

IIC3253

Seguridad en la Web



fintual.cl



Hola de nuevo 

Email

ejemplo@ejemplo.com

Contraseña

.....



Entrar



fintual.cl



Hola Martín 

Invirtiendo fácil hace 477 días

+ Nuevo Objetivo

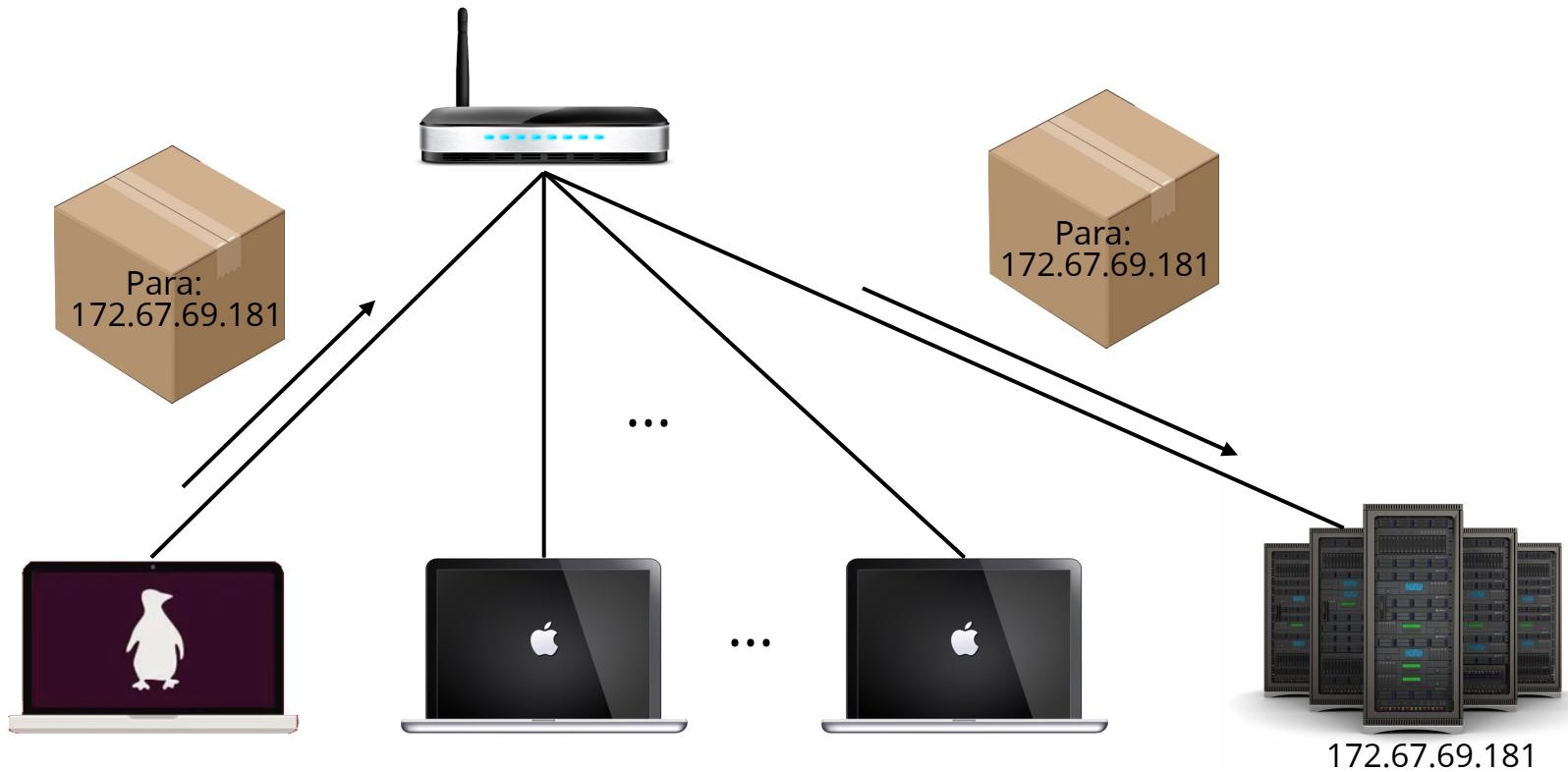
 Invertir más



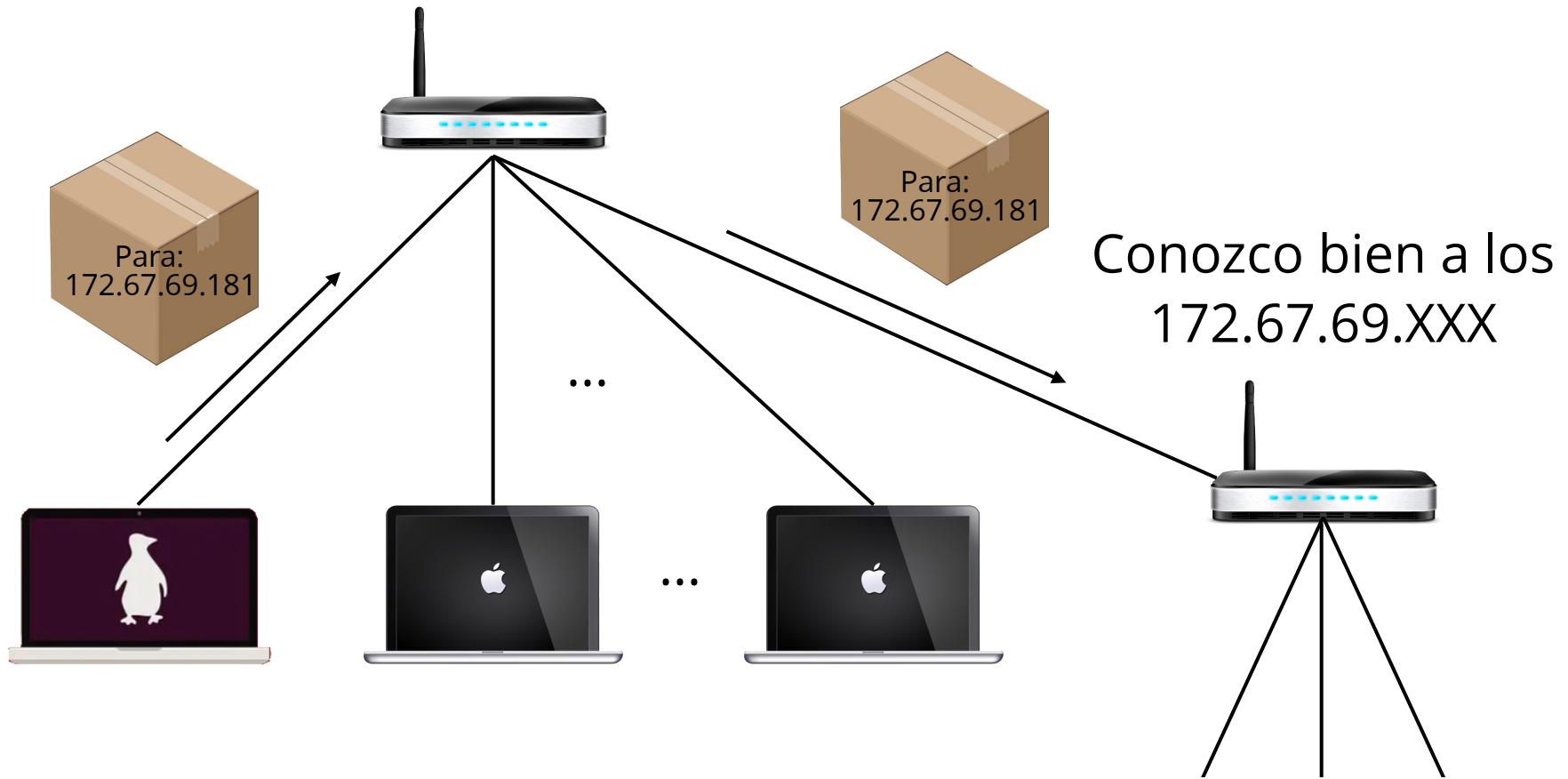
THAT'S IT?

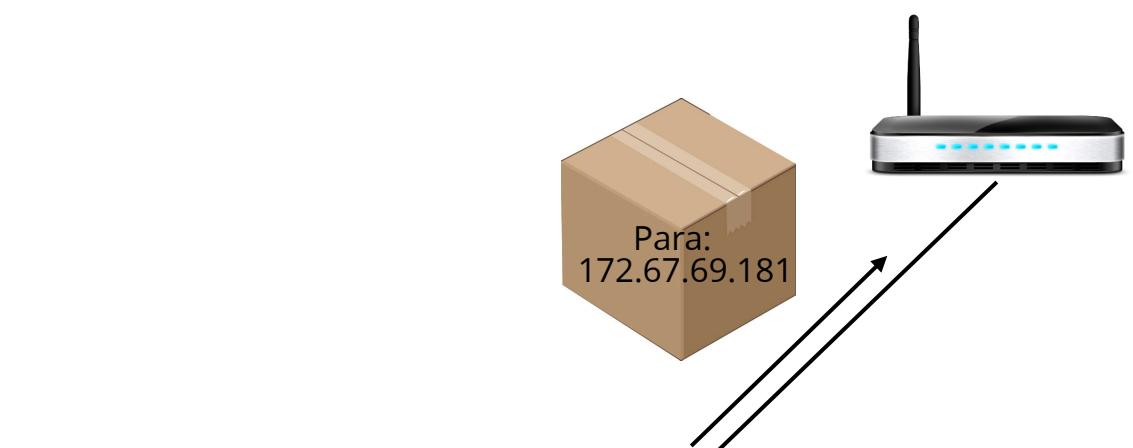
TOO EASY.

Conozco esa dirección?



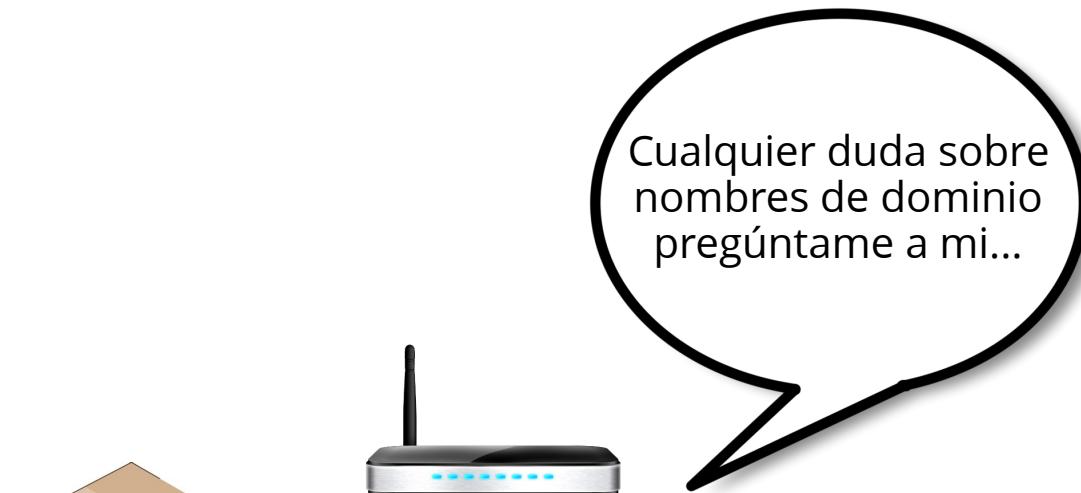
Conozco a alguien que
conozca esa dirección?





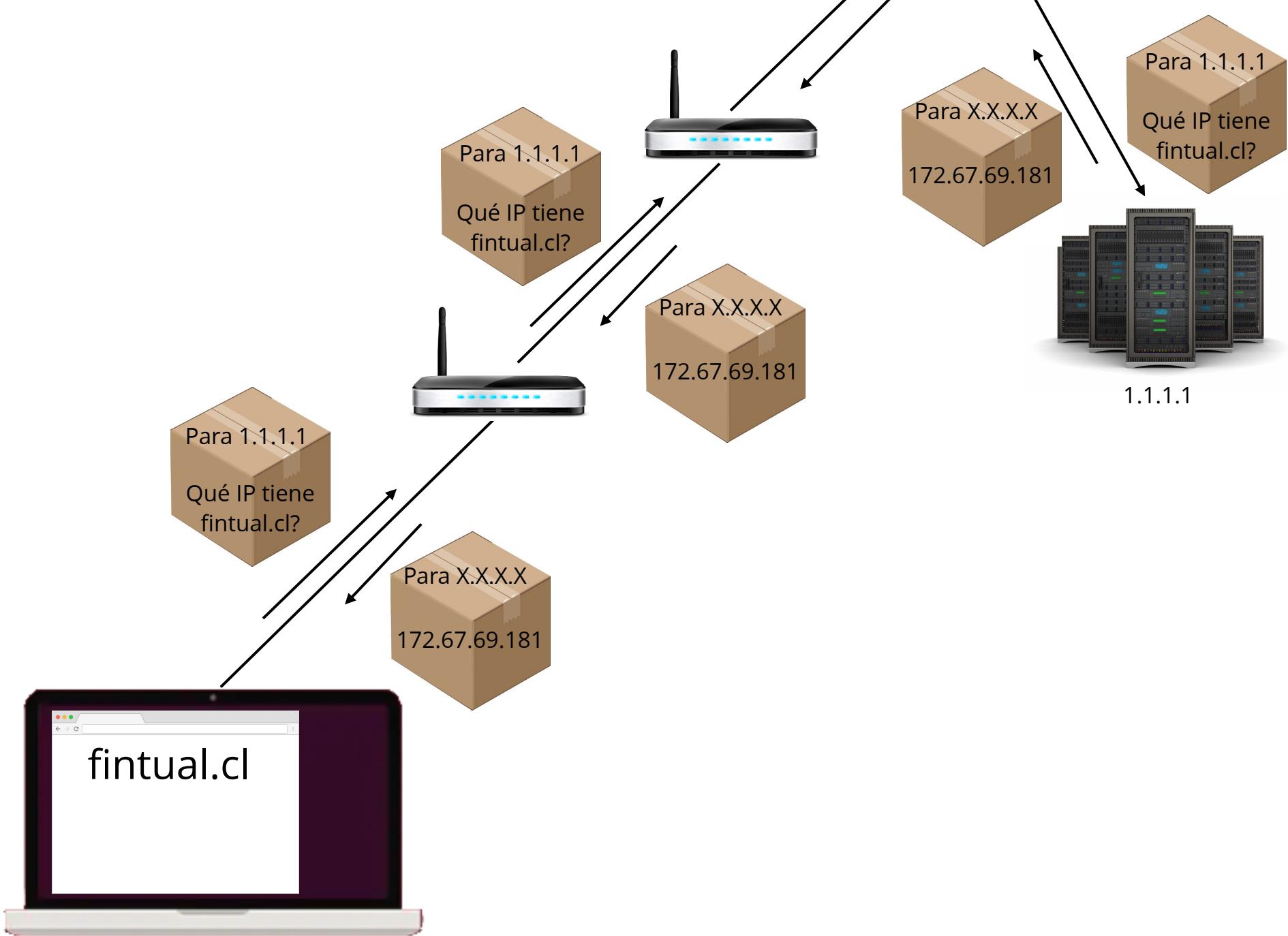
Conozco esa dirección?
Conozco a alguien que
conoce esa dirección?
Ni idea, default route...

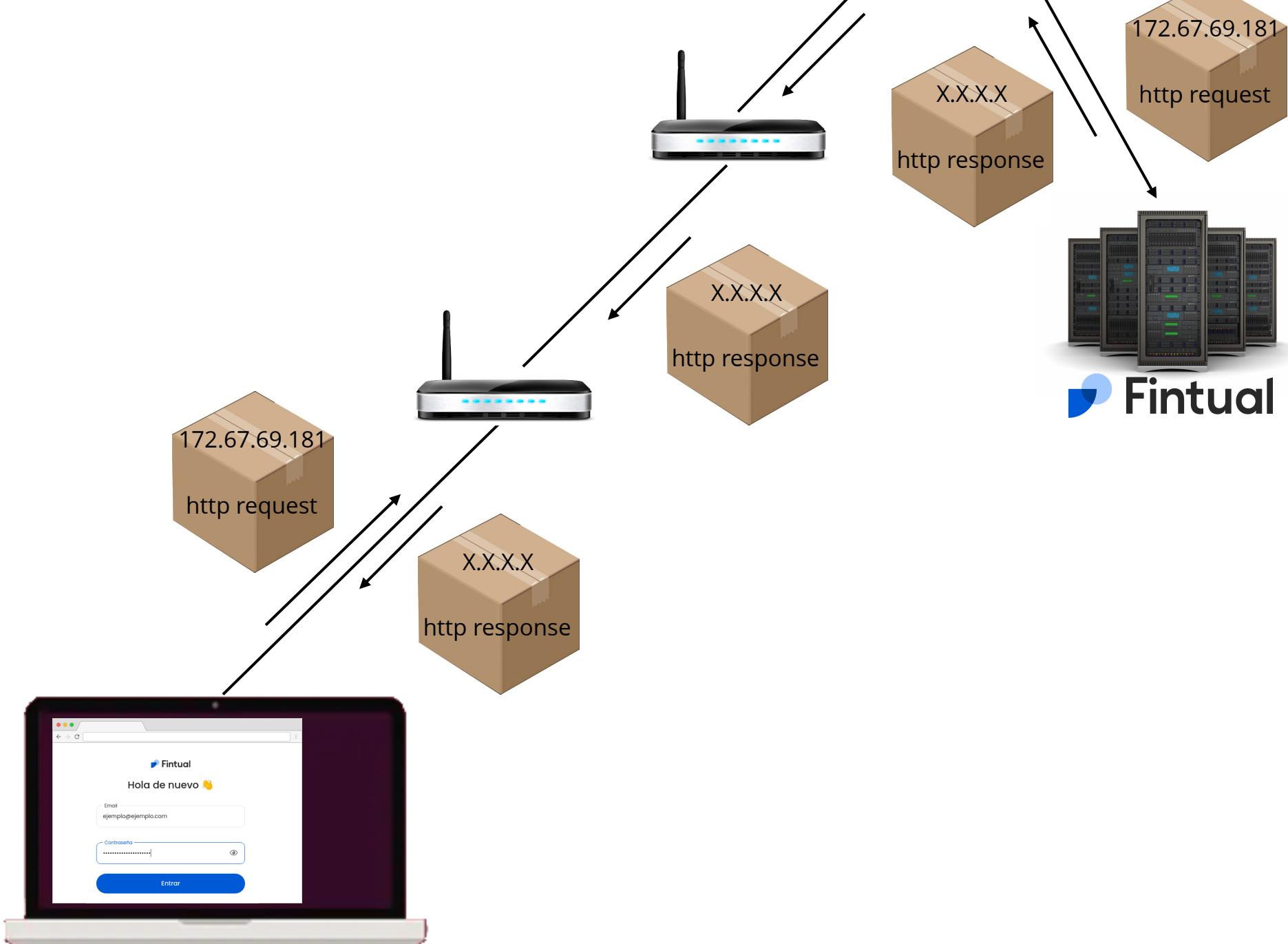




Qué dirección IP tiene fintual.cl?

Le pregunto a mi servidor de
DNS (Domain Name System)...





Llegamos a Fintual...

Vamos bien?

**¿Problemas de
seguridad?**

IDC 2021 Global DNS Threat Report

DNS Threat Landscape

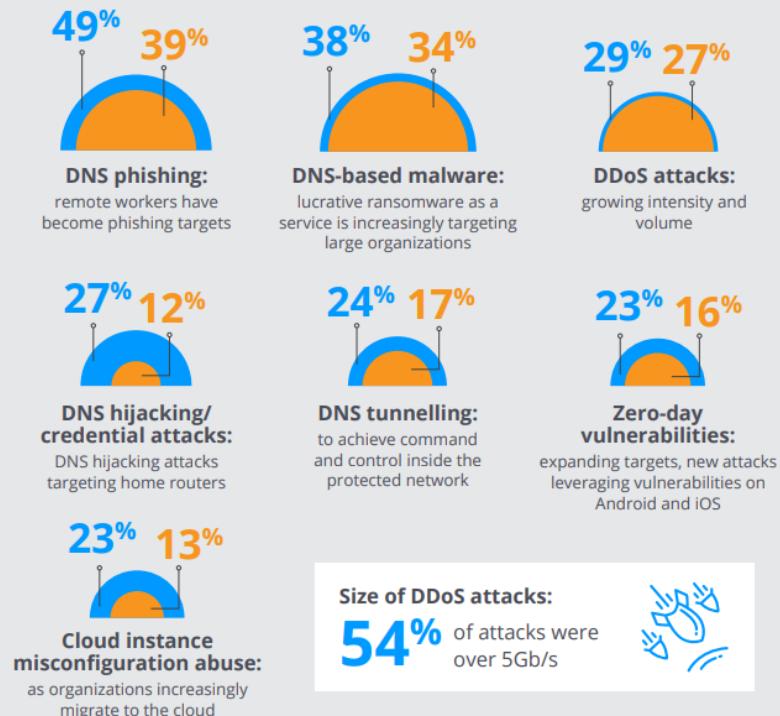
DNS remains a prime target for hackers as it enables them to gain first entry into networks and gain access to data for exfiltration:



With the pandemic rapidly increasing cloud usage and the number of people remote working, the attack surface has increased considerably. As a result, organizations have suffered more diverse types of attacks than ever before, showing that cybercriminals are using all the tools at their disposal to exploit both the DNS protocol and misconfigurations.

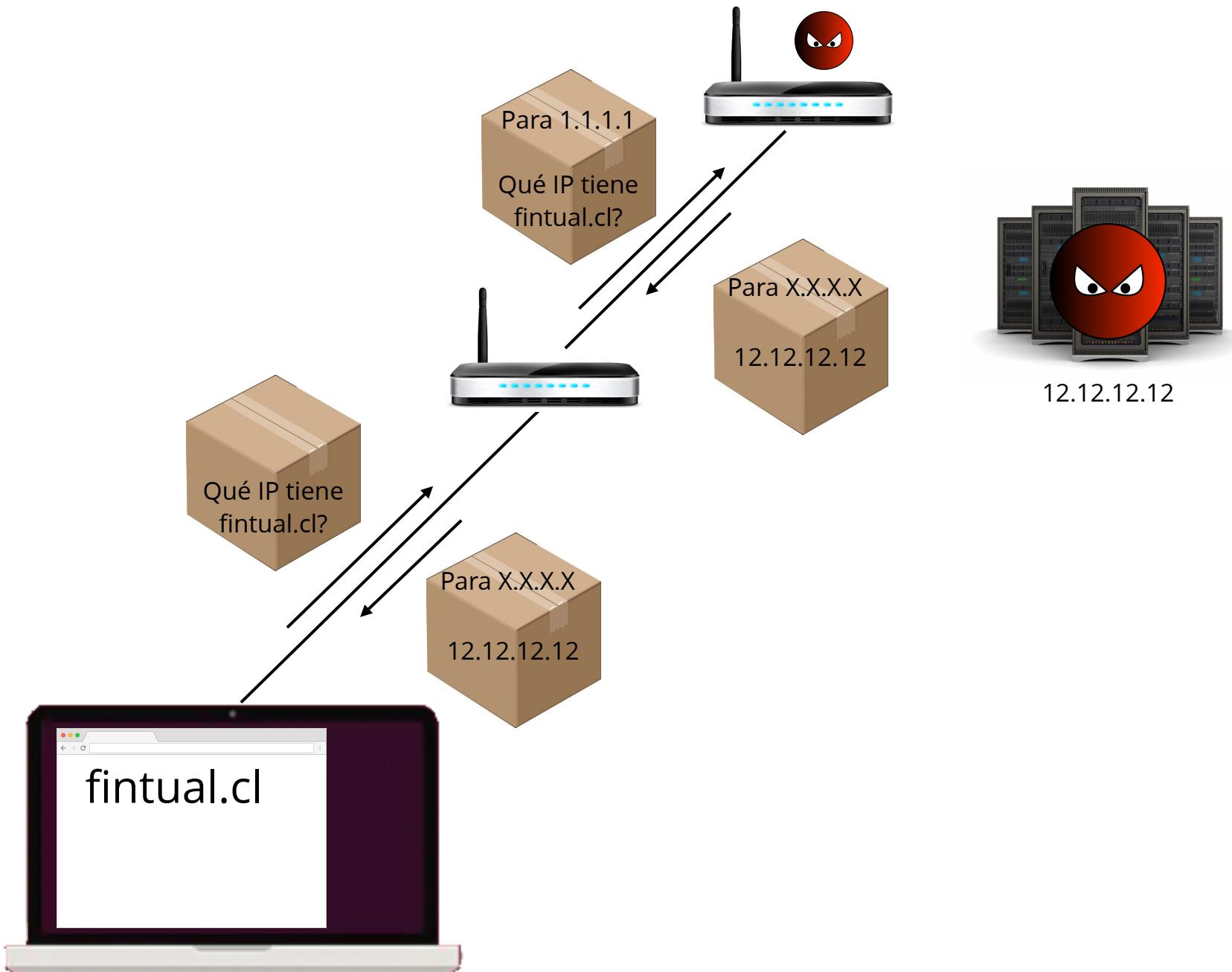
Top DNS-based attacks:

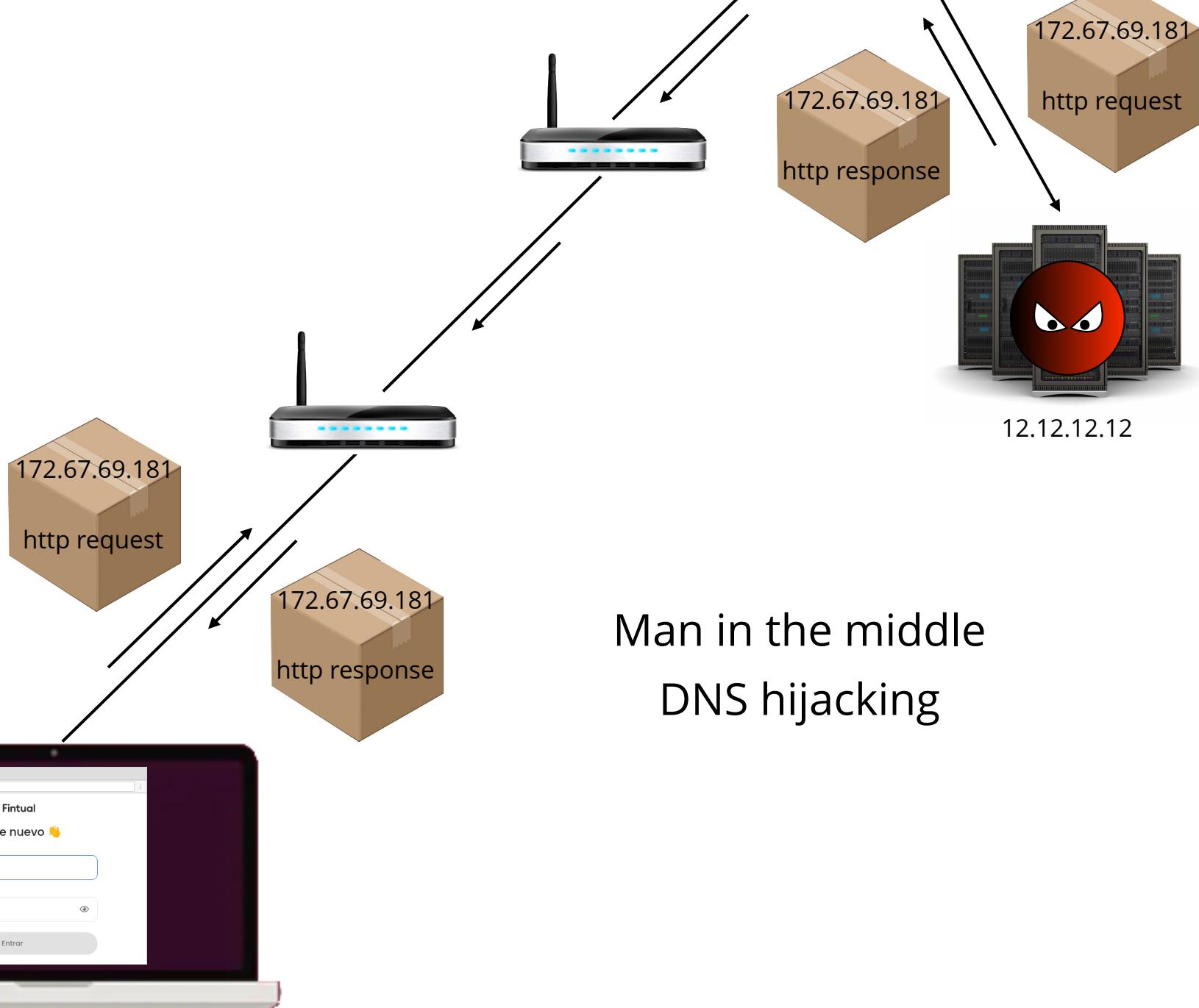
● 2021 ● 2020



The COVID-19 pandemic has created new challenges for businesses as they adapt to WFH operating models. DX initiatives are accelerated, and cybersecurity becomes a major concern:

- Remote workers fall more for phishing scams
- Vulnerabilities leading to credential stuffing and DNS spoofing
- Use of personal devices for work and corporate PC for personal use
- VPNs not user friendly, using too much bandwidth, creating latency leading to poor user experience
- Reliance on home Wi-Fi and home security





Soluciones?



Public-key crypto to the rescue





Public key





Problemas?



Enter Certificate Authorities (CAs)





Y cómo se yo que
esta es realmente la
llave pública de
Fintual?



Public key

Seguro y autentificado



Firmado por la CA



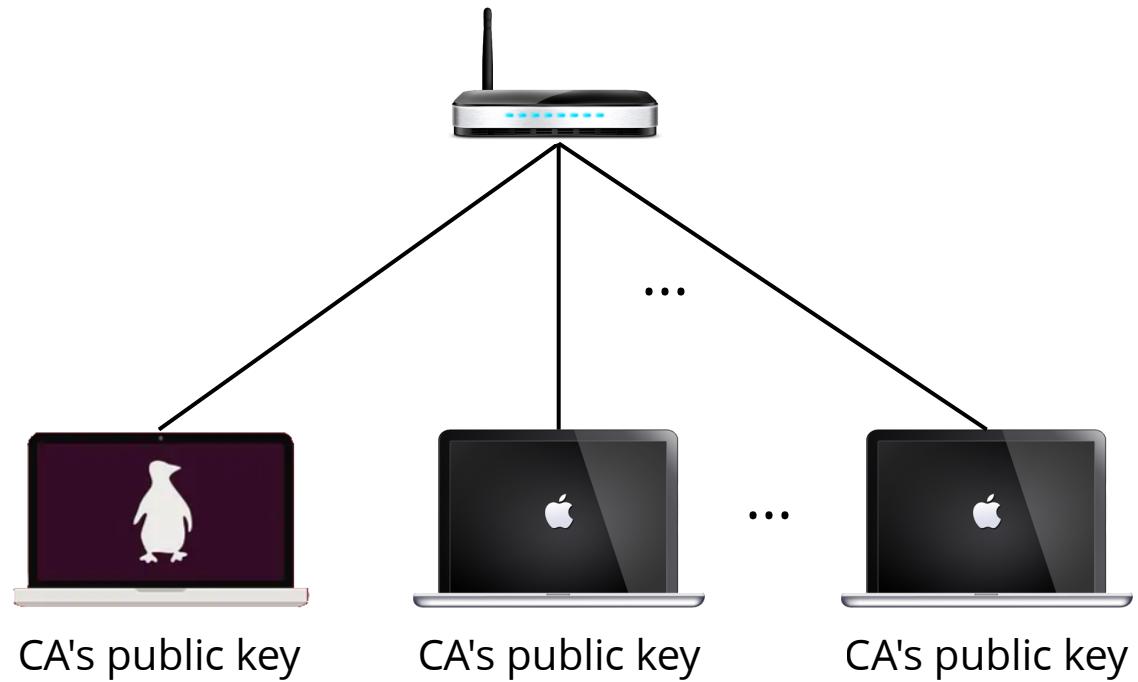
Te dejo un
certificado
firmado por la
CA, dice que esa
es mi llave
pública



Private key

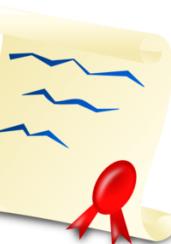
¿Más problemas?







Y cómo se yo que
esta es realmente la
llave pública de
Fintual?



Public key

Seguro y autentificado



 **Fintual**
Private key

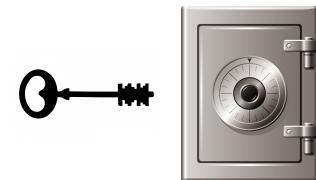
Firmado por la CA



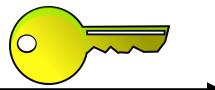
Te dejo un
certificado
firmado por la
CA, dice que
esa es mi llave
pública

¿Cómo se obtiene este certificado?

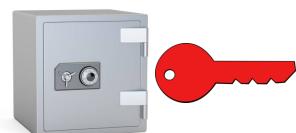




Quisiera sacar certificados para fintual.com, aquí mi llave pública



Primero, no te vayas a equivocar, firma <nonce> con la llave privada



Listo!



Además, tienes que poner este <nonce2> en fintual.com/<nonce3>

Todo en orden!

Bacán! me darías un certificado para asegurar fintual.com con esta otra llave pública?



Listo!



Es la llave de fintual.com

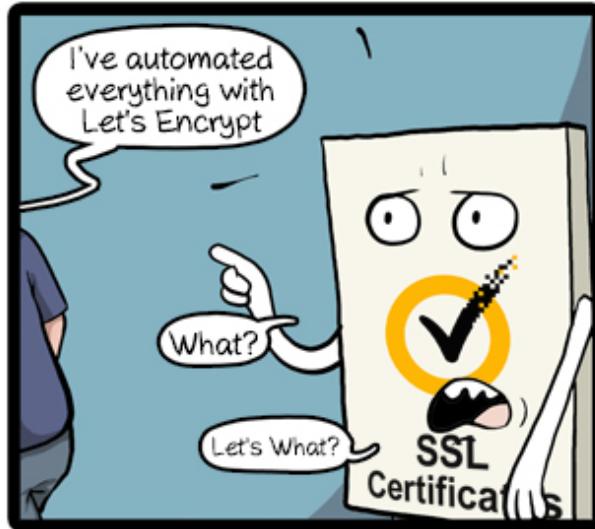
Gracias!

Estos certificados son bastante más complejos en estructura, pero el flujo anterior resume cómo se obtienen

Teniendo certeza de que estoy hablando con el dueño del sitio y tengo la llave pública, aseguramos la sesión con DH

<https://tls12.ulfheim.net/>

para (muchísimos) más detalles







https://fintual.cl



Hola de nuevo 🙌

Email

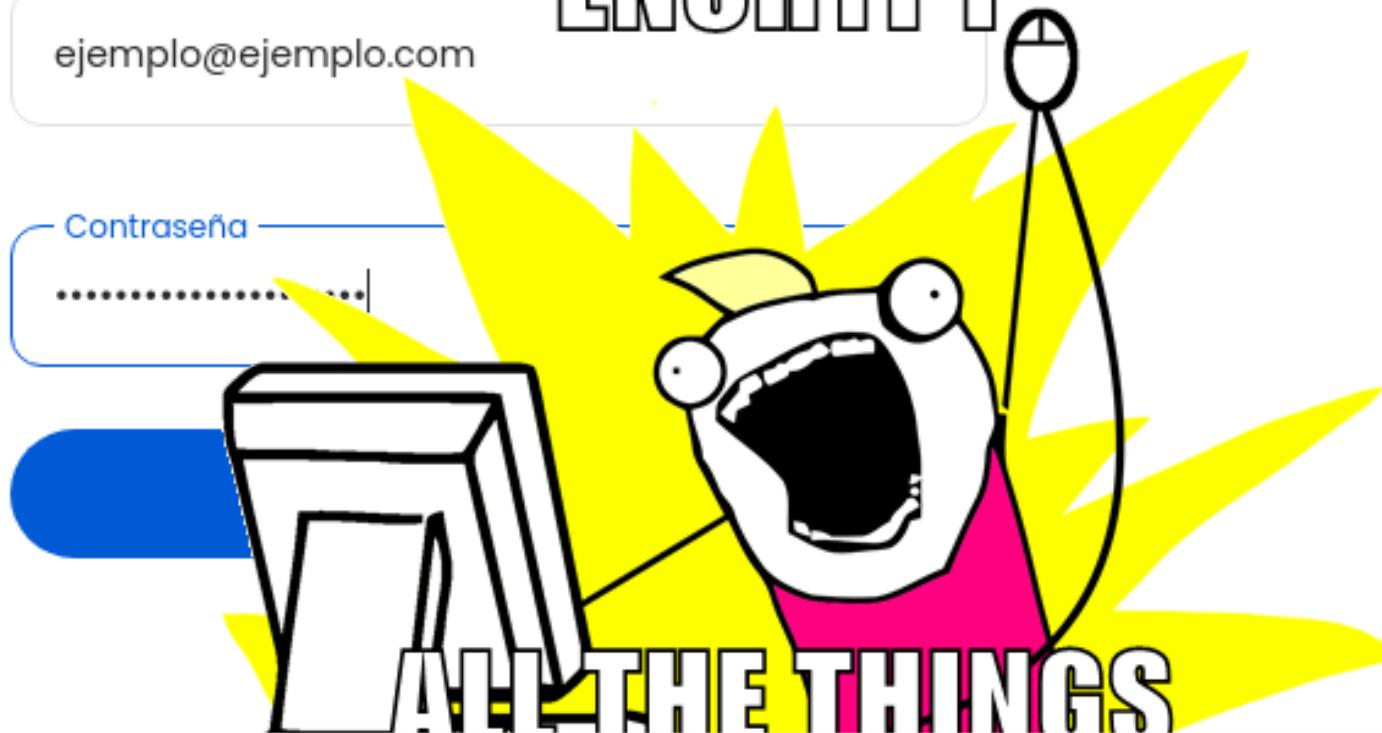
ejemplo@ejemplo.com

Contraseña

.....

ENCRYPT

ALL THE THINGS



Ruteo IP

DNS

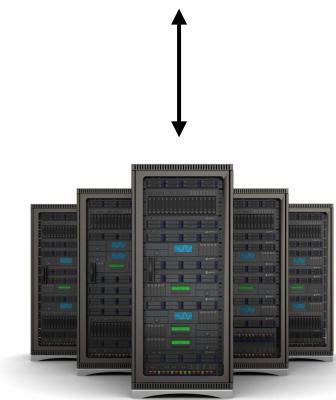
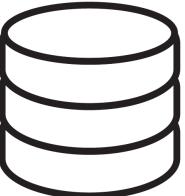
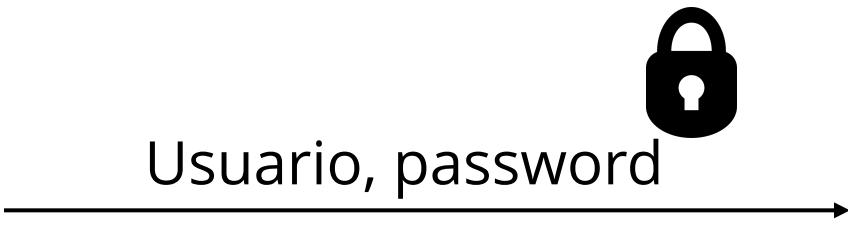
Https

Autoridades Certificadoras

Vamos bien?

Todavía?





 Fintual

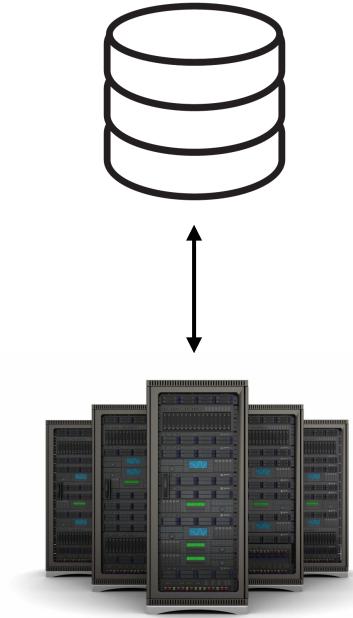
The Fintual logo, which consists of a blue speech bubble-like shape followed by the word "Fintual" in a bold, lowercase, sans-serif font.

Es cierto que
este usuario
tiene este
password?

A large block of text in a black sans-serif font. It contains a question mark at the end, suggesting a query or a challenge related to the user's identity.

Correo	Password
atac@ble.com	1Cl4v3muyM4l4
vulner@ble.cl	1Cl4v3P3s1m4

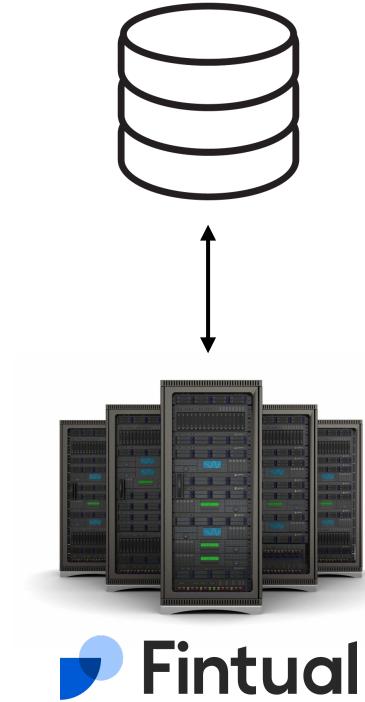
Cualquier persona que gane acceso a la base de datos podría ver correos y contraseñas...



Es cierto que este usuario tiene este password?

¿Cómo lo arreglamos?

Correo	SHA256(password)
atac@ble.cl	ef52045429b9094900170095 d91e2bb6b78c514b
vulner@ble.cl	30df6af7eb3dd9e5b9944020 440b9fc6d325beec



Mejor, pero todavía hay problemas...

Es cierto que este usuario tiene este password?

Rainbow Tables

Las 500.000 Contraseñas más comunes de 2021

123456	356a192b7913b04c54574d18c28d46e6395428ab
123456789	da4b9237bacccdf19c0760cab7aec4a8359010b0
picture1	77de68daecd823babbb58edb1c8e14d7106e83bb
password	1b6453892473a467d07372d45eb05abc2031647a
12345678	ac3478d69a3c81fa62e60f5c3696165a4e5e6ac4
111111	c1dfd96eea8cc2b62785275bca38ac261256e278
123123	902ba3cda1883801594b6e1b452790cc53948fd
12345	da4b9237bacccdf19c0760cab7aec4a8359010b0
1234567890	77de68daecd823babbb58edb1c8e14d7106e83bb
...	...

Correo	SHA256(password)
atac@ble.cl	ef52045429b9094900170095d91e2 bb6b78c514b
vulner@ble.cl	30df6af7eb3dd9e5b9944020440b9f c6d325beec

Hay algún hash de mi rainbow table en la tabla de usuarios?

Cómo arreglamos esto?

Correo	Salt	Hash(password Salt)
c@lidad.cl	fz4/fho#hg%gjs	ef52045429b909490017 0095d91e2bb6b78c514b
mejor@s.cl	zxc\$f4(w@hvg>	30df6af7eb3dd9e5b994 4020440b9fc6d325beec

Por qué no podemos atacar con rainbow tables?

Hagámoslo todavía más desagradable para los atacantes!

Correo	HKDF(password)
impec@ble.cl	pbkdf2_sha256\$260000\$W0U57Kqw5UDvasFO 0YQccX\$GAbxNa/PfEtEnS3APi5eV356wpdkfo3ba QNdGsNn2e8=
inmejor@ble.cl	pbkdf2_sha256\$260000\$JxxEv17MH36GQeNao qScmQ\$5vfidwdL96PEWmaZMH3WrVPkoNXoM cO6JrOUKK24vf8=



Es cierto que
este usuario
tiene este
password?

¡Ganamos acceso!



https://fintual.cl



Hola de nuevo 

Email

ejemplo@ejemplo.com

Contraseña

.....



Entrar



https://fintual.cl



Fintual

Hola Martín 

Invirtiendo fácil hace 477 días

+ Nuevo Objetivo

 Invertir más





Quiero invertir más



¿Cómo lo arreglamos?



¿Dónde lo guardamos?

¿Opciones?

Variable en JavaScript

LocalStorage

Cookie

Variable en JavaScript

Muy volátil, difícil de saber si se cambia

LocalStorage

Podría ser buena idea, ¿pero qué pasa si alguna librería en mi *node_modules* está infectada?

Cookies

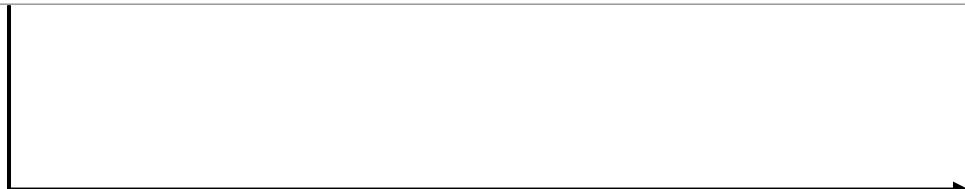
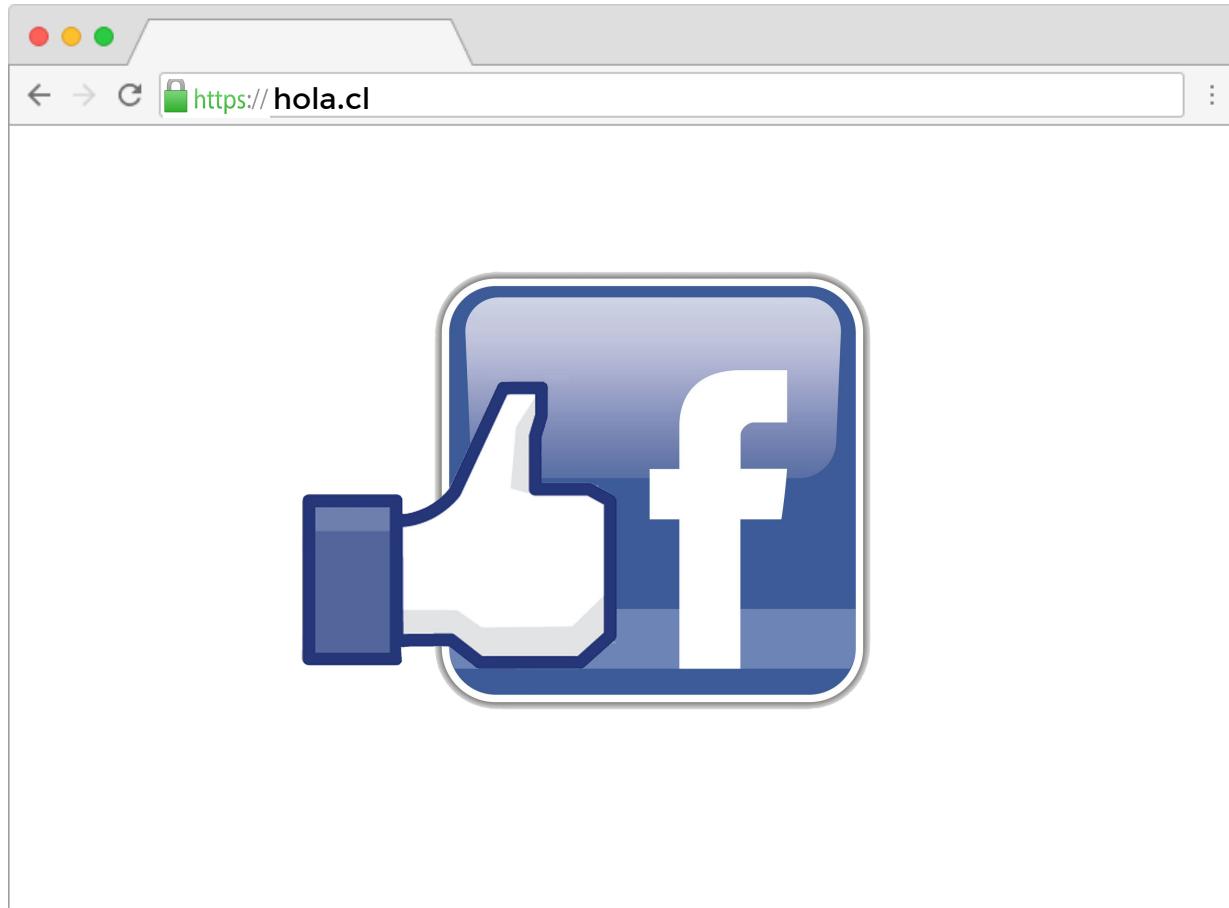
Suena razonable. ¿Qué problema podríamos tener? 

HTTP_ONLY: Para que no la pueda leer el JS



Martín me dio un like!!





Martín me dio un like!!
(Acá van sus cookies)



Perfecto!

¿Problemas?

To be continued...