ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Firewalls

ISEL – Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 | 1959-007 Lisboa

Filtragem estática

- Observa os campos dos cabeçalhos dos pacotes
  - Endereços IP de origem/destino
  - Porto de origem/destino
  - *Flags*
- Cada pacote é avaliado individualmente
- Não mantém informação sobre o estado de uma ligação
- Pode deixar passar pacotes manipulados

Problemas com a filtragem estática

- Não inspeciona o conteúdo dos pacotes

- Causa problemas em protocolos complexos
  - Múltiplas ligações
  - Portos aleatórios
  - Ligações entre pares
  - Tráfego ICMP
    - A mensagem que originou o erro vai no conteúdo do pacote ICMP

Utilização de *firewalls* estáticas

- Filtragem na entrada (*ingress*)
  - Pacotes com endereços IP da rede interna, loopback
  - Endereços IP de origem privados ou reservados
- Filtragem na saída (*egress*)
  - Deixar sair apenas pacotes do nosso espaço de endereçamento
- Entrada e Saída
  - Ligações para serviços críticos
- Opções específicas
  - Filtrar pacotes com opções (*source routing*)

Filtragem na entrada (1)

- Pacotes com IP da rede interna
  - Previne o *spoofing*
  - Funciona na mesma se for sobre uma VPN
- Endereço *loopback*
  - O 127.0.0.1/8 nunca deve circular na rede
- Endereços de broadcast
  - Usado para *probes*
- ICMP
  - Echo-request
  - Redirects

Filtragem na entrada (2)

- Endereço IP de origem privados ou reservados
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 169.254.0.0/16
  - 0.0.0.0/8
  - 192.0.2.0/24
  - 192.0.0.0/24, 198.18.0.0/15, 198.51.100.0/24, 203.0.113.0/24
  - 224.0.0.0/4
  - 240.0.0.0/4
- Endereços IP não alocados
- Endereço IP da própria *firewall*
- E IPv6…

Filtragem na saída

- Deixar sair apenas pacotes cujo endereço de origem seja o nosso
  - Bloqueia tentativas de *spoofing* internas
  - É boa vizinhança
  - Identifica *hosts* comprometidos
- Registar o endereço MAC para identificar o infrator
- SMTP
  - Filtrar tudo exceto o que venha do nosso servidor de e-mail
- IRC
  - Utilizado por *bots*
- …
- Filtrar tudo o que se desconheça!

Entrada/Saída

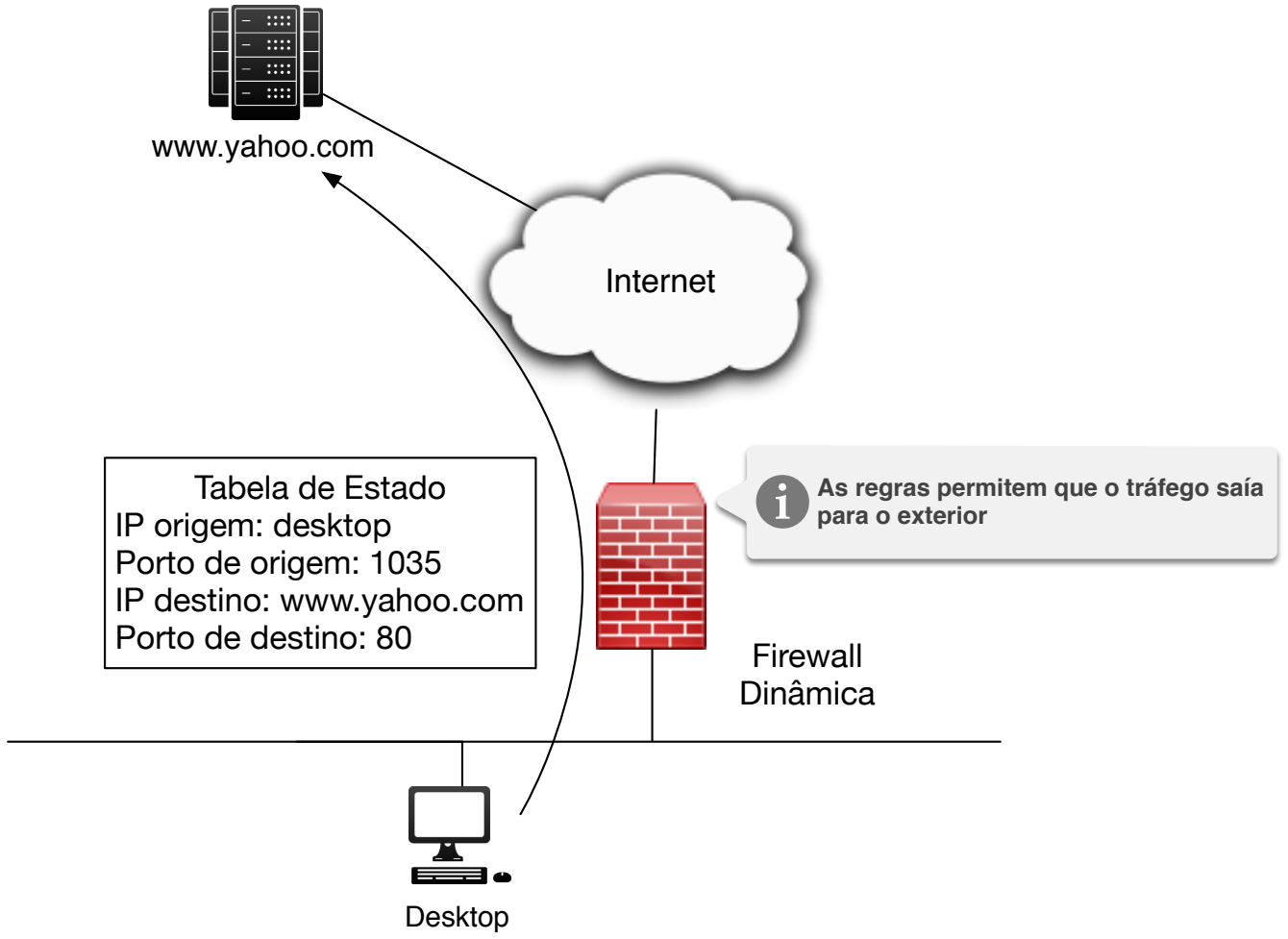
- Serviços críticos
  - Ambientes Windows
    - TCP/UP 135-139 e 445 (SMB, CIFS)
  - Unix
    - TCP 23, 22, TCP/UDP 111, 2049 (RPC, NFS, X)
  - Em geral
    - DHCP, SNMP
  - Opções como *source routing* ou *record route*
- Casos especiais
  - Tráfego sobre SSH ou IPSec

Filtragem dinâmica / com estado

- É mantido o estado das ligações
- Lembra-se do tráfego anteriormente permitido
- Identifica as respostas a pedidos anteriormente feitos
  - As correspondências podem ser aceites
  - As não correspondências são rejeitadas

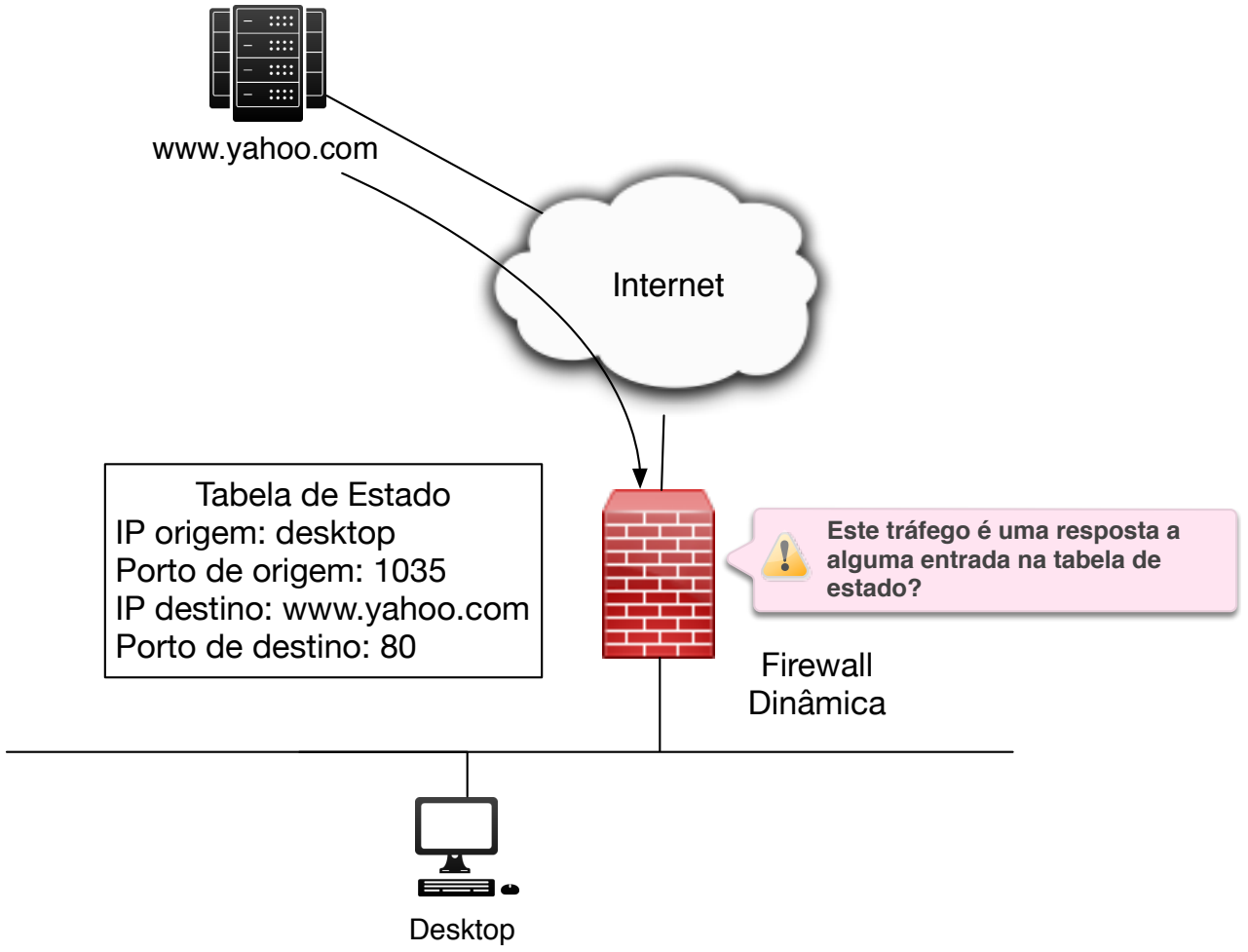
Filtragem dinâmica

Como funciona?



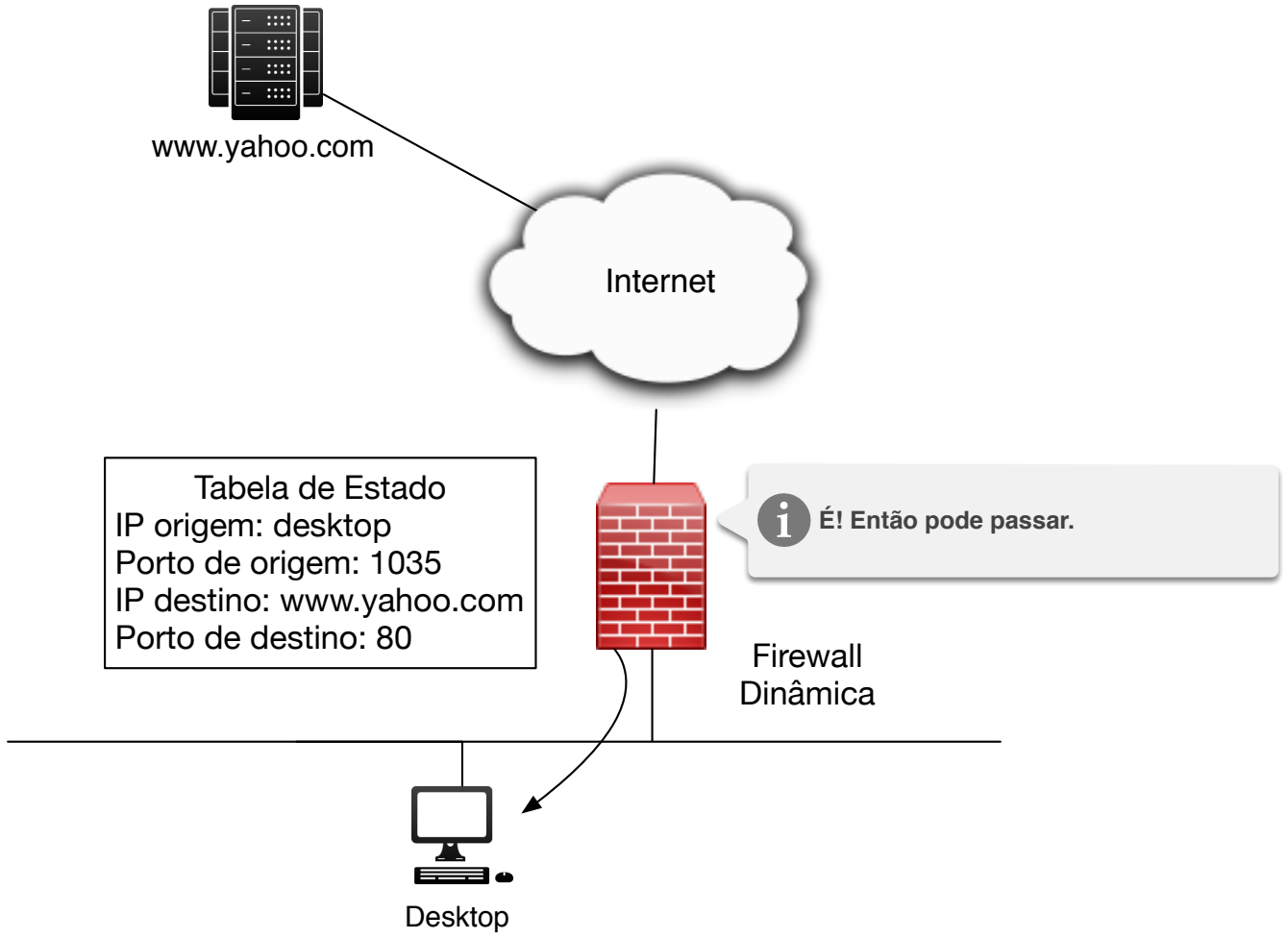
Filtragem dinâmica

Avaliação das respostas



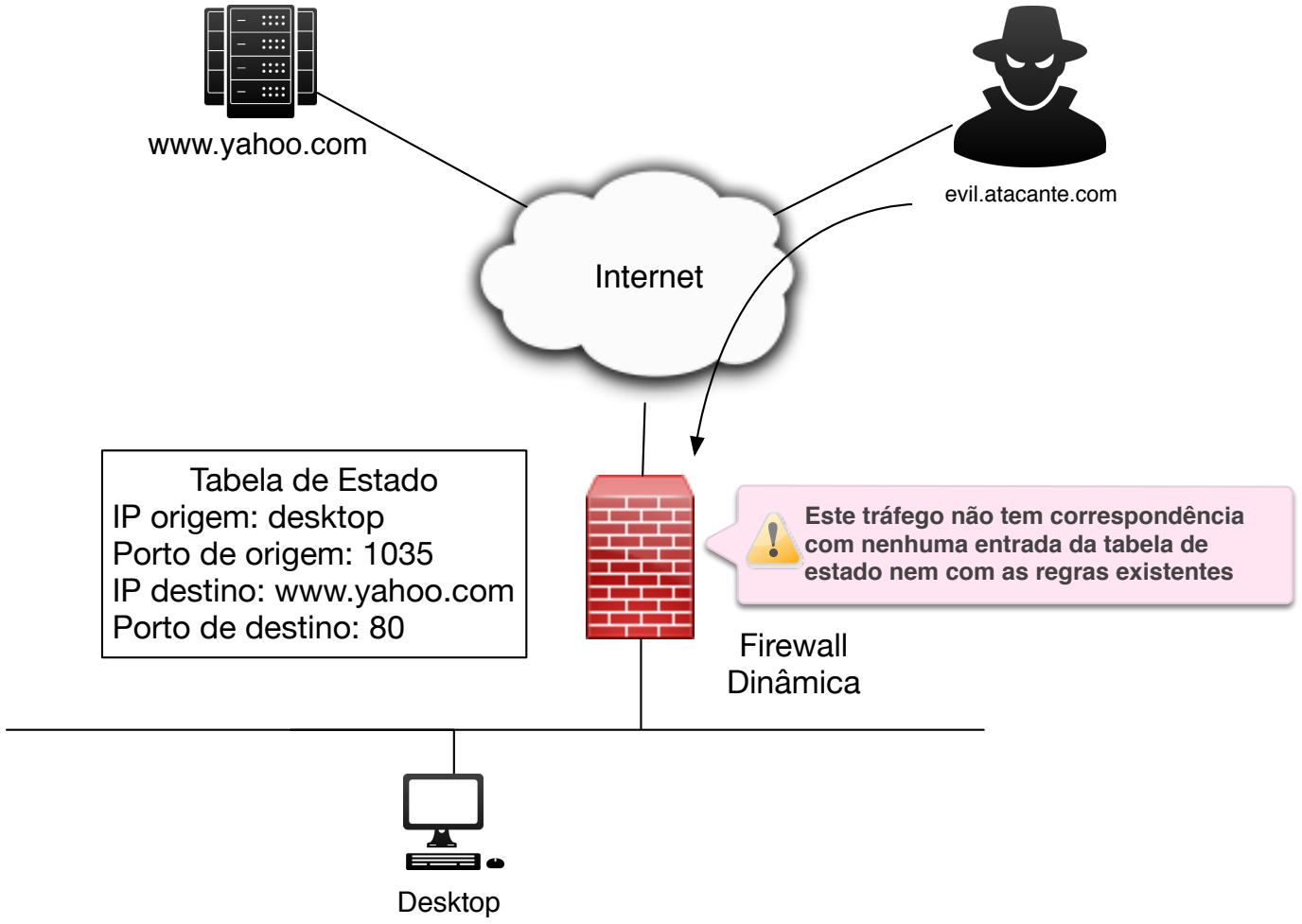
Filtragem dinâmica

Permitir os pacotes com correspondência



Filtragem dinâmica

Pacotes de um atacante



O que é avaliado?

- Endereços IP de origem e destino
- Portos de origem e destino
  - Apenas para TCP e UDP
- Tipos de pacotes ICMP
- Extras
  - Números de sequência
  - Flags

Remoção de entradas da tabela de estado

As entradas existem sempre até que:

- A ligação termine (TCP)
  - RST enviado
  - Troca de FIN/ACK
- Um contador expire
  - Útil para UDP
  - Expira apenas se não existirem dados a circular
- Pode provocar problemas com alguns protocolos
  - Respostas que demoram mais tempo que o contador a expirar

Exemplo de uma tabela de estados

```
tcp      6 30 TIME_WAIT src=85.246.154.85 dst=193.137.100.233 sport=58193 dport=443
src=193.137.100.233 dst=85.246.154.85 sport=443 dport=58193 [ASSURED] mark=0 use=1

udp      17 0 src=194.210.204.154 dst=8.8.8.8 sport=61025 dport=53
src=193.137.220.130 dst=194.210.204.154 sport=53 dport=61025 mark=0 use=1

tcp      6 10821 ESTABLISHED src=194.210.198.247 dst=64.233.167.188 sport=33120
dport=5228 src=64.233.167.188 dst=194.210.198.247 sport=5228 dport=33120 [ASSURED]
mark=0 use=1

udp      17 26 src=193.137.129.118 dst=8.8.8.8 sport=58097 dport=53 src=8.8.8.8
dst=193.137.129.118 sport=53 dport=58097 mark=0 use=1

tcp      6 118 SYN_SENT src=194.210.203.38 dst=1.32.72.35 sport=54617 dport=25238
[UNREPLIED] src=1.32.72.35 dst=194.210.203.38 sport=25238 dport=54617 mark=0 use=1

tcp      6 336106 ESTABLISHED src=10.10.5.106 dst=64.233.166.188 sport=39532
dport=5228 src=64.233.166.188 dst=194.210.186.172 sport=5228 dport=39532 [ASSURED]
mark=0 use=1
```

Limitações

- Funciona como um semáforo num cruzamento

- Espera-se que o tráfego em determinado porto seja pré-definido
  - Exemplo TCP/80 é **suposto** ser WEB, mas na realidade pode ser outra coisa qualquer

- Não existe nenhuma verificação do conteúdo

- Ataques às aplicações podem não ser detetados
- VPNs podem ultrapassar as *firewalls*
- Existem outras áreas em que a *firewall* não tem impacto
  - Passwords
  - Atualizações
  - Cifra

Módulos Extra

- Extras para *firewalls* dinâmicas

- Adicionam conhecimento sobre alguns protocolos
  - FTP
  - VoIP

- Analisam as mensagens trocadas para extrair conhecimento
  - Mensagens FTP para extrair portos das ligações FTP-DATA
  - Mensagens SIP para extrair portos dos dados multimédia (protocolo RTP)

Exemplos

Cisco:

```
ip access-list extended redemaissegura
 permit tcp 10.10.0.0 0.0.255.255 gt 1023 any eq 80
 permit ip any any
exit
```

Linux/Netfilter:

```
iptables -A INPUT -p icmp --icmp-type 8/0 -j ACCEPT

iptables -A FORWARD -m conntrack –ctstate RELATED,ESTABLISHED -j ACCEPT
```

Resumo

- Filtragem estática
  - Cada pacote é analisado isoladamente
  - Apenas é verificado os campos dos cabeçalhos dos pacotes
  - Bom para condições absolutas
- Filtragem dinâmica (com estado)
  - Adiciona a capacidade de se lembrar dos pacotes para mais tarde tomar decisões
  - Melhor controlo do tráfego
  - Não tem a capacidade de analisar o conteúdo
    - Exceto para alguns protocolos em particular