INTERNET Y BLOQUEOS

Andres Azpurua, VE inteligente

“Internet interpreta la censura como un daño y busca rutas alrededor”

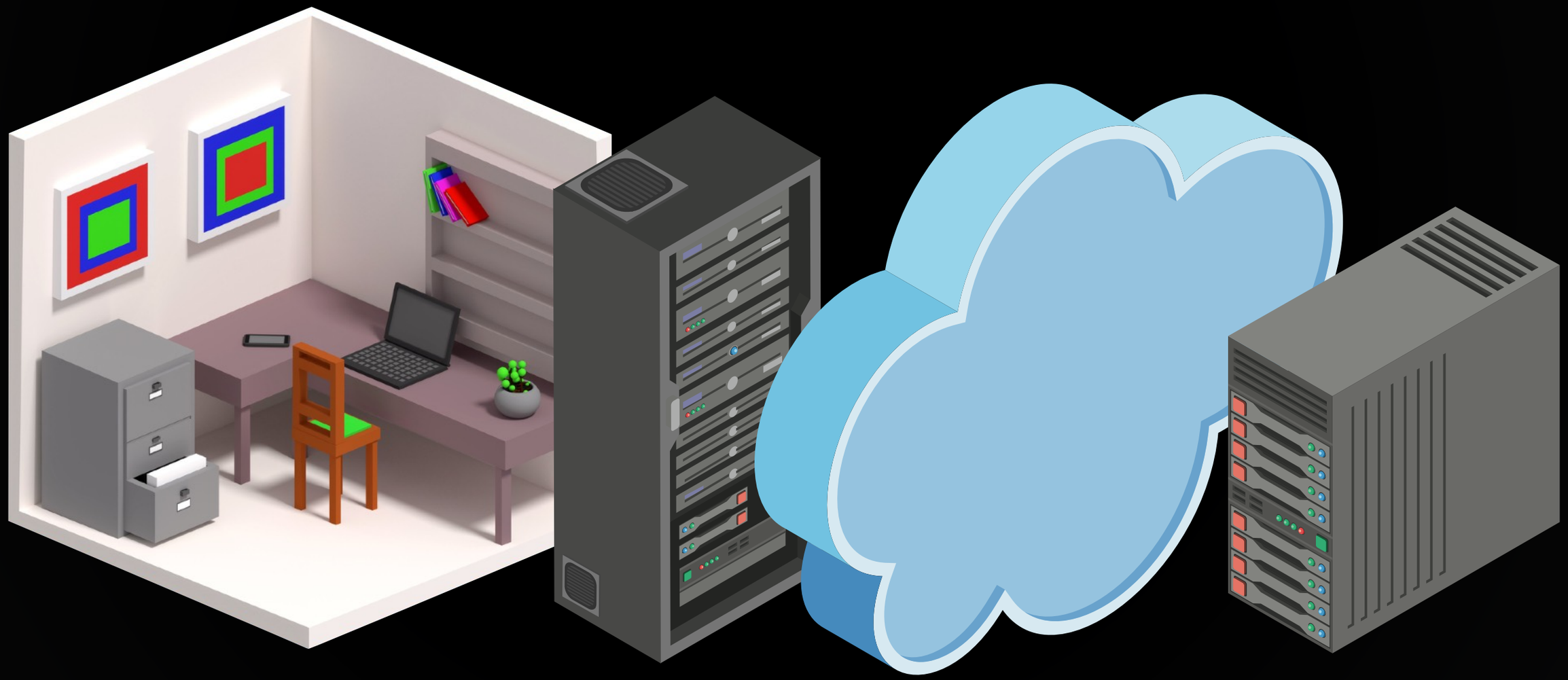
/ John Gilmore

¿Qué dudas y prioridades tienen?

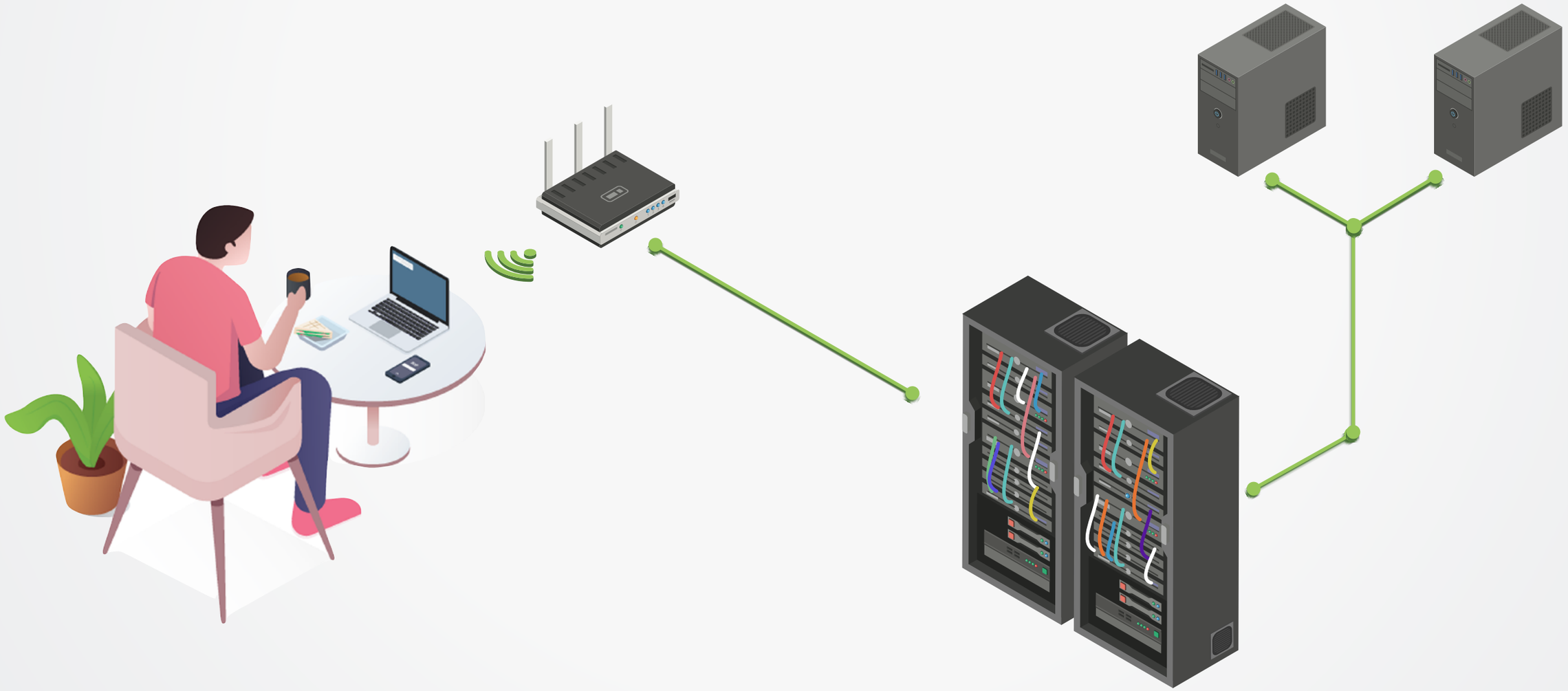
A LO BÁSICO:

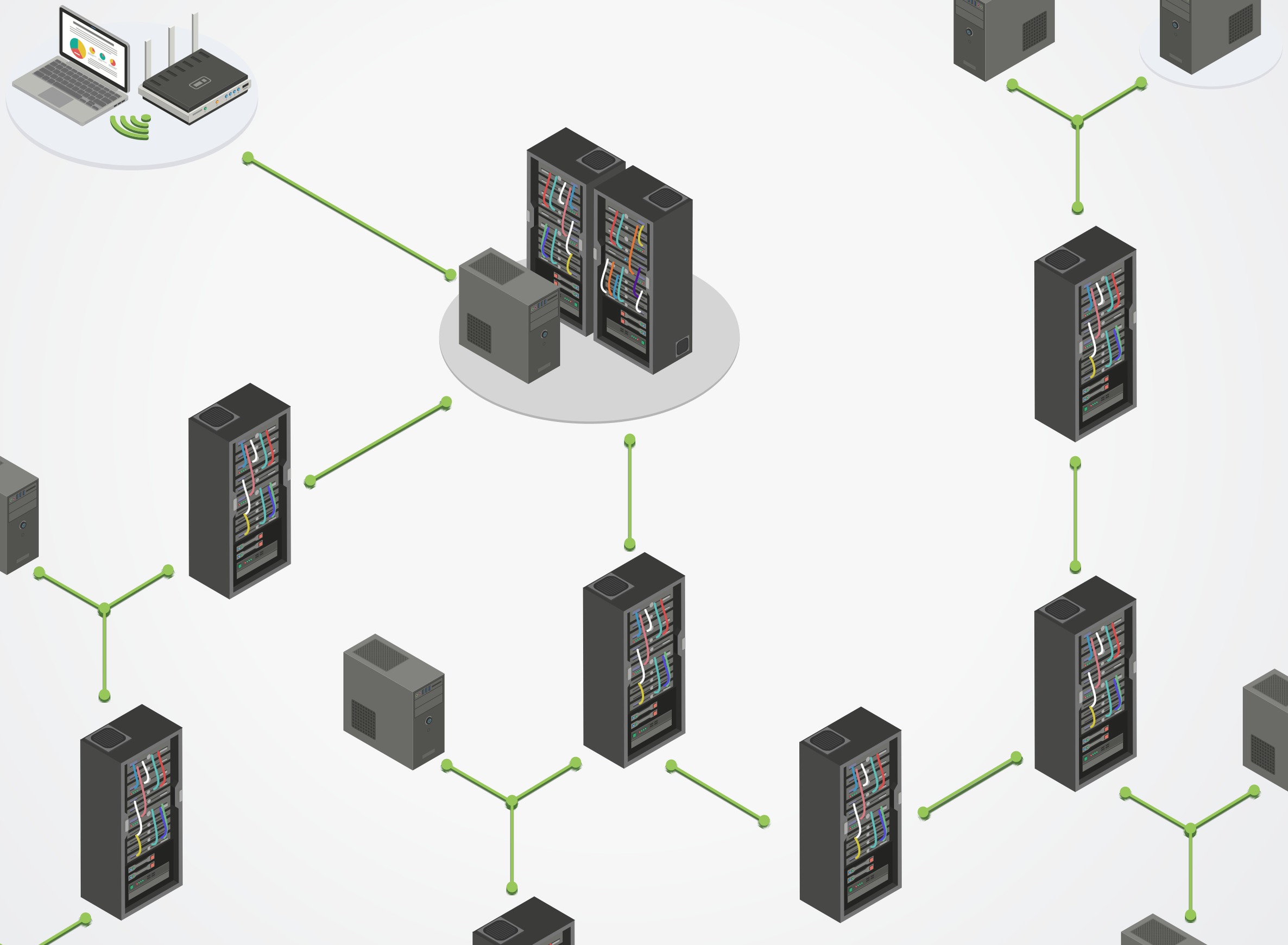
ENTENDIENDO INTERNET

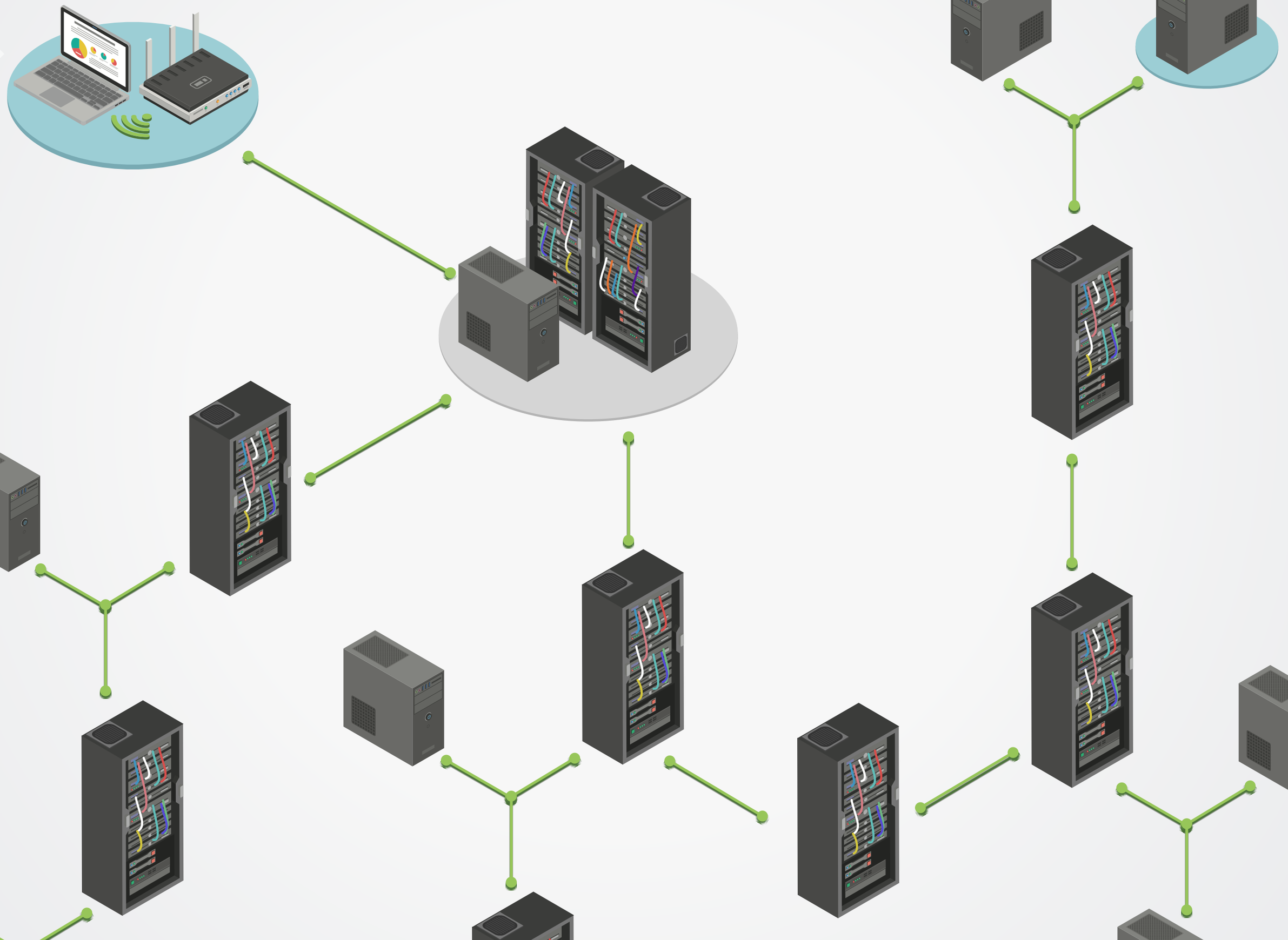
Internet es...

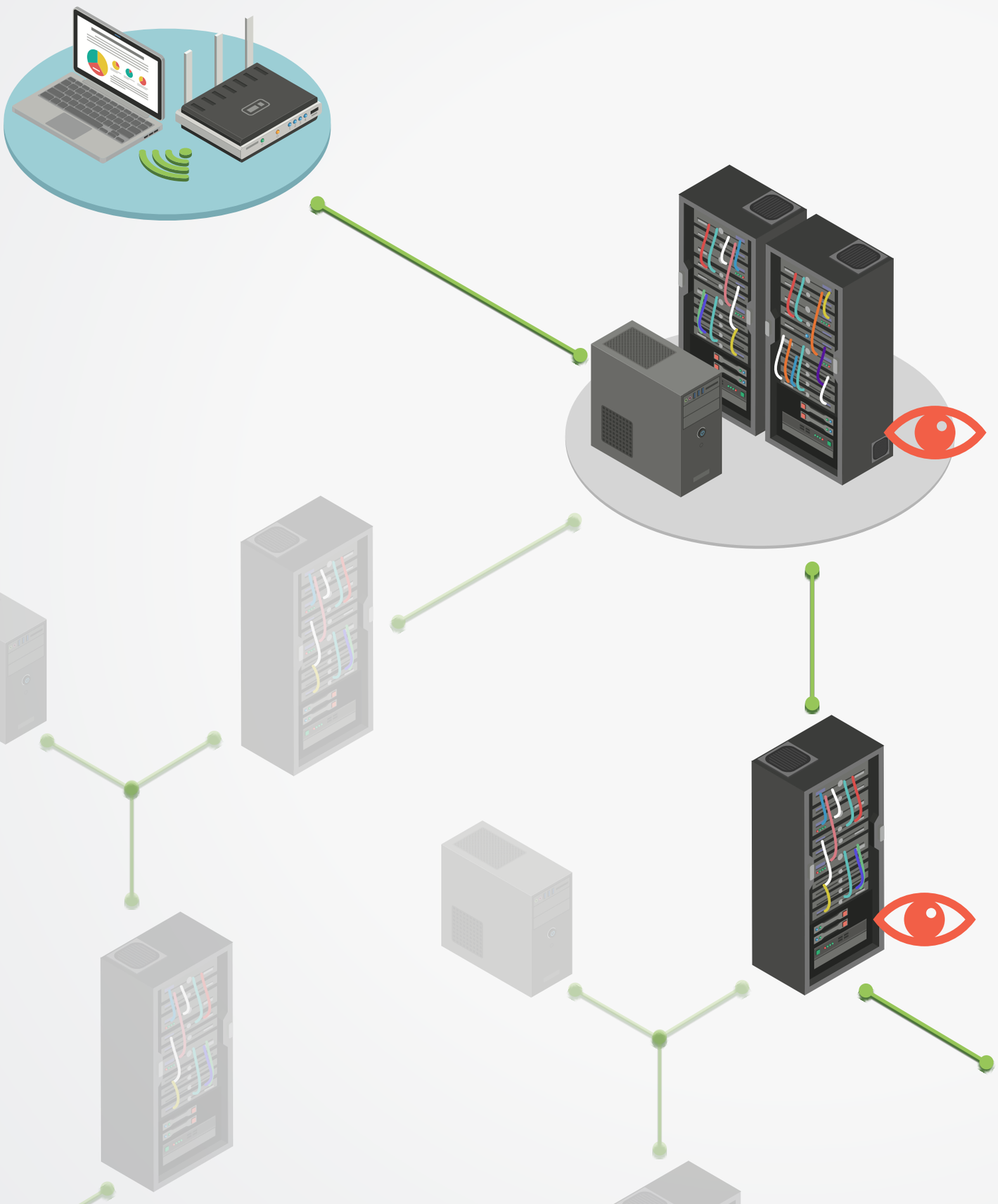


De forma simplificada



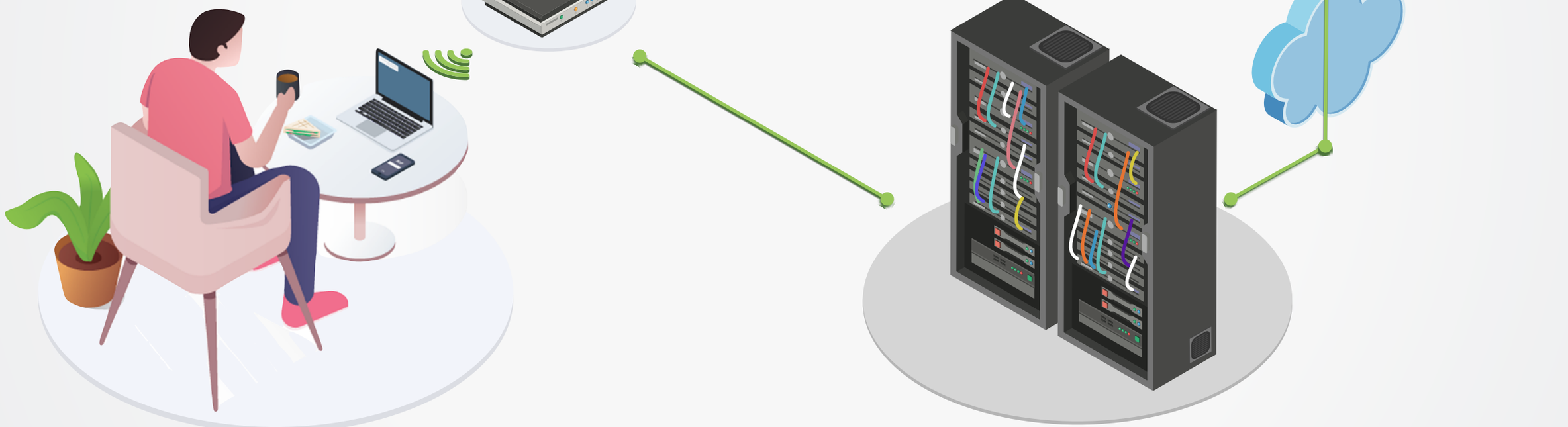






Servidor

Router



Equipos personales

Proveedor de Internet (ISP)

EJERCICIO

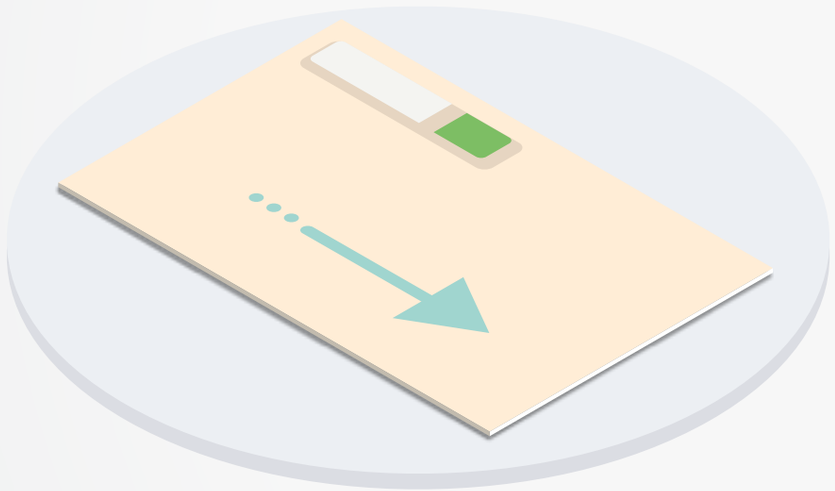
INTERNET DE GENTE

Vulnerabilidades del internet

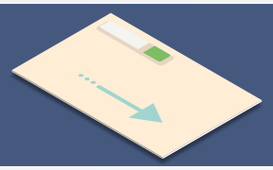
- Diseño ingenuo
- **Son como postales,**
  no como cartas
- Muchas manos en la masa
- Confianza en carteros
- Principio de “mejor esfuerzo"

Paquete

Paquete



- Dirección de **Destino**
- Dirección de **Origen**
- Puerto (proposito)
- Secuencia
- **Contenido**



Paquete (simplificado)

IP origen

IP destino

TCP

(ó UDP)

Puerto

Secuencia

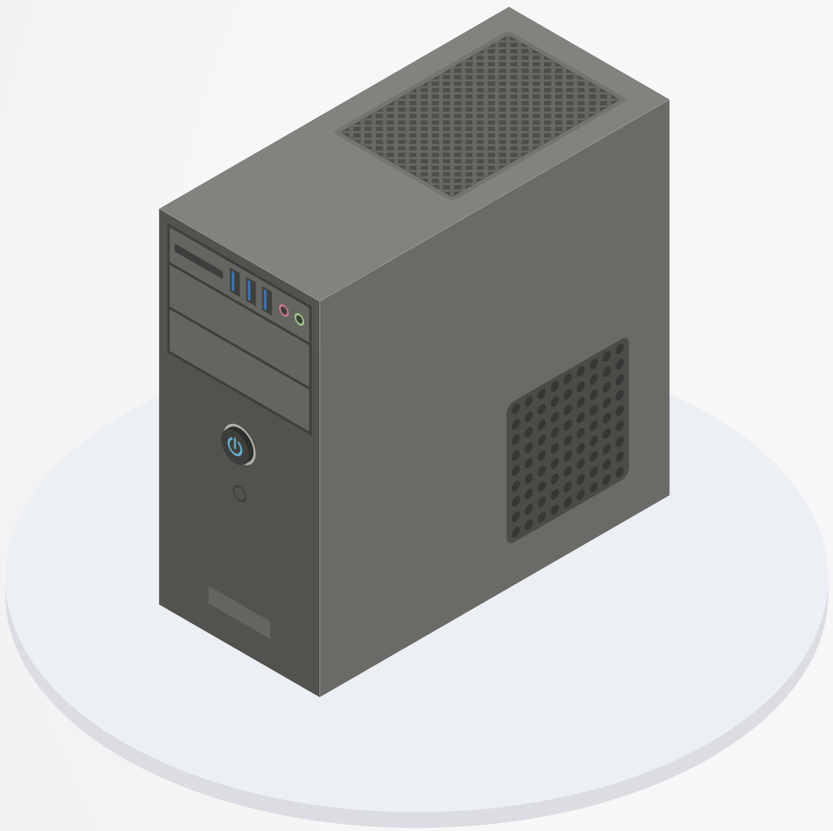
Contenido

HTTP

GET

Host: google.com

Servidor

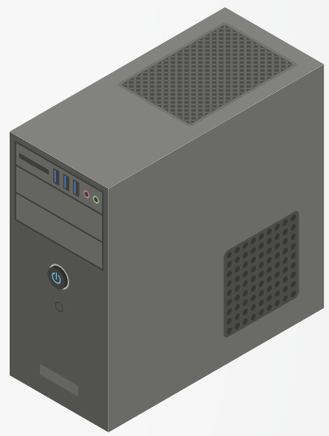


- **Dirección IP**
- Dirección de hardware
- Capacidad para **servir** una o más **aplicaciones**

Dirección IP

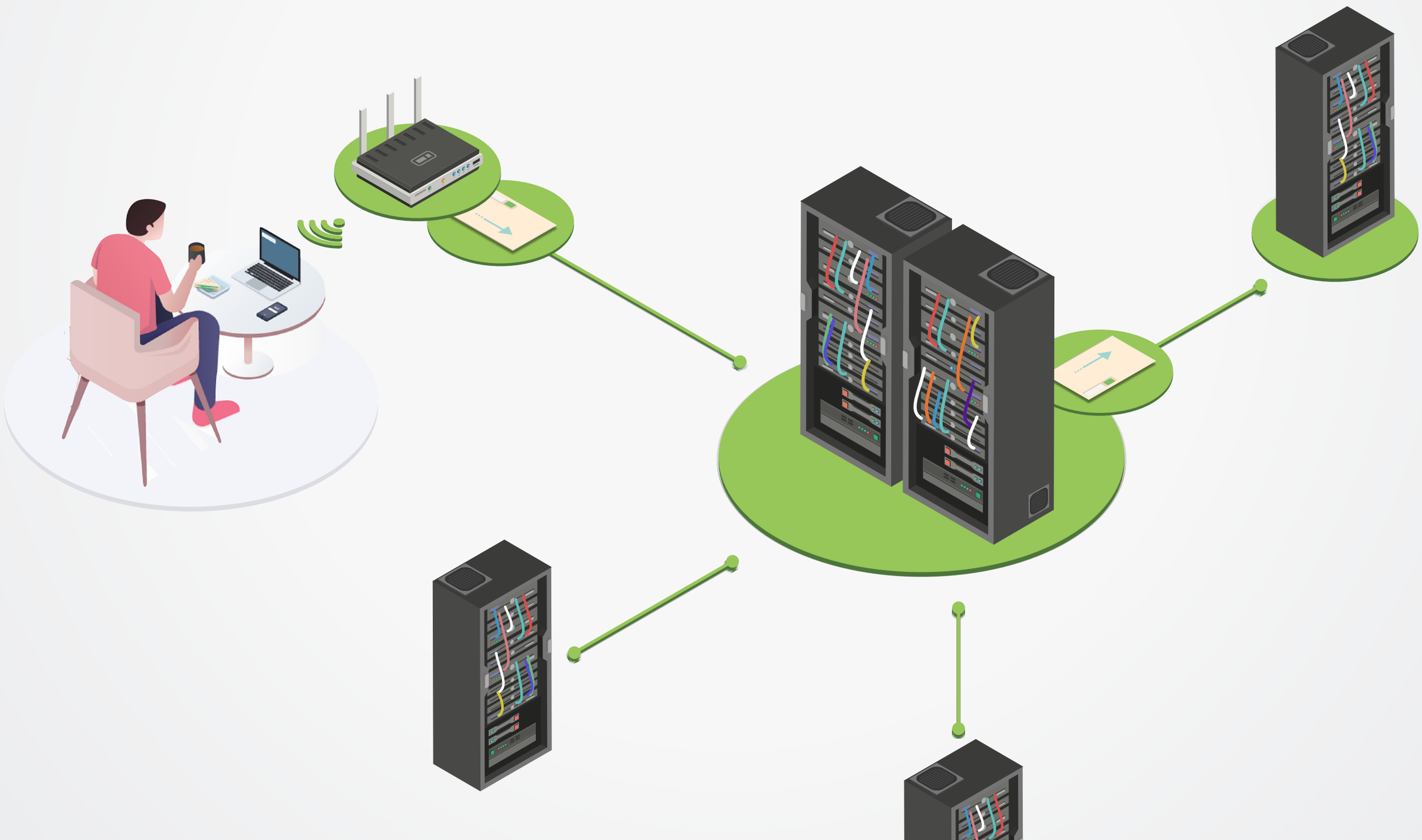
192.168.0.102
(Dirección interna)

46.16.64.188

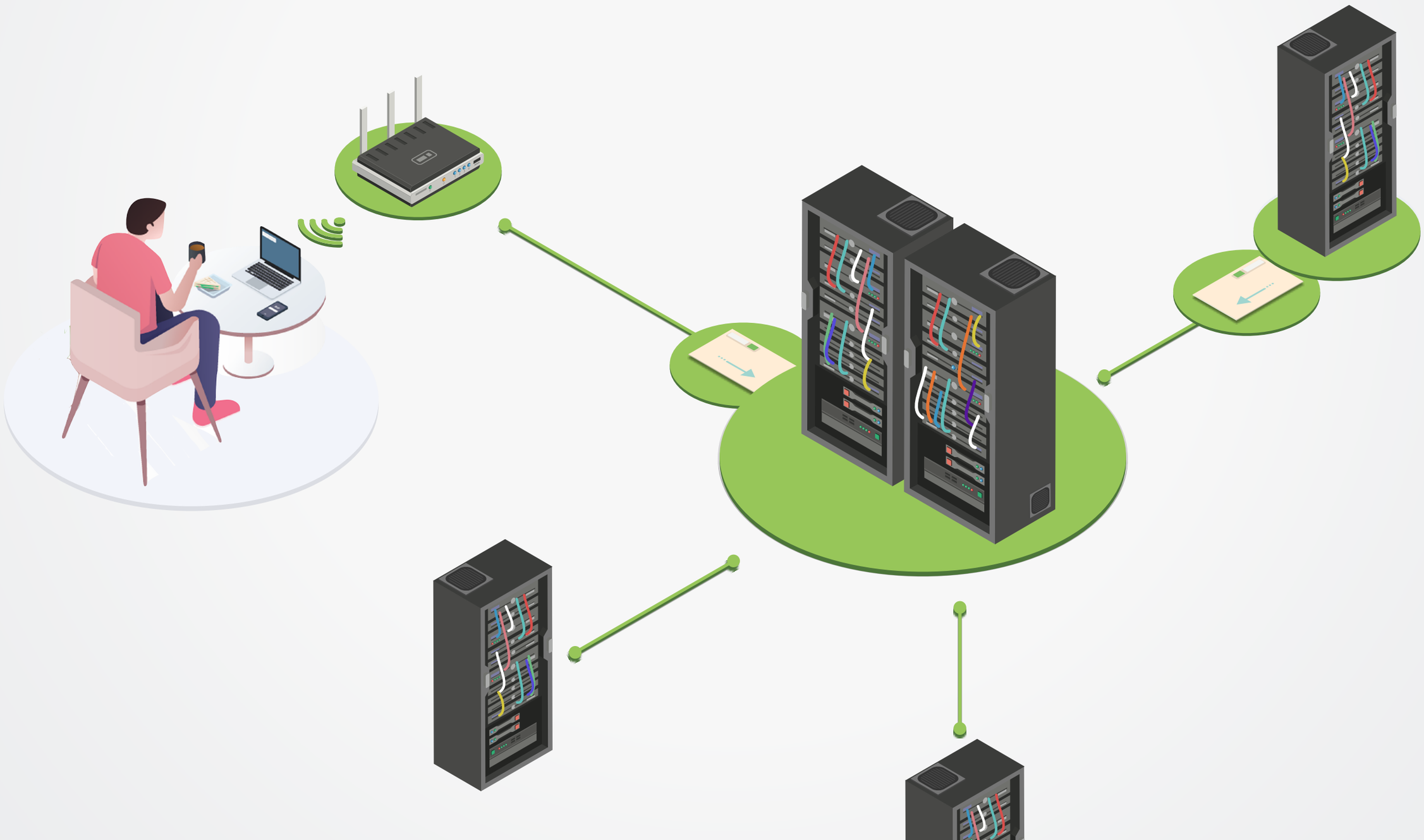


77.235.208.171

Paquetes



Paquetes



CÓMO FUNCIONAN

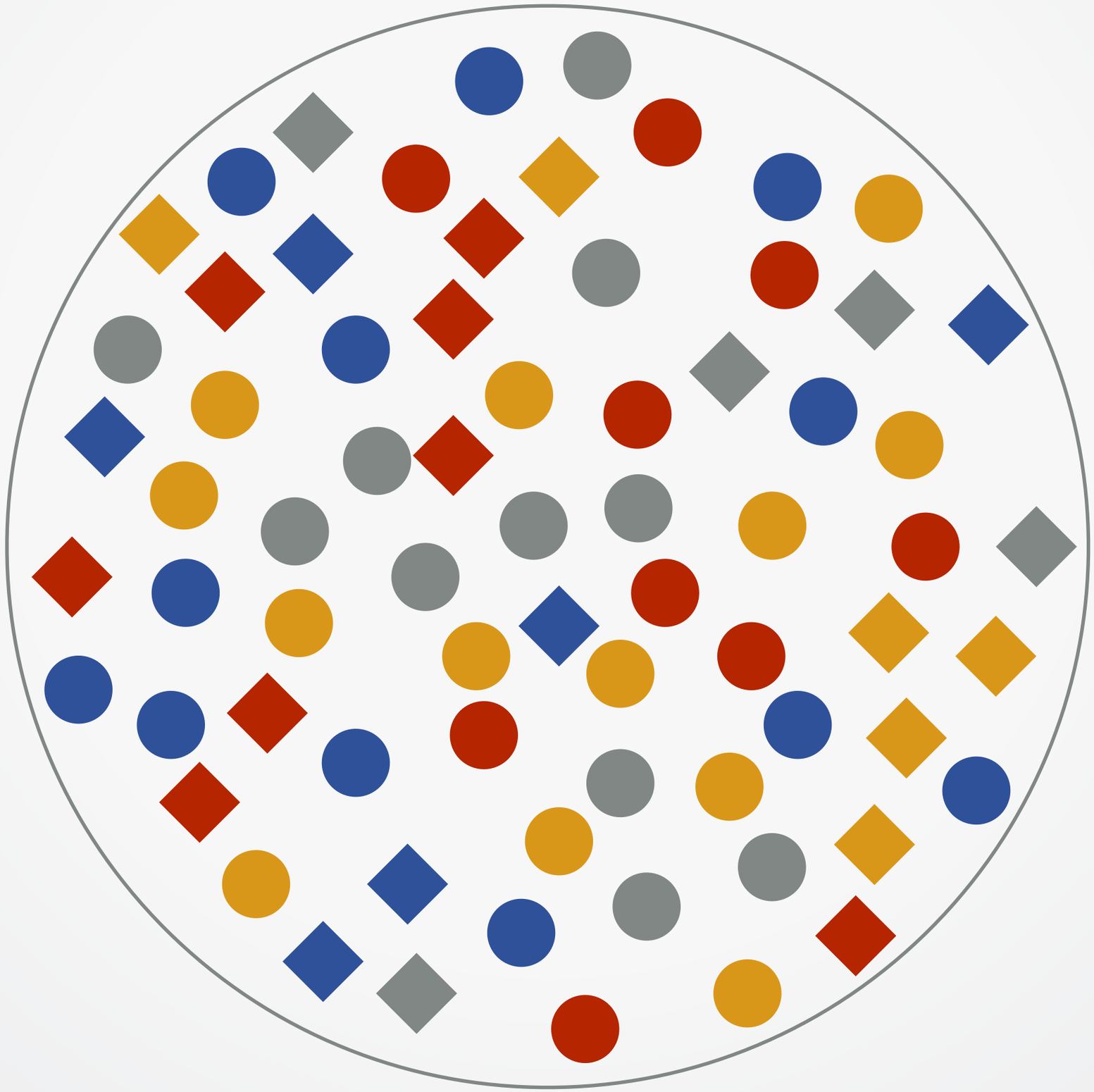
LOS BLOQUEOS

Bloqueo de internet

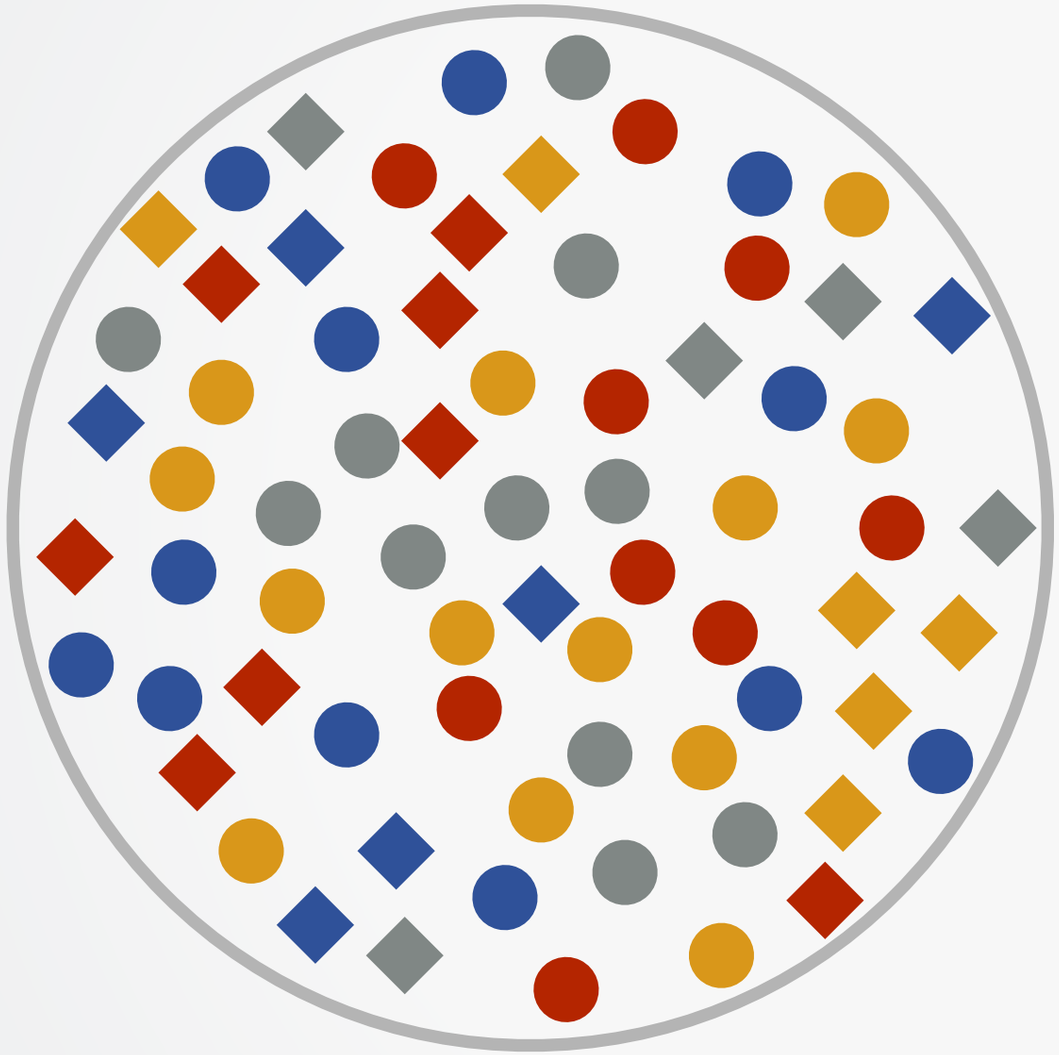
Bloqueo de internet

Medida técnica con la intención de **impedir acceso** a una información, servicio o servidor **en internet.**

¿Qué deseas bloquear hoy?



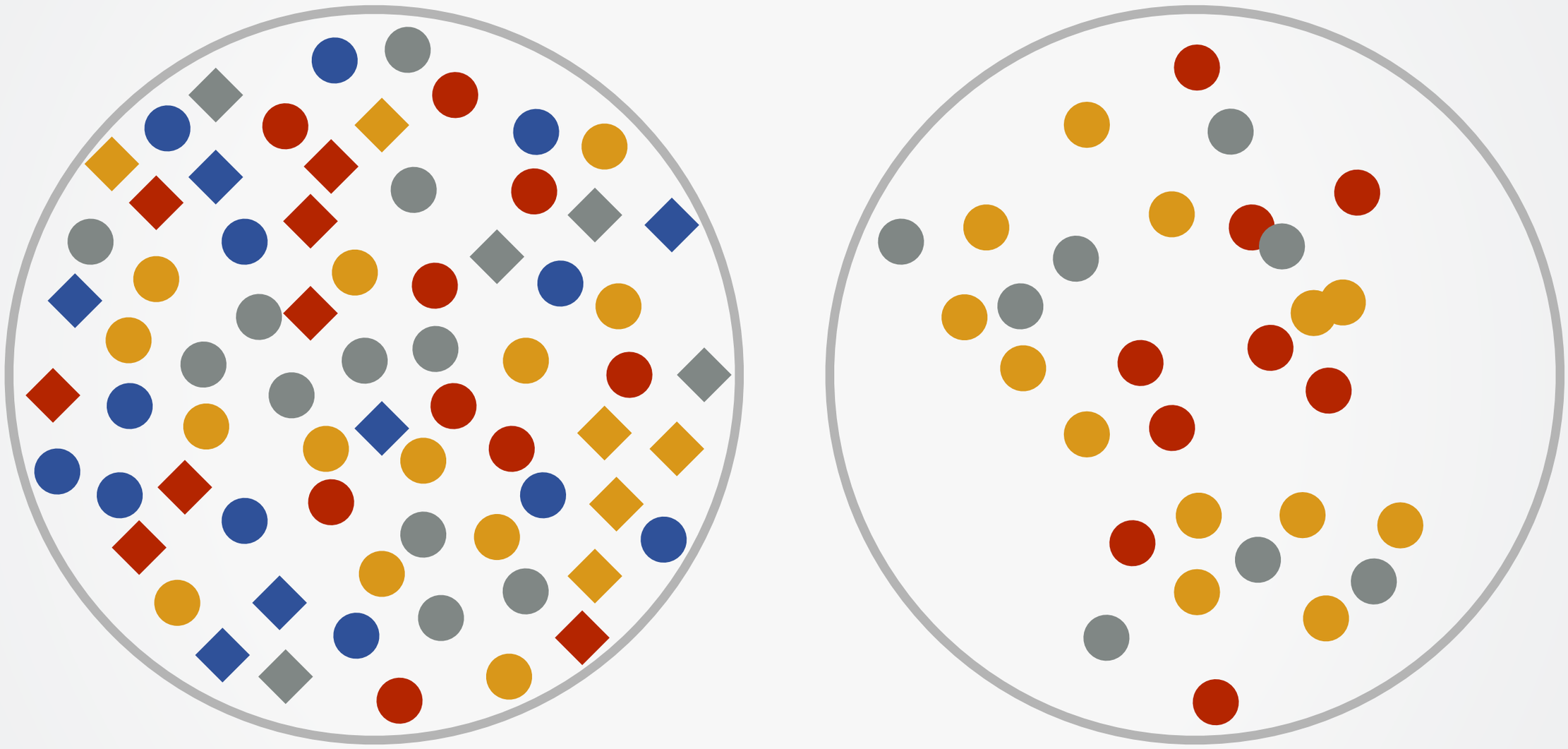
¿Qué debería pasar el filtro?



Como se define qué bloquear

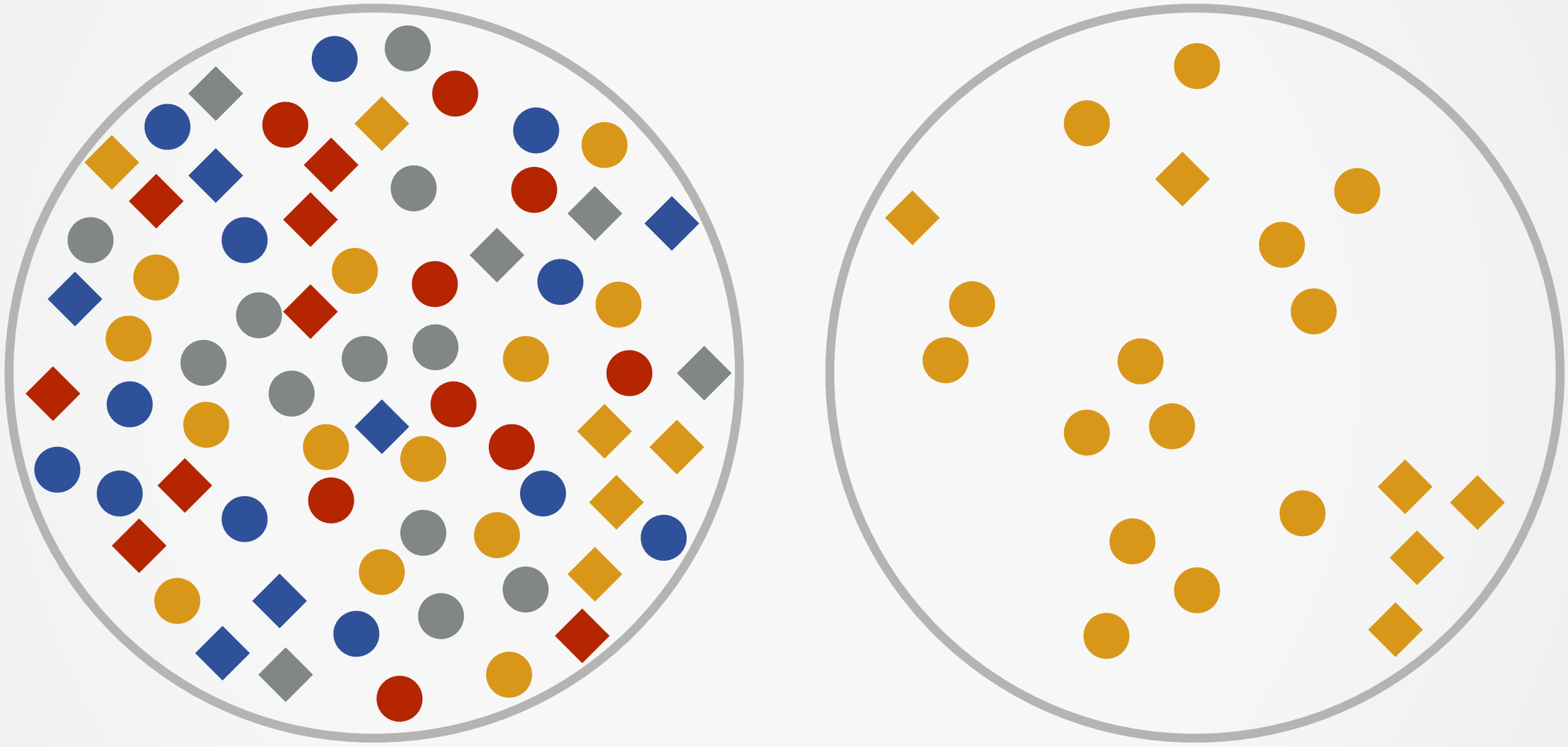
VE SIN FILTRO

Lista Negra



Bloquear los azules, bloquear los rombos

Lista Blanca



Sólo pasan los amarillos

Bajo qué base se bloquea

- **Lista Negra**
- **Lista Blanca**

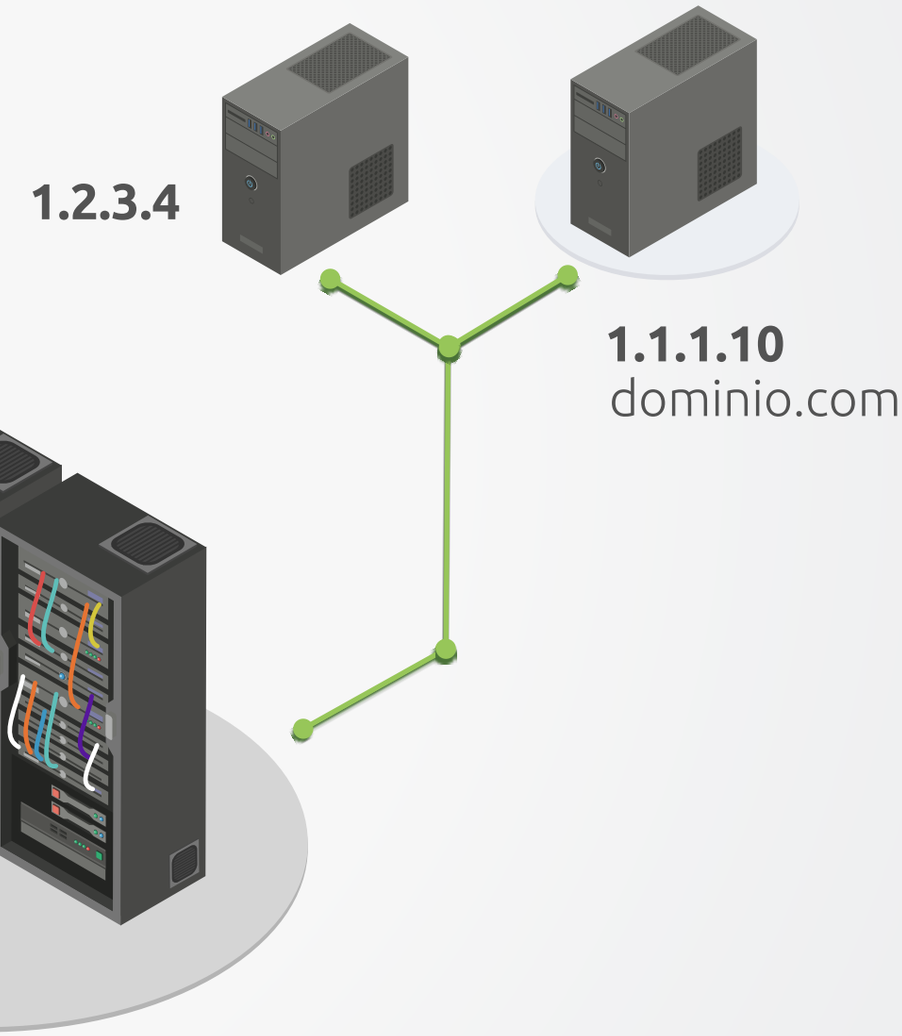
- De usuarios
- De sitios
- De dominios
- De servidores

TÉCNICAS DE BLOQUEO

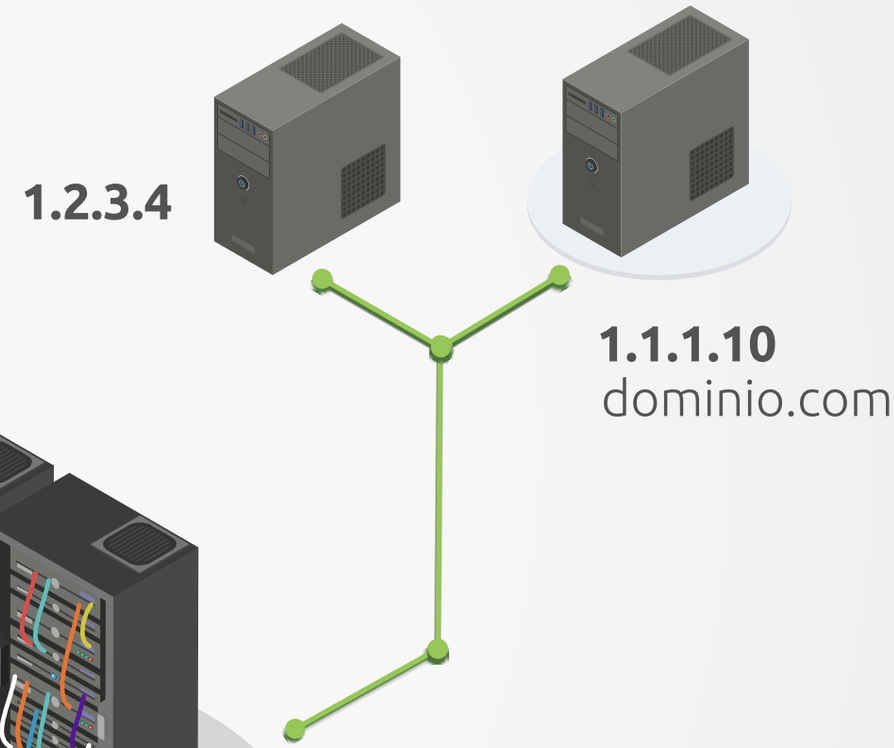
EJERCICIO

¿ALÓ 113?

Bloqueo DNS



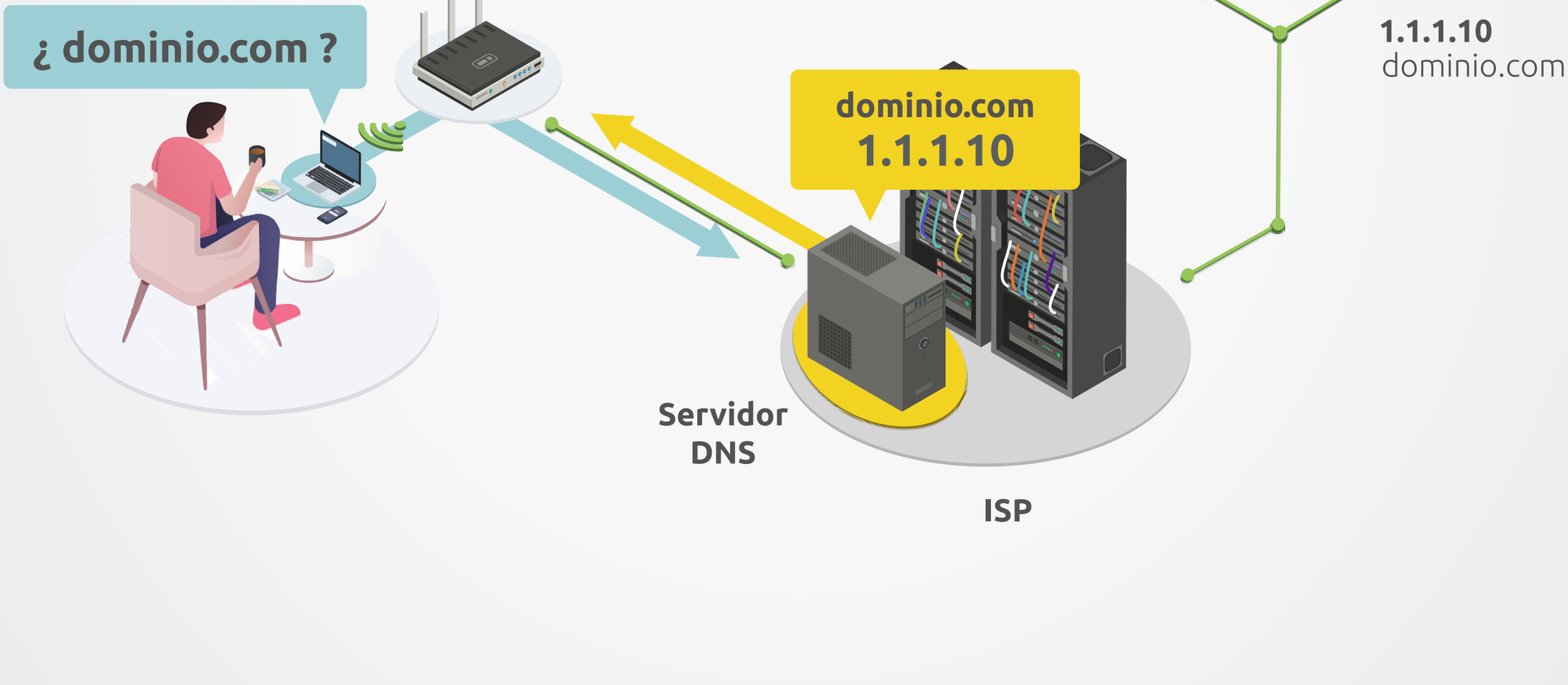
Bloqueo DNS



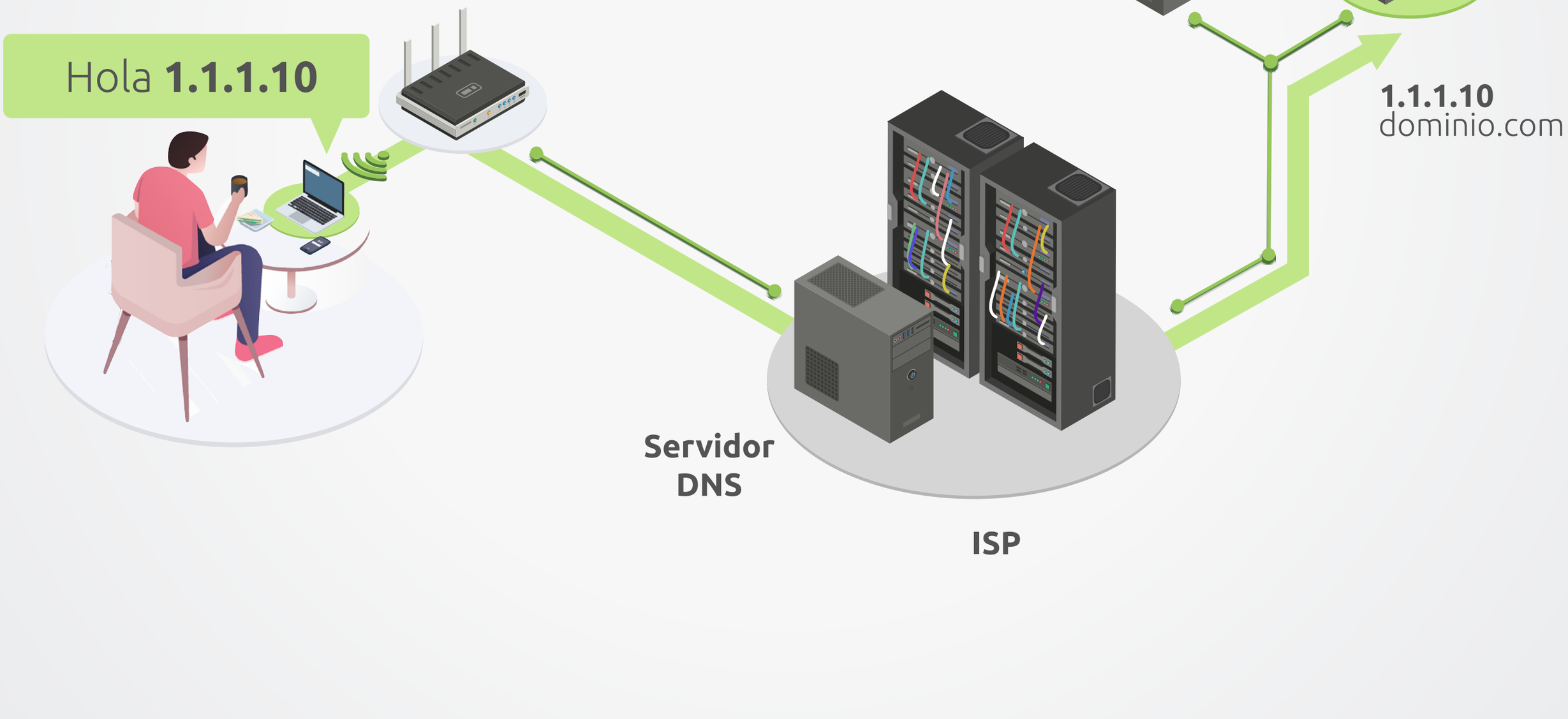
Servidor
DNS

ISP

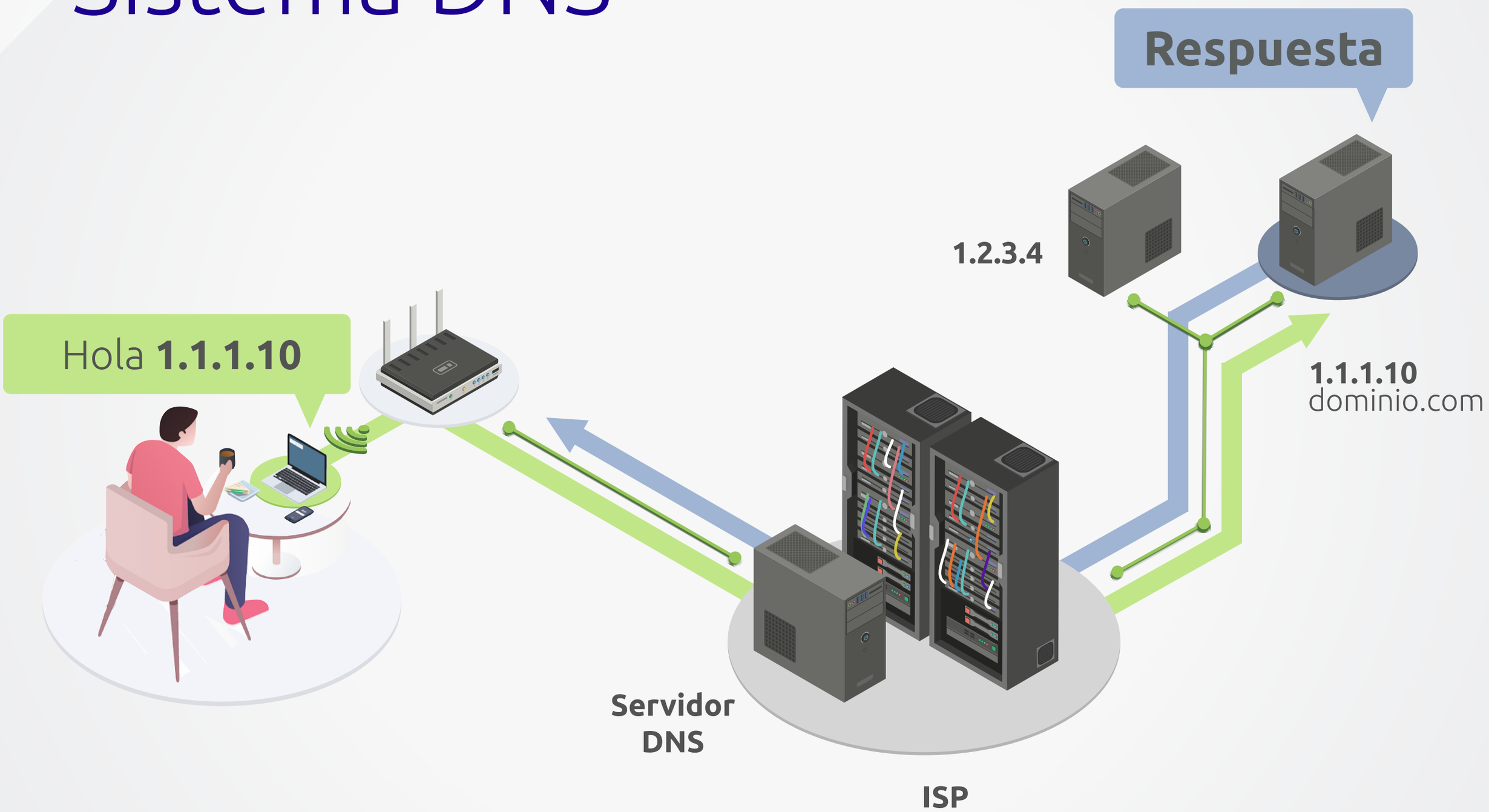
Sistema DNS


¿ dominio.com ?
1.2.3.4
1.1.1.10
dominio.com
dominio.com
1.1.1.10
Servidor
DNS
ISP

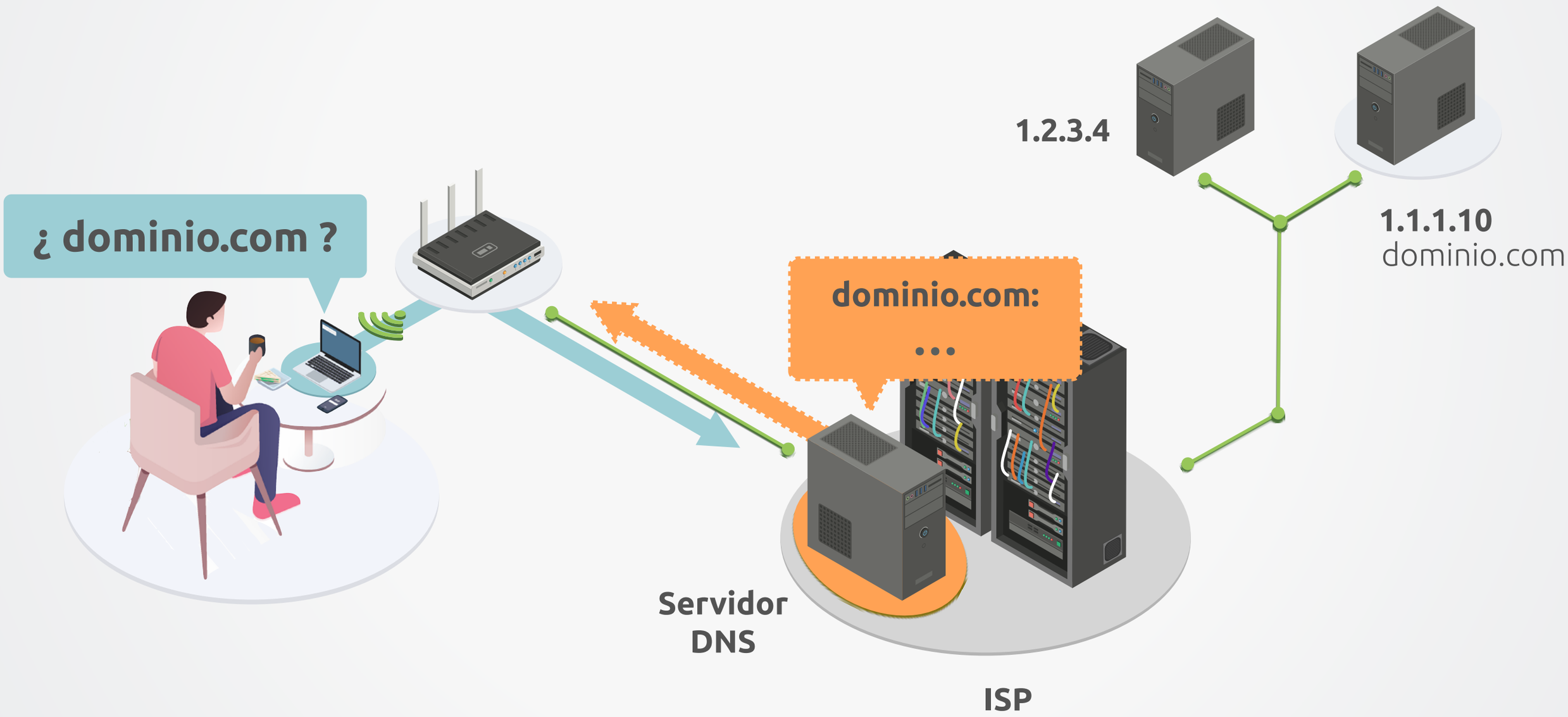
Sistema DNS



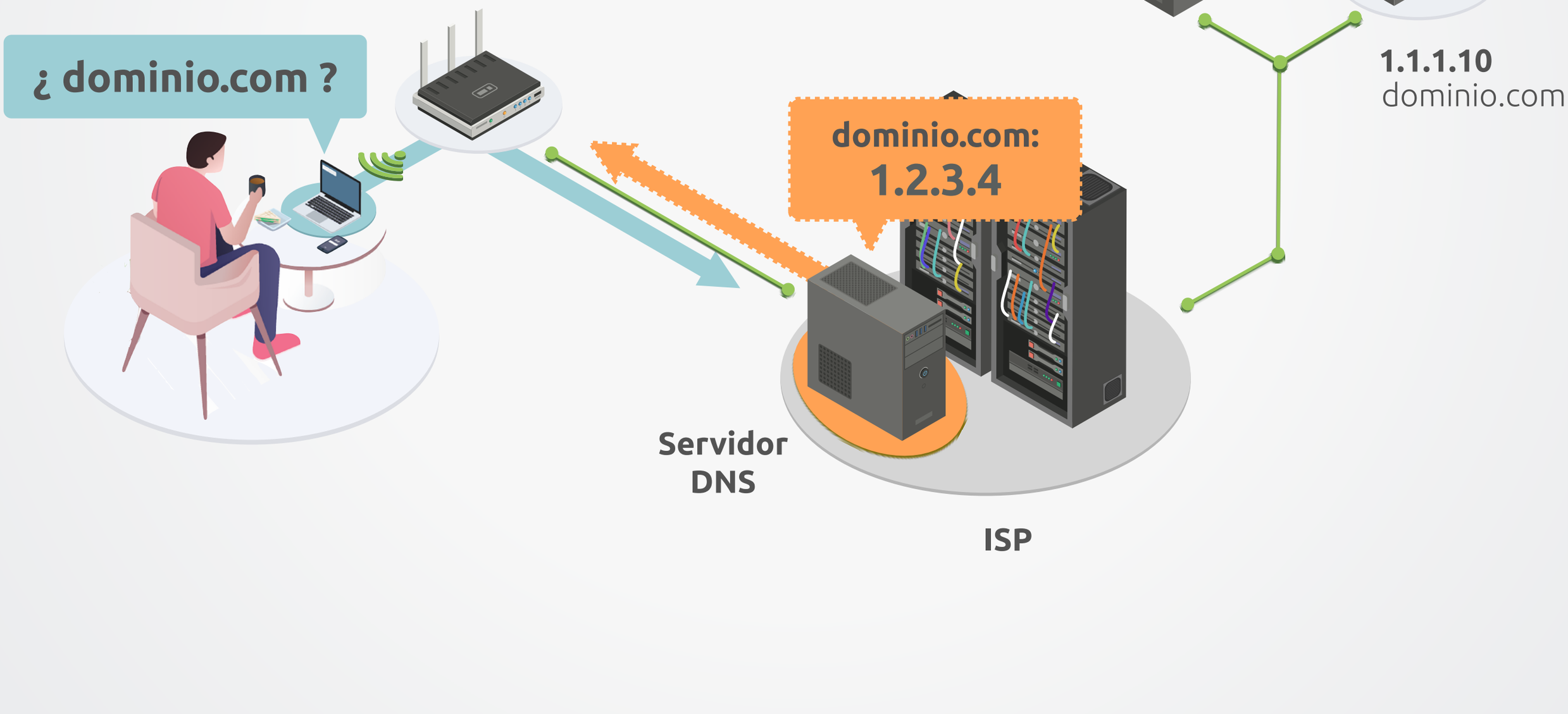
Sistema DNS


Respuesta
1.2.3.4
1.1.1.10
dominio.com
Hola 1.1.1.10
Servidor
DNS
ISP

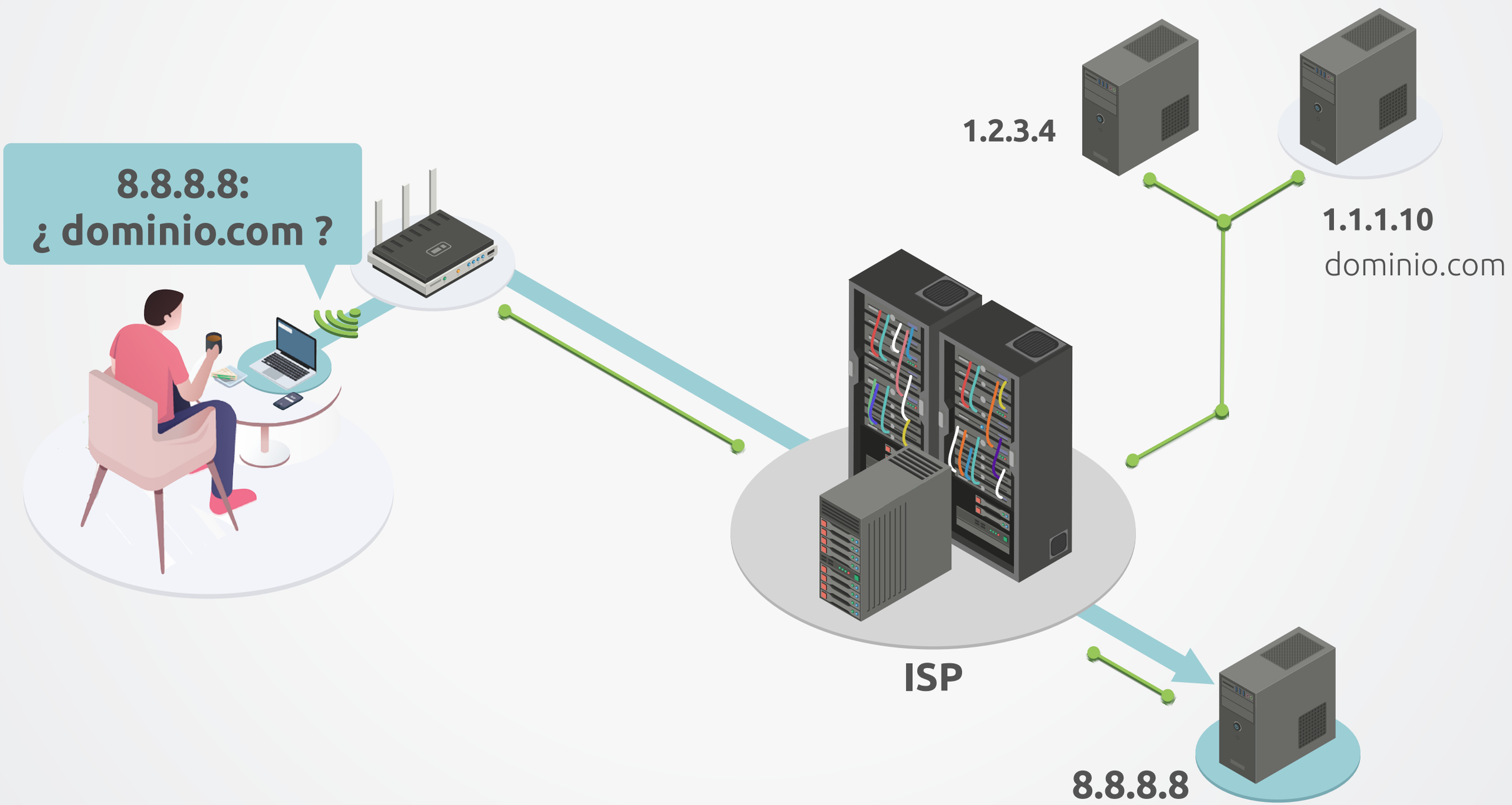
Bloqueo DNS


¿ dominio.com ?
dominio.com:
...
1.2.3.4
1.1.1.10
dominio.com
Servidor
DNS
ISP

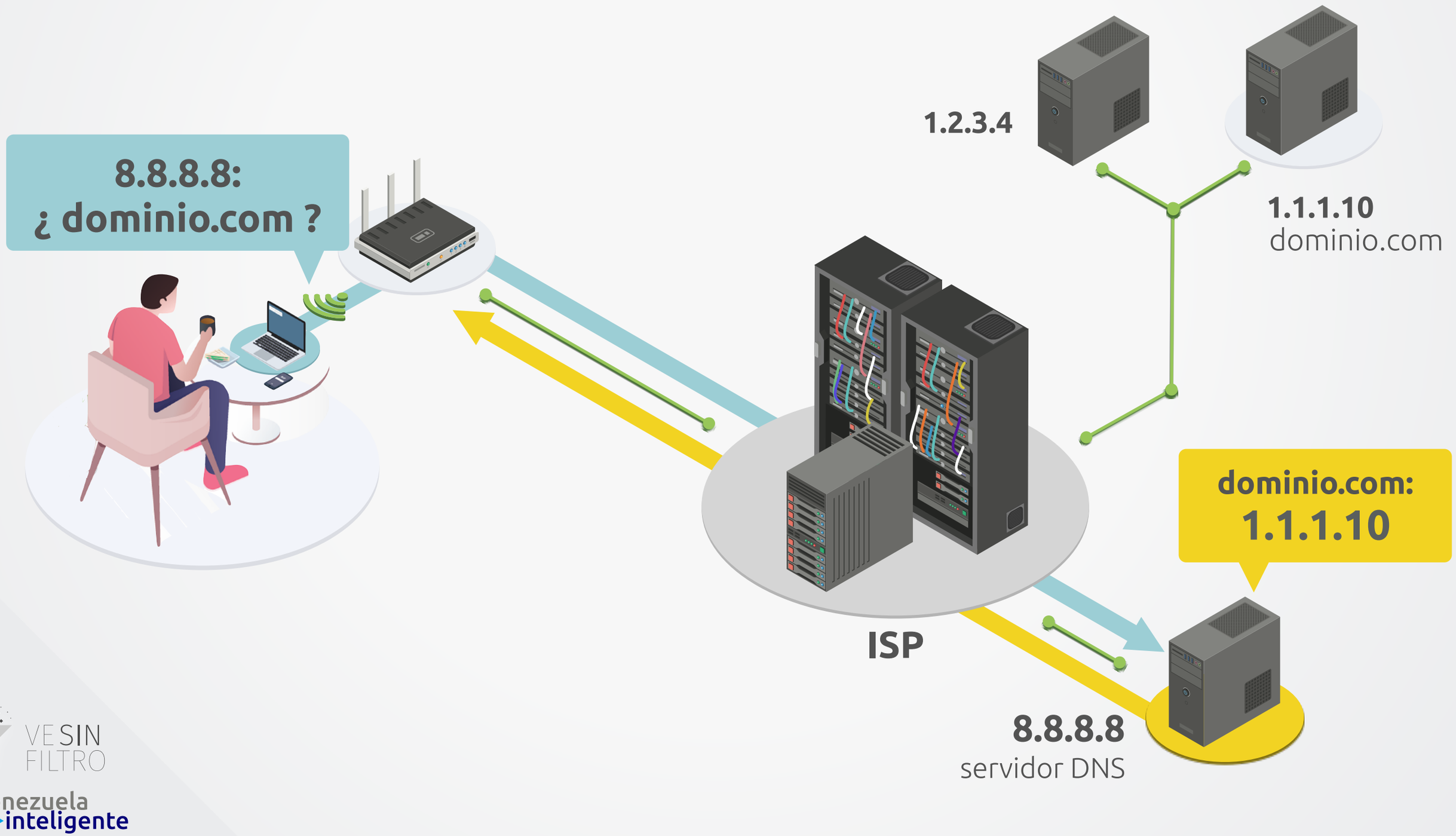
Respuesta en DNS maliciosa



Sistema DNS



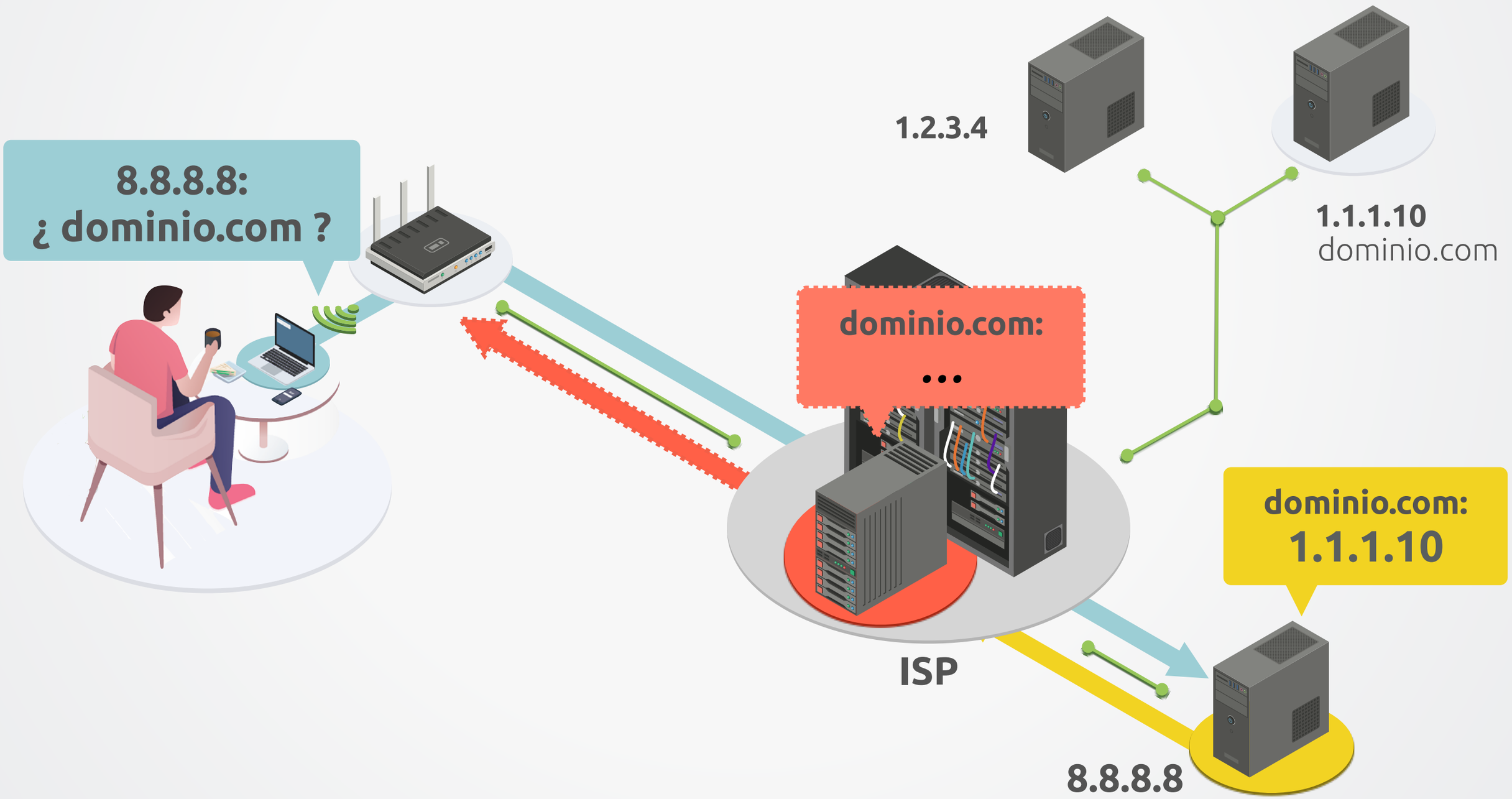
Bloqueo DNS



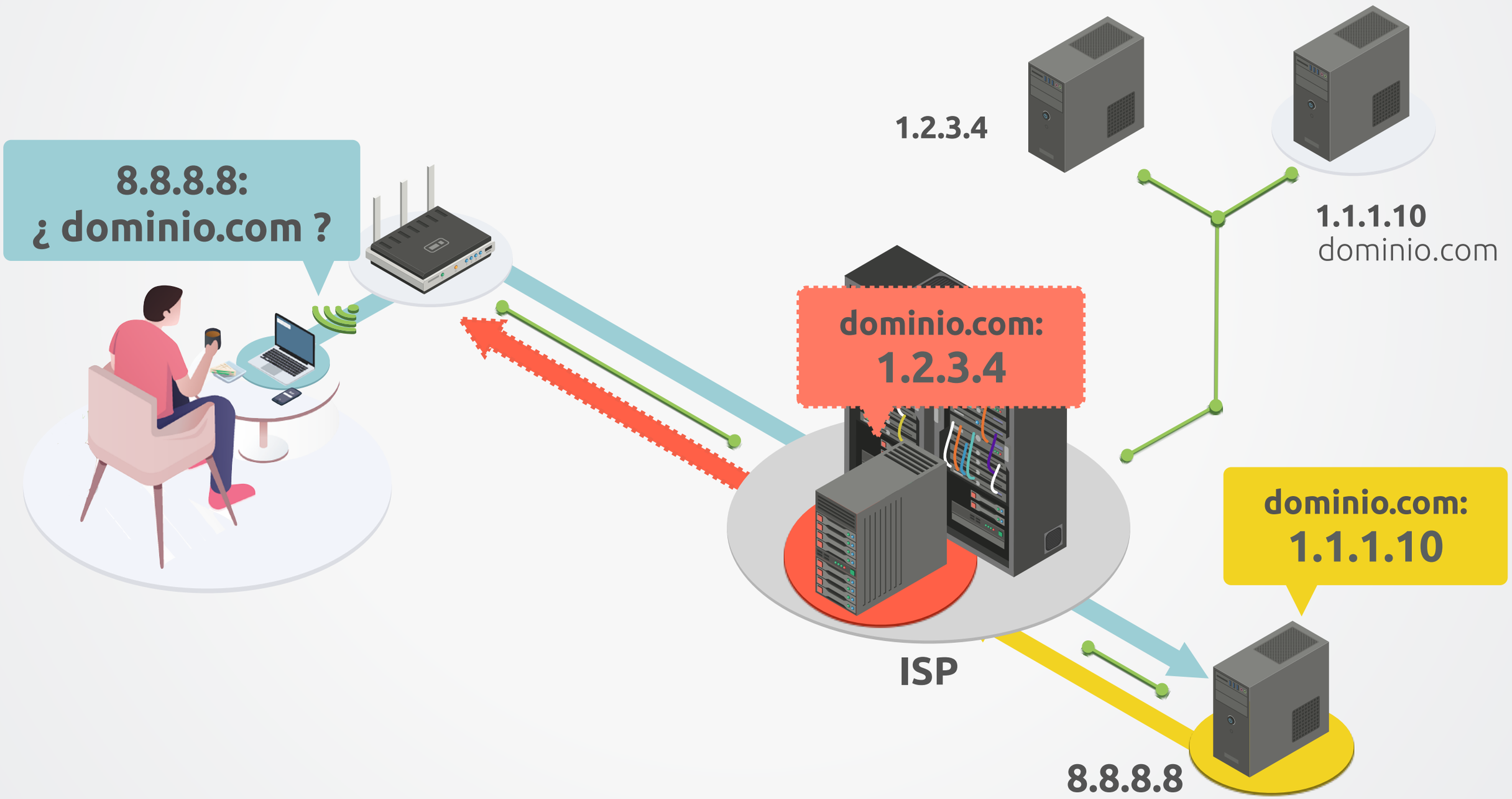
VE SIN FILTRO

Venezuela inteligente

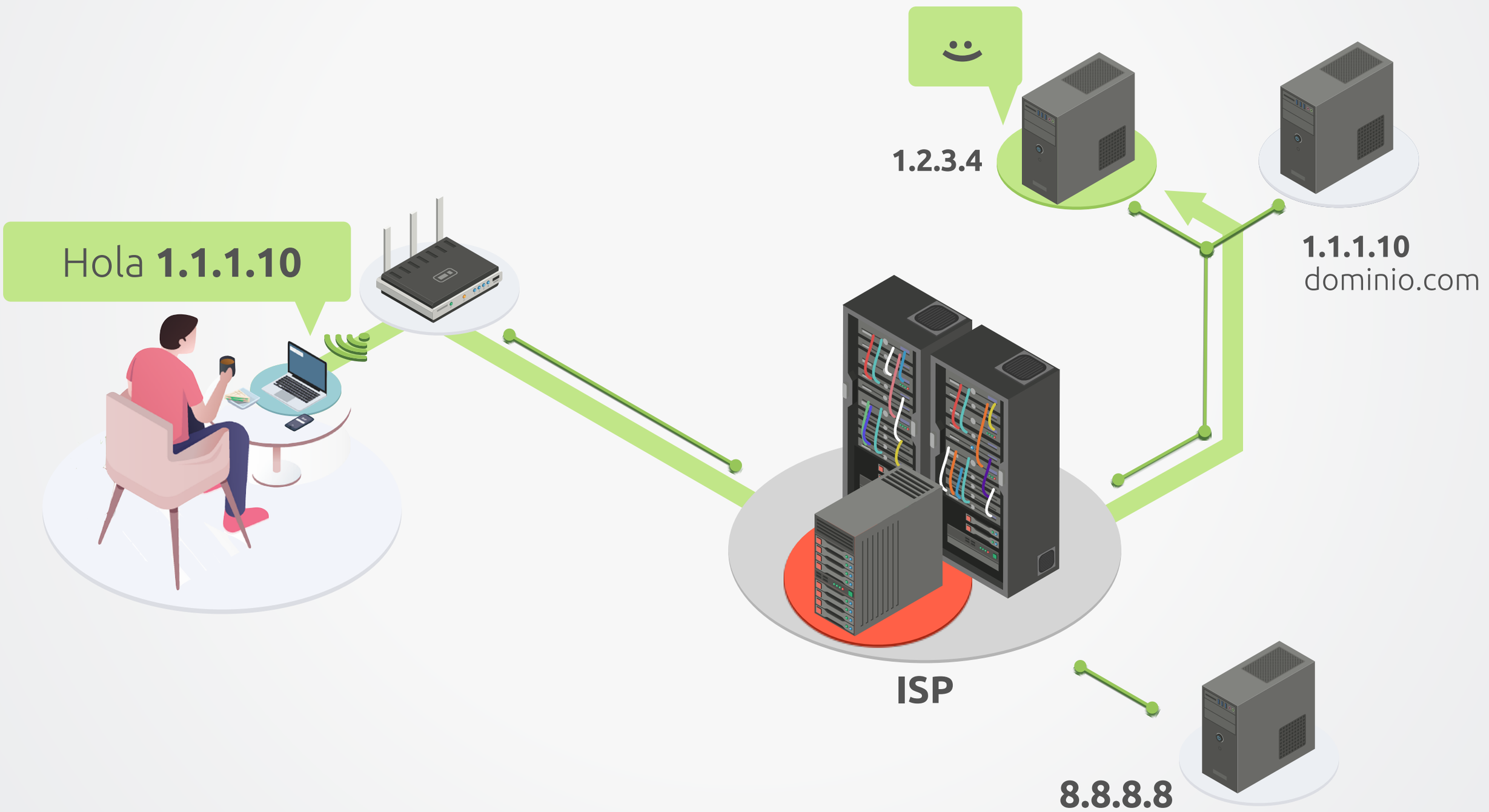
Inyección de respuesta DNS



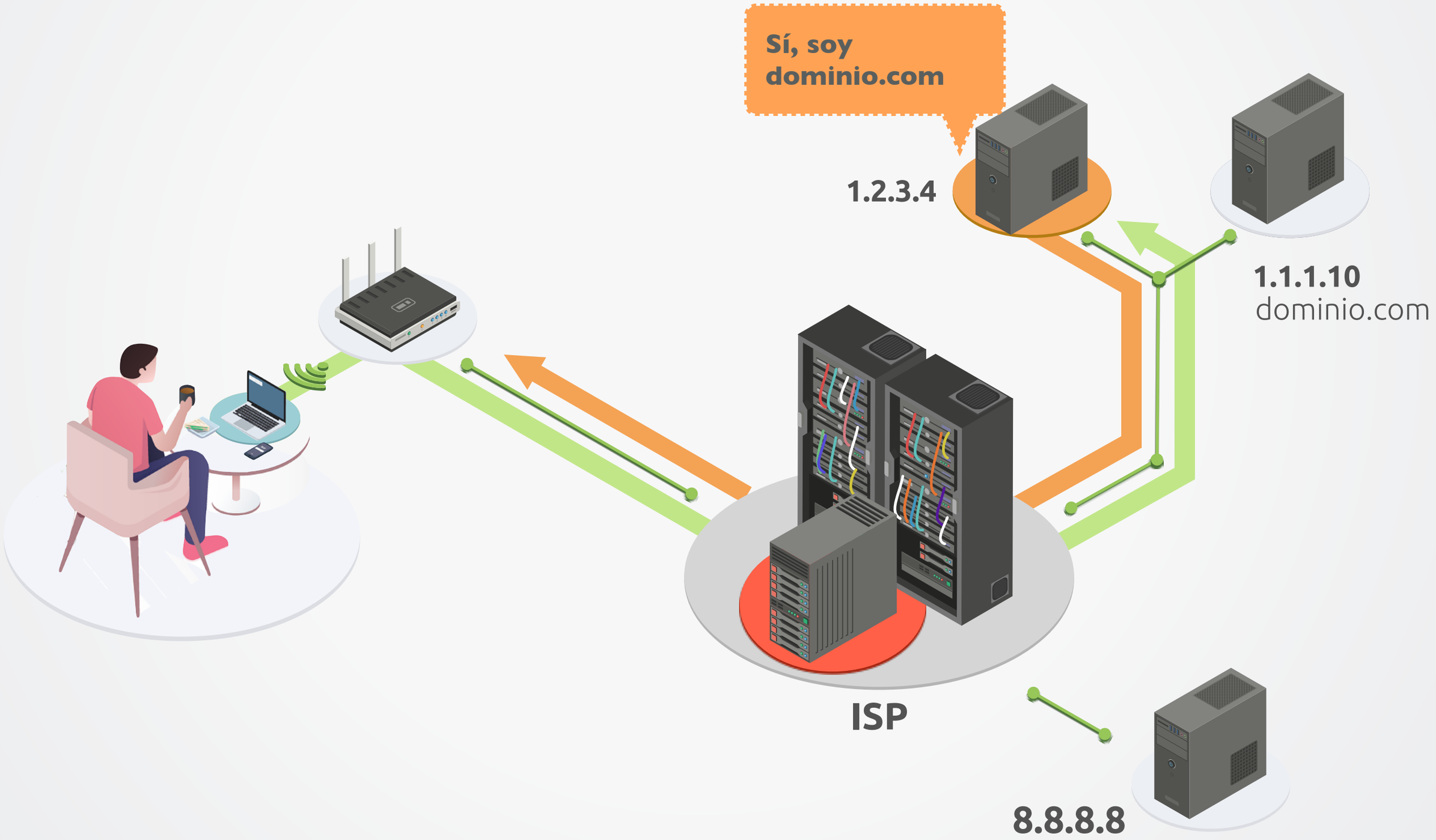
Inyección de respuesta DNS



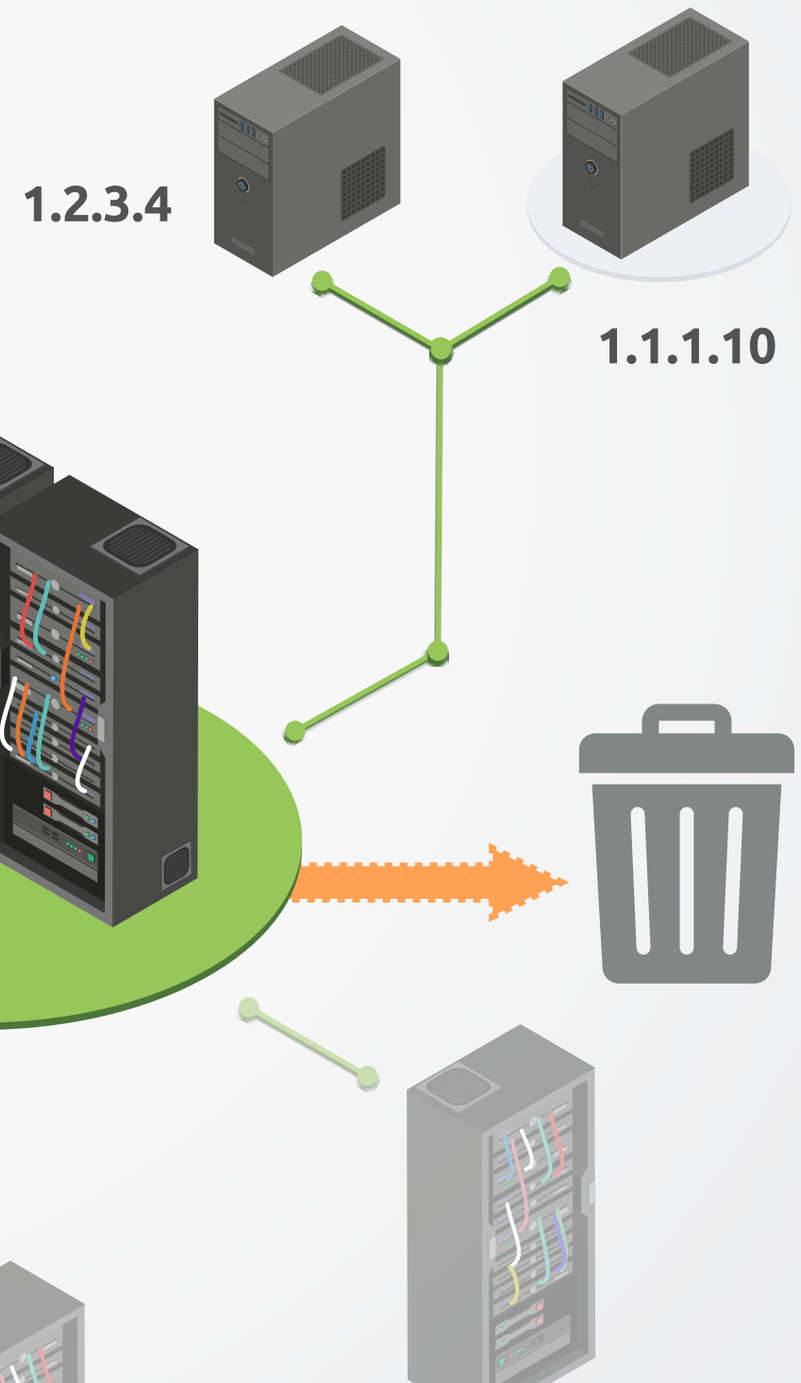
Inyección de respuesta DNS



Inyección de respuesta DNS

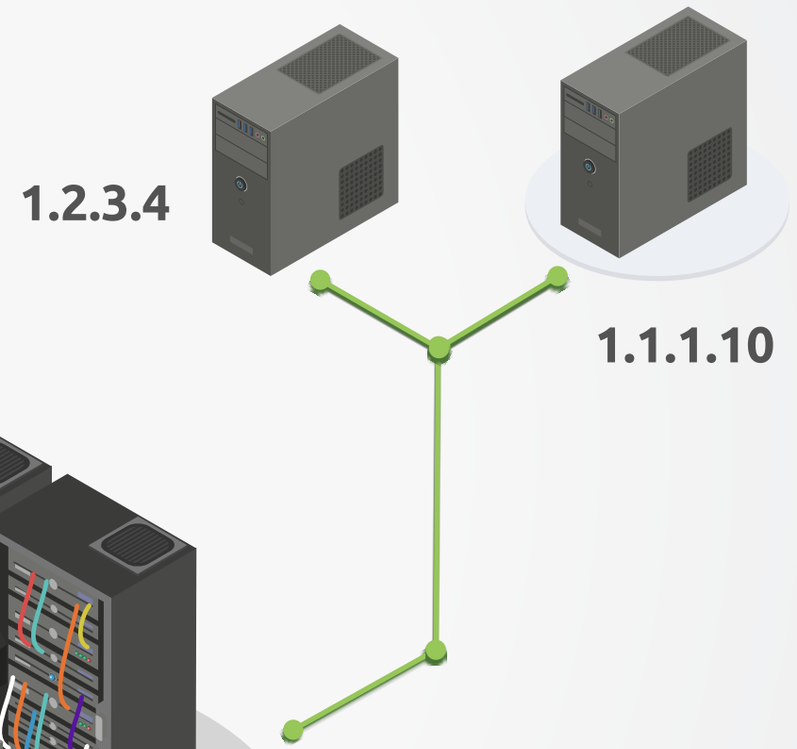


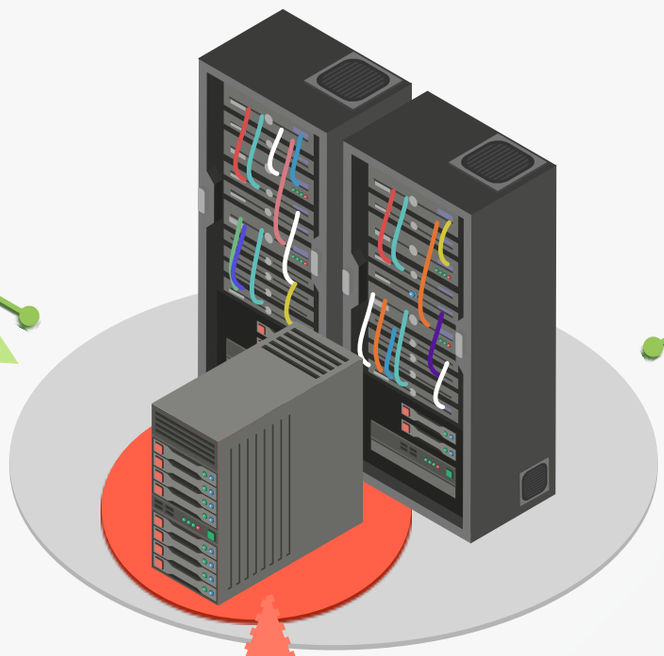
Bloqueo por IP

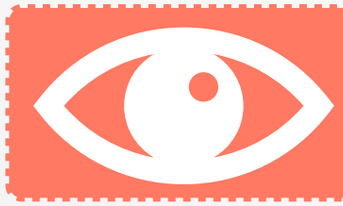


Bloqueo TCP

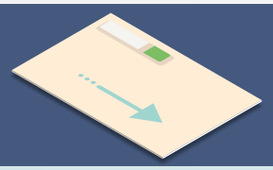
1.1.1.10:
Puerto 80 (**http**)
“Hola"







1.1.1.10 ?
Puerto 80 (**http**)?



Paquete (simplificado)

IP origen

IP destino

TCP

(ó UDP)

Puerto

Secuencia

Contenido

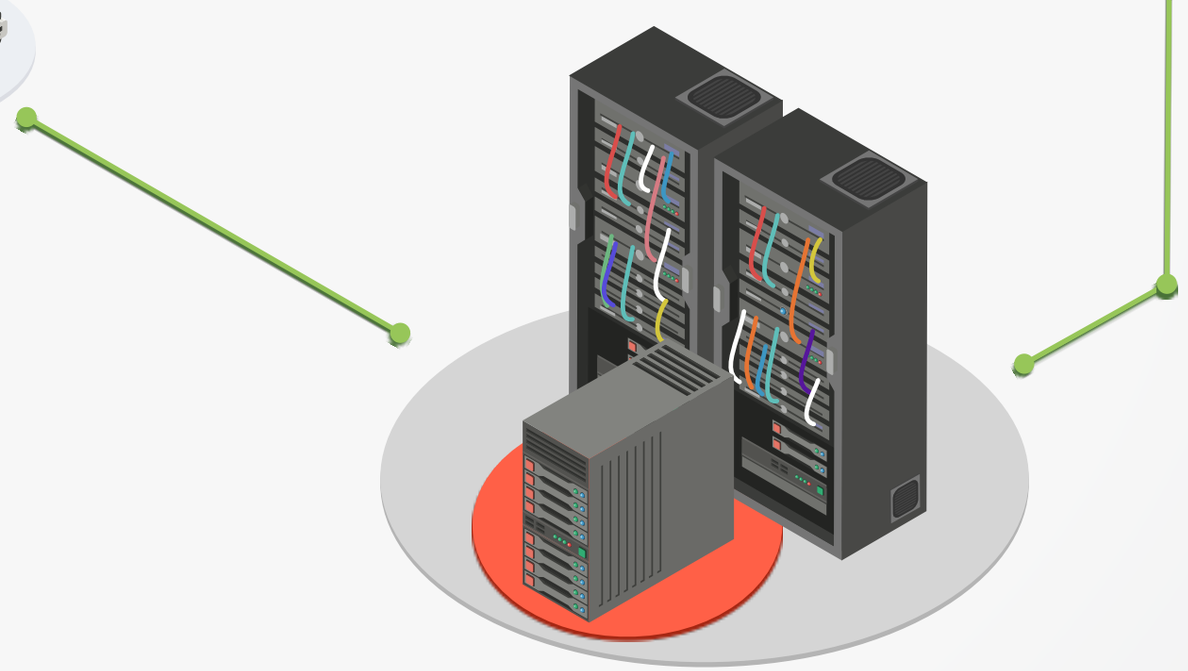
HTTP

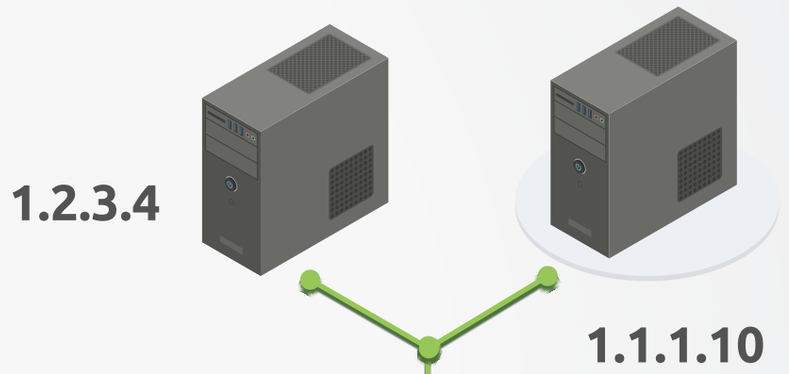
GET

Host: google.com

Bloqueo TCP

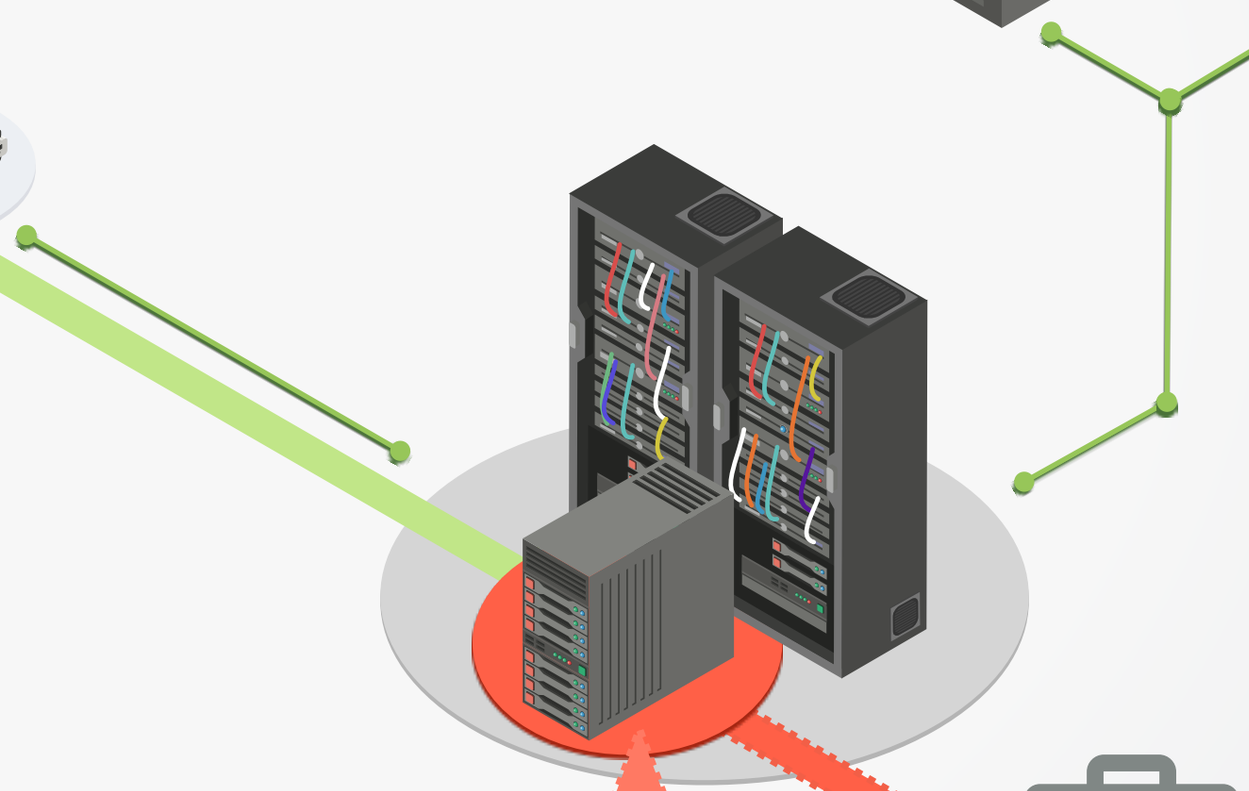
1.1.1.10:
Puerto 80 (**http**)
“Hola"

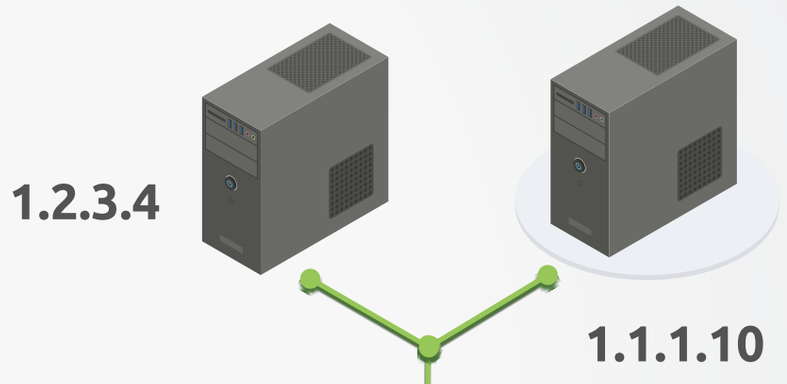




Bloqueo TCP

1.1.1.10:
Puerto 80 (**http**)
“Hola"





1.1.1.10
Puerto 80 (**http**)

EJERCICIO

MENOS MAL QUE NO ES IPOSTEL

EJERCICIO

DEFINITIVAMENTE

MENOS MAL QUE NO ES IPOSTEL

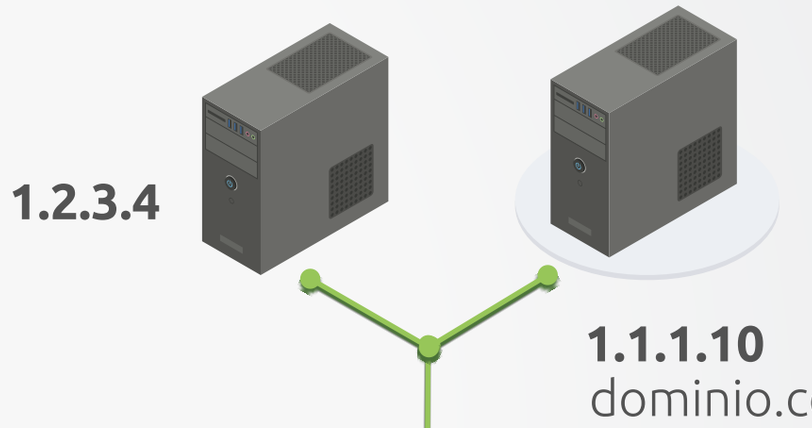
Con modelo más complejo
y más paquetes

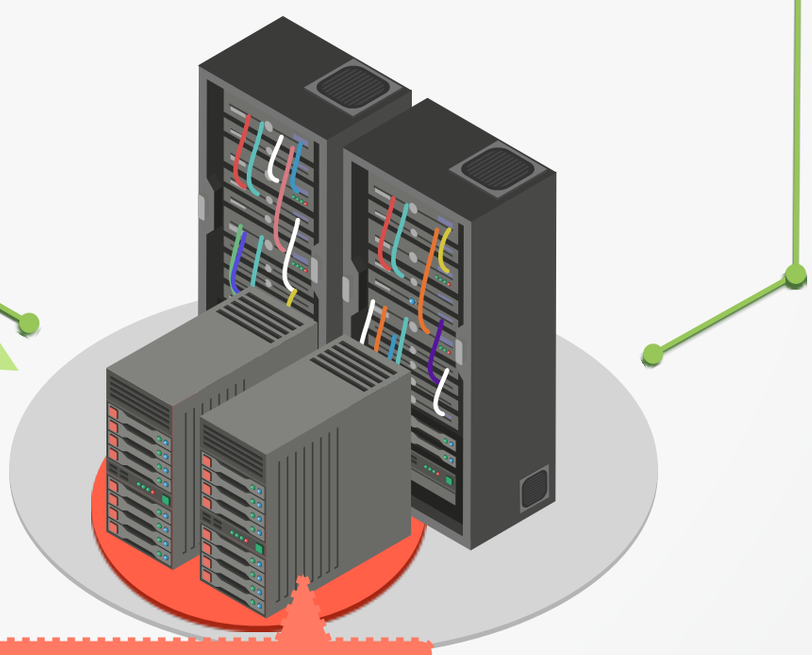
Modelamos la dificultad
de revisar más dentro del
paquete con un sobre

Bloqueo por Filtrado SNI

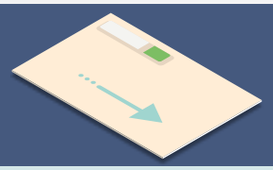
1.1.1.10:
Puerto 443 (https)

"**Quiero la página dominio.com**"





¿Solicitudes sobre dominio.com?



Paquete (simplificado)

IP origen

IP destino

TCP

(ó UDP)

Puerto

Secuencia

Contenido

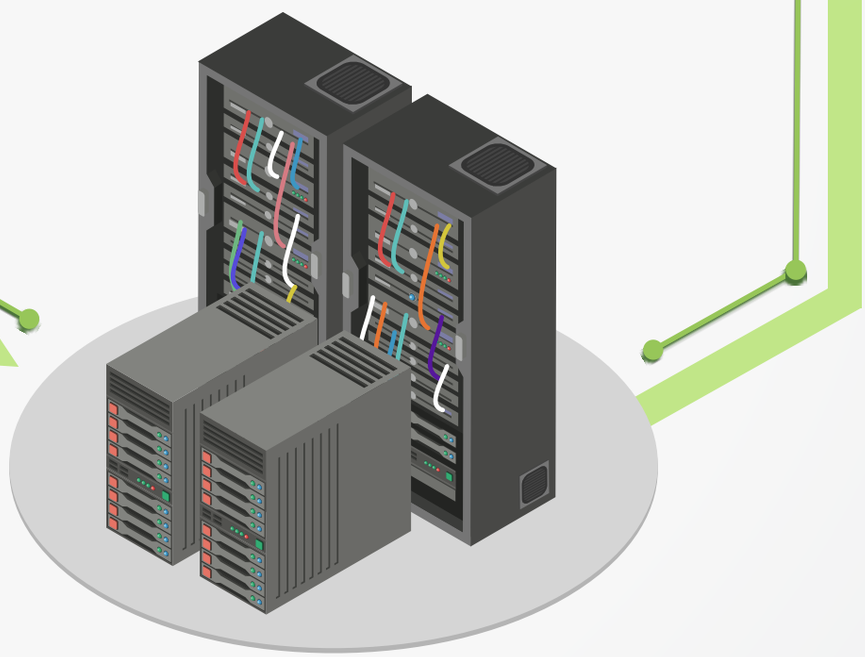
HTTP

GET

Host: google.com

1.1.1.10:
Puerto 443 (https)

"**Quiero la página dominio.com**"



1.2.3.4

1.1.1.10
dominio.com

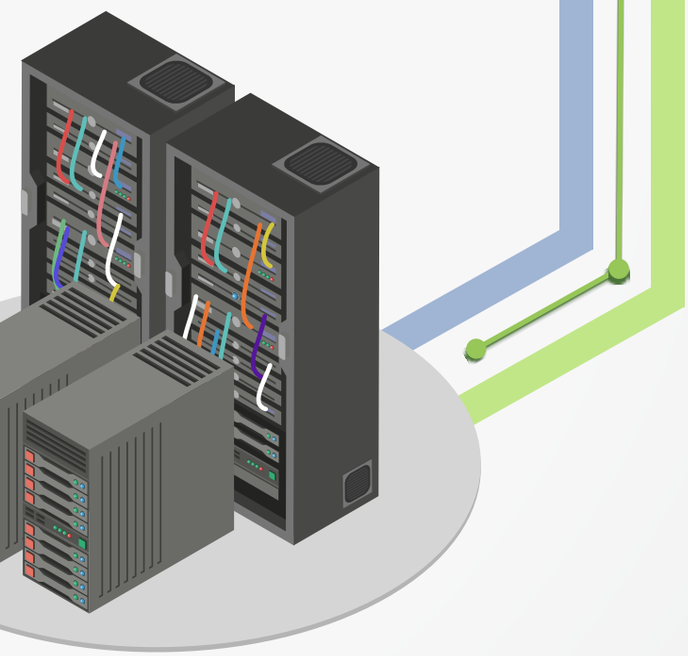
1.1.1.10:
Puerto 443 (https)

"**Quiero la página dominio.com**"

Tengo **dominio.com**

1.2.3.4

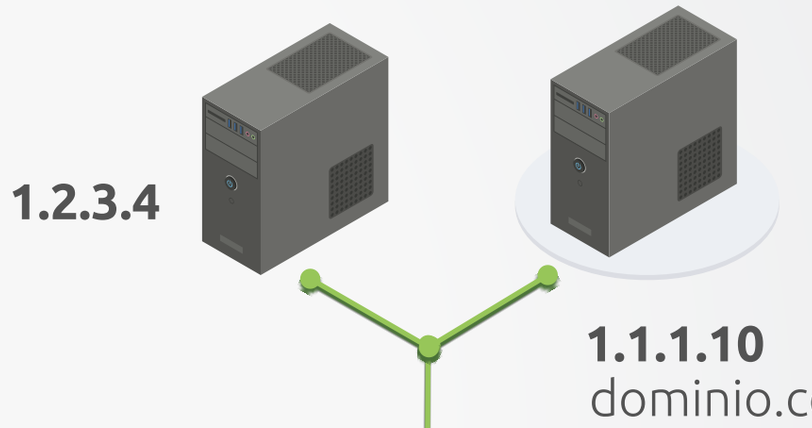
1.1.1.10
dominio.com

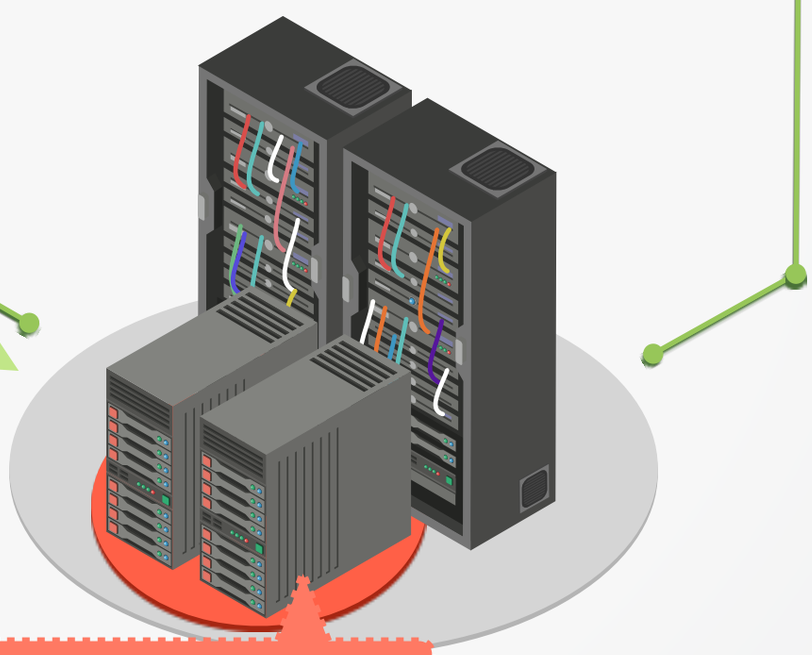


Bloqueo por Filtrado SNI

1.1.1.10:
Puerto 443 (https)

"**Quiero la página dominio.com**"



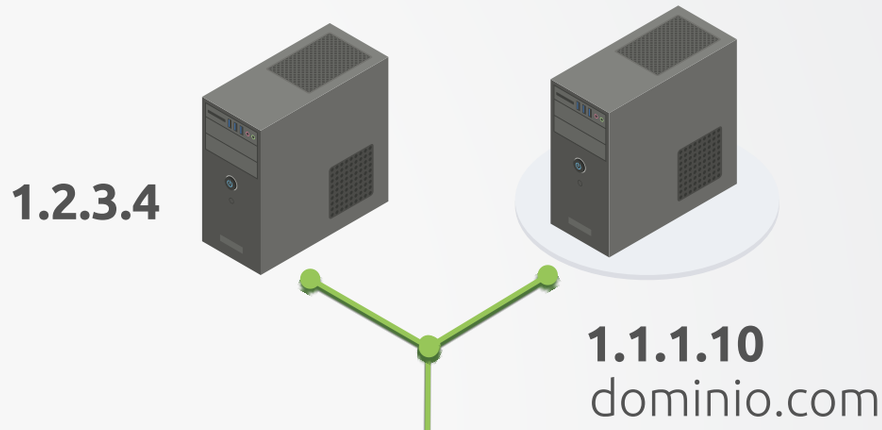


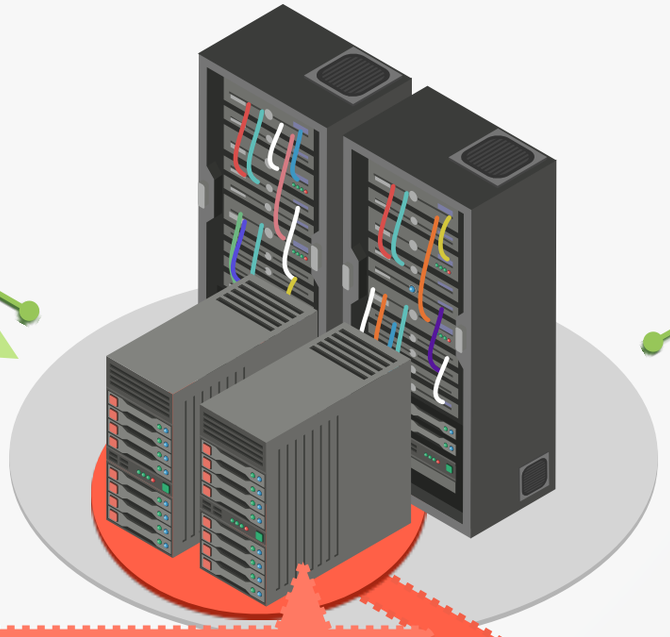
¿Solicitudes sobre dominio.com?

Bloqueo por Filtrado SNI

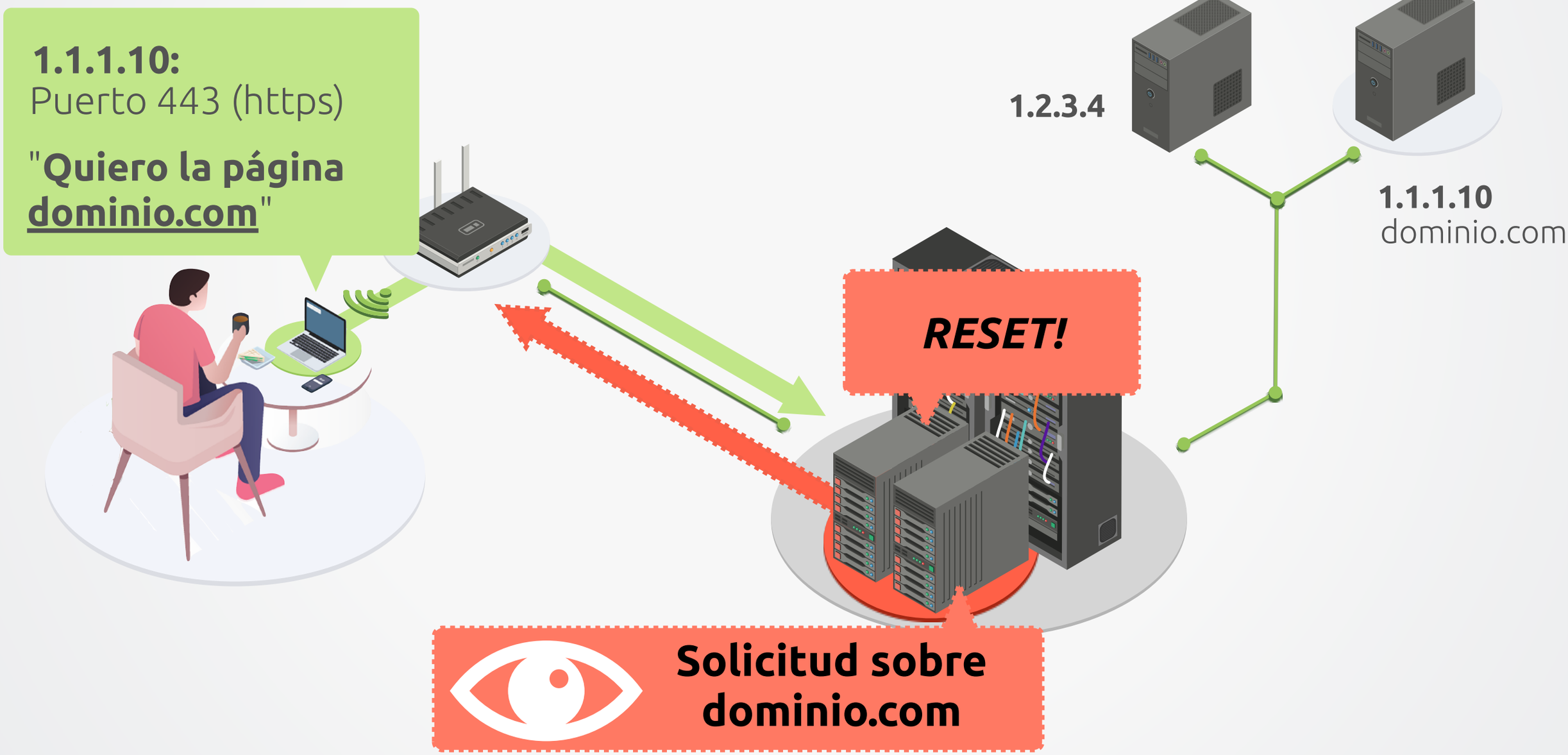
1.1.1.10:
Puerto 443 (https)

"**Quiero la página dominio.com**"

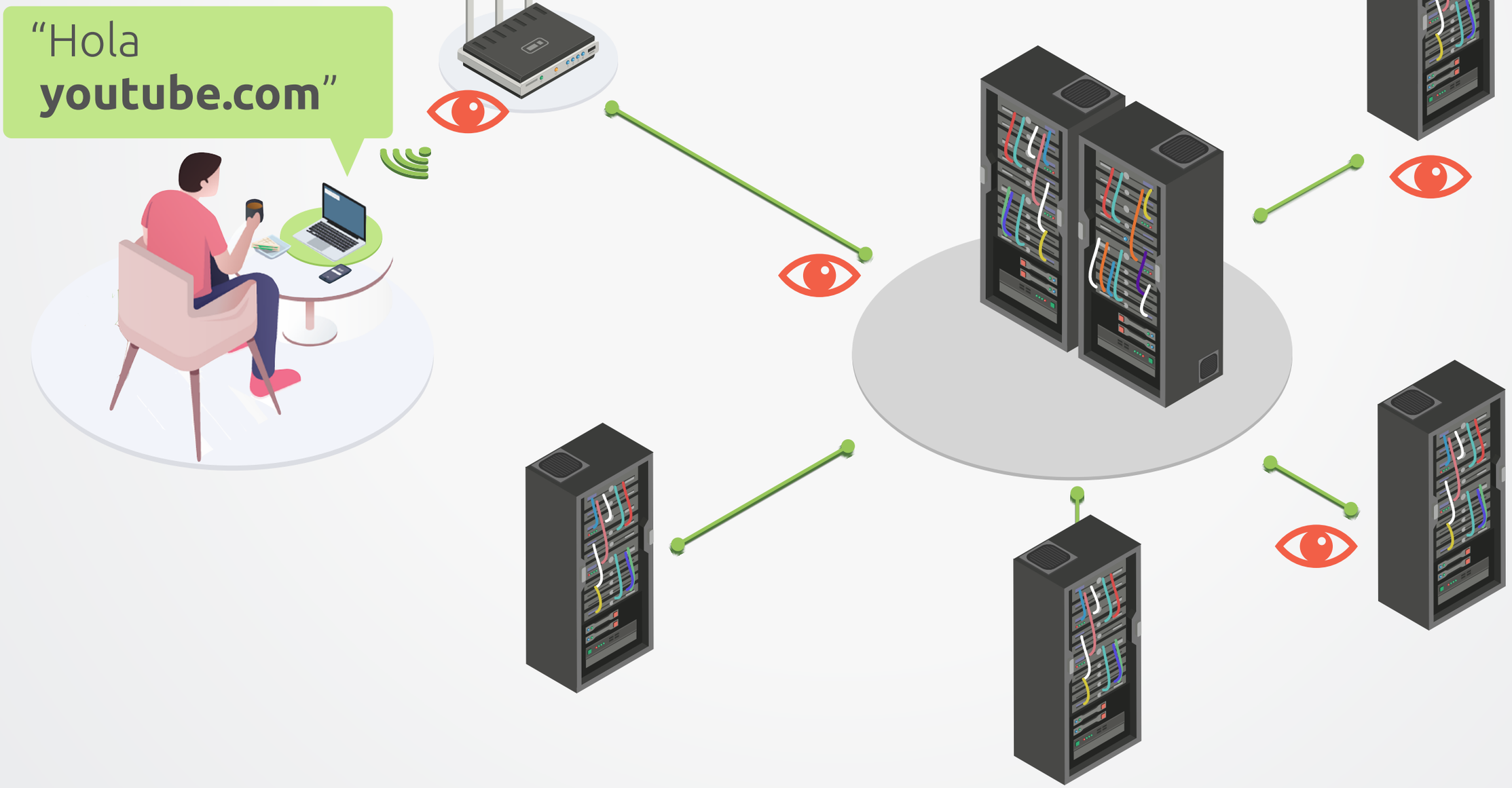




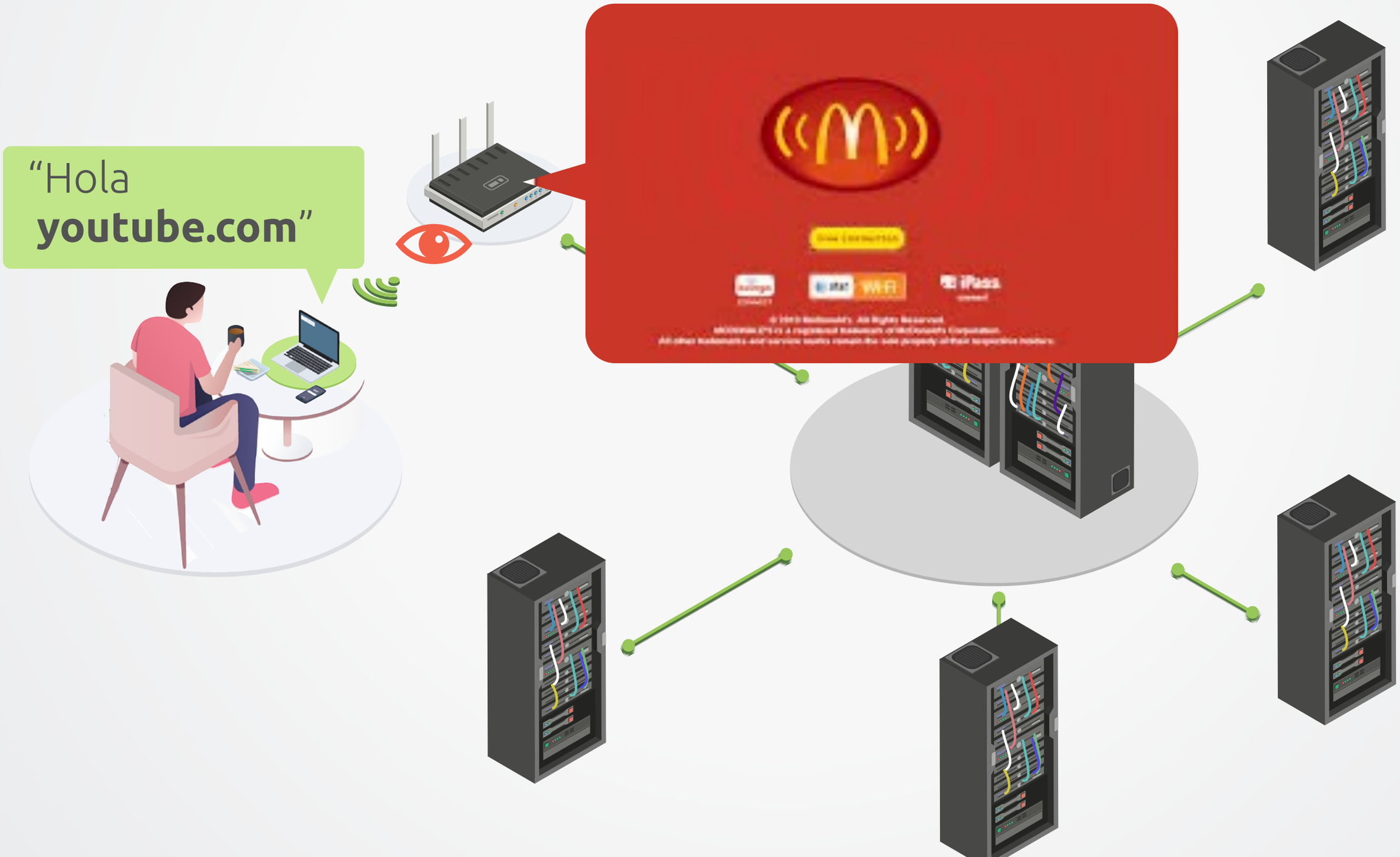
Bloqueo por Filtrado SNI

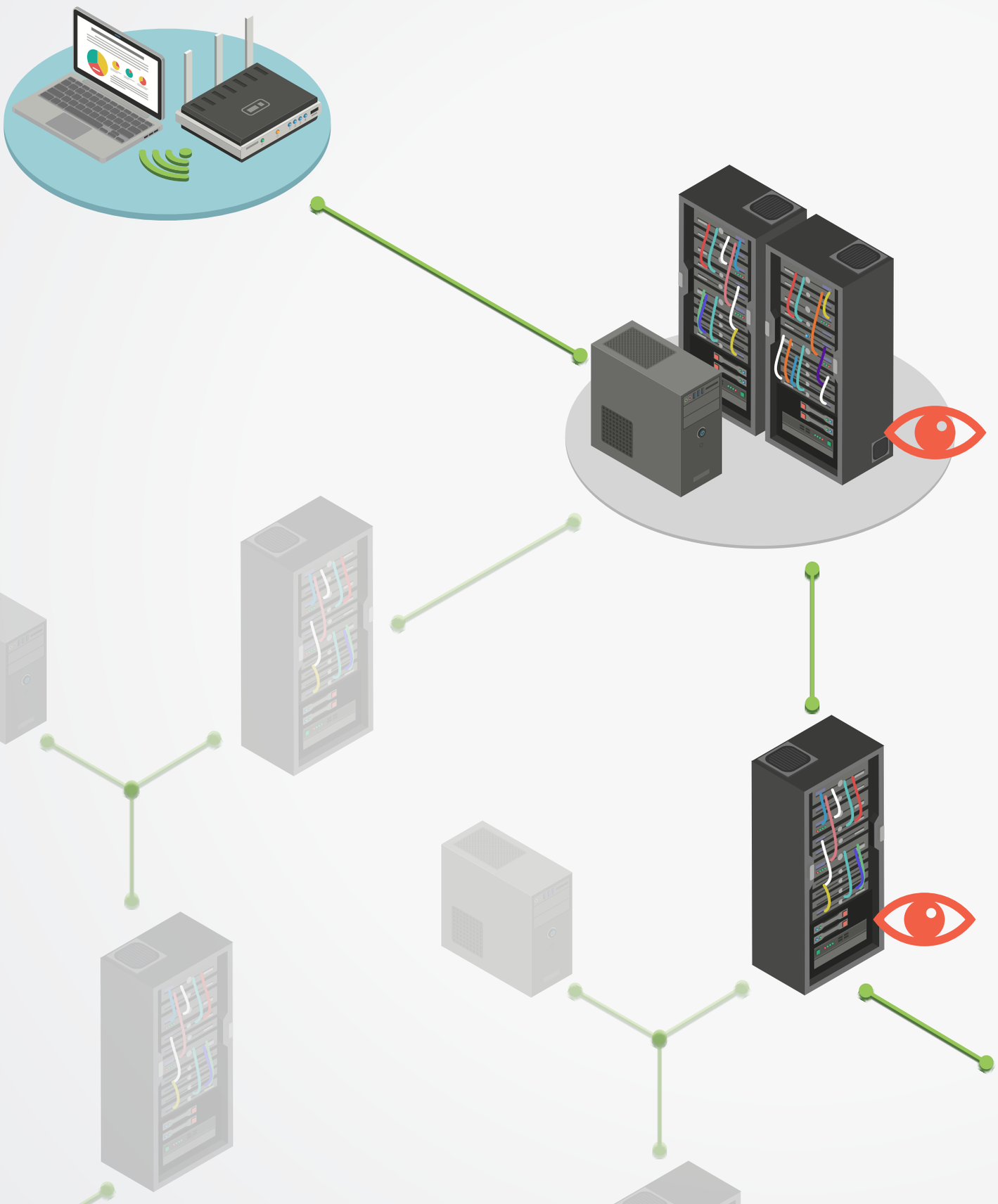


No solo ISPs



No solo ISPs





Vulnerabilidades del internet

- Diseño ingenuo
- **Son como postales,**
  no como cartas
- Muchas manos en la masa
- Confianza en carteros
- Principio de “mejor esfuerzo"

COMO EVADIRLOS

COMO LO MEDIMOS

Criterios de VE sin Filtro

- Limitación de acceso identificada
- **Es medible/documentable**
- **Consiste en el tiempo y desde los otros puntos de medición**
- **Se comprende qué está ocurriendo y no hay otra explicación para el comportamiento observado**

OTRAS FORMAS DE **LIMITAR ACCESO**

También es posible

- Ralentización
- Ataques informáticos
- Hackeo
- Ataque de Denegación de Servicio (DoS)
- DoS Distribuído (DDoS)

También es posible

- Solicitudes del estado
- Solicitudes por violación de derechos de autor
- Censura de la plataforma
- Reportes de abuso injustificados

También es posible

- Desinformación, manipulación de la opinión pública
- Brigading
- Envenenamiento de datos
- Bots y cuentas falsas dirigidas

¡Gracias!