# Clase de Seguridad - Parte I

## Capa de (?)

DC - FCEyN - UBA

31 de Octubre de 2017

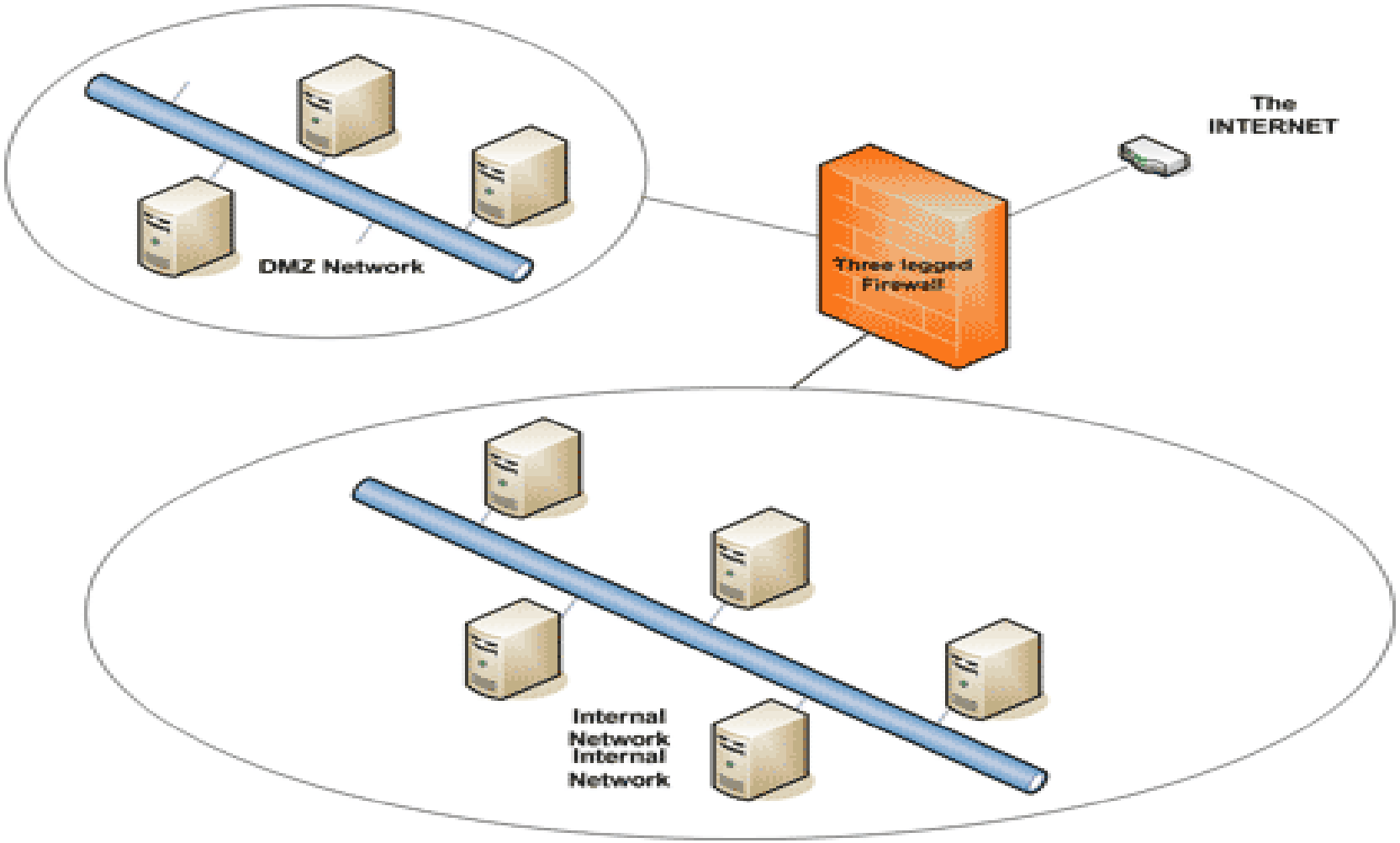
# Menú del día

1. Modelos de seguridad
   - Firewalls
2. Ejercicio Firewalling
   - Stateless
   - Stateful
   - Cerrando

# Definición

Conjunto de sistemas encargado de mediar todas las comunicaciones entre dos redes implementando una política de seguridad de **control de acceso** mediante el **filtrado de paquetes**. Esencialmente verifica cada paquete independientemente de los demás y permite o denegado su paso dependiendo de un **conjunto de reglas**.

# Definición


The
INTERNET
DMZ Network
Three legged
Firewall
Internal
Network
Internal
Network

# Distintos tipos

- **Stateless**: Utiliza reglas sencillas sobre los mensajes entrantes / salientes del tipo:
  $< dir_{origen}, puerto_{origen}, dir_{dst}, puerto_{dst}, protocolo >$
- **Stateful**: Mantiene estado de conexiones entrantes o salientes y puede permitir o denegar teniendo en cuenta la sesión a la que pertenece.
- **Gateways de aplicación**: Proxy inteligente. Entiende ciertos protocolos. Sirve para aplicar filtros de capa de aplicación.

# Demo iptables

## Requisitos

1. Acceder a cualquier PC con Linux.
2. Cargar el módulo de kernel
   **modprobe ip_tables**
3. Levantar server escuchando en el puerto 8081
   **python -m SimpleHTTPServer 8081**

## iptables 101

- -L sirve para listar las reglas existentes.
- -F sirve para eliminar todas las reglas existentes.
- -p indica el protocolo que se quiere bloquear (tcp, udp)
- -A indica que se quiere agregar una regla mientras que -D que se quiere borrar.

# Demo iptables

## Ejercicio

1. Bloquear con firewall iptables
   **sudo iptables –A INPUT –p tcp ––dport 8081 –j REJECT**
2. Bloquear con firewall iptables
   **sudo iptables –A INPUT –p tcp ––dport 8081 –j DROP**

Cuál es la diferencia? Cómo puedo probar que mis reglas funcionan ?

## Lo mismo pero de otra forma

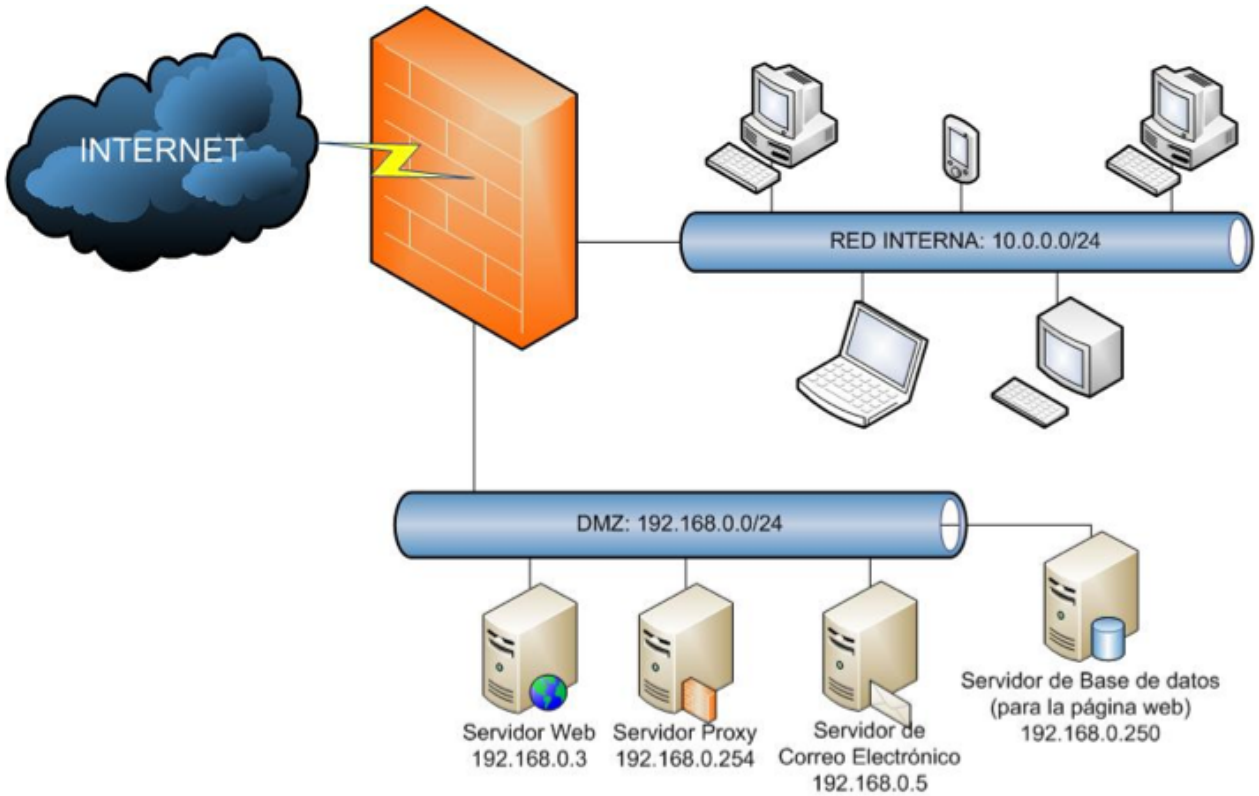
1. Cambiar política por defecto
   **sudo iptables –P INPUT DROP**
2. Aceptar conexiones solo al server
   **sudo iptables –A INPUT –p tcp ––dport 8081 -j ACCEPT**

# Referencias

- Artículo con info para setup de iptables
  **https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-iptables-on-ubuntu-14-04**
- Generador online de script para armar iptables
  **http://www.mista.nu/iptables/**

# Práctica 9

Definir reglas y políticas de seguridad a implementar en un firewall stateful la siguiente organización.



# Dato

- Servidor de mail usa POP3 e IMAP.
- Servidor web usa solo HTTP.
- El servidor web es autónomo, no necesita resolver nombres ni salir a inet.
- El servidor de bd solo se usa para los sitios web.
- Los usuarios de la red interna pueden acceder a:
  1. Servidor de mail para envío y recepción de correo.
  2. Servidor proxy para navegar internet.
  3. Servidor web de la intranet de manera directa.

# Esquema

| DESDE□HACIA | INTERNET | DMZ | RED INTERNA |
|---|---|---|---|
| INTERNET | | Servidor Web: HTTP<br>Servidor Mail: SMTP | **DROP** |
| DMZ | Servidor Mail: DNS<br>Servidor Mail: SMTP<br>Servidor Proxy: DNS<br>Servidor Proxy: HTTP<br>Servidor Proxy: HTTPS | | **DROP** |
| RED INTERNA | **DROP** | Servidor Web: HTTP<br>Servidor Proxy: PROXY<br>Servidor Mail: SMTP<br>Servidor Mail: POP3<br>Servidor Mail: IMAP | |

# Reglas

Politica de filtrado por defecto: **DROP**.

1. $< Mail, *, Internet, 25, TCP >$
2. $< Mail, *, Internet, 53, UDP >$
3. $< Proxy, *, Internet, 53, UDP >$
4. $< Proxy, *, Internet, 80, TCP >$
5. $< Proxy, *, Internet, 443, TCP >$
6. $< Internet, *, Web, 80, TCP >$
7. $< Internet, *, Mail, 25, TCP >$
8. $< Interna, *, Web, 80, TCP >$
9. $< Interna, *, Proxy, Proxy(8080), TCP >$
10. $< Interna, *, Mail, 25, TCP >$
11. $< Interna, *, Mail, 110, TCP >$
12. $< Interna, *, Mail, 143, TCP >$

# ¿Repasando...?

¿Dudas?,

¿Preguntas?