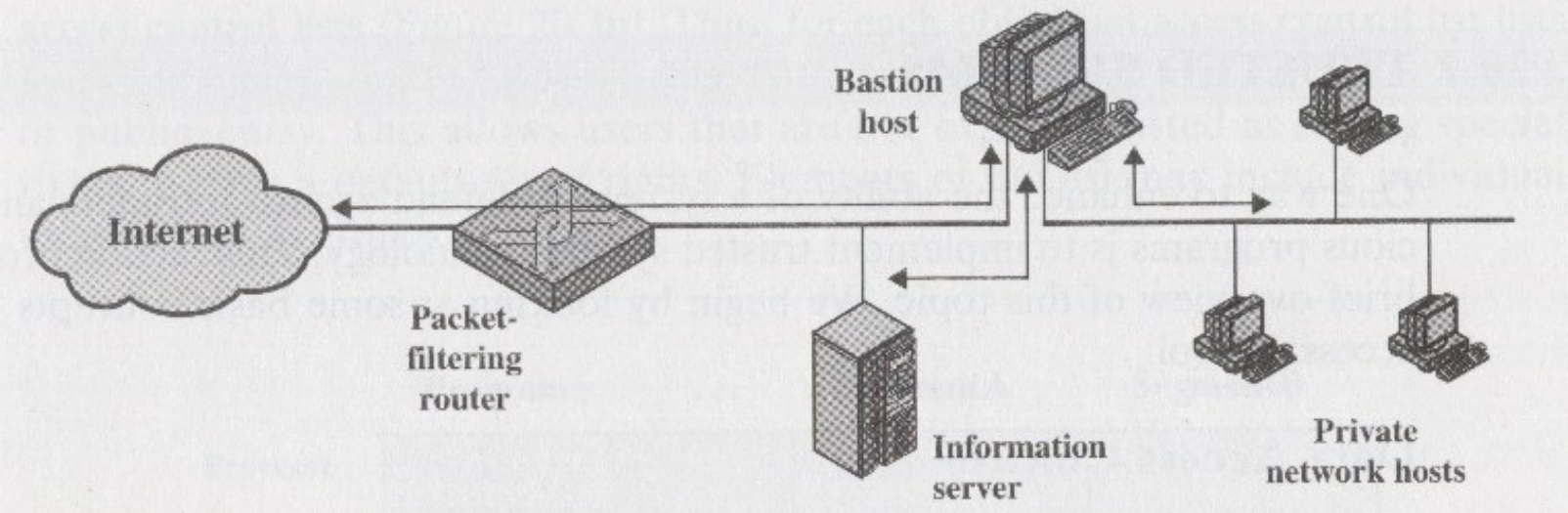
- Configuração simples



(a) Screened host firewall system (single-homed bastion host)

Configurações típicas (3)

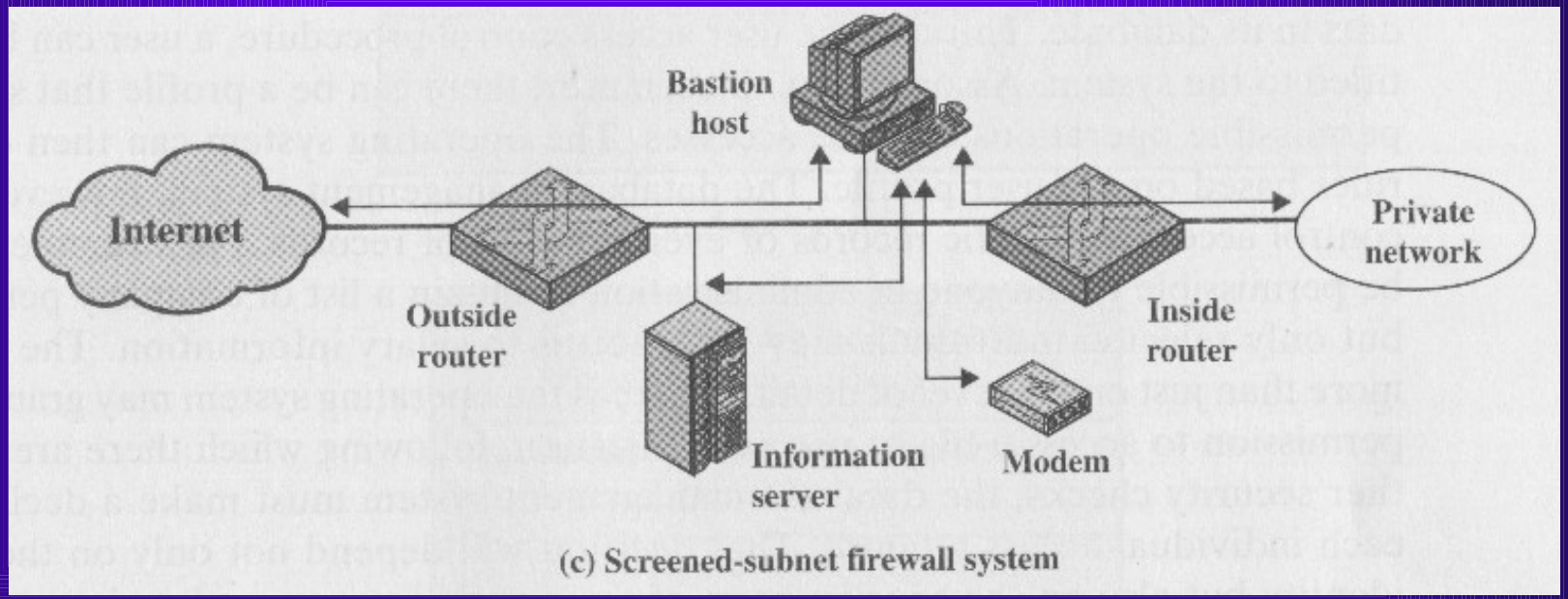
- Configuração com separação das redes



(b) Screened host firewall system (dual-homed bastion host)

Configurações típicas (4)

- Configuração DMZ



(c) Screened-subnet firewall system

Aplicações Firewall (1)

- Windows
  - Sygate Personal Firewall (freeware)
  - Tiny Personal Firewall (freeware)
  - Kerio Personal Firewall (freeware)
  - ZoneAlarm
  - LooknStop
  - AtGuard
  - etc

Aplicações Firewall (2)

- Linux
  - Netfilter/Iptables (freeware)
    - Ferramentas:
      - Guarddog
      - FireHOL
      - Easy Firewall Generator
  - Squid proxy (freeware)
  - SmoothWall
  - etc

Netfilter/IPtables (1)

- Já vem instalada na maior parte das distribuições de Linux, incluindo o Kanotix
- Se não estiver instalada de raiz pode ser necessário recompilar o Kernel
- É uma *firewall* de filtragem de pacotes *statefull*
- A sua configuração é feita na linha de comandos, manualmente ou através de *scripts*

Netfilter/IPtables (2)

- Contém 3 listas de base para escrevermos as regras de filtragem, cujos nomes são:
  - INPUT
  - OUTPUT
  - FORWARD
- Devemos definir a política por omissão para cada lista
  - Negar tudo: `iptables -P <nome da lista> DROP`
  - Aceitar tudo: `iptables -P <nome da lista> ACCEPT`

Netfilter/IPtables (3)

- Exemplo da definição da política por omissão "negar tudo"
  1. Iniciar a sessão como **root**
  2. Criar um ficheiro para fazer a *script* de configuração **`touch firewall.sh`**
  3. Dar permissões de execução **`chmod 700 firewall.sh`**
  4. Editar o ficheiro firewall.sh e escrever:

```
#!/bin/sh

# politica por omissão: negar tudo
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# eliminar regras
iptables -F
```

Netfilter/IPtables (4)

- Criar um ficheiro para desactivar a firewall
  1. Iniciar a sessão como **root**
  2. Criar um ficheiro para fazer a *script* de configuração **touch desactiva_firewall.sh**
  3. Dar permissões de execução **chmod 700 desactiva_firewall.sh**
  4. Editar o ficheiro desactiva_firewall.sh e escrever:

```
#!/bin/sh

# politica por omissão: negar tudo
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

# eliminar regras
iptables -F
```

Netfilter/IPtables (5)

- Testar as scripts:
  - Verificar o acesso à Internet
  - Na linha de comando escrever: `./firewall.sh`
  - Verificar novamente o acesso à Internet e fazer `ping 127.0.0.1`
  - **Conseguem ligação?**
  - Na linha de comando escrever: `./desactivar_firewall.sh`
  - Verificar novamente o acesso à Internet
  - **E agora?**

Netfilter/IPtables (6)

- Adicionar ao ficheiro `firewall.sh` as regras para permitir o todo o tráfego da interface loopback (127.0.0.1)
  - `iptables -A INPUT -i lo -j ACCEPT`
  - `iptables -A OUTPUT -o lo -j ACCEPT`

Na interface "loopback" no sentido de entrada

Adicionar à lista OUTPUT

Na interface "loopback" no sentido de saída

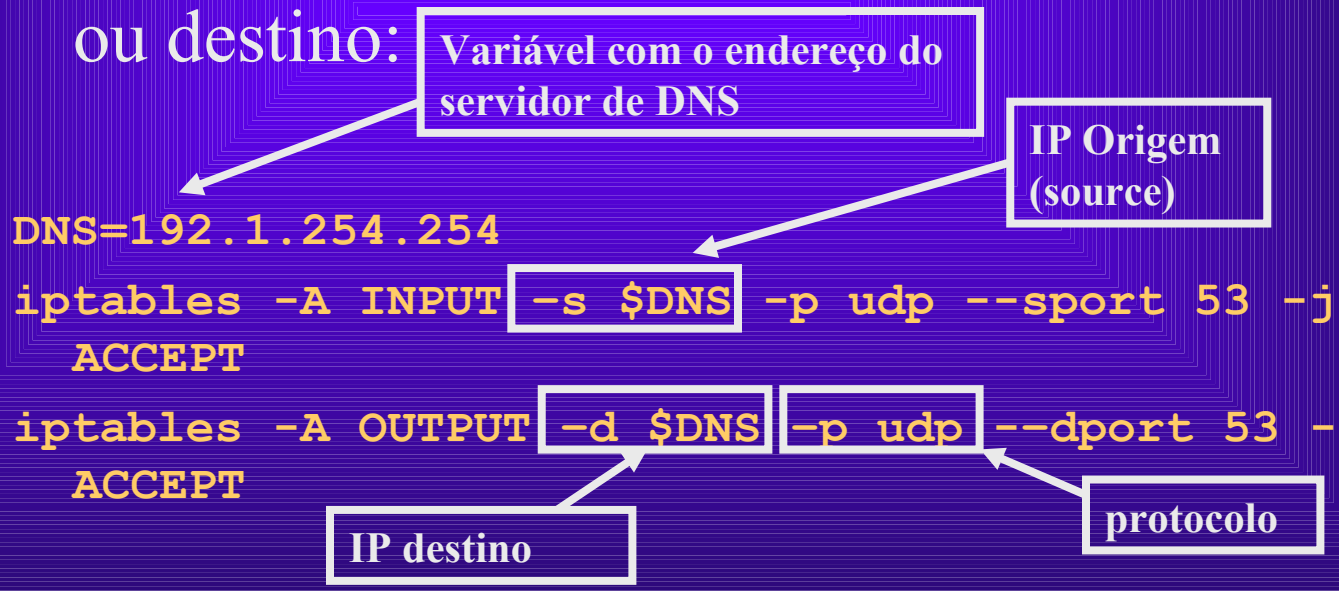
Destino "aceitar"

Netfilter/IPtables (7)

- Testar as regras
  - Executar a script (como *root*): `./firewall.sh`
  - Fazer: `ping 127.0.0.1`
  - **Conseguiram ligação?**
  - Fazer: `ping 192.1.254.254`
  - **Conseguiram ligação?**

Netfilter/IPtables (8)

- Regras para permitir o DNS
  - `iptables -A INPUT -p udp --sport 53 -j ACCEPT`
  - `iptables -A OUTPUT -p udp --dport 53 -j ACCEPT`
  - Também podemos acrescentar o IP de origem ou destino:



Netfilter/IPtables (9)

```
#!/bin/sh

# variáveis
DNS=192.1.254.254

# politica por omissão: negar tudo
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

iptables -F # eliminar regras anteriores

# loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# DNS
iptables -A INPUT -s $DNS -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d $DNS -p udp --dport 53 -j ACCEPT
```

A configuração que temos até agora

Netfilter/IPtables (10)

- Exercício: Acrescentar regras ao ficheiro anterior para permitir:
  - ping (entrar e sair)
  - http para o *proxy* no porto 8080
  - messenger (porto 1863)
  - ssh (entrar e sair)
    - é necessário verificar se servidor SSH está activo
  - samba (entrar e sair)
    - é necessário activar o servidor para efectuar os testes: na linha de comandos, como *root*, fazer:

```
/etc/init.d/samba start
smbpasswd -a root
```

Cuidados – Tráfego de entrada (1)

- Eliminar os pacotes cujos endereços de origem correspondem aos endereços usados na rede interna (ver RFC 2827).
- Permitir as ligações TCP apenas se forem iniciadas a partir da rede interna.
- Todas as outras ligações (da Internet para a rede interna) só devem poder aceder aos servidores na DMZ.

Cuidados – Tráfego de entrada (2)

- Eliminar os pacotes dos protocolos BOOTP, Trivial File Transfer Protocol (TFTP) e traceroute.
- Eliminar os pacotes IP designados por bogon. Estes endereços não são privados, mas normalmente são endereços IP reservados que não devem ser usados. Lista de endereços IP bogon agregada:
  - http://www.cymru.com/Documents/bogon-bn-agg.txt

Cuidados – Tráfego de saída (1)

- Permitir apenas a saída de pacotes para a Internet cujos endereços de origem correspondem ao da rede interna.
- Eliminar os pacotes cuja saída da rede interna não é permitida pela política de segurança

Cuidados – Tráfego de saída (2)

- Ter sempre em conta os seguintes aspectos:
  - Desligar serviços não usados, portos ou protocolos.
  - Limitar o acesso aos serviços, portos ou protocolos. Por exemplo se existir um número limitado de utilizadores com necessidade de usar um serviço específico, limitar o acesso apenas a esses utilizadores.