EXERCÍCIOS DE APLICAÇÃO

Firewall

A comutação de pacotes de nível 3 (“routing”) garante que os pacotes apenas são transferidos quando pertencem ao protocolo correto e o seu endereço de destino está de acordo com a configuração (“tabela de routing”). Os “routers” asseguram por isso algum grau de proteção sob o ponto de vista de segmentação. É neste tipo de dispositivo que são normalmente instalados os “firewalls”.

Os controlo de acesso pela rede tem como objetivo condicionar as transferências de informação entre diferentes zonas das infraestrutura de rede, por isso normalmente são implementados nos nós intermédios que asseguram a respetiva ligação, tipicamente os “routers”. O “software” que assegura este controlo de acesso é designado de “firewall”.
Os nós finais (clientes e servidores) também devem implementar um “firewall”, neste caso para controlar a saída de dados e especialmente a entrada de dados no nó.
Os nós intermédios (“routers”) que implementam a funcionalidade de “firewall” são eles próprios muitas vezes designados de “firewalls”.

Tipos de “firewall”

“Packet Filter”

Um “firewall” analisa o tráfego de rede e com base num conjunto de regras pré estabelecidas pelo administrador determina se a informação deve passar ou ser bloqueada (descartada).

Designa-se “firewall” estático, “packet filter” ou “screening router” um “firewall” em que as regras são estáticas e o seu comportamento é sempre igual independentemente das comunicações existentes.

As regras de filtragem são definidas com base em ACLs (“Access Control Lists”) que são percorridas sequencialmente para cada pacote analisado. Idealmente a política da ACL é bloquear, ou seja, chegando ao fim da lista sem encontrar nenhuma regra que permita explicitamente a passagem do pacote, ele deve ser bloquado.

As regras são definidas com base nas propriedades observadas no pacote, em especial: interfaces de entrada e saída, endereço de origem e destino, protocolo de transporte e números de porto de origem e destino (serviços de rede).

“Firewall” dinâmico – “Stateful Firewall”

A principal caraterística de uma “firewall” dinâmico é a de detetar contextos específicos (tipicamente ataques maliciosos) e reagir criando regras temporárias nas ACLs.

Continuam a existir regras estáticas de filtragem pacote a pacote como as do “packet filter”, mas adicionalmente são previstas situações anómalas para as quais serão automaticamente inseridas regras adicionais. Esta capacidade é designada “stateful packet inspection” (SPI).
Embora os “firewall” dinâmicos possam ser implementados em vários níveis do modelo OSI, tipicamente analisam informação acima da camada de rede, incluindo até dados transportados pelos protocolos de aplicação como HTTP ou SMTP.
Enquanto um “packet filter” analisa cada pacote individualmente, fora de contexto, os “firewall” dinâmicos fazem o seguimento da todas as trocas de informação, mantendo informação de contexto sobre conexões e sessões entre clientes e servidores.

PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Social Europeu

Os “firewalls” dinâmicos assumem o papel de ferramentas de deteção de intrusos.

“Firewalls” de aplicação e “Proxies”

Um “firewall” de aplicação tem princípios de funcionamento semelhantes ao de um “firewall” dinâmico, mas opera mais claramente na camada de aplicação analisando em detalhe as informações transferidas através dos protocolos desse nível.

Um “proxy” é um serviço de rede que funciona com intermediário no acesso a serviços de aplicação. Por exemplo no caso de um “proxy” HTTP o cliente (“browser”) não acede diretamente aos servidores HTTP, solicita ao “proxy” a página pretendida através do respetivo URL, o “proxy” obtém a página do servidor e fornece-a ao cliente.
A principal vantagem dos “proxy” é que podem manter cópias locais da informação e desta forma otimizar a utilização da ligação à “internet”. Sob o ponto de vista de segurança são o local ideal para implementar o “firewall” de aplicação.

Para cada protocolo de aplicação é necessário um “proxy” distinto, além disso o número de protocolo de aplicação que suporta o uso de “proxies” é limitado, por esta razão, em muitos casos, o “firewall” de aplicação não é associado a nenhum “proxy”.

Nos equipamentos cisco as firewalls podem ser implementadas com recurso a ACL (access control lists).

Access Control List

A filtragem de pacotes e protocolos permite-nos controlar o tipo de acessos (internos e/ou externos) que circulam na rede Essa filtragem pode ser efetuada através de uma lista de controlo de acessos (ACL Access Control List) num router

As ACL’s filtram conteúdos baseados em critérios. Os critérios diferem de acordo com o tipo de ACL. São lidas sequencialmente até encontrar uma linha que faça o match com o pacote IP em análise. Se o match não ocorrer, o pacote é descartado

Podem coexistir várias ACL’s num dispositivo, sendo diferenciadas por um número identificador E por ser uma lista, podem existir várias linhas por ACL.

Uma ACL só é processada se aplicada a um interface

- Sentido inbound: a ACL é aplica da aos pacotes que entram no router por esse interface
- Sentido outbound: a ACL é aplicada aos pacotes que saem do router por esse interface

Não podem coexistir várias ACL’s no mesmo sentido do mesmo interface, mas pode existir uma em cada sentido.

Como parâmetros de qualquer tipo de ACL temos:

- Permitir (permit) ou negar (deny) o pacote de acordocom os restantes parâmetros
- O endereço ou gama de endereços IP a analisar
- A definição de uma gama de endereços é efectuada com recurso a um par constituído por:
    - um endereço IP base
    - um wildcard

Há vários tipos de ACL's de acordo com o tipo de filtragem pretendida

Dois tipos muito utilizados são as ACL's standard e extended

Os primeiros filtram os pacotes de acordo com o endereço IP origem

Os segundos filtram os pacotes de acordo com vários critérios

- Protocolo (obrigatório)
- IP origem (obrigatório)
- IP destino (obrigatório)
- Serviço (opcional)

ACL standard

Possui um identificador (número) entre 1 e 99 há outros conjuntos de identificadores dependendo da versão do sistema operativo do dispositivo
Filtra com base no endereço IP de origem

Sintaxe

access-list identificador [permit/deny] endereço_ip wild-card [log]

A opção log envia uma mensagem para a consola sempre que houver um match (pode não estar disponível na versão do IOS)

ACL extended

Possui um identificador (número) de 100 a 199

Há outros conjuntos de identificadores dependendo da versão do sistema operativo do dispositivo
Filtra os pacotes baseadas no protocolo, endereço origem, no endereço destino e opcionalmente no serviço (porto)

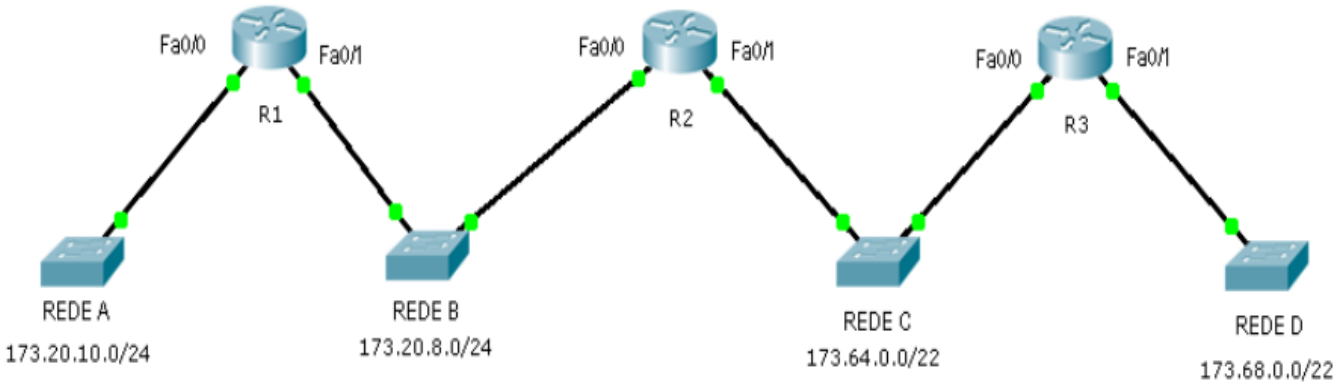
Sintaxe

access-list identificador [permit/deny] protocolo ip_origem wildcard_origem ip_destino wildcard_destino [comparação porto_destino | tipo | [established] [log]

Exemplo:

access-list 100 permit ip any 192.168.0.0 0.0.0.3

1. Quatro redes (A; B; C e D) estão interligadas por três “routers” (R1; R2 e R3) de acordo com o diagrama seguinte:



Escreva os comandos (CISCOIOS) a utilizar nos “routers” para implementaras seguintes regras de acesso:

- A rede A pode enviar para as redes C e D, mas não para a rede B;

- Da rede B, os nós 173.20.8.192 e 173.20.8.208 podem enviar para todas as outras redes, mas os restantes nós da rede B apenas podem enviar para a rede D;

- As redes C e D podem enviar para todas as redes.