POLITÉCNICO DE LEIRIA

FIREWALLS

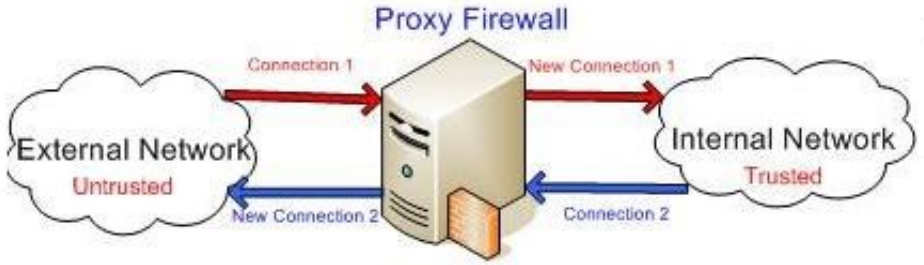
SQUID

Curso de Engenharia Informática 3º ano – Segurança de Sistema

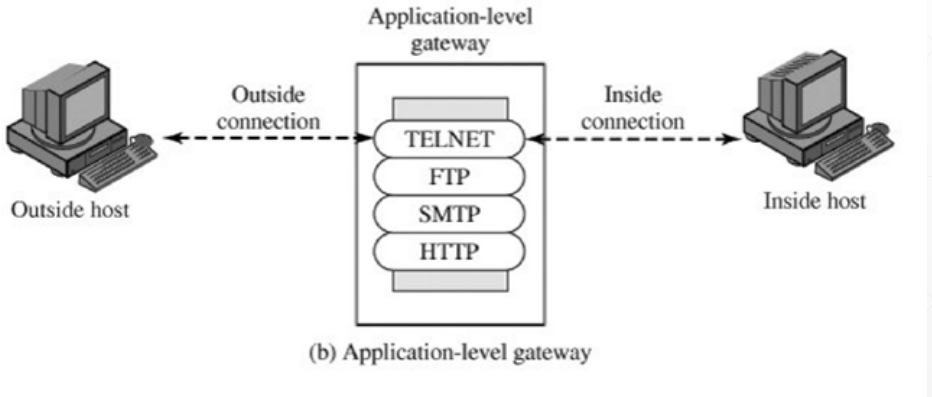
© 2020 **Miguel Frade** miguel.frade@ipleiria.pt
Francisco Santos francisco.santos@ipleiria.pt

Firewall - Filtragem na camada de aplicação

- É um programa executado dentro da firewall.
  - Application gateway | Application proxy | Application-level proxy
  - Proxy web | Telnet | SMTP | FTP



- Exemplo: Proxy WEB
  - O cliente na rede interna pede ao proxy acesso a determinado website
  - O proxy, caso autorizado, estabelece o contacto com o website pedido e age como mordomo do cliente, pedindo o website e entregando-o ao cliente.
  - São criadas duas comunicações:
    - Entre o cliente o e o proxy
    - Entre o proxy e o servidor web
- Os computadores da rede interna ficam protegidos pela firewall.
- “Deep packet inspection”



Squid

- Software de proxy
- Serve como intermediário de comunicações HTTP e FTP.
- Mais segurança e controle de tráfego web.
- Pode implementar Cache de objetos web (html, dns, etc):
  - Navegação web mais rápida
  - Menos tráfego desperdiçado
- Pode ser usado:
  - Configuração nos browser de cada cliente, informando qual é o endereço IP e o porto onde está a ser executado.
  - Automaticamente na rede, através de “proxy transparente”

Squid – instalação e controlar o serviço

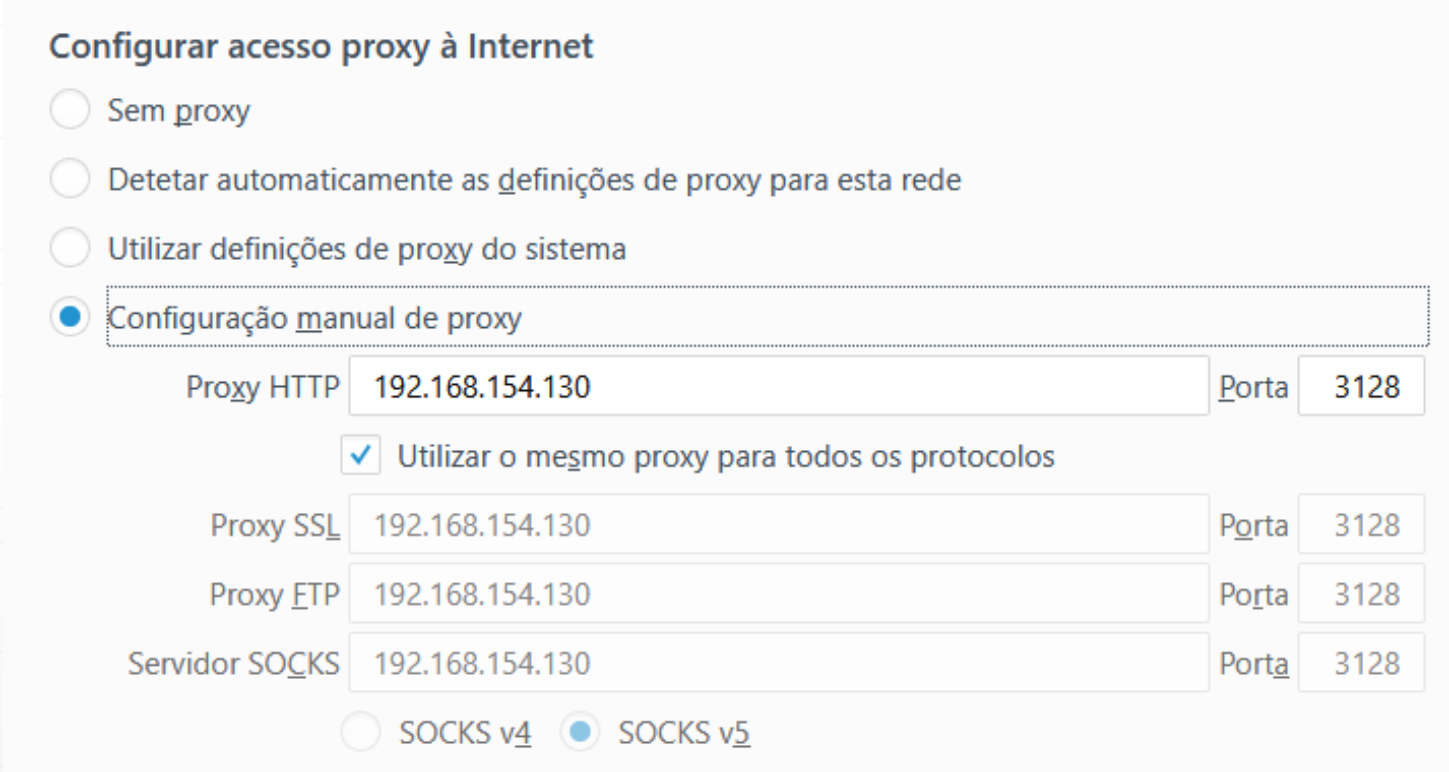
- Instalação no sistema operativo Linux Ubuntu:
  - *sudo apt install squid squid-common*

- Controlar o serviço:
  - *sudo service squid start | stop | restart | reload*
  - *sudo systemctl start | stop | restart | reload squid*

- Verificarsintaxe ds onfurações:
  - *sudo squid –k check*

Squid – configuração clientes

- Para usarem o squid, os utilizadores da rede interna precisam de configurar o browser com a informação do servidor.



Squid – Recursos do serviço

- Diretoria /etc/squid
  - Todos os ficheiros importantes de configuração.
- Diretoria /var/spool/squid
  - Ficheiros de cache para utilização
- Diretoria /var/log/squid
  - Ficheiros onde são guardadas os registos de informação/alertas

Squid – Configuração Serviço

- Ficheiro **/etc/squid/squid.conf**
  - Todas as configurações do Squid por omissão
  - Ficheiro original com toda a documentação tem cerca de 8000 linhas.
  - Para apagar toda a documentação e tornar o ficheiro mais perceptível:
    - Criar um backup do ficheiro original:
      - *sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.backup*
    - “Limpar” ficheiro de configuração e substituir o ficheiro
      - *grep -v '^#' /etc/squid/squid.conf.backup | uniq | sudo sort > ~/squid.conf*
      - *sudo cp ~/squid.conf /etc/squid/squid.conf*

Squid – Configuração Serviço

- Utiliza ACLs para definir o tipo de tráfego permitido ou negado.
- A ordem de aplicação das regras interessa (idêntico ao iptables).
- É possível também definir regras por omissão.
- Algumas tags:
  - auth (autenticação de utilizadores)
  - acl (definição das listas de controlo de acessos)
  - http_access (definições de acesso HTTP)
  - network (definições de rede)
  - logs (definições relacionadas com logs)

Squid – Configuração Mínima Recomendada

- acl all src 0.0.0.0/0.0.0.0
- acl manager proto cache_object
- acl Safe_ports port 1025-65535 # unregistered ports
- acl Safe_ports port 210 # wais
- acl Safe_ports port 21 # ftp
- acl Safe_ports port 280 # http-mgmt
- acl Safe_ports port 443 # https
- acl Safe_ports port 488 # gss-http
- acl Safe_ports port 591 # filemaker
- acl Safe_ports port 70 # gopher
- acl Safe_ports port 777 # multiling http
- acl Safe_ports port 80 # http
- acl SSL_ports port 443
- acl CONNECT method CONNECT

- coredump_dir /var/spool/squid

- http_access deny CONNECT !SSL_ports
- http_access deny !Safe_ports
- http_access allow localhost manager
- http_access deny manager
- http_access allow localhost
- http_access deny all
- http_port 3128
- coredump_dir /var/spool/squid3

Squid – Configurações

- ***# http_port [port] [opções]***
  - Define a porta onde está a ser executado o serviço Squid.
  - Exemplo: host_port 8080

- ***# visible_hostname [nome]***
  - Define o nome do Squid a ser apresentado nas páginas de erro/informação.
  - Exemplo: visible_hostname proxy.eiss.ipleiria.pt

Squid – Configurações

- Definir ficheiros de log:
  - ***access_log [ficheiro]***
    - Define o ficheiro onde são guardados as informações de acesso dos utilizadores
    - Exemplo: access_log /var/log/squid/access.log
  - ***cache_log [ficheiro]***
    - Define o ficheiro onde são guardados as informações de comportamento da cache
    - Exemplo: cache_log /var/log/squid/cache.log
  - ***Exemplo:***
    - access_log /var/log/squid/access.log squid

Squid –Error Page options

- A *tag* `error_directory` permite definir a localização das páginas de erro.
- Sintaxe:
  - `error_directory <caminho_diretoria>`
  - Exemplo:
    - `error_directory /usr/share/squid/errors/pt`

Squid – Configurações de Cache

- Para ativar a cache no proxy:
  - ***cache_mem [quantidade]***
    - Indica a quantidade de memória a ser usada para guardar dados de tráfego.
    - Exemplo: cache_mem 64 MB
  - ***cache_dir [formato] [diretoria] [quantidade em MB] [diretorias] [subdiretorias]***
    - Formato: indica o formato de armazenamento da cache
    - Diretoria: indica a diretoria onde vão ser guardadas a cache
    - Quantidade em MB: indica o espaço em disco a ser usado para cache
    - Diretorias e subdiretorias: quantidade de diretorias que serão criados para cache
    - Exemplo: cache_dir ufs /var/spool/squid 1000 16 256
      - Especifica o diretório de cache e os paramentos abaixo:
      - 1000 - Espaço em MB;
      - 16 - Quantidade de diretórios que serão criados
      - 256 - Quantidade de subdiretórios dentro dos 16 principais.

Squid – Configurações de Cache (2)

Na linha de comandos é necessário criar a estrutura de diretorias para a cache:

- **sudo squid –z**
  - Este comando deve ser realizado com o serviço **squid parado.**

- **Opção Refresh_Pattern:**
  - *usage: refresh_pattern [-i] regex min percent max [options]*

- Exemplos:
  - Para fazer cache de imagens:
    - *refresh_pattern -i \.(png|jpg|gif)$ 120 50% 86400 ignore-reload*
  - Para fazer cache de ficheiros js ou css:
    - *refresh_pattern -i \.(css|js)$ 120 50% 86400 ignore-reload*

Squid – Configurações de Cache (3)

- Informações no ficheiro de log *access.log*:
  - **TCP_MISS**
    - O objeto pedido não estava em cache;
  - **TCP_HIT**
    - O objeto pedido estava em cache;
  - **TCP_REFRESH_HIT**
    - O objeto pedido estava em cache, mas já tinha expirado.
- Mais informações em:
  - https://wiki.squid-cache.org/SquidFaq/SquidLogs#Squid_result_codes

Squid – Configurações de ACL (1)

- ACL (Access Control List):
  - Listas de controlo de acessos / Regras

  - ***acl [nome_da_ACL] [tipo] [valores/dados]***
    - Nome_da_ACL: indica um nome para a regra
    - Tipo: indica o tipo de ACL
    - valores/dados: indica as informações a inserir na ACL

Squid – Configurações de ACL (2)

- Tipos de ACL:
  - **src**: endereço de origem (*source*)
    - acl rede_interna src 192.168.1.0/255.255.255.0
  - **dst**: endereço de destino (*destination*)
    - acl sites_empresa dst 193.137.239.1/255.255.255.252
  - **dstdomain**: domínio de destino
    - acl rede_social dstdomain .facebook.com
  - **time**: indica dia da semana e hora
    - acl horario_trabalho time MTWHF 08:00-18:00

Squid – Configurações de ACL (3)

- Tipos de ACL:
  - **url_regex**: expressão regular no URL
    - acl proibir_exe url_regex -i \.exe$
  - **port**: porto de destino
    - acl porto_seguro port 80
  - **proxy_auth**: autenticação
    - acl patrao proxy_auth Manuel
    - Exige a identificação do tipo de autenticação a realizar.
    - Não funciona com proxy transparente.

Squid – Configurações de ACL (4)

- Aplicar as ACL
  - **http_access [allow|deny] [nome_da_ACL]**
    - Indica se determinada ACL tem a ação de permitir ou bloquear.
    - Exemplo:
      - http_access allow patrao
      - http_access allow horario_trabalho
  - Para negar uma ACL, usar caracter !
    - http_access deny !patrão
    - Nega todos, excepto o patrão
  - É importante a ordem das regras de ACL
  - Por omissão devem ser negado tudo no final da lista de regras de ACL
    - Exemplo: http_access deny all

Squid – Configurações de ACL (4)

- Combinando ACL
  - Podemos combinar duas ACL na mesma linha de configuração http_access

  - **# http_access [allow|deny] [nome_da_ACL] [nome_da_ACL]**
    - Exemplo:
      - http_access allow rede_local horário_trabalho
      - http_access deny rede_local

      - Permite que a rede local aceda dentro do horário de trabalho ao proxy.
      - Não permite que a rede local aceda a qualquer site.

Squid – Aplicar Configurações

- Para finalizar as configurações é necessário informar o squid que houve alterações na configuração:
  - Comando:
    - # squid –k reconfigure
    - ou
    - # /etc/init.d/squid reload
  - Quando existem erros no ficheiro de configuração, este comando informa o utilizador de que as configurações não estão corretas.

Squid – Proxy transparente

- Como fazer com que todos os utilizadores da rede usem o proxy sem terem necessidade de o configurar?
  - Resposta = Proxy transparente.
    - é completamente transparente ao utilizador.
  - Configurar o Squid com um porto adicional e com a opção intercept:
    - **http_port 3128**
    - **http_port 3129 intercept**
  - Gateway desvia todos os pedidos web para o proxy web
  - Com iptables é fácil. Duas opções:
    - **# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.1.1:3129**
    - **# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3129**

Squid – Autenticação

- Nesta secção poderemos definir e personalizar dados relativos à autenticação de utilizadores no proxy.
- A tag `auth_param` permite definir os parâmetros utilizados para a autenticação dos clientes do proxy.
- Sintaxe:
  - `auth_param <esquema> <parâmetro> [valor]`
- Tipos de esquema:
  - basic
  - digest
  - NTLM
  - negotiate

Squid – Autenticação - Exemplo

- `sudo apt install apache2-utils`
  - `sudo htpasswd -c /etc/squid/squid_passwd ss`
- Editar `/etc/squid/squid.conf`
  - `auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/squid_passwd`
  - `auth_param basic utf8 on`
  - `auth_param basic children 5`
  - `auth_param basic realm Autenticação`
  - `auth_param basic credentialsttl 2 hours`
  - `acl auth_users proxy_auth REQUIRED`

Squid – Softwares adicionais

- Existem diversos software que podem funcionar em conjunto com o Squid:
  - SquidGuard
    - Plugin do Squid.
    - Filtros de blacklists e whitelists.
  - Webalizer
    - Gera páginas de estatísticas da informação contida nos logs do squid.
  - SARG
    - *Squid Analysis Report Generator*
    - Permite ver algumas estatísticas dos sites visitados pelos utilizadores do squid.
  - Calamaris
    - Gera relatórios do uso do squid em formato html.

SQUID – Bibliografia

- man iptables
- man iptables-save
- man iptables-restore
- man squid
- Ficheiro original squid.conf