Fundamentos de Seguridad Informática
- Práctico: Seguridad en Redes TCP/IP -

GSI - FING

1. **Seguridad Redes TCP/IP: Firewall**

   (a) ¿Que información utiliza un firewall que realiza el filtrado de paquetes *sin estado*?

   (b) ¿Que desventaja/s presentan los firewalls con filtrado sin estado (stateless)?

   (c) ¿Que diferencia hay entre el filtrado de paquetes *sin estado* (stateless) y *con estado* (statefull)?

   (d) ¿Que características comparten los *host bastion*?

2. **Seguridad Redes TCP/IP: packet-filtering**

Regla	**Dirección**	**Src address**	**Dest address**	**Protocol**	**Dest port**	**Acción**
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Cuadro 1: Reglas de filtrado sin estado (packet-filtering)

   (a) Describir el efecto que produce cada una de las reglas del cuadro.

   (b) Este conjunto de reglas presenta varios problemas. Identifique las reglas con problemas y proponga mejoras.

3. Una organización instala un servidor web (HTTP) en su red interna corporativa con dirección IP 5.6.7.8/24. Se cuenta con un firewall con capacidades de filtrado de paquetes (sin estado) que controla el flujo de datos entre la red interna corporativa e internet. En la figura 1 se muestra un diagrama simplidicado de la arquitectura de red.

   (a) Proponga un conjunto de reglas mínimo que el firewall debería contar considerando el agregado del servidor web.

   (b) El área de TI de la organización piensa en el corto y mediano plazo incorporar el servicio de acceso remoto vía SSH y un servidor de correo. ¿ Propondría realizar algún cambio en la arquitectura de seguridad de la organización? Justifique.

4. **Seguridad Redes TCP/IP**
   Supongamos que disponemos de un firewall que controla el flujo de datos de red entre la red interna e Internet.

   (a) ¿Puede el firewall proteger contra infecciones de virus? Considere distintos tipos de firewall en su respuesta.

   (b) ¿Como afecta la protección criptográfica implementada a nivel del protocolo TCP/IP o la capa de aplicación, afectar la habilidad del firewall de protección contra virus?

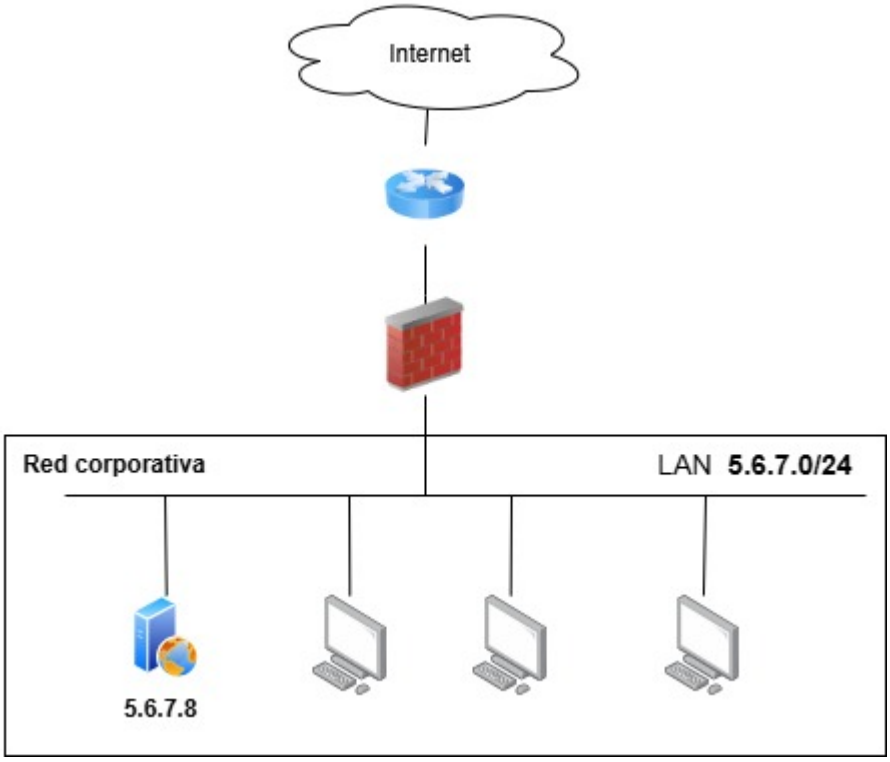

Figura 1: Arquitectura simplificada

5. Una compañía decide habilitar a sus empleados el uso de laptops en sus hogares o cuando están de viaje. Proponga una arquitectura de seguridad y medidas para proteger los laptops y la intranet de la empresa.