



Introducción a las Redes(TUR)

Introducción a los Sistemas Operativos y Redes(TUW y Prof.)

Clase 8 : Introducción a la Seguridad en Redes

SEGURIDAD EN REDES

“El único sistema verdaderamente seguro es aquel que está apagado, encerrado en un bloque de hormigón y sellado en una habitación recubierta de plomo con guardias armados.... y aún así tengo mis dudas!”

Eugene Spafford, “Computer Recreations of Worms, Viruses and Code War”, Scientific American, marzo 1998, p. 110



SEGURIDAD EN REDES

¿Qué protejemos en una Red?

¿Qué es más importante?

¿Pueden hacerse todas las redes seguras?

...



SEGURIDAD EN REDES

Toda organización DEBE definir CUÁL es el concepto de seguridad para ella, es decir: ¿Qué se debe cuidar?

Por ejemplo:

- ✓ Una red es segura si nadie ajeno puede acceder a sus computadoras.
- ✓ Una red es segura cuando se permite el acceso a los datos, pero se prohíbe cambiarlos.
- ✓ Una red es segura cuando se permiten accesos a los datos públicos y no a los datos privados.

La seguridad en redes busca minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos.

SEGURIDAD EN REDES

- ✓ **Vulnerabilidad:** es alguna característica del sistema informático que puede ser usado por una amenaza.
- ✓ **Amenaza:** es un evento no deseado, el cual puede perjudicar a la organización.

Ejemplos de vulnerabilidades:

- Uso de SO no actualizados
- Comunicaciones sin cifrar
- Falta de antivirus
- No existe control de accesos al sistema
- No tener el control de software que se descarga de internet
- Ex empleados que conserven acceso a los recursos.

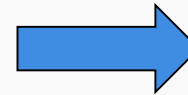
¿QUÉ ES UNA POLÍTICA DE SEGURIDAD?

Conjunto de reglas y prácticas a aplicar en una organización a fin de dirigir, proteger y distribuir sus recursos para cumplir con los objetivos de seguridad informática definidos previamente.



ARQUITECTURA DE SEGURIDAD

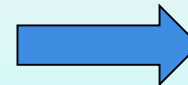
Los sistemas informáticos permiten el intercambio de información.



Arquitectura de Comunicaciones

Conexiones con otros Sistemas → Nuevos riesgos

Se debe integrar políticas, estándares, evaluaciones de riesgos, mecanismos, servicios y funciones de seguridad al Sistema de Comunicaciones.



Arquitectura de Seguridad de la información.



ARQUITECTURA DE SEGURIDAD




Ataques a la
Seguridad

Detectan -
Previenen -
Reestablecen



Mecanismos
de
Seguridad

Hacen uso



Servicios de
Seguridad



ARQUITECTURA DE *Ataques a la Seguridad*

Tipos:

✓ Pasivos

No afectan a los recursos del sistema.

→ Prevenir

✓ Activos

Buscan alterar el funcionamiento o los recursos del sistema.

→ Detectar y Recuperar



ARQUITECTURA DE SEGURIDAD

Ataques a la Seguridad

Pasivos

a) Obtención del contenido del mensaje



Ejemplo: Escuchar una conversación telefónica, observar mensajes de correo electrónico, obtener archivos digitales, etc.

ARQUITECTURA DE SEGURIDAD

Ataques a la Seguridad

Pasivos

b) Análisis de Tráfico



Objetivo:

Determinar localización e identidad de los servidores, descubrir frecuencia y longitud de los mensajes que se intercambian.



ARQUITECTURA DE SEGURIDAD

Ataques a la Seguridad

Activos

a) Suplantación de identidad



Ejemplo: Phishing, IP spoofing



ARQUITECTURA DE SEGURIDAD

Ataques a la Seguridad

Activos

b) Repetición

Activos





ARQUITECTURA DE SEGURIDAD

Ataques a la Seguridad

Activos

Pasivos

c) Modificación del Mensaje





ARQUITECTURA DE SEGURIDAD

Ataques a la Seguridad

Activos

d) Interrupción de servicio



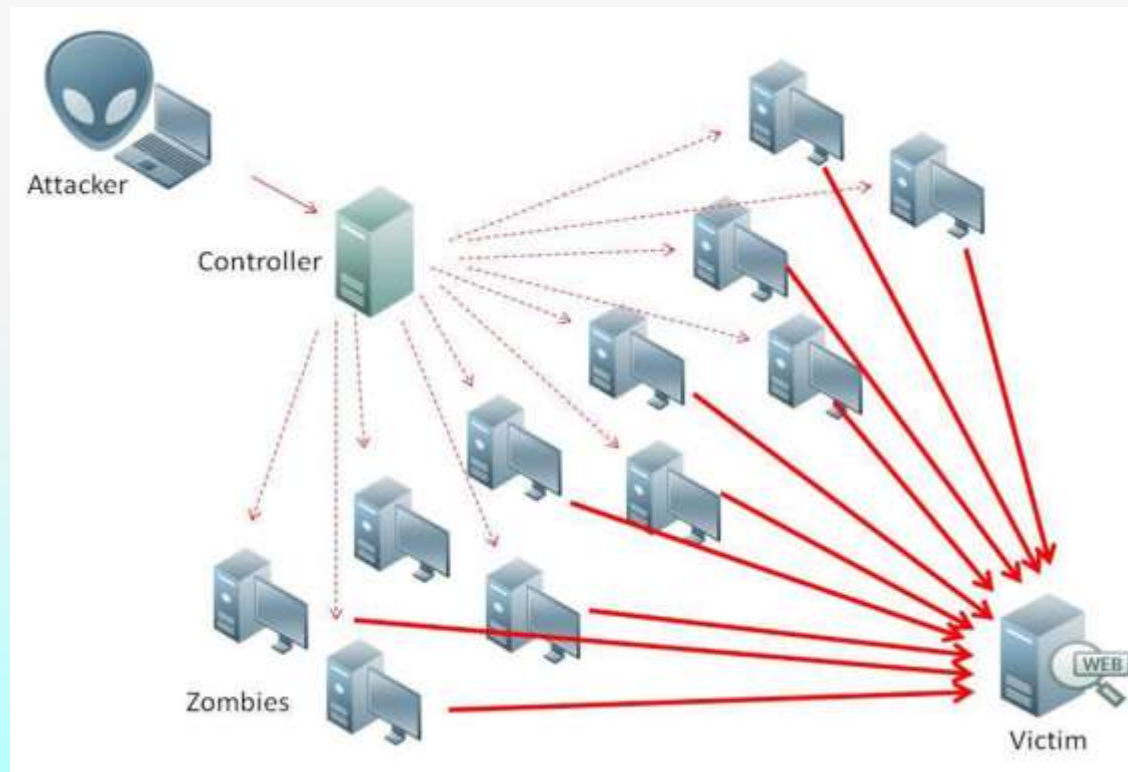
Ejemplos: DoS, DDoS, malware, etc.

ARQUITECTURA DE SEGURIDAD

Ataques a la Seguridad

Activos

d) Ejemplo de Interrupción de servicio: DDOS



ARQUITECTURA DE SEGURIDAD

Servicios de Seguridad

Aspectos Principales



ARQUITECTURA DE SEGURIDAD

Servicios de Seguridad

Otros Aspectos

También podemos mencionar otros servicios a tener en cuenta:

- ✓ **Autenticación:** Controla que la entidad que se comunica es quien dice ser.
- ✓ **No Repudio:** Prueba que el mensaje fue enviado o recibido por una entidad de la comunicación.



ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

Los mecanismos se clasifican en:

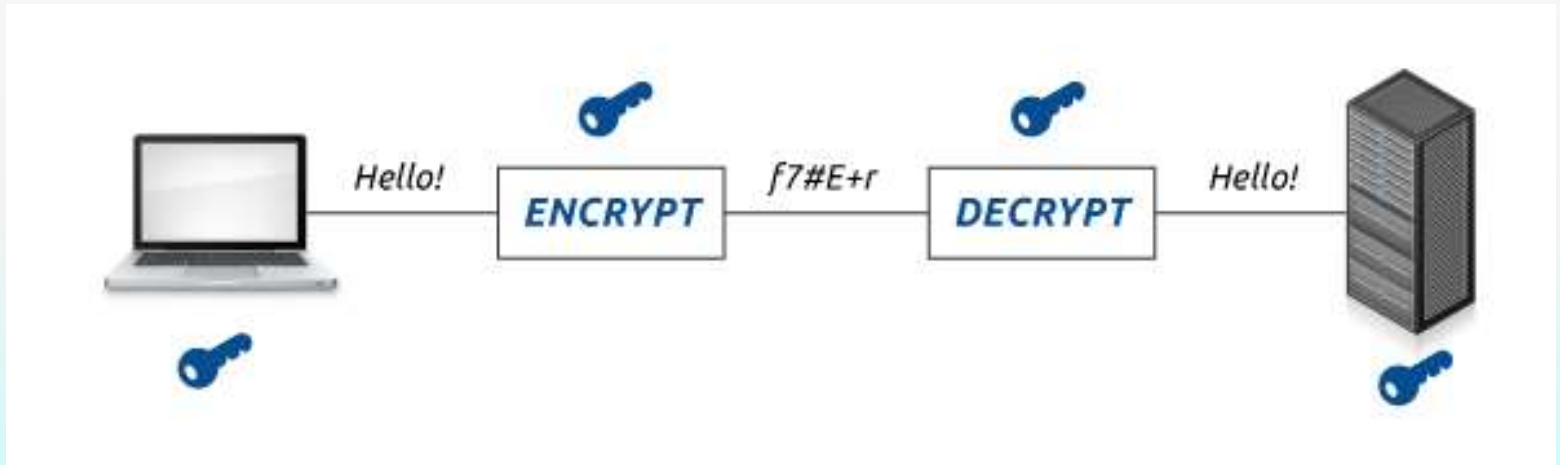
- ✓ Cifrado o encriptación
 - Asimétrico
 - Simétrico
 - Híbrido
- ✓ Integridad de datos
 - Función de Hash
 - Firma Digital
- ✓ Control de acceso
 - Firewall
 - Proxy
- ✓ Intercambio de autenticación



ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

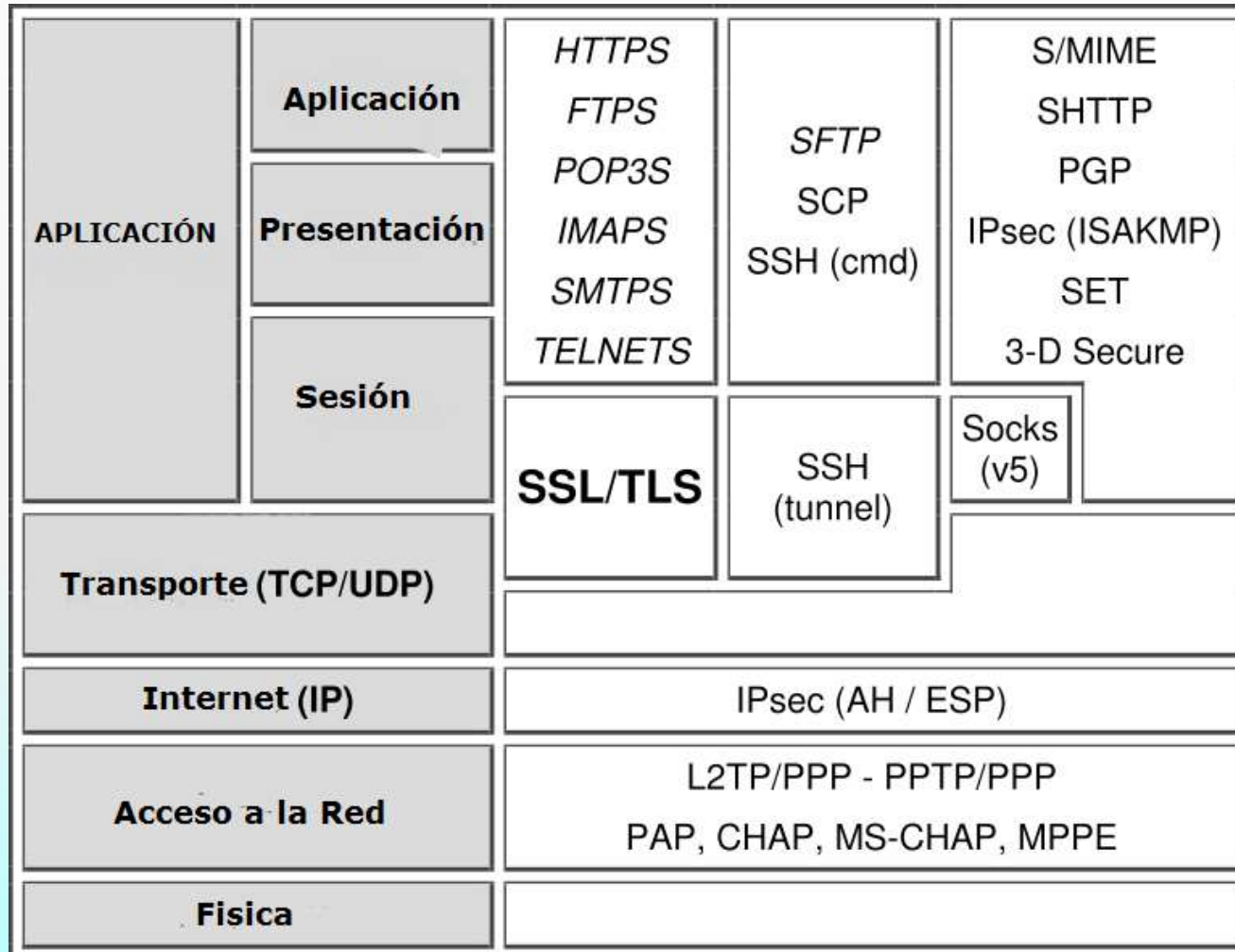
- ✓ **Cifrado:** convierte texto claro a algo inentendible mediante una traducción reversible (algoritmo de cifrado).



ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

COMUNICACIONES SEGURAS: CIFRADO





ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

CONTROL DE ACCESO: FIREWALL

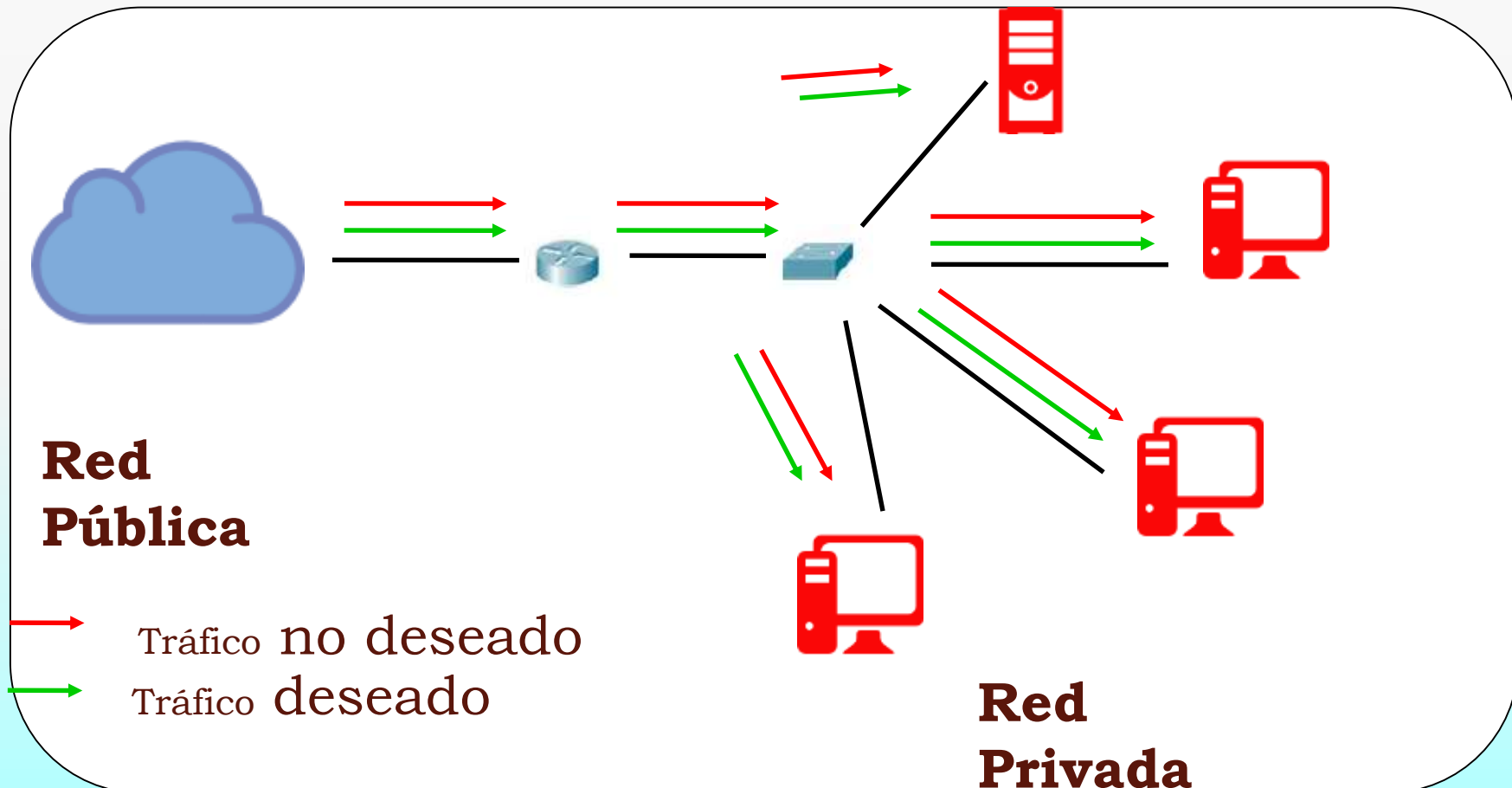




ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

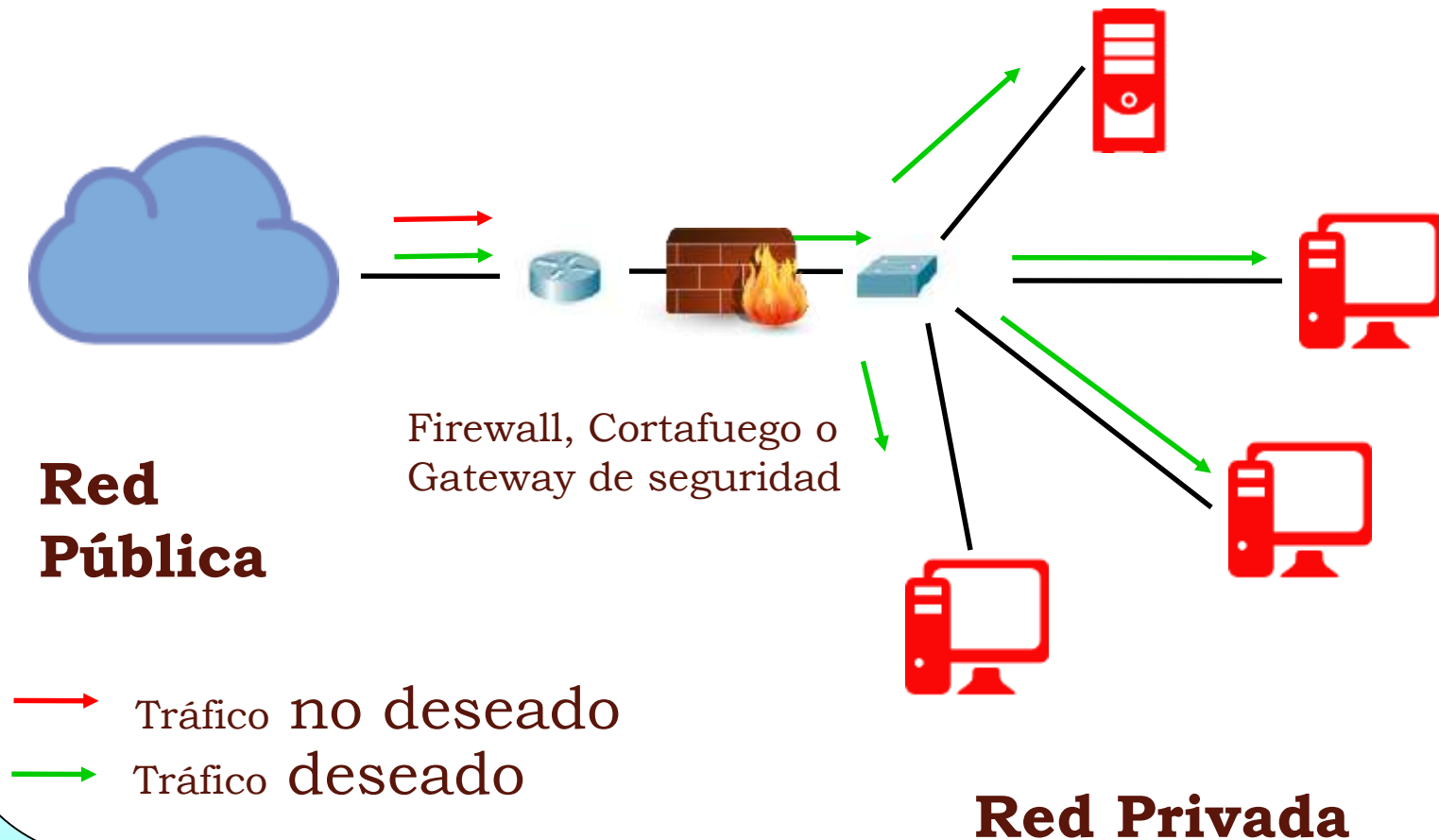
CONTROL DE ACCESO: RED SIN FIREWALL



ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

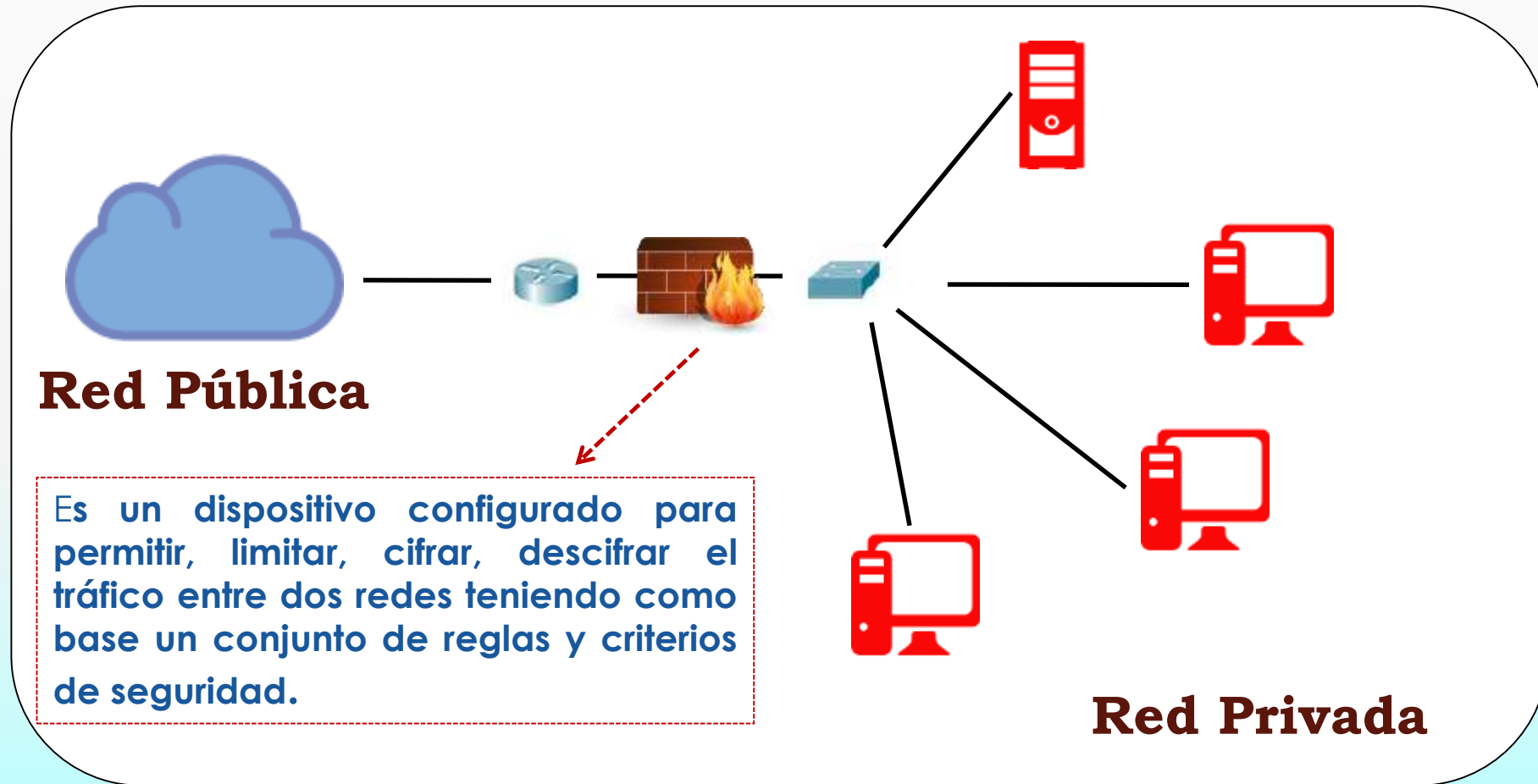
CONTROL DE ACCESO: RED CON



ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

CONTROL DE ACCESO: RED CON



Implementación: Software: iptables ----- Hardware

ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

FIREWALL

Características

- ✓ Todo el tráfico DEBE pasar por el firewall.
- ✓ Se permite SÓLO el tráfico autorizado.
- ✓ El firewall debe ser INMUNE a los ataques.
- ✓ El objetivo es CONTROLAR la información a acceder.

Funciones

- ✓ Permitir o denegar los accesos desde la red local hacia el exterior y viceversa.
- ✓ Filtrar los paquetes.
- ✓ Monitorizar el tráfico.
- ✓ Almacenar total o parcialmente los paquetes que circulan a través de él para analizarlos en caso de problemas.

ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

FIREWALL

Ventajas

- ✓ Protege de intrusiones.
- ✓ Protección de información privada.
- ✓ Disminuye el tráfico indeseado.
- ✓ Centraliza los accesos.
- ✓ Genera alarmas de seguridad.
- ✓ Monitorea y registra el uso de Internet.

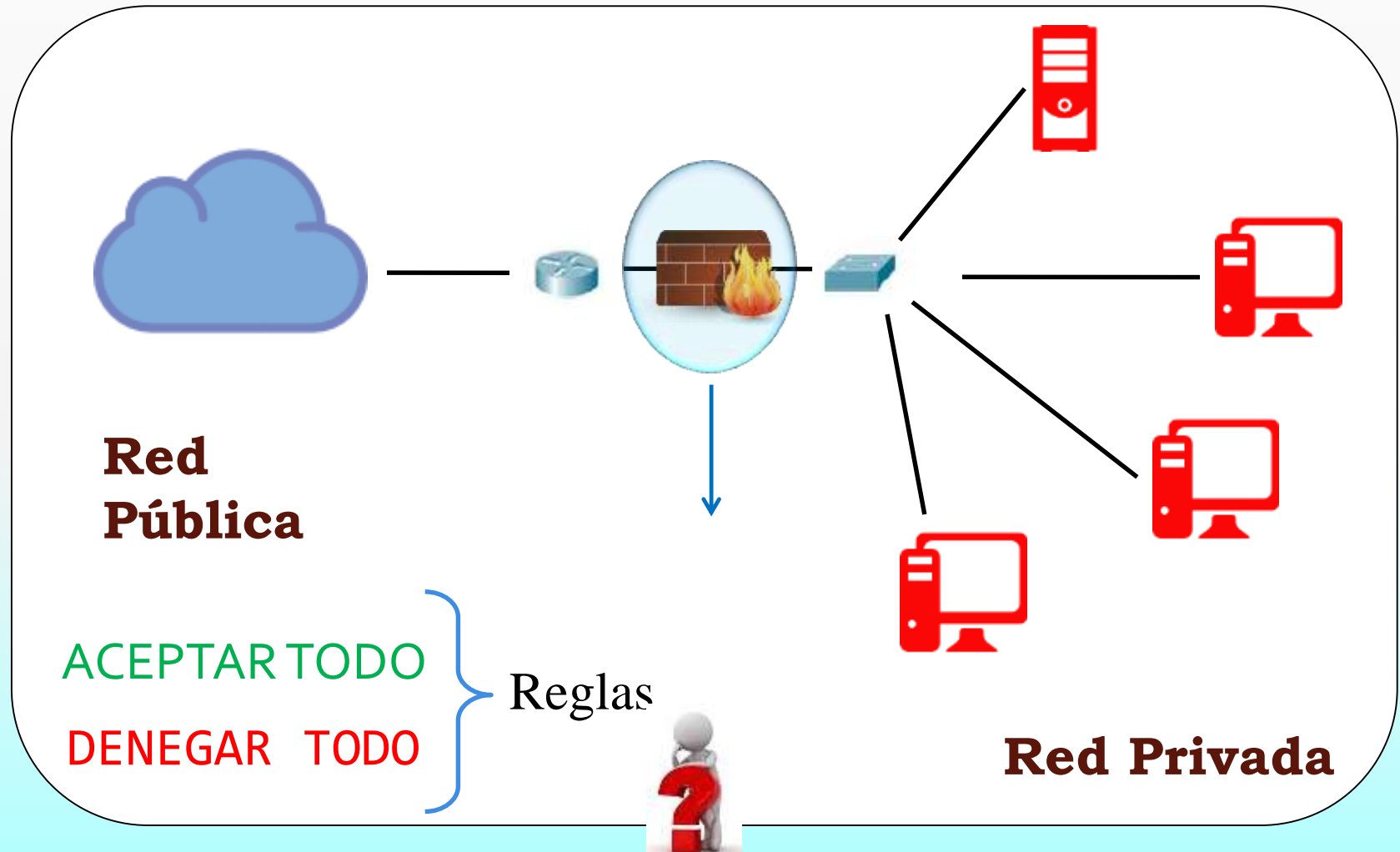
Desventajas

- ✓ No puede proteger ataques que no pasen por él.
- ✓ No puede protegerse de las amenazas a que está sometido por traidores o usuarios inconscientes.
- ✓ No puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software.
- ✓ No protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico.

ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

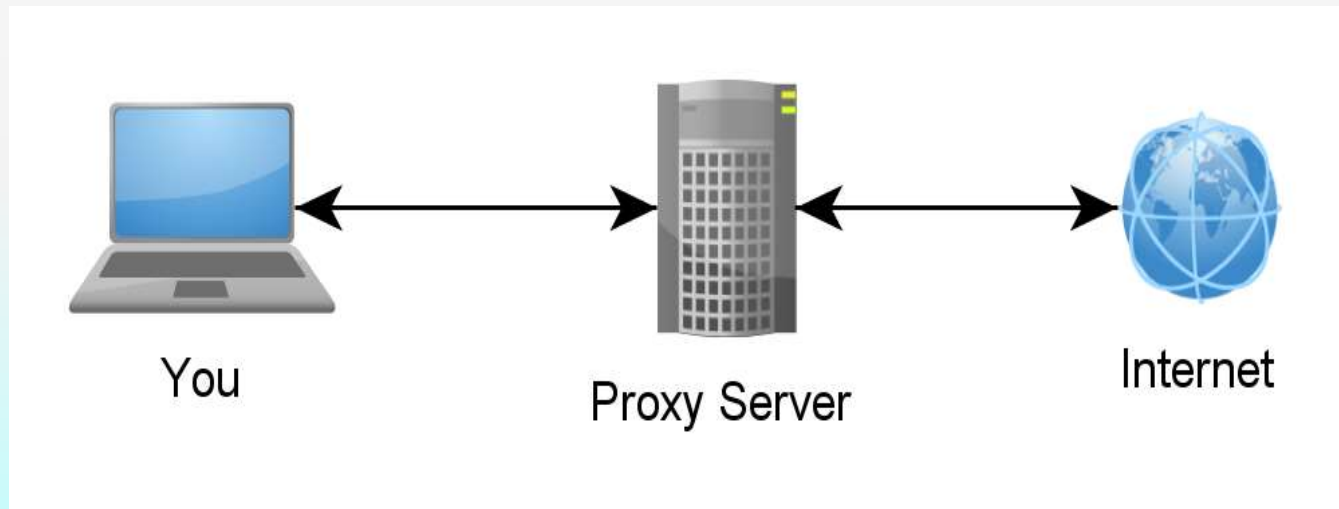
POLÍTICA DE FIREWALL



ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

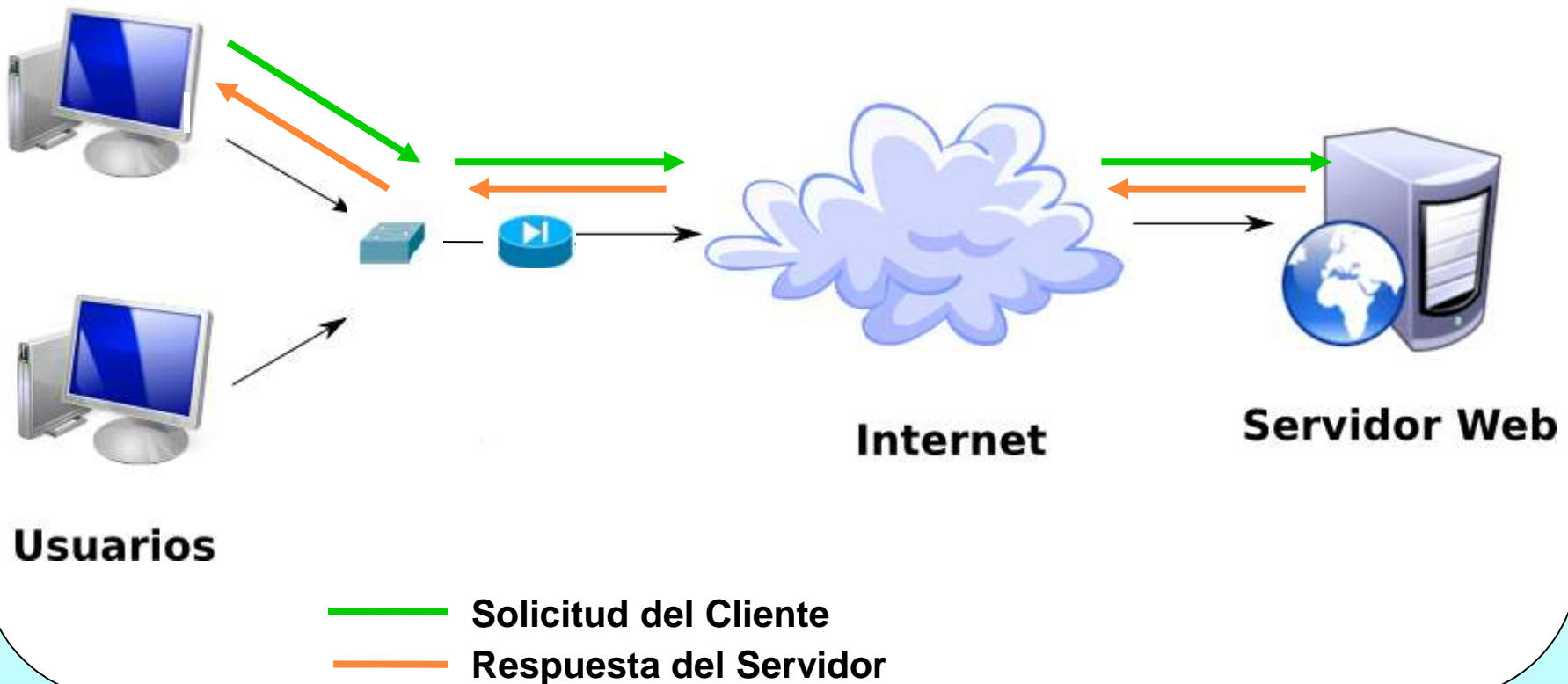
CONTROL DE ACCESO: PROXY



ARQUITECTURA DE SEGURIDAD





Mecanismos de Seguridad

CONTROL DE ACCESO: RED SIN PROXY



CONTROL DE ACCESO: RED CON PROXY

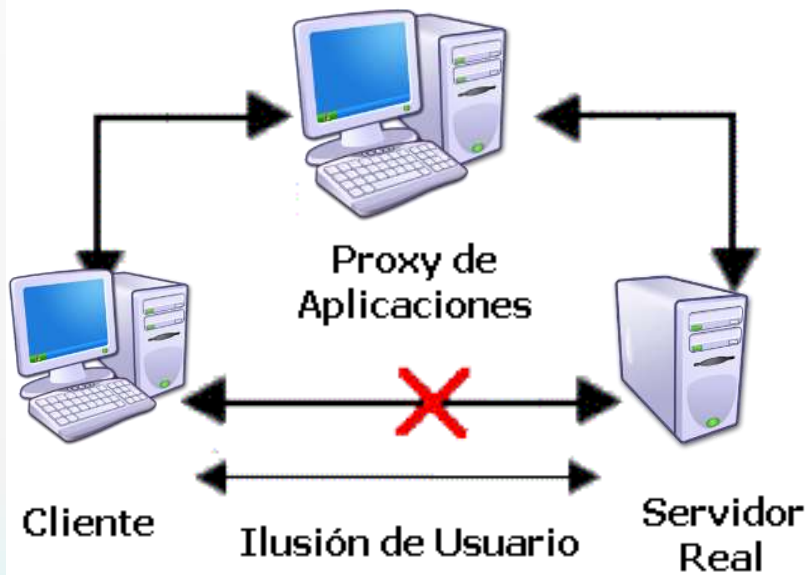
cliente

-  Solicitud del Cliente
-  Solicitud del Proxy
-  Respuesta del Servidor
-  Respuesta del Proxy

ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY



Es un programa o dispositivo que actúa como *intermediario* (en representación de otro) entre el programa cliente y el servidor.

Objetivo:

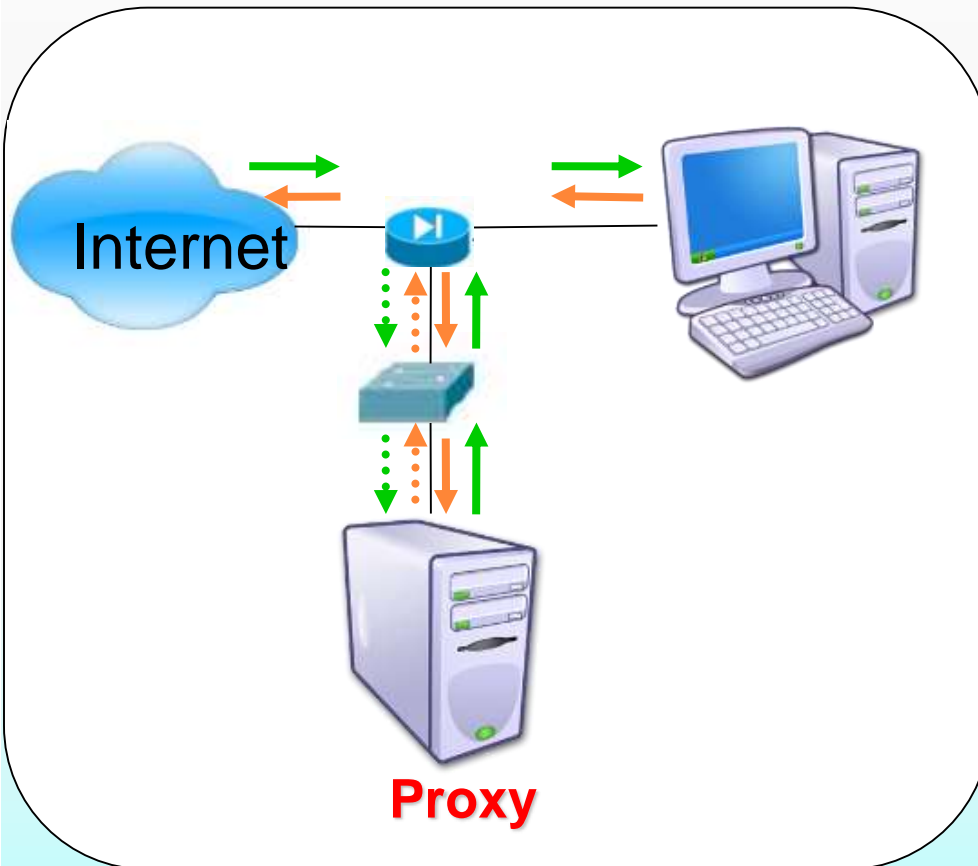
Evitar la comunicación directa entre la computadora que solicita el servicio con el servidor real.

ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY

FUNCIONES



- ✓ Mantener máquinas en el anonimato.
- ✓ Aplicar políticas de acceso a servicios.
- ✓ Auditar el uso de Internet.
- ✓ Escaneo del contenido en busca de malware antes de reenviarlo.
- ✓ Mejorar el tiempo de respuesta y ahorro de tráfico

ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY-CACHE

Un servidor proxy mantiene copia de pedidos frecuentemente solicitados en una memoria local denominada memoria caché.

Permitiendo:

- ✓ Mejorar Performance
- ✓ Incrementar el Ancho de Banda

Utilizando para ello Algoritmos de manejo de caché

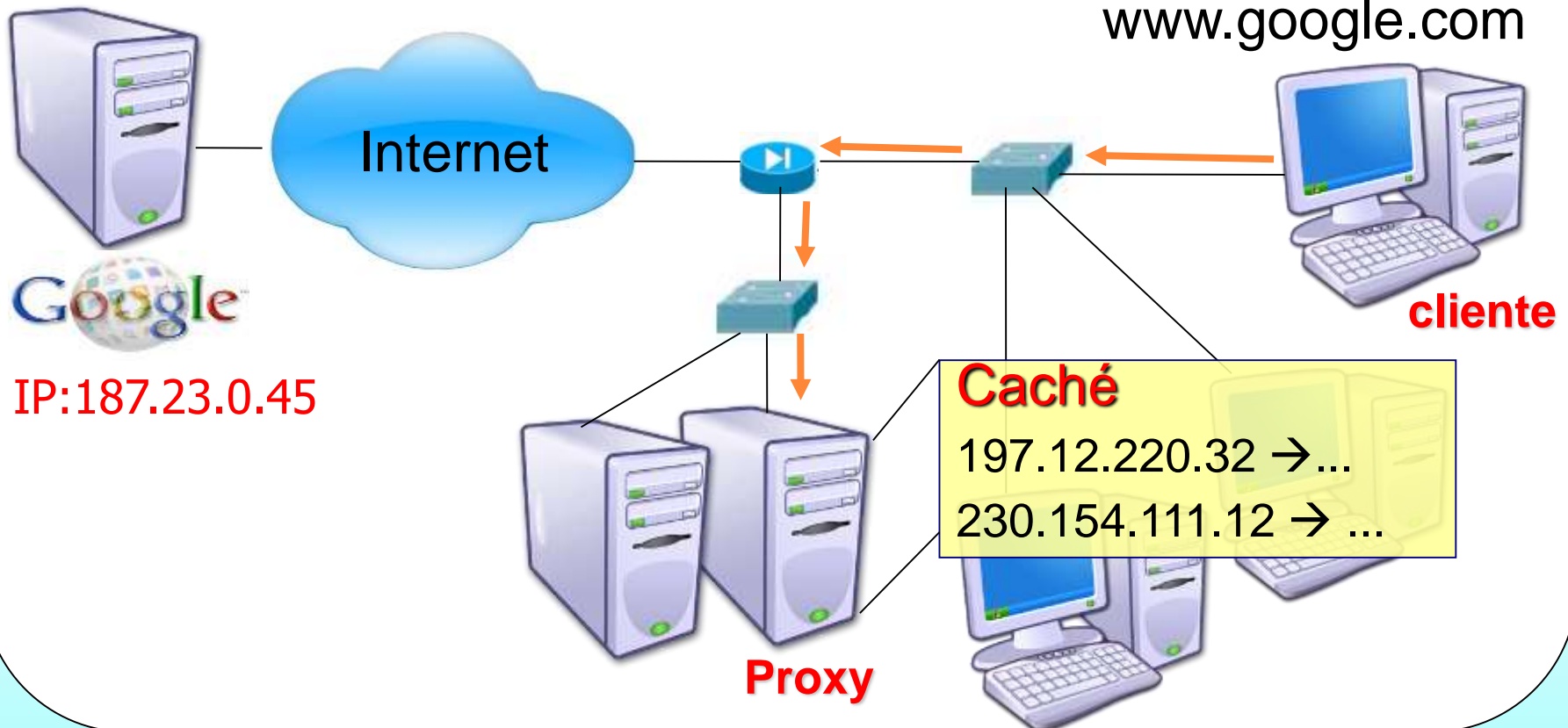
ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY-CACHE

Solicitud de servicio con proxy

1° Paso

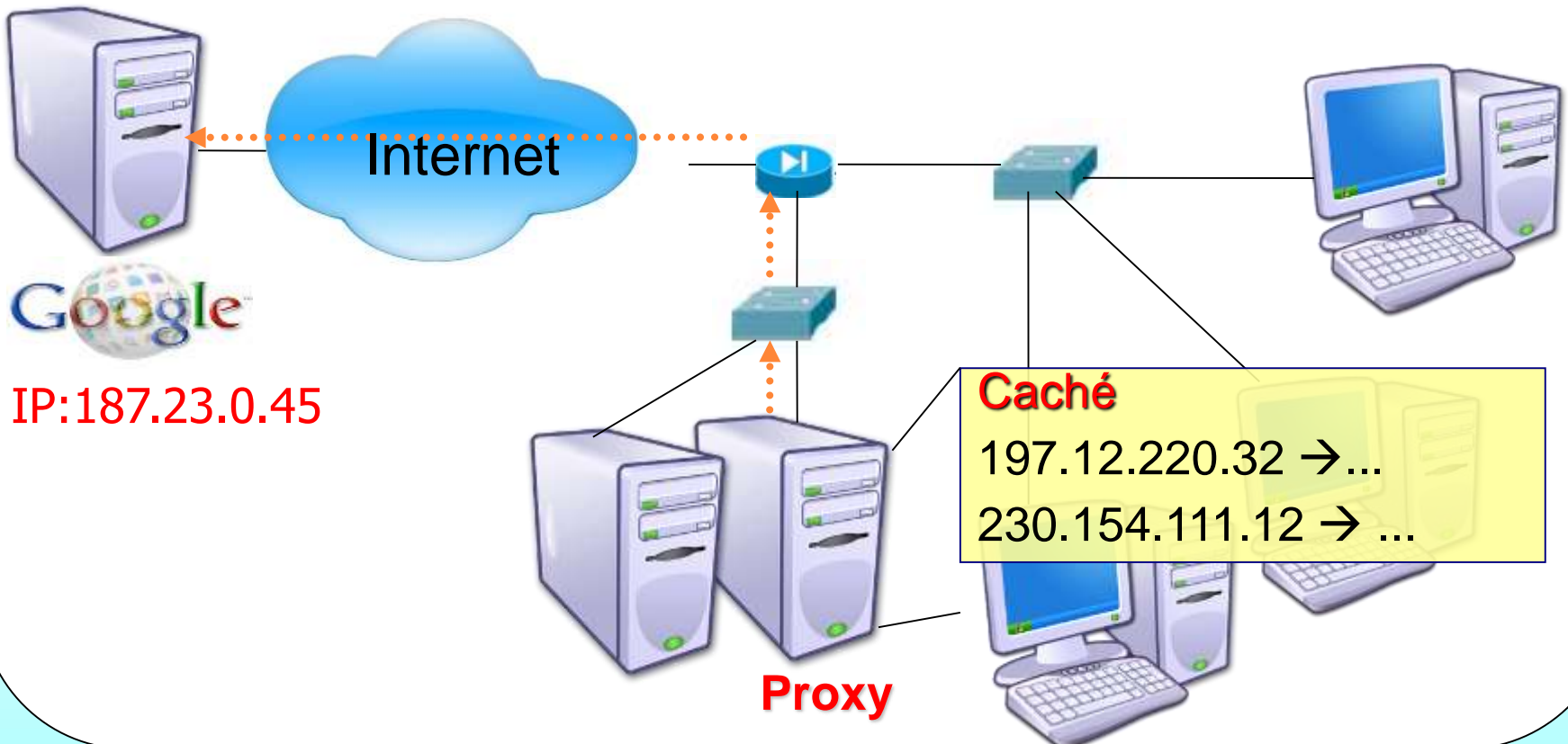


ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY-CACHE

Solicitud de servicio con proxy
2º Paso

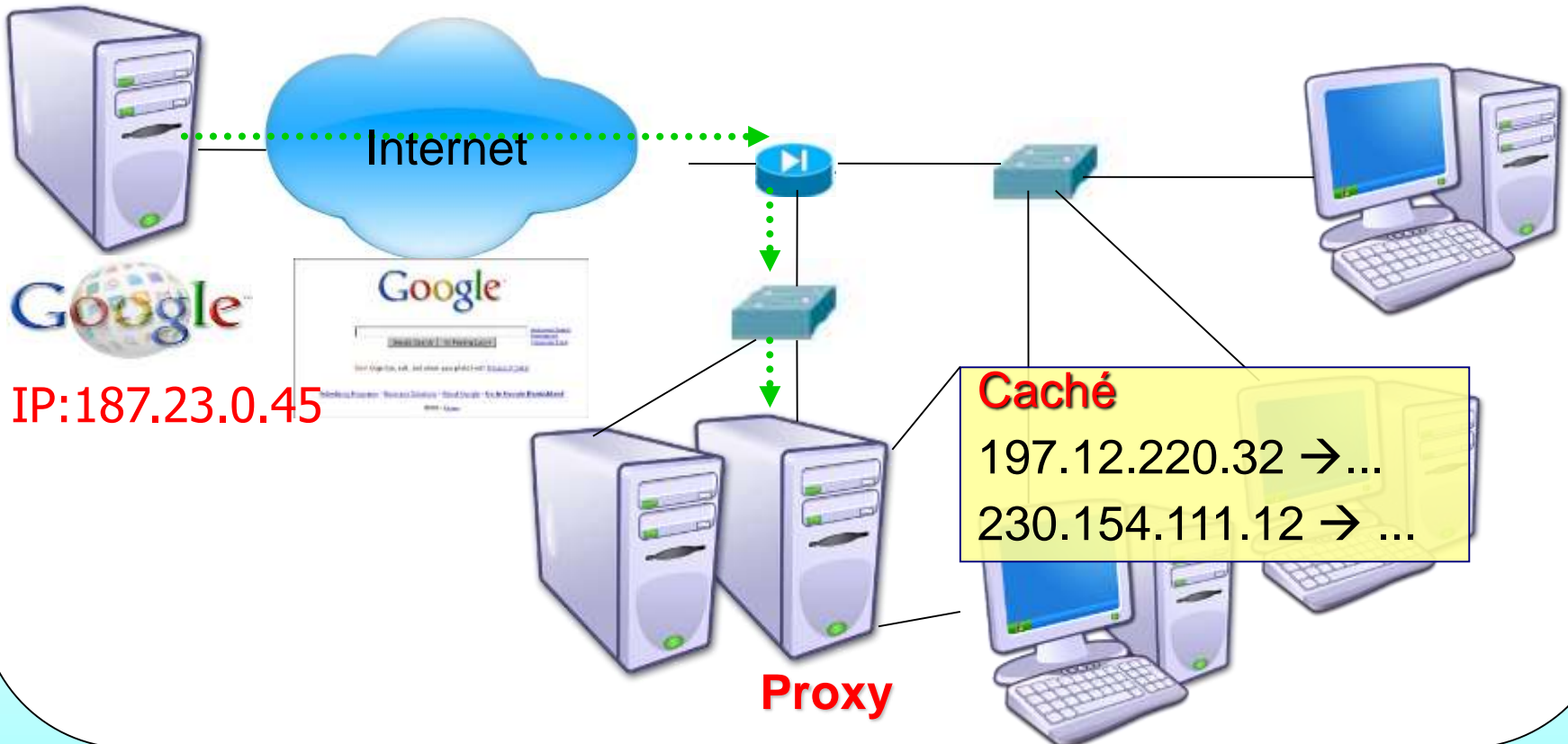


ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY-CACHE

Solicitud de servicio con proxy
3° Paso

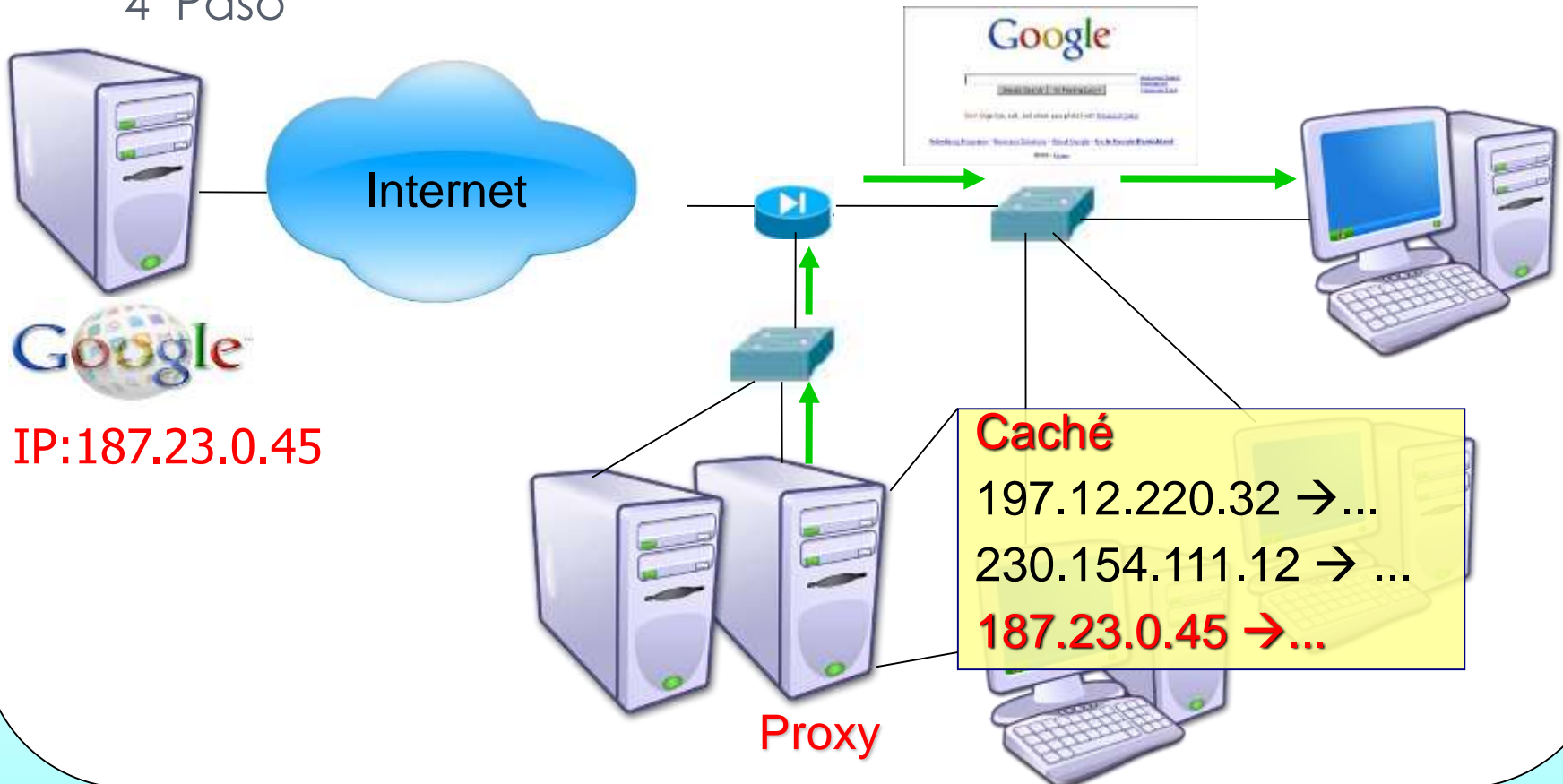


ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY-CACHE

Solicitud de servicio con proxy
4° Paso

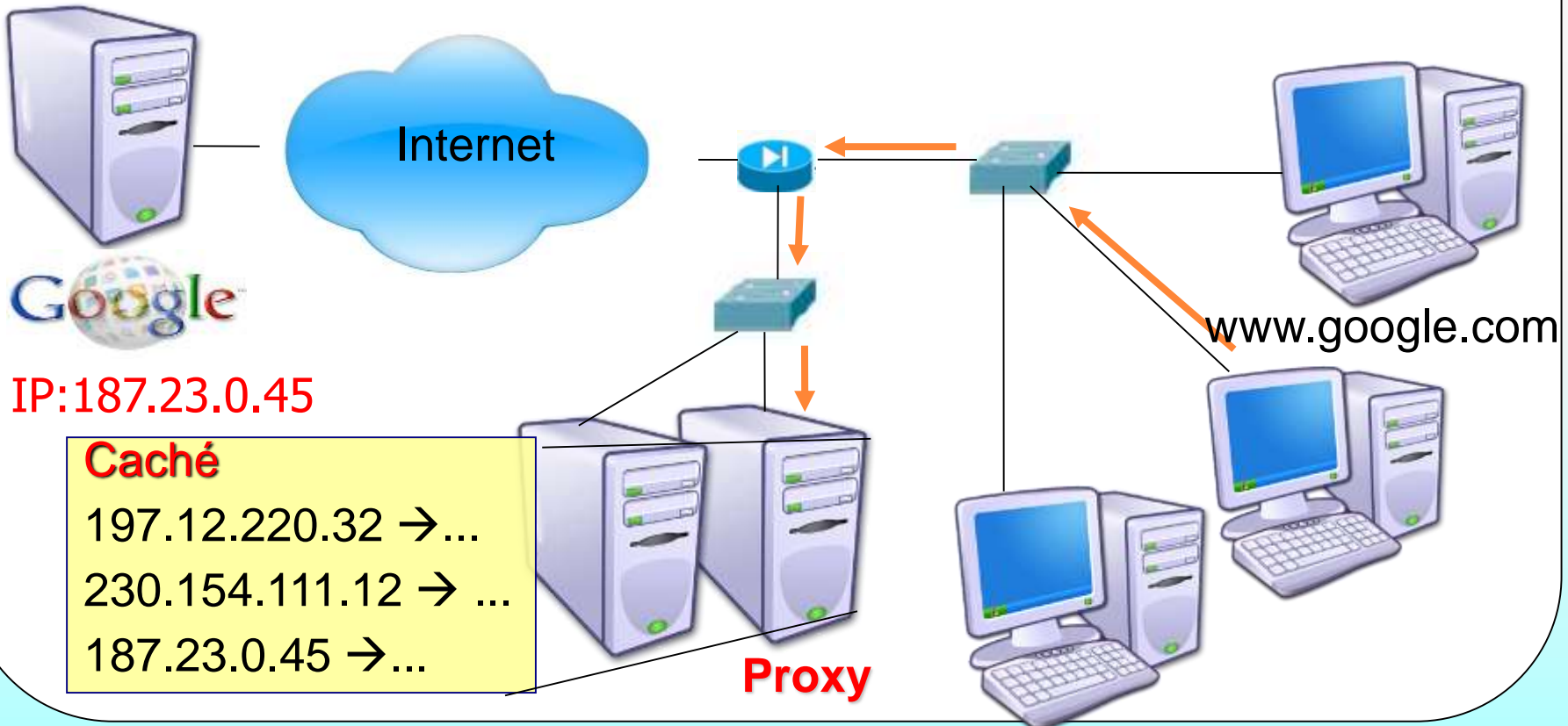


ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad

PROXY-CACHE

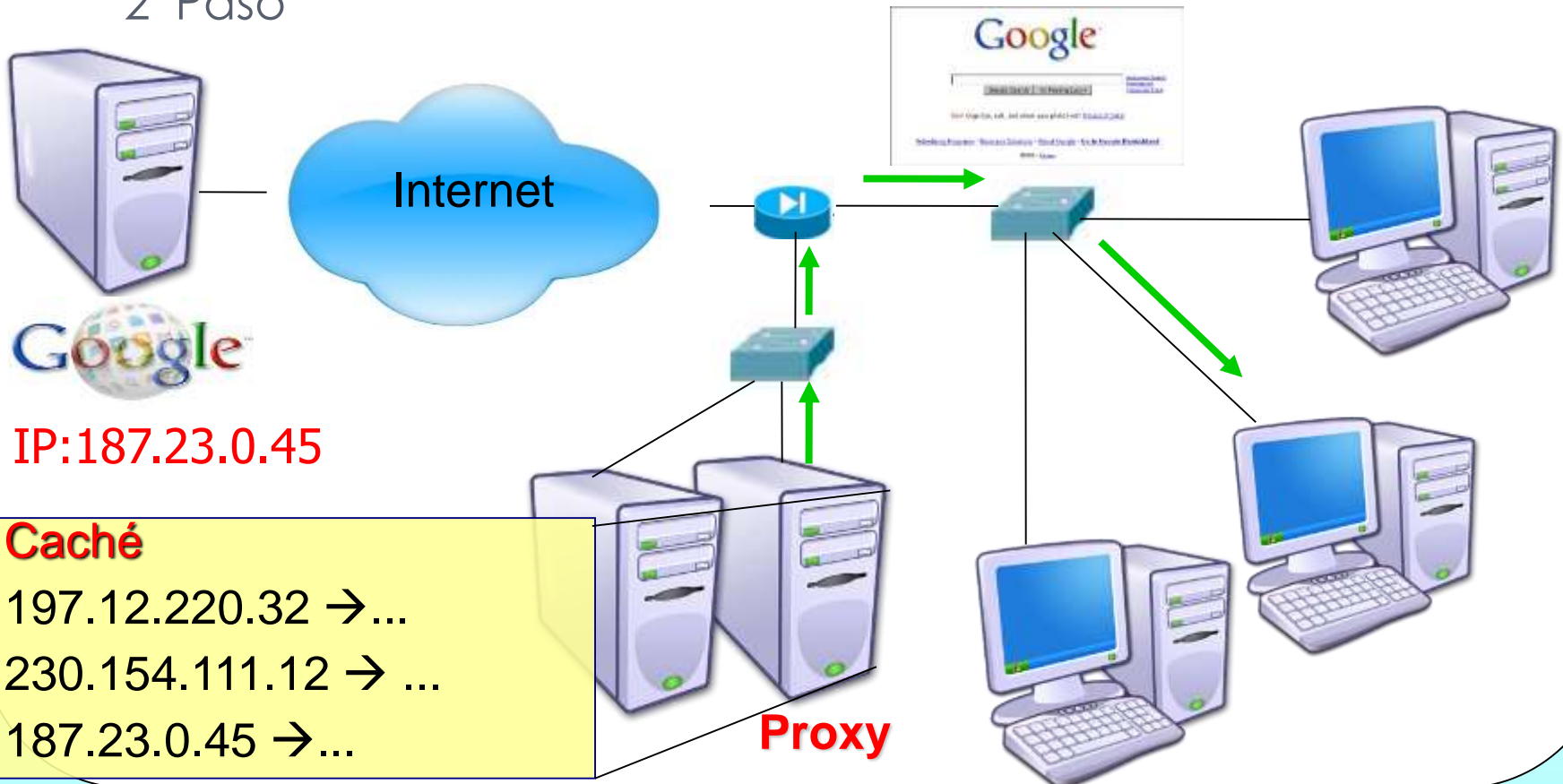
Nueva solicitud de servicio con proxy
1º Paso



PROXY-CACHE

Nueva solicitud de servicio con proxy

2° Paso



ARQUITECTURA DE SEGURIDAD

Mecanismos de Seguridad **PROXY**

Ventajas

- ✓ Ahorro de Tráfico
- ✓ Velocidad en Tiempo de respuesta
- ✓ Filtrado de contenidos
- ✓ Anonimato

Desventajas

- ✓ **Intromisión:** se puede no querer guardar copias de los datos.
- ✓ **Incoherencia de caché:** es posible que el proxy dé una respuesta equivocada.
- ✓ **Sobrecarga.**

RESUMEN

Implementación de los servicios a través de los diversos mecanismos:

Confidencialidad

- Encriptación

Integridad

- Encriptación

Control de Acceso

- Firewall
- Proxy

Autenticación

- Acceso encriptado: https
- Acceso remoto: ssh

Disponibilidad

- Redundancia
- Backup