



Taller de Infraestructura: Firewalls

FING - IMM - 2017



Firewall

- Equipo o aplicación que controla el flujo de tráfico entre dos o más segmentos de la red.



Funcionalidades (1/2)

- Control de acceso basado en las direcciones de emisor o receptor.
- Control de acceso basado en el servicio requerido.
- Esconder la topología, direcciones y tráfico de una red interna al resto del mundo.



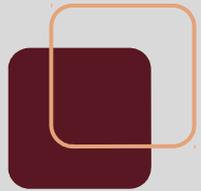
Funcionalidades (2/2)

- Detección y eliminación de malware en archivos de entrada.
- Autenticación basada en origen del tráfico
- Log de actividades de internet.

¿Qué NO puede hacer un firewall?



- Proteger del tráfico que no pasa por el firewall.
- Detener todos los virus.
- Detener ataques a través del tráfico permitido.
- Configurarse sólo correctamente.



Filtrado de paquetes

Se puede realizar en base a:

- Dirección origen
- Dirección destino
- Protocolo utilizado
- Conexión: Filtrar paquetes si no son la respuesta de algún paquete saliente de la red interna.



Función por defecto

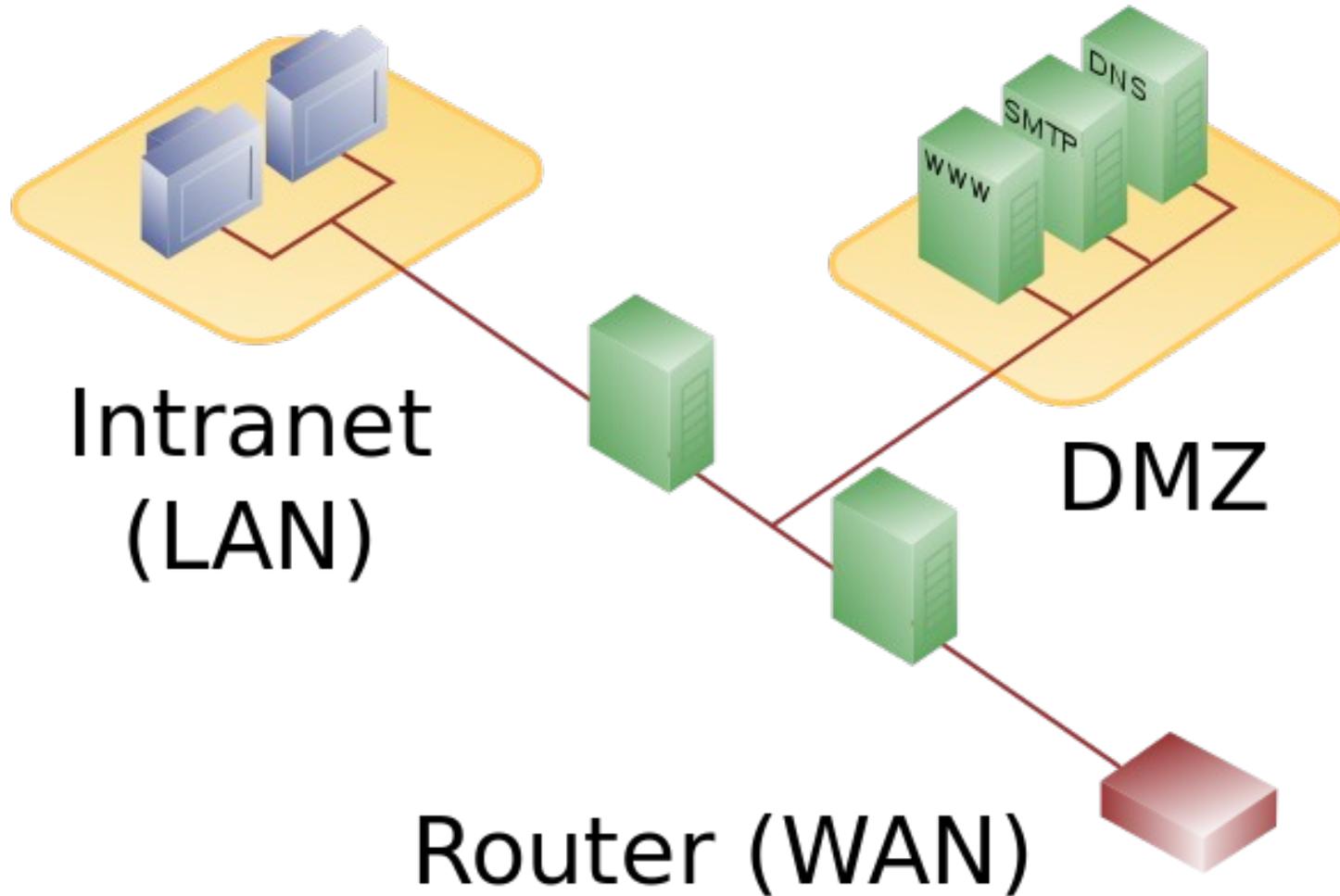
- Una de las cuestiones a definir en el firewall es qué se hace con el tráfico no definido en las reglas. Hay dos opciones:
 - Por defecto se permite el tráfico.
 - Por defecto se bloquea el tráfico.
- ¿Cuál es mejor?



Servidor Proxy

- Un servidor proxy se encarga de realizar consultas a nombre de otro equipo.
- Típicamente un servidor proxy implementa funcionalidades de firewall.
- Se deben configurar los equipos para que redirijan el tráfico al proxy.

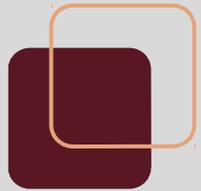
Ejemplo de red con firewall





Firewall Builder

- En el curso utilizaremos el software Firewall Builder, el cual permite configurar firewalls de manera remota.



Referencias

- Dieter Gollmann: Computer Security
- Curso Fundamentos de Seguridad Informática. Facultad de Ingeniería, Udelar