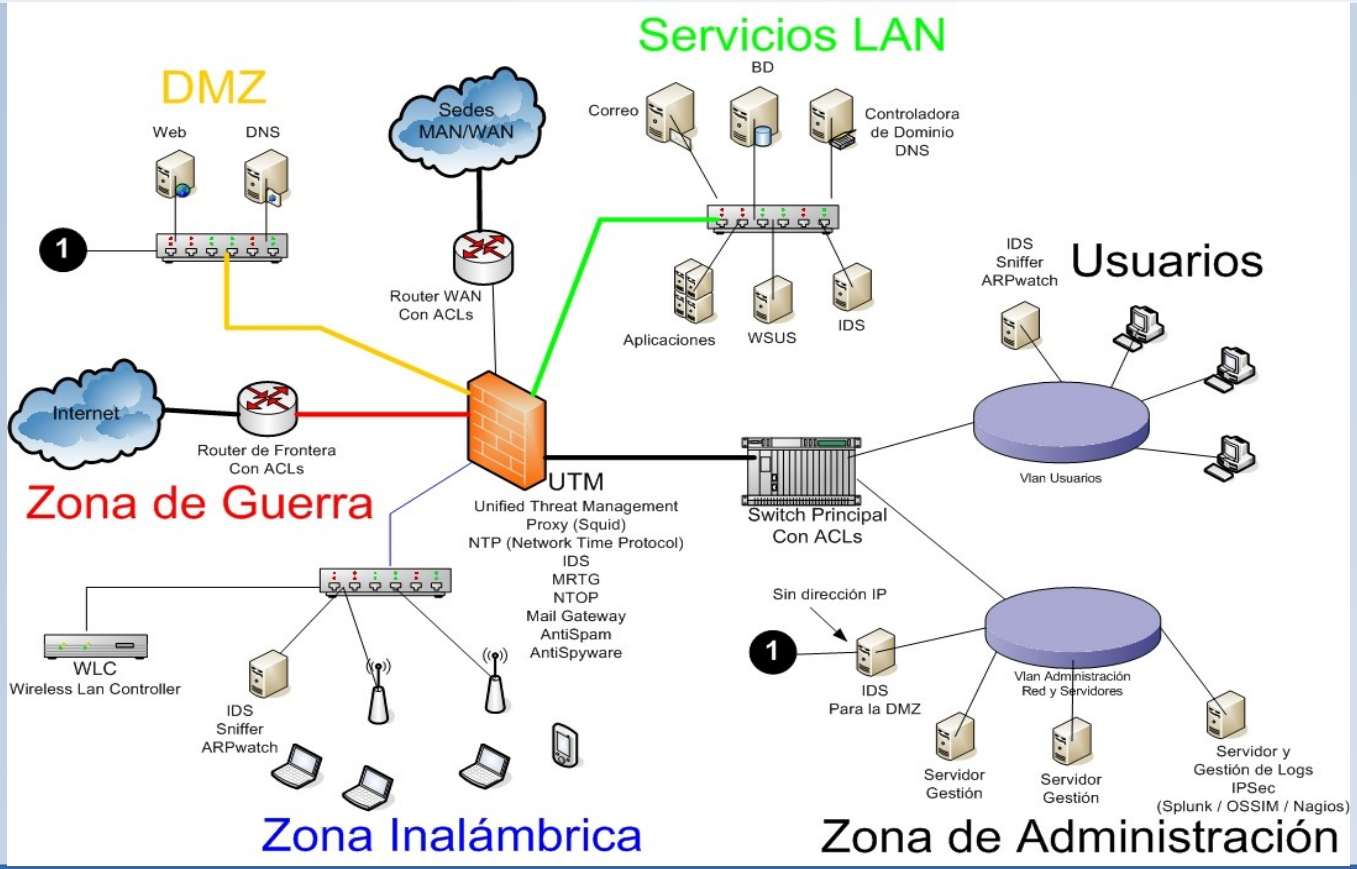
Iptables: el firewall de Linux

Pontificia Universidad
JAVERIANA
Bogotá

"Hablar es fácil, muéstrame tu código."

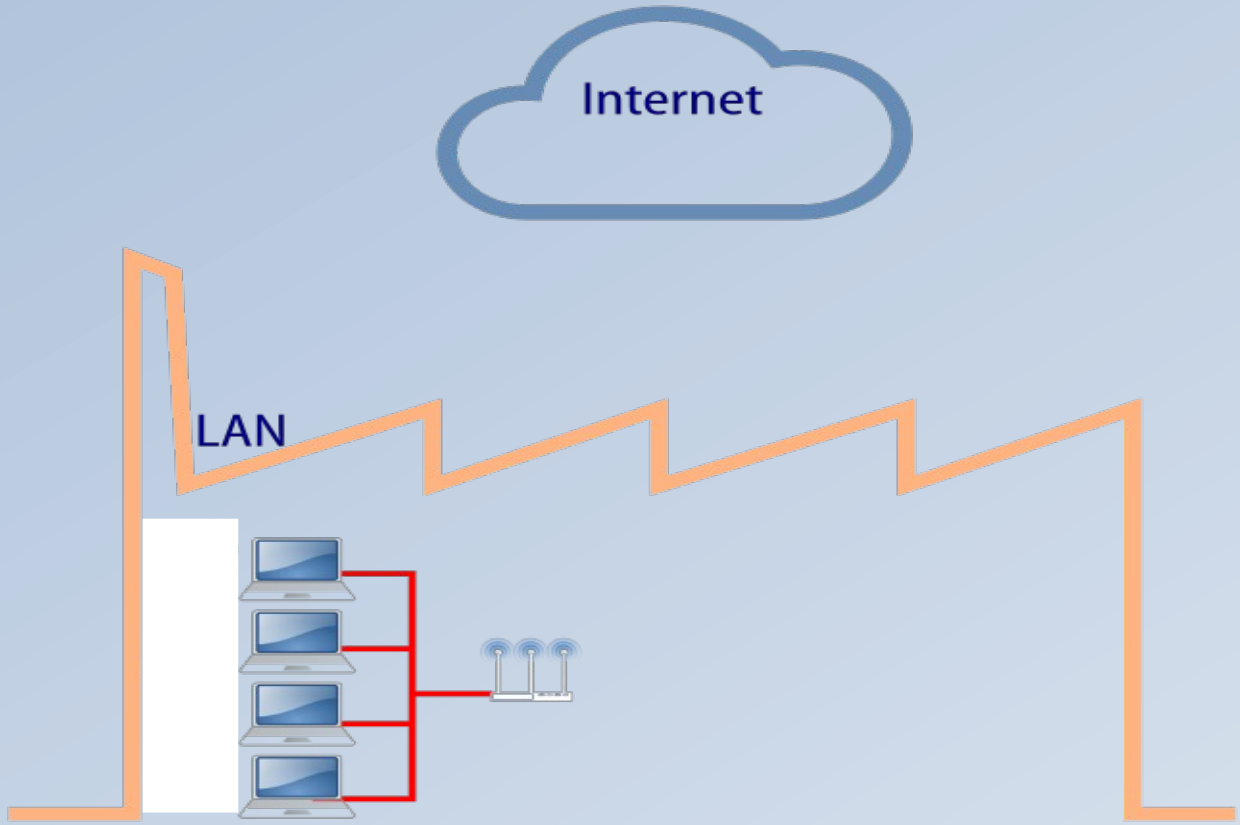
Linus Torvalds

Segmentación de la red



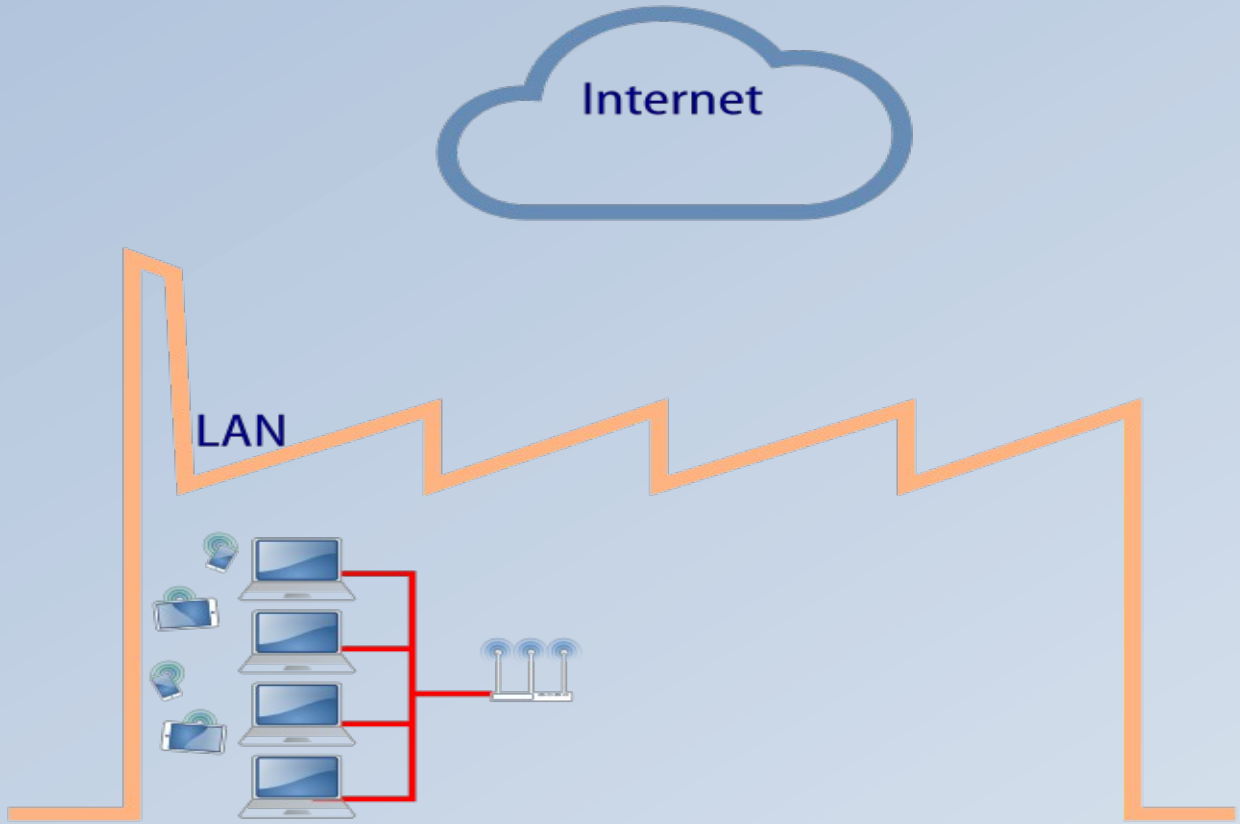
Memorias de la charla

Segmentación de la red



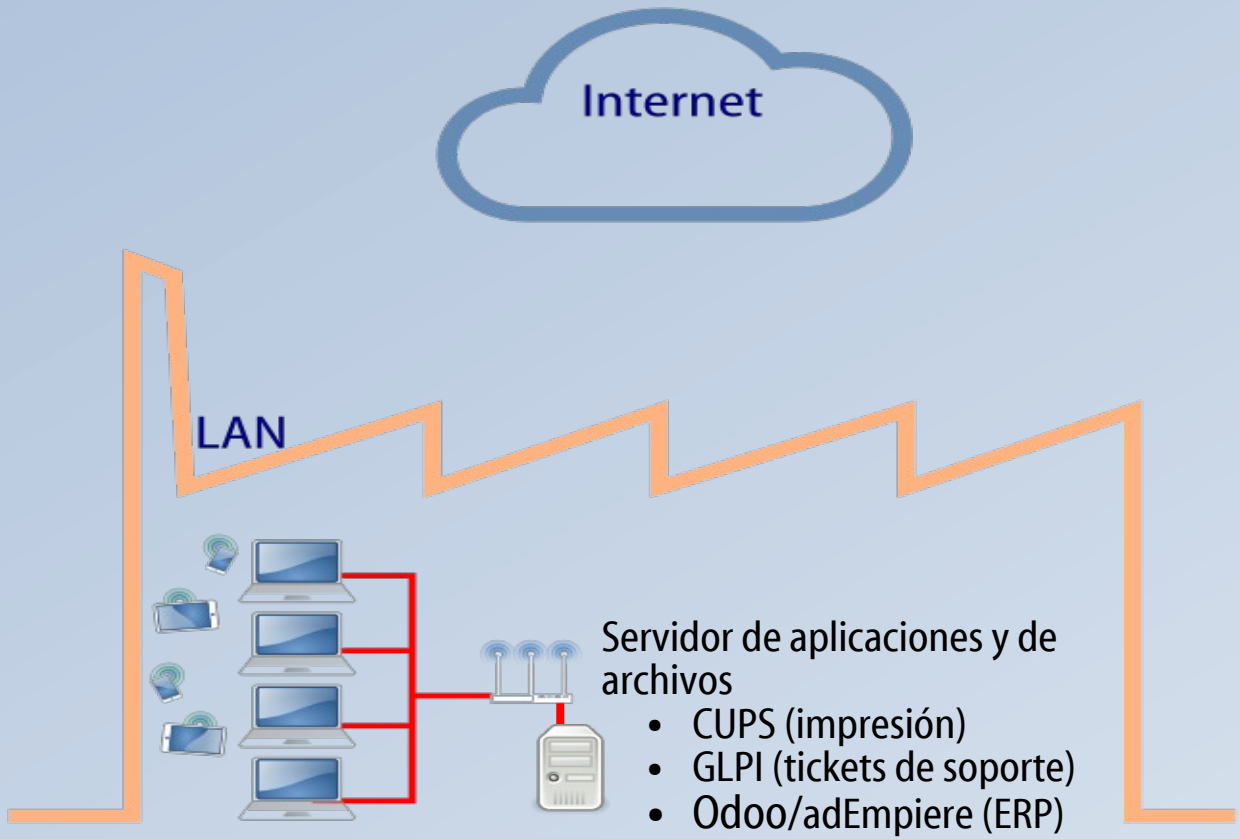
Memorias de la charla

Segmentación de la red



Memorias de la charla

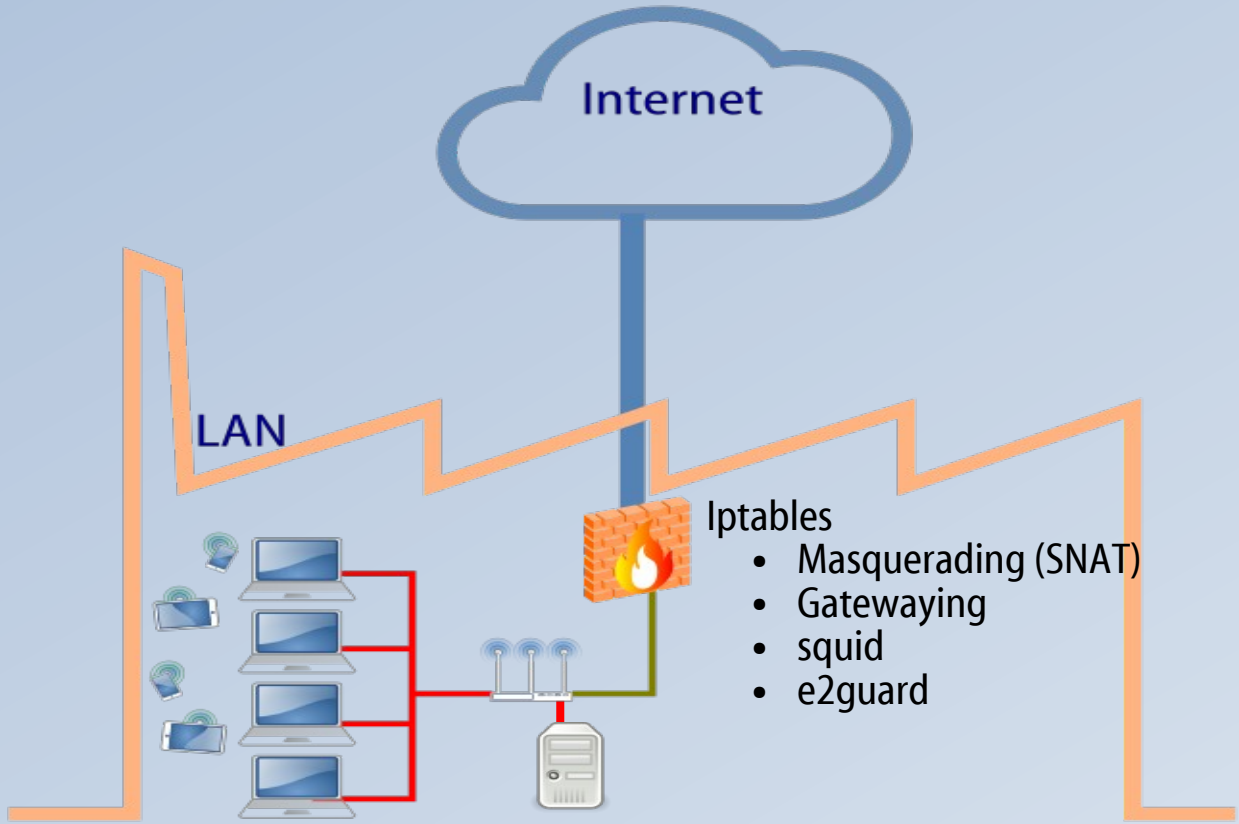
Segmentación de la red



Servidor de aplicaciones y de archivos

- CUPS (impresión)
- GLPI (tickets de soporte)
- Odoo/adEmpiere (ERP)
- SugarCRM (CRM)
- ...

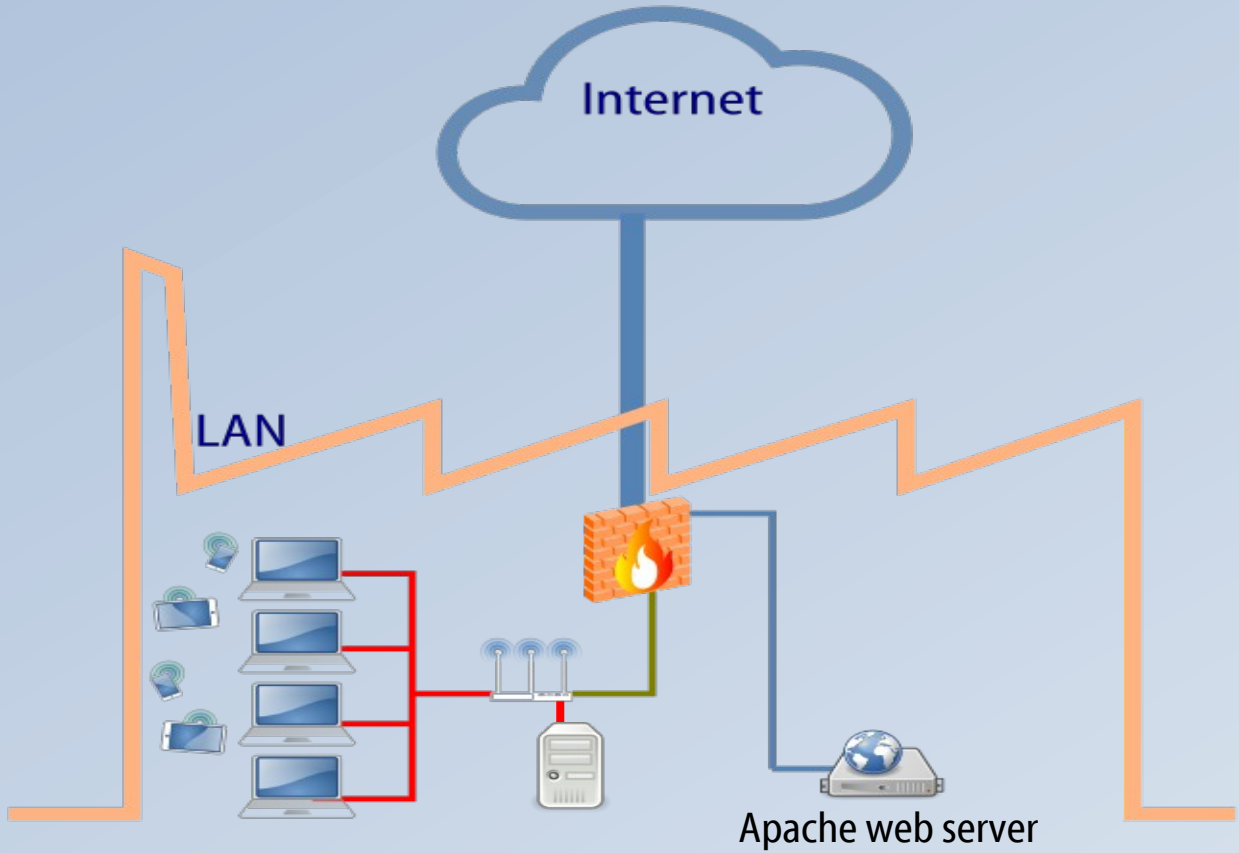
Segmentación de la red



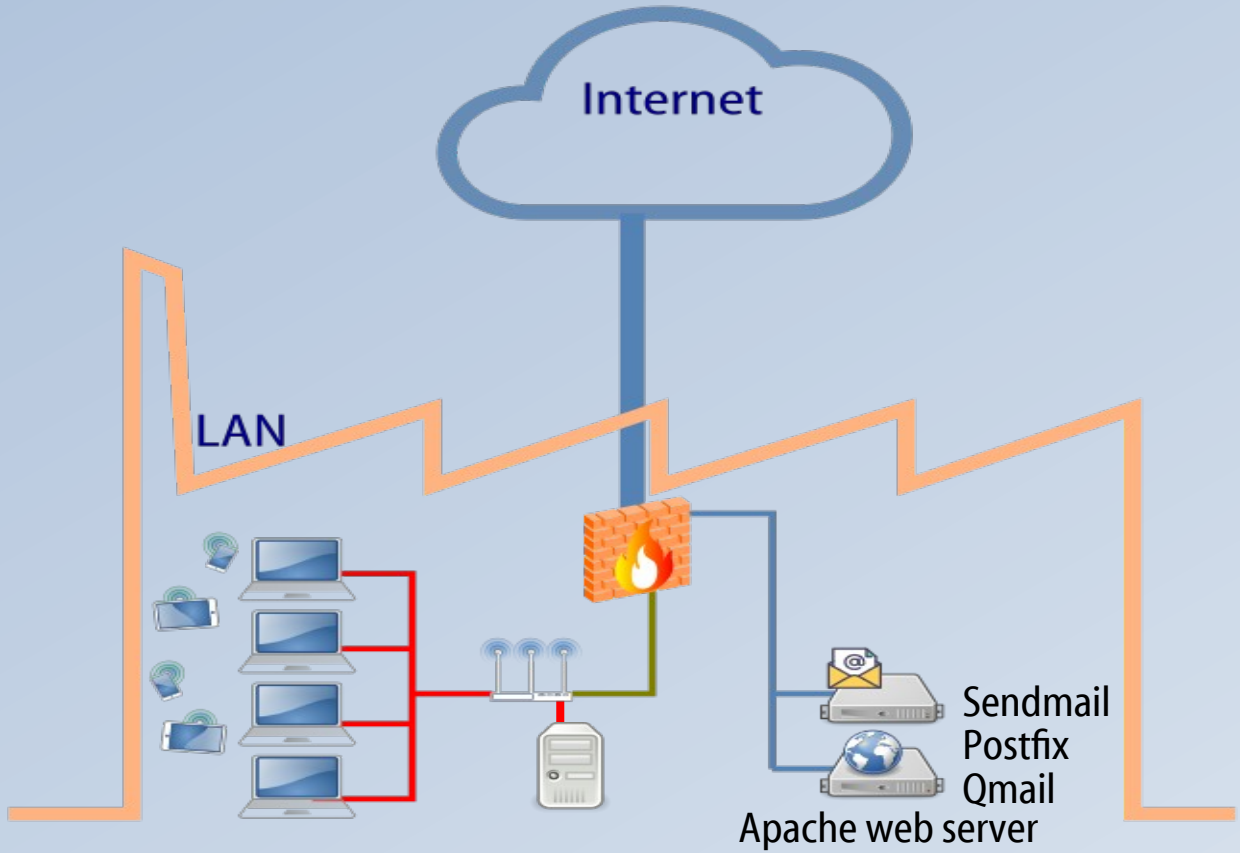
Iptables

- Masquerading (SNAT)
- Gatewaying
- squid
- e2guard

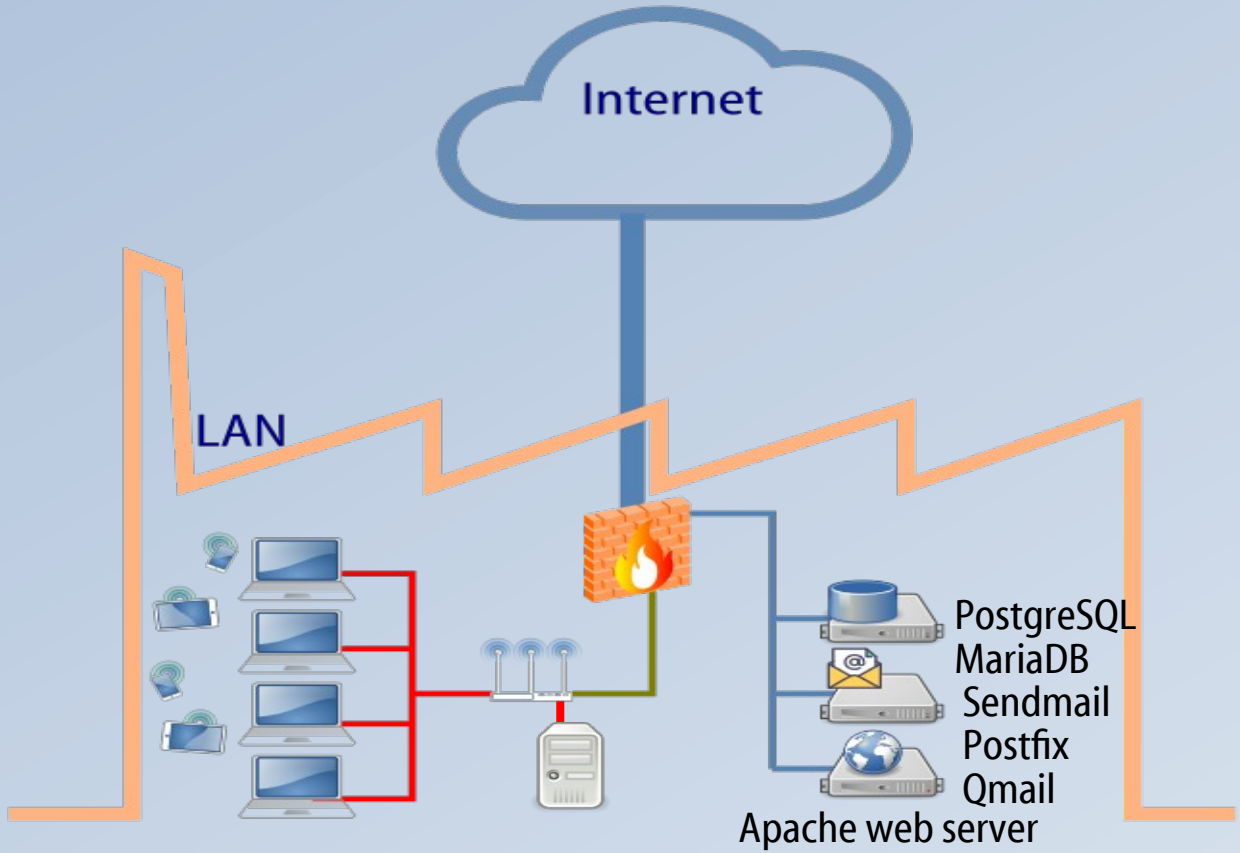
Segmentación de la red



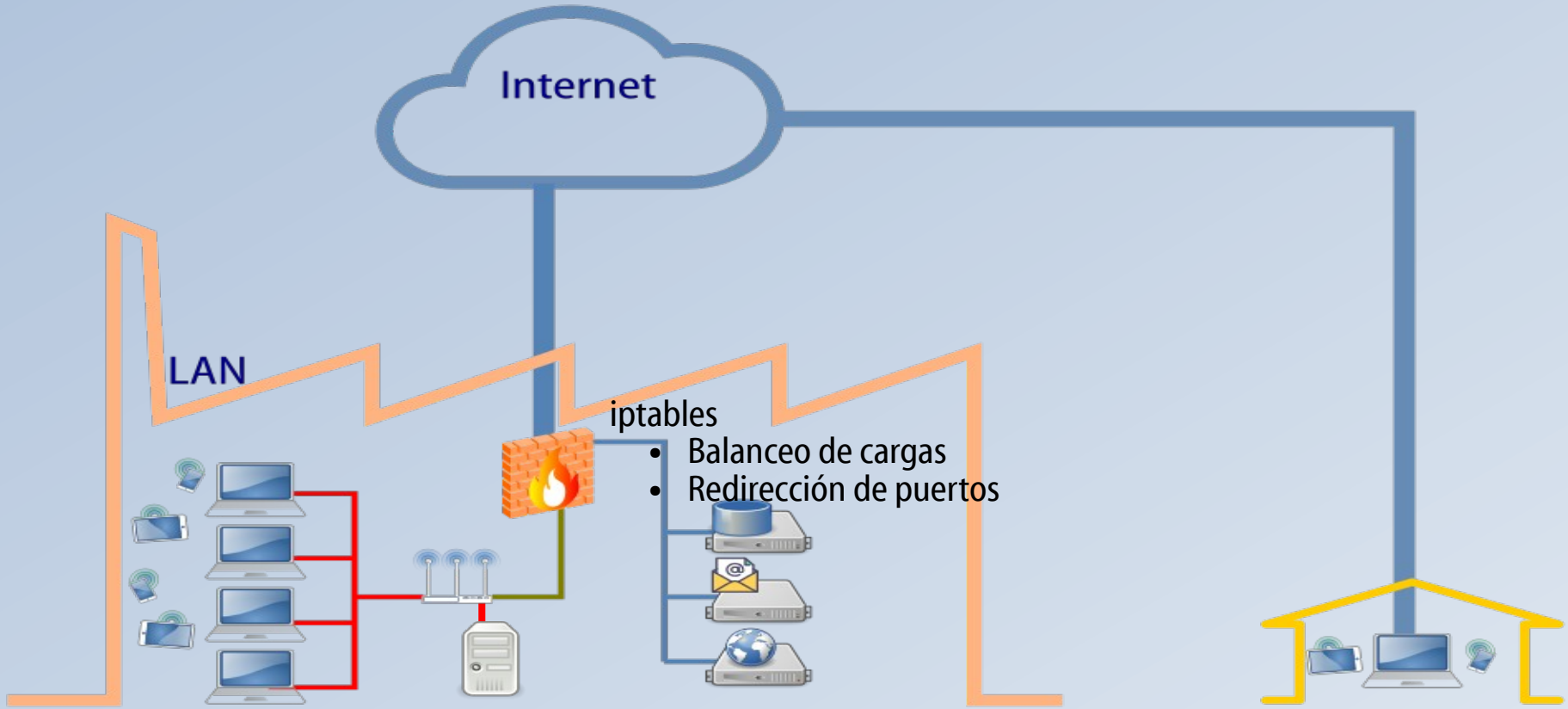
Segmentación de la red



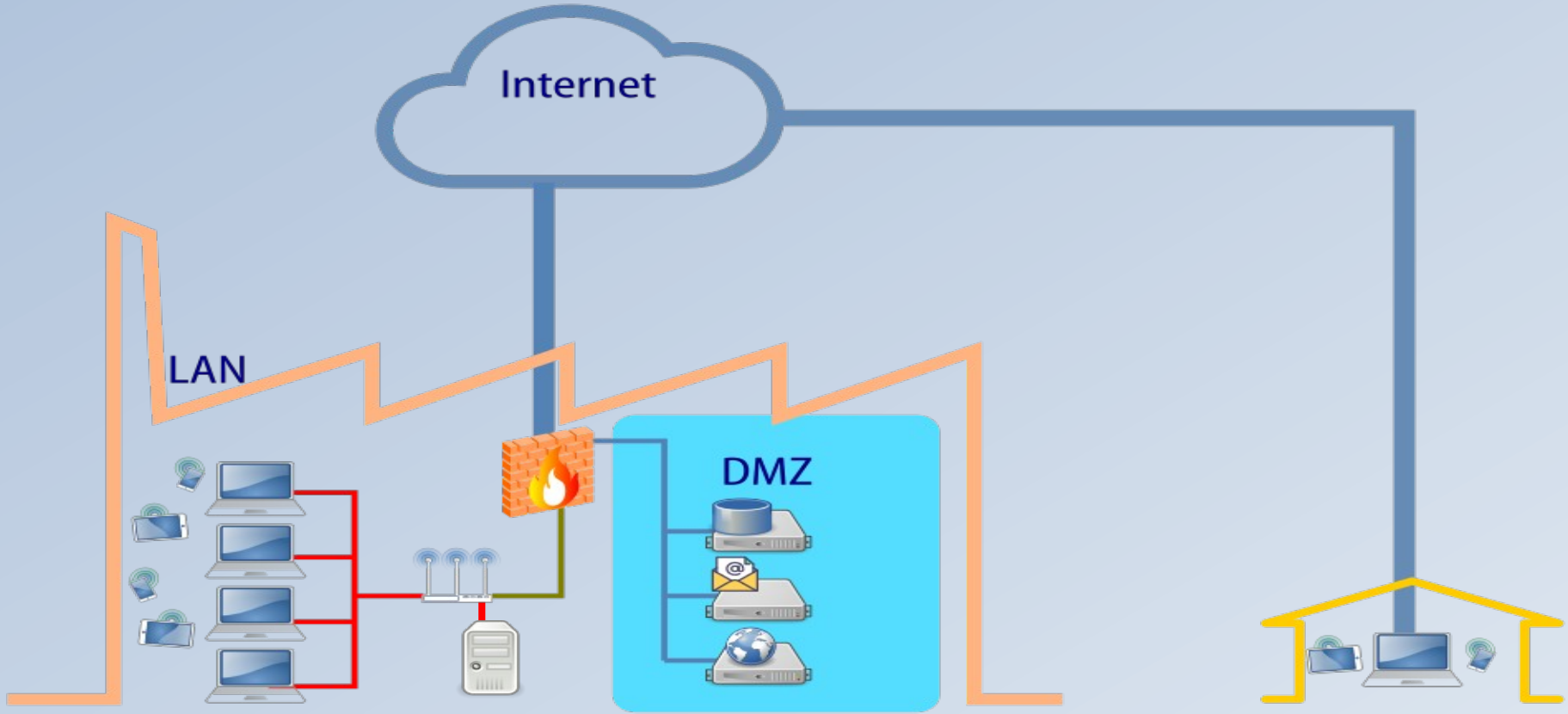
Segmentación de la red



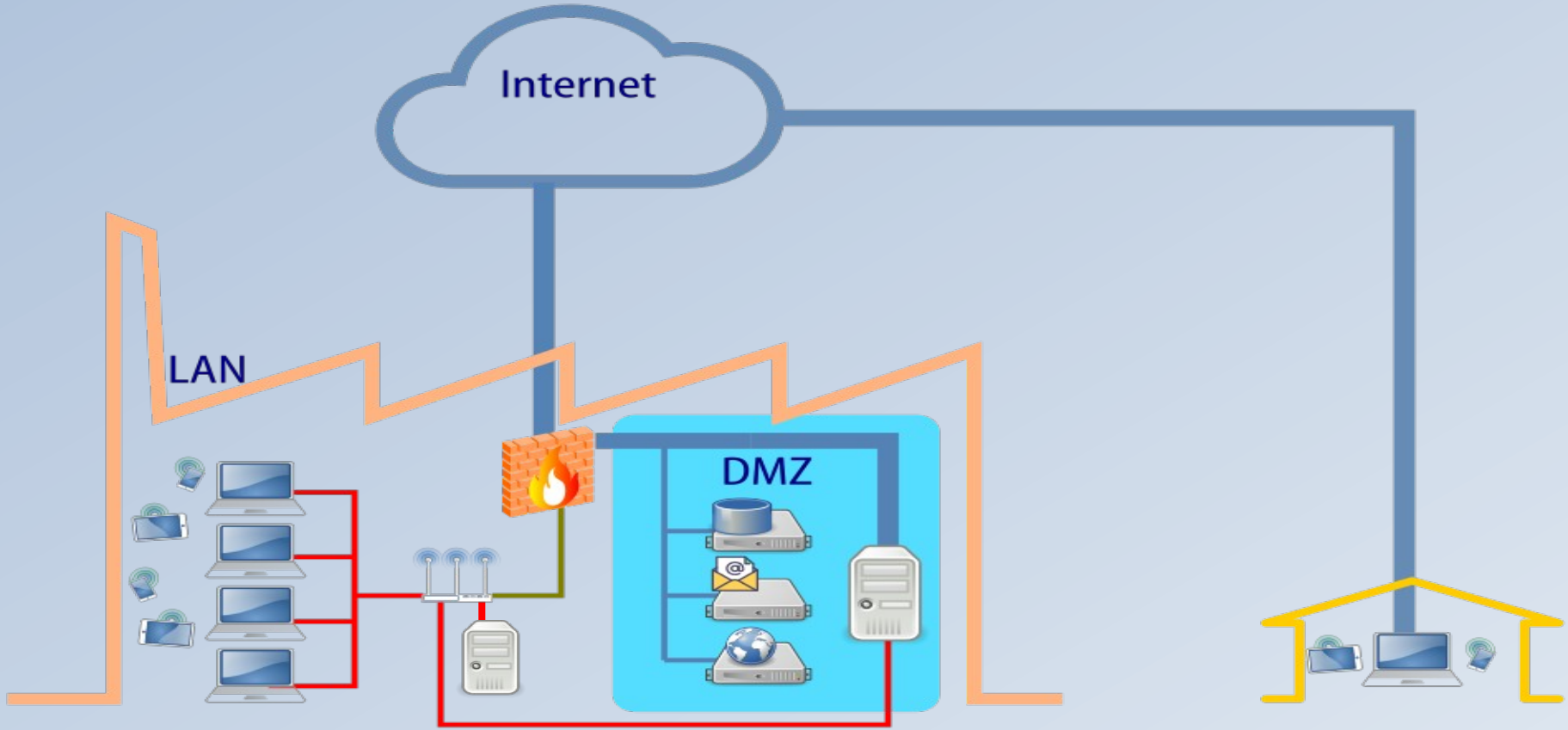
Segmentación de la red



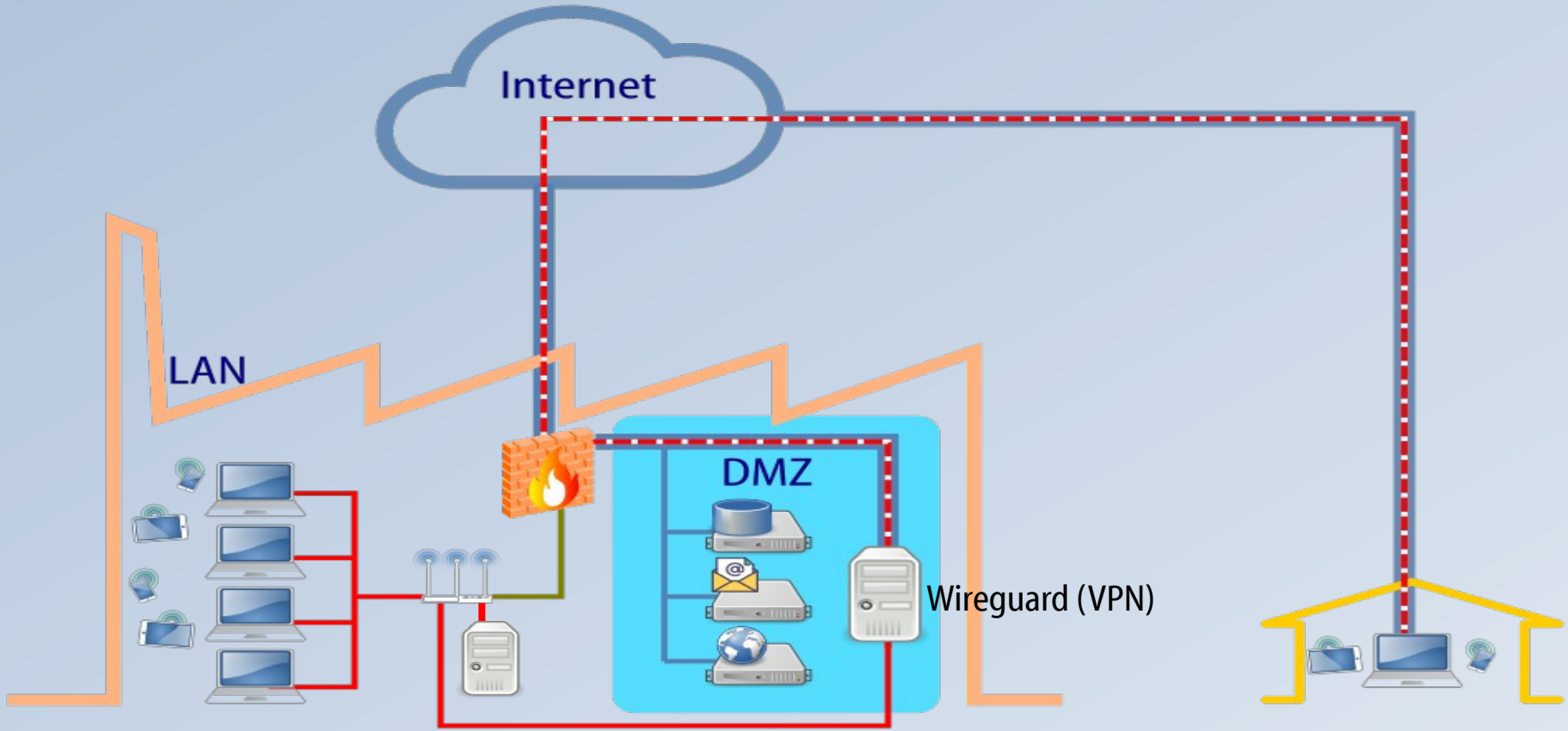
Segmentación de la red



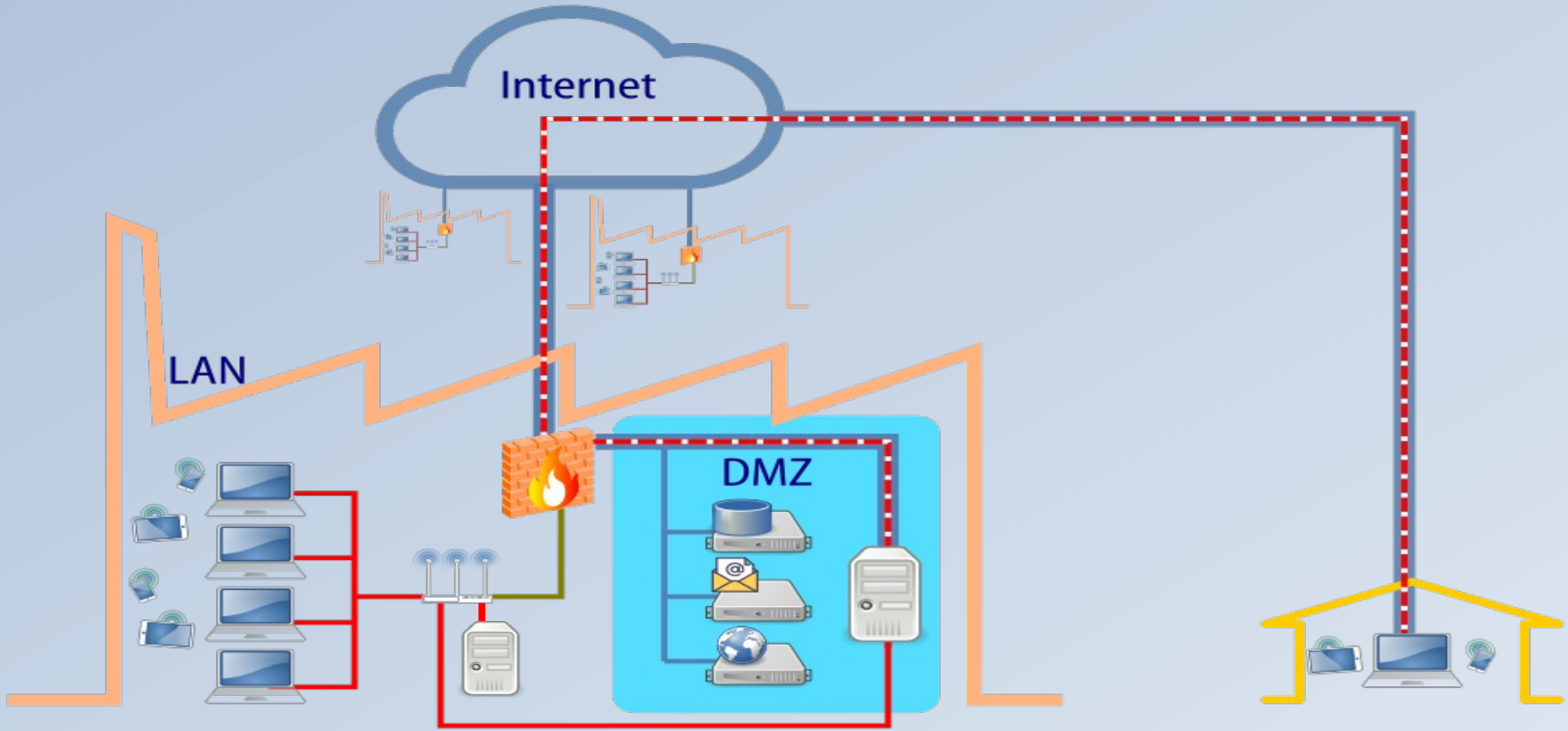
Segmentación de la red



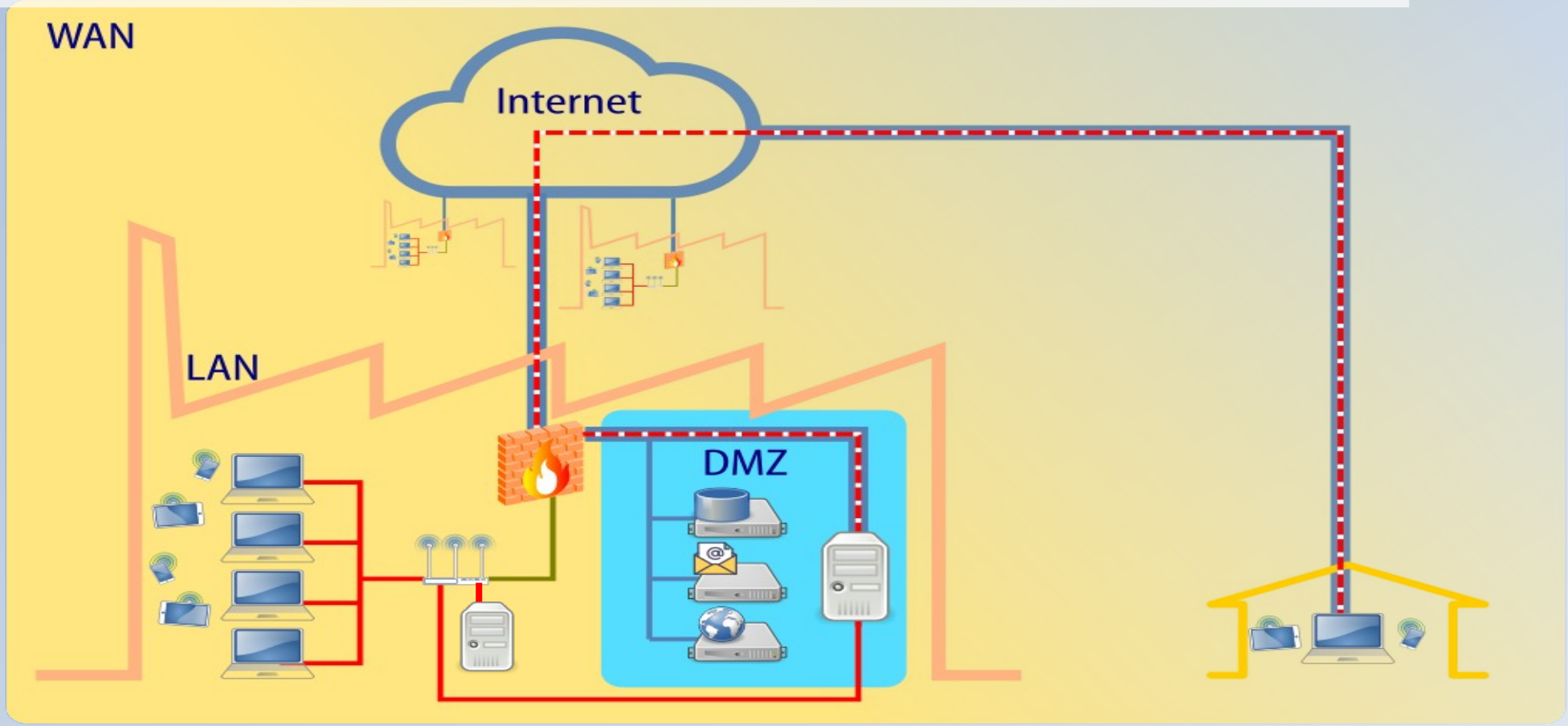
Segmentación de la red



Segmentación de la red



Segmentación de la red

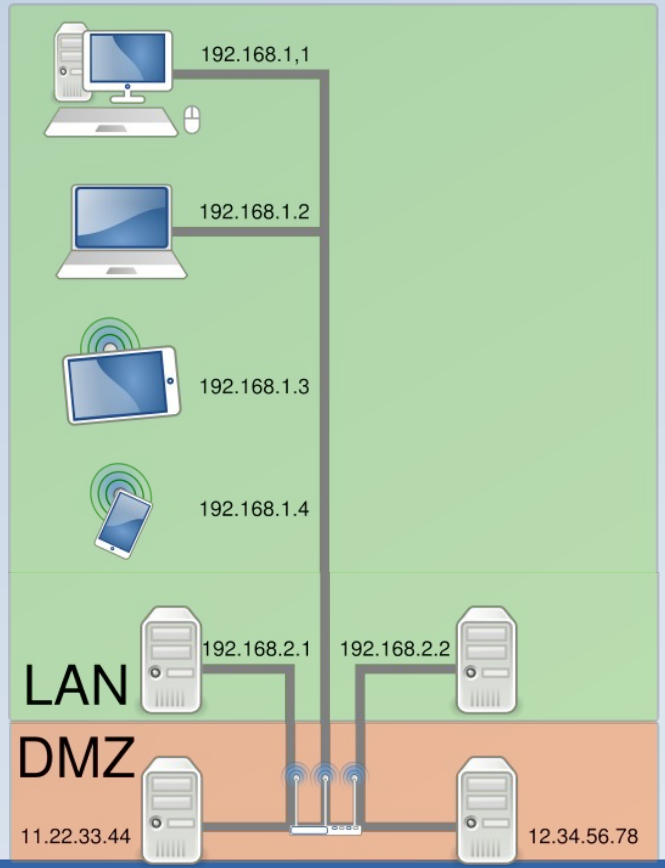


Segmentación de la red

- Zona Roja (Internet):
  - Conexión directa con Internet.
  - Todo el tráfico que entra o sale de esta zona debe ser cuidadosamente filtrado
- DMZ (Zona Desmilitarizada):
  - Aislada para alojar servidores y servicios que necesitan ser accesibles desde el exterior
  - Pueden ser accesibles desde la Zona Roja (Internet)
- LAN de Usuarios:
  - Los dispositivos de los usuarios comunes, como estaciones de trabajo, computadoras portátiles y dispositivos móviles.
- LAN de Administradores:
  - Equipos y dispositivos utilizados por el personal administrativo o de TI para gestionar y administrar la infraestructura.
  - Los administradores tienen privilegios más elevados => Exige más protección.
- LAN de Servidores Internos:
  - Los servidores que ofrecen servicios solo dentro de la red interna, como bases de datos, servidores de aplicaciones o controladores de dominio.

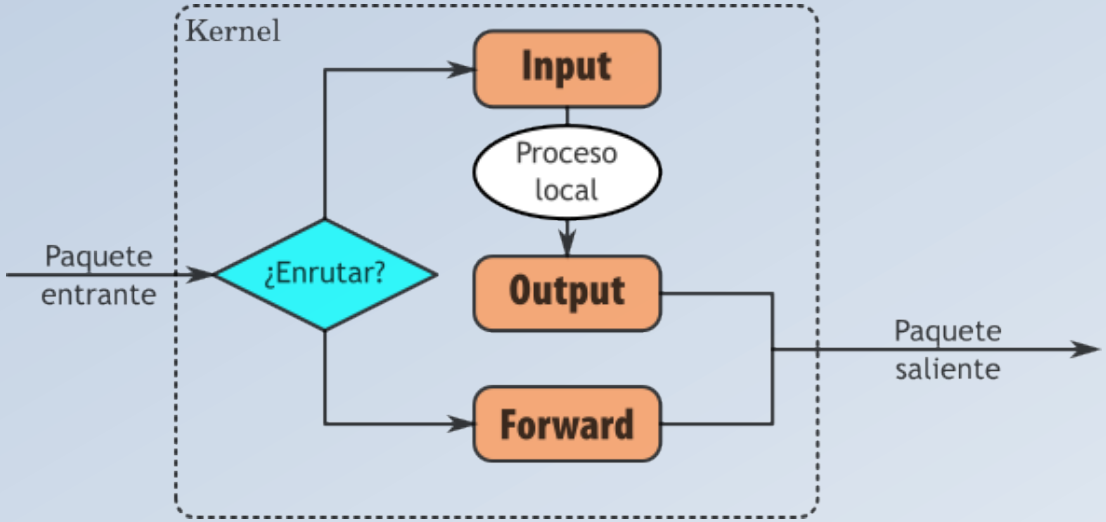
Segmentación de la red

- Beneficios de la segmentación
  - Aislar el tráfico entre áreas críticas y áreas menos seguras.
  - Limitar los daños y contener los incidentes en caso de que alguna zona sea comprometida.
  - Aplicar políticas de seguridad específicas para cada zona, de acuerdo con sus requerimientos.
  - Facilitar la gestión de reglas del firewall mediante el control del tráfico permitido entre las diferentes zonas, mejorando el rendimiento y la seguridad.



Las cadenas de filtrado

- Input:
  - Paquetes entrantes que tienen como destino el propio sistema.
- Output:
  - paquetes que son generados y enviados desde el sistema hacia otros equipos o redes
- Forward:
  - paquetes que no están destinados al sistema local pero lo atraviezan para ser reenviados



Las reglas de filtrado

Objetivo	Descripción
ACCEPT	Permite el tráfico.
DROP	Bloquea el tráfico sin notificación.
REJECT	Bloquea el tráfico con notificación.
LOG	Registra el tráfico sin bloquearlo.
SNAT	Cambia la IP de origen.
DNAT	Cambia la IP de destino.
MASQUERADE	Como SNAT pero para IPs dinámicas.
MARK	Marca el paquete para procesamiento avanzado.

Administración de iptables

- Instalación:
  - No se requiere, viene por defecto con cualquier distribución de Linux
- Gestión del servicio:
  - Siempre como usuario root: `su - / sudo`
  - `systemctl enable iptables`
  - `systemctl disable iptables`
  - `systemctl status iptables`
  - `systemctl start iptables`
  - `systemctl stop iptables`
  - `systemctl restart iptables`
  - `systemctl save iptables`

Los parámetros de configuración de reglas

- -s (Source)
  - `-s 192.168.1.10`
  - `-s 192.168.1.0/24`
- -d (Destination)
  - `-d 10.0.0.5`
  - `-d 10.0.0.0/8`
- -p (Protocol)
  - `-p tcp`
  - `-p udp`
- --dport (Destination Port)
  - `--dport 80`
  - `--dport 1000:2000`
- -j (Jump)
  - ACCEPT: Permite el tráfico.
  - DROP: Descarta el tráfico sin notificar al origen.
  - REJECT: Rechaza el tráfico, enviando una notificación al origen.
  - LOG: Registra el tráfico en el registro de sistema.
  - `-j ACCEPT`
- -i (Input Interface)
  - `-i eth0`
- -o (Output Interface)
  - `-o eth1`

Establecer reglas

- Siempre como usuario root: `su - / sudo`
- Permitir conexiones entrantes al puerto 80 (HTTP):
  - `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
- Bloquear todas las conexiones entrantes desde una IP específica:
  - `iptables -A INPUT -s 192.168.1.100 -j DROP`
- Permitir que el sistema envíe paquetes a través del puerto 443 (HTTPS):
  - `iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT`
- Bloquear el acceso a una IP específica desde el sistema local:
  - `iptables -A OUTPUT -d 203.0.113.1 -j DROP`

Ayudas para la configuración

- Ejemplos de uso de Firewalld:
  - Para agregar una regla permanente que permita el tráfico HTTP en la zona pública y recargue el cortafuegos para que tome la nueva regla:
    - `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
    - `firewall-cmd --zone=public --add-service=http --permanent`
    - `firewall-cmd --reload`
  - Para asociar una interfaz de red a una zona:
    - `iptables -A INPUT -i eth0 -j ACCEPT`
    - `firewall-cmd --zone=work –change-interface=eth0`

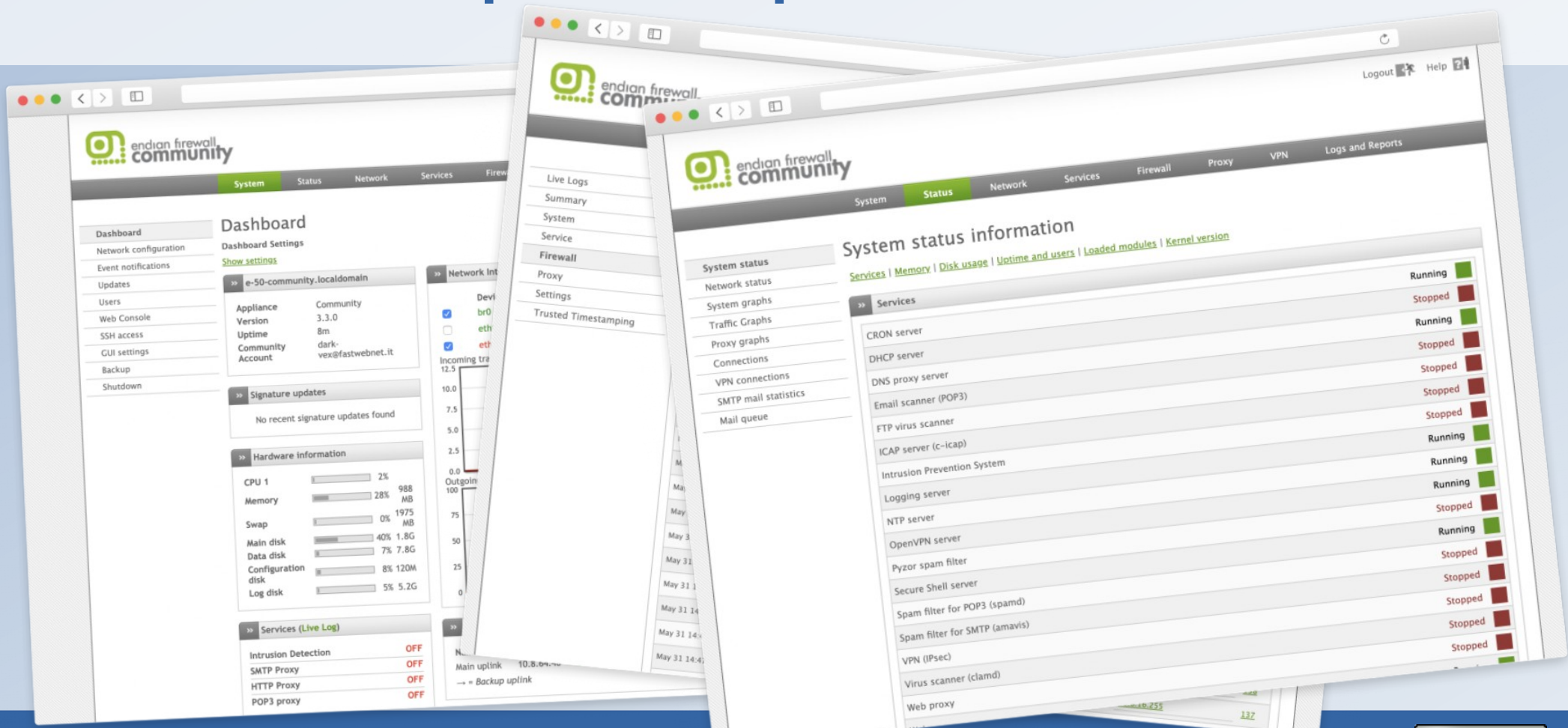
Ayudas para la configuración

- Ejemplos de uso de Easyfirewall:
  - Abrir un puerto específico para un servicio, como el puerto 80
    - `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
    - `easyfirewall --add-service http`
  - Bloquear el acceso de una dirección IP específica, por ejemplo, 192.168.1.10, puedes ejecutar:
    - `iptables -A INPUT -s 192.168.1.10 -j DROP`
    - `easyfirewall --block-ip 192.168.1.10`
  - Permitir conexiones SSH entrantes, puedes usar el siguiente comando:
    - `easyfirewall --add-service ssh`
  - Abrir un rango de puertos, por ejemplo del 1000 al 2000, para un conjunto de aplicaciones:
    - `easyfirewall --add-port 1000-2000/tcp`

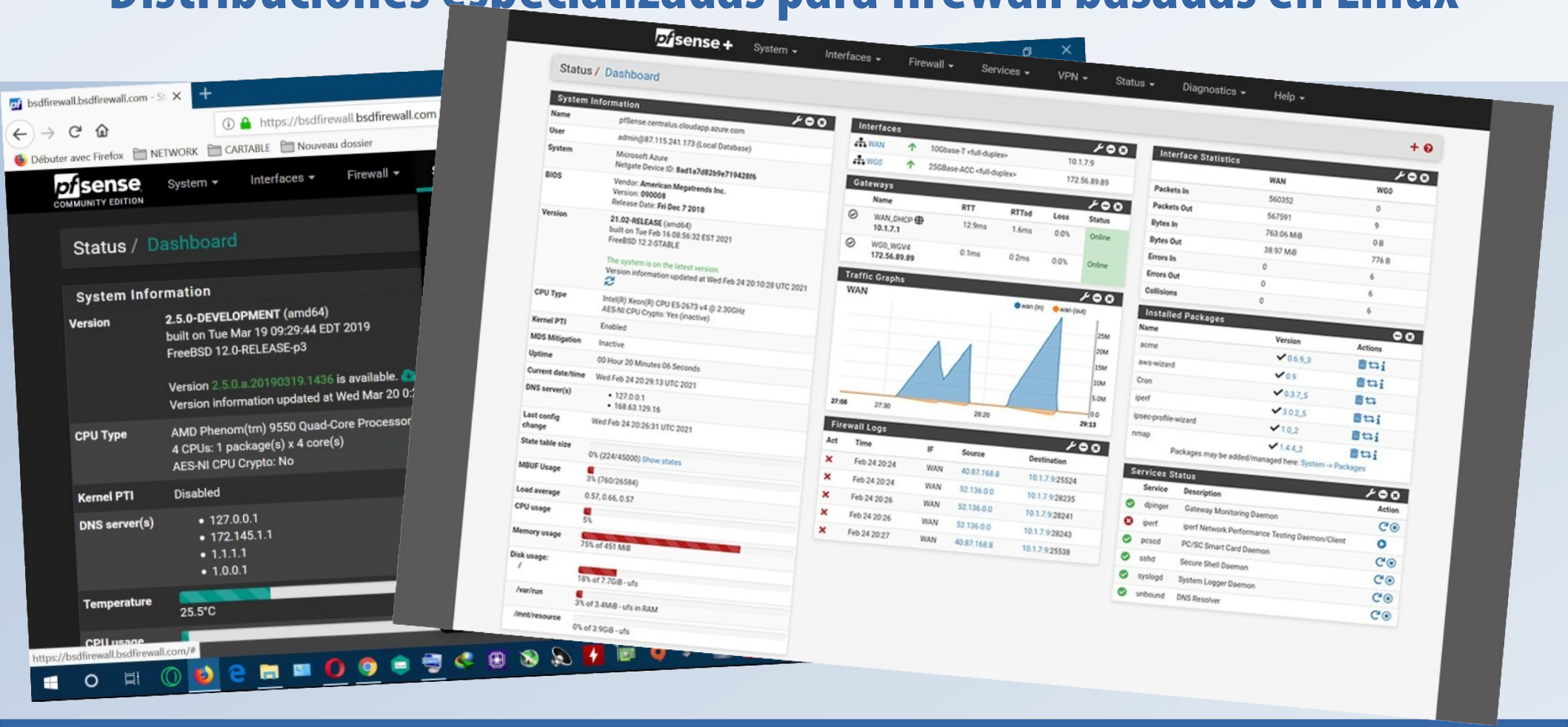
Ayudas a la configuración

Solución	Dificultad de Uso	Características Clave	Ideal Para
Firewalld	Media	Zonas, gestión dinámica, línea de comandos y GUI	Usuarios de sistemas Red Hat, CentOS, Fedora
EasyFirewall	Baja	Configuración intuitiva y reglas básicas	Usuarios novatos y domésticos
UFW	Baja	Comandos simples, fácil de usar	Servidores básicos en Ubuntu o Debian
Shorewall	Alta	Configuración avanzada en archivos	Redes grandes o complejas

Distribuciones especializadas para firewall basadas en Linux



Distribuciones especializadas para firewall basadas en Linux



Distribuciones especializadas para firewall basadas en Linux

Característica	Endian Firewall	pfSense	OPNsense	IPFire	ClearOS
Base	Linux (Red Hat)	FreeBSD	FreeBSD	Linux (LFS)	Linux (CentOS)
Tipo de Firewall	UTM (Unified Threat Management)	Firewall/ Router avanzado	Firewall/ Router avanzado	Firewall básico con IPS	Gateway, Firewall, Servidor
GUI	Sí, interfaz web	Sí, interfaz web	Sí, interfaz web	Sí, interfaz web	Sí, interfaz web
Sistema de Gestión de Red	Segmentación de red (zonas verde, rojo, azul, naranja)	Avanzado, Soporta VLAN, NAT, DMZ	Similar a pfSense	Soporte NAT, VLAN y DMZ	Soporte completo de red

Distribuciones especializadas para firewall basadas en Linux

Característica	Endian Firewall	pfSense	OPNsense	IPFire	ClearOS
VPN	IPsec, OpenVPN	IPsec, OpenVPN, WireGuard	IPsec, OpenVPN, WireGuard	IPsec, OpenVPN	IPsec, OpenVPN
Intrusion Detection	Sí, con Snort	Sí, con Snort o Suricata	Sí, con Snort o Suricata	Sí, con Snort	No (módulos adicionales disponibles)
Balanceo de Carga	Sí	Sí	Sí	Sí	Sí, con módulos adicionales

Distribuciones especializadas para firewall basadas en Linux

Característica	Endian Firewall	pfSense	OPNsense	IPFire	ClearOS
Control de Ancho de Banda	Sí	Sí	Sí	No	Sí, con módulos adicionales
Filtrado de Contenido	Sí	A través de plugins adicionales	A través de plugins adicionales	Sí, proxy integrado con filtrado web	A través de marketplace
Facilidad de Uso	Alta, orientado a usuarios empresariales	Media, requiere conocimientos avanzados	Alta, interfaz más moderna	Media, más simple que pfSense	Alta, orientado a pequeñas empresas
Actualizaciones	Moderadas	Frecuentes	Frecuentes	Moderadas	Moderadas

Distribuciones especializadas para firewall basadas en Linux

Característica	Endian Firewall	pfSense	OPNsense	IPFire	ClearOS
Plugins/ Extensiones	No	Sí, a través de paquetes	Sí, sistema de plugins	No	Sí, a través del marketplace
Comunidades y Soporte	Amplia comunidad y soporte comercial	Gran comunidad y soporte comercial	Creciente comunidad	Activa comunidad y soporte comercial	Soporte comercial y comunidad
Uso Ideal	PYMEs y medianas empresas	Redes grandes, empresas e ISP	Redes grandes y medianas	Pequeñas redes y hogares	PYMEs y pequeñas organizaciones

¿Preguntas?

Memorias de la charla