Universidad de La Laguna

Laboratorio de redes

Práctica 8. Seguridad básica (FW y NAT)

Clemente Barreto Pestana
cbarretp@ull.edu.es
Profesor Asociado

Área de Ingeniería Telemática
Departamento de Ingeniería Industrial
Escuela Superior de Ingeniería y Tecnología

Introducción

Firewall (en RouterOS): Un FW proporciona seguridad filtrando los paquetes que pasan a través de él.

- Se basa en el uso de **cadenas** (chains).
  - Hay 3 **por defecto**:
    - Input: tráfico dirigido al FW
    - forward: tráfico que atraviesa el FW
    - output: tráfico que genera el FW
  - Cadena(chain) = **conjunto de reglas**.
- **Regla** = **patrón** + **acción**
  - **patrón**:
    - basado en tráfico (campos paquete): *src-address y dst-address, src-port y dst-port, protocol, in-interface y out-interface, icmp-options, ..*
    - basado en estado (conexión): *si el paquete pertenece a una conexión previa: connection-state=....*
  - **acción**: accept, drop, jump, ...

Introducción

Firewall - RouterOS (II):

- **Procesamiento**.
  - Cuando un paquete entra/sale/atraviesa el firewall.
  - Pasa a la cadena por defecto (input/ouput/forward).
  - Se analiza en orden una a una las reglas de la cadena.
  - Si hay match en una regla, se **ejecuta la acción y no sigue con el resto** de reglas.
  - Si NO hay match se deja pasar (**implicit allow**).
- **Organización de reglas**: mejora de eficiencia y administración
  - Cadenas personalizadas (para anidar con las default):
    - Crear nueva cadena.
    - Añadir salto (jump) desde cadena (por defecto): p.e.:
      - forward
        - jump trafico_tcp
          - jump trafico_80
        - jump icmp
        - drop

Introducción

Seguridad perimetral:

- **Amenazas**:
  - Sniffing o snooping:
    - Escuchar el tráfico y ver contenido (criptografía).
  - Modificación de datos:
    - Alterar el contenido (criptografía).
  - Spoofing:
    - Suplantar identidad.
    - IP Spoofing
      - Entrada: filtrar direcciones privadas (generales o utilizadas internamente), multicast, loopback, clase E, ..
      - Salida: filtrar las que no tengan como origen las direcciones privadas empleadas.

Introducción

Seguridad perimetral:

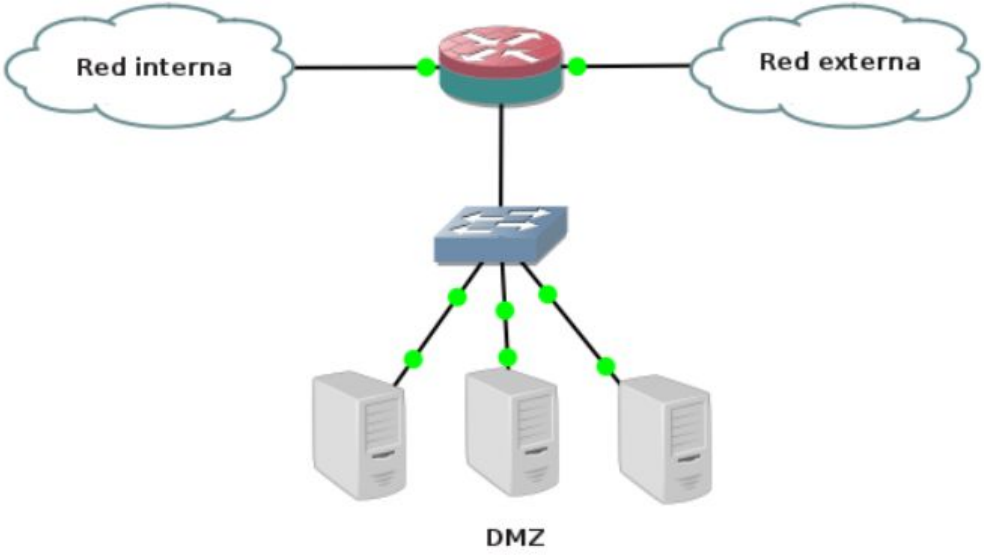
- **Amenazas (II)**:
  - Ataques de fuerza bruta:
    - Descubrimiento de contraseñas (Autenticación de dos factores: 2FA).
  - Denegación del servicio (DoS):
    - Bloquear servicio con peticiones masivas (limitarlas).
  - Hombre en el medio:
    - Colocarse en medio de la comunicación entre dos partes interceptando todos los mensajes.

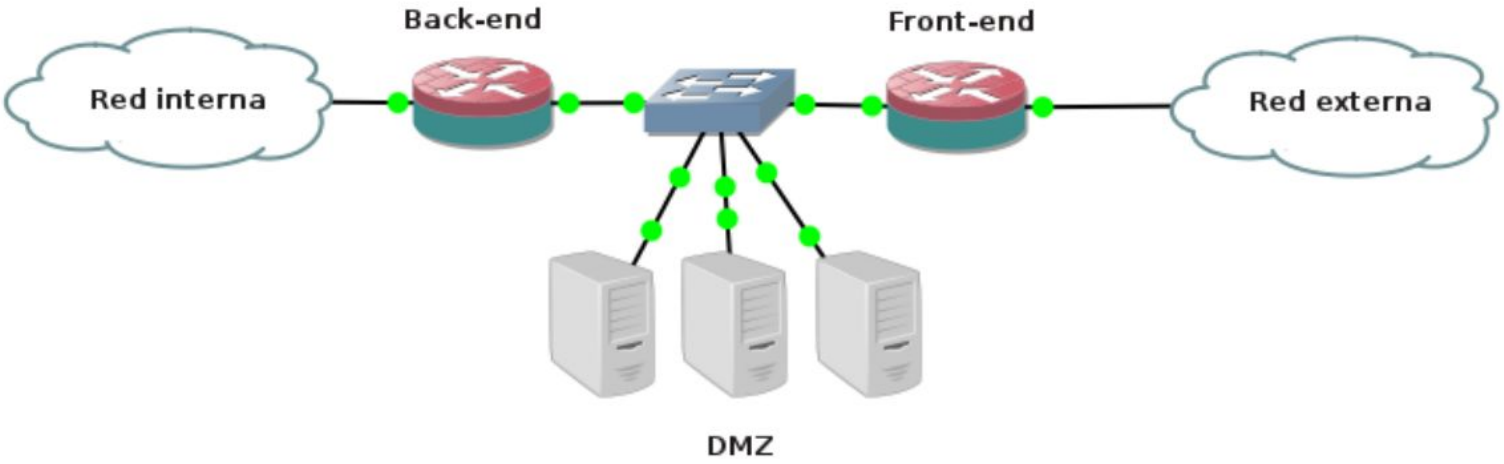
Introducción

Seguridad perimetral:

- **Arquitecturas de seguridad**:
  - Subredes separadas por cortafuegos/fw.
  - Cada subred tiene equipos con requisitos de seguridad similares → Minimizar reglas.
  - Nunca acceso directo desde subredes no confiables a subredes confiables:
    - p.e.: acceso desde Internet a recursos en red interna → subred especial: DMZ (Demilitarized Zone).
      - Una capa
      - Dos capas (dual)
      - Tres capas

Introducción





Introducción

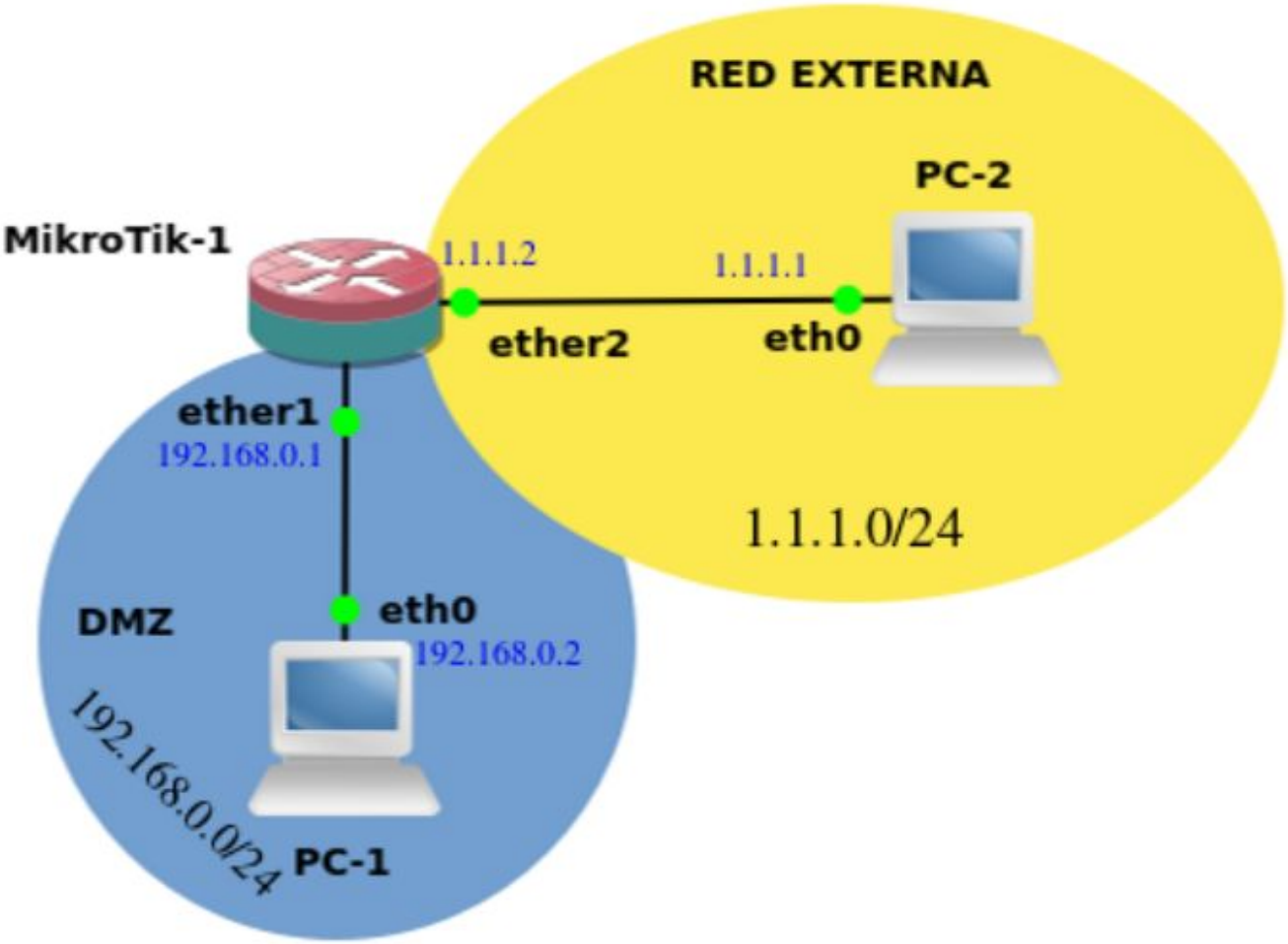
Seguridad perimetral:

- **NAT Network Address Translation**:
  - Modifica la dirección y/o el puerto de los paquetes IP.
  - Objetivo:
    - Ahorro de Dir IPv4.
    - Valor añadido en seguridad.
      - Oculta el direccionamiento interno.
  - Tipos según mapeo:
    - **one-to-one (static NAT)**: 1 IP priv <-> 1 IP púb.
    - **many-to-many (dynam. NAT)**: N IP priv <-> N IP púb.
    - **many-to-one (PAT)**: N IP priv <-> 1 IP púb + Port
  - Tipos según sentido:
    - **Source Nat**: salida navegación a Internet (desde una red nateada).
    - **Destination Nat**: para entrada de tráfico a servicios publicados (hacia una red nateada).

PARTES

- **I Montaje (laboratorio)**

I. Montaje de la práctica



I. Comandos FW en Mikrotik (I)

/ip firewall filter ... (los restantes comandos desde aquí)

Añadir regla a la cadena forward

add **chain**=forward **src-address**=127.0.0.0/8 **action**=drop
add chain=forward action=accept

Ver contenido de la cadena forward

print **chain**=forward

Crear cadena personalizada y añadir salto

add chain=trafico_tcp **protocol=tcp** dst-port=69 action=drop
add chain=forward **protocol=tcp** action=**jump** **jump-target**=trafico_tcp

I. Comandos FW en Mikrotik (II)

Mover reglas (de orden)

add chain=forward src-address=10.0.0.0/8 action=drop
in-interface=ether2 **place-before=0**
move 0 2

Crear reglas basadas en estado

add chain=forward protocol=tcp **connection-state=invalid**
action=drop
add chain=forward **connection-state=established**
action=accept
add chain=forward **connection-state=related**
action=accept (protocolos que usan varios puertos)


Universidad
de La Laguna