

Web “Profunda”

Dice valles que esto es todo fruta que dicen en los cursitos

¿Cuántos sitios existen ?

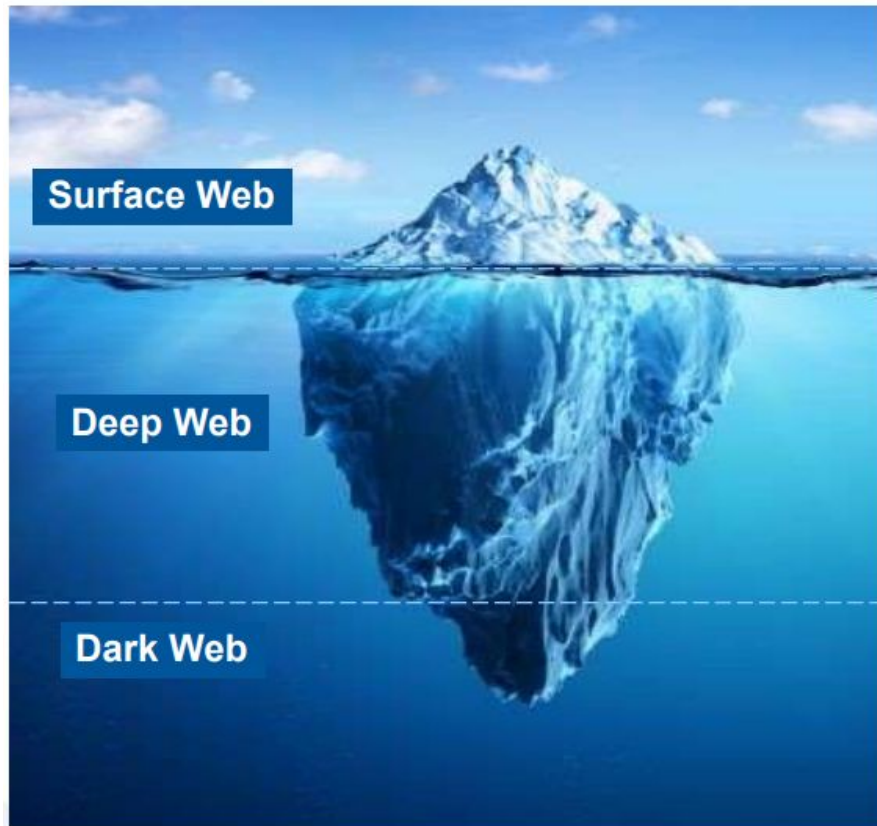
- ClearNet (Encontrada por buscadores)
- DeepWeb (NO encontrada)
- DarkWeb (Sitios NO públicos en red plana)
 - Están dentro de una DarkNet

Hay muchos juicios por "derecho al olvido", de gente que pide que después de tanto tiempo se borren sus datos de internet. Esta gente, en vez de iniciar una acción legal en contra de la página web que está utilizando su imagen (por ejemplo), inician acción legal contra Google.

Deep y Dark (?)

Esto tambien es fruta.

Un concepto importante es que NO existen dos internet distintas, los cables son todos lo mismo, cabase es el mismo, etc.



Anonimizar

¿Cómo lograr anonimizar a un **cliente** que quiere acceder a un sitio?

¿Como logro anonimizar un **sitio** web ?

La deep web tiene dos objetivos:

- Anonimizar clientes
- Anonimizar servidores

Anonimizar

■ Opciones en “clearnet”

Los proveedores VPN gratuitos, te bajan un certificado SSL de ellos, y pueden utilizar tus datos.

- ☐ Proxy
- ☐ VPNs (ej. Plugins)

■ Opciones DarkNet

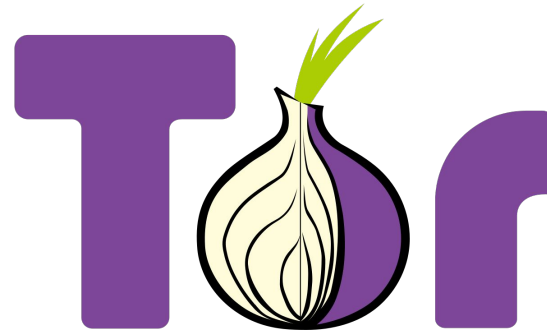
Estas son aplicaciones que crean capas de software con cifrado para anonimizar al cliente o el servidor, utilizando las mismas redes, IP y routers que se usan en internet normal.

- ☐ Tor network + **Aplicación**
- ☐ FreeNet
- ☐ I2P
- ☐

El mas conocido es TOR. Freenet y I2P son proyectos similares

TOR

- The Onion Router
- Puede anonimizar
 - ☐ Al Cliente
 - ☐ Al servidor
 - ☐ A ambos



Es un proyecto comunitario.

Para que esto funcione, se necesita gente que colabore con el proyecto en todo el mundo (uno participa bajandose la aplicacion).

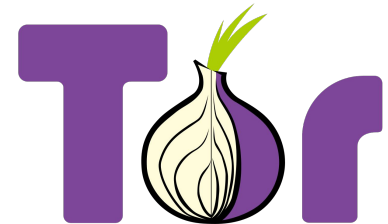
Otro proyecto comunitario en el que uno puede ser un nodo, es la blockchain. Uno puede hostear un nodo de blockchain y colaborar.

TOR

■ Componentes

Es un proyecto comunitario que requiere de la colaboracion de la gente.
Otro proyecto comunitario es la blockchain.

- Cliente
 - Servicio de directorio
 - Nodos de entrada
 - Nodos intermedios (relay servers)
 - Nodo de salida (exit servers)
-
- No resuelve todo el anonimato.





Anonimizar Cliente

Cómo funciona TOR

Las computadoras con + tienen instalada la app de tor

How Tor Works: 1

Ejemplo: Alicia se quiere conectar a clarín, y no quiere que clarín sepa que ella se conectó. Si no utilizara TOR, entonces clarín podría hacer un WHOIS de la IP, averiguar nuestro ISP, y tal vez hacer un pedido por medio judicial al ISP pidiendo quien tenía esa IP y puerto en tal día tal momento.



Hay países en donde no hay regulación en el estado en donde le obligue a los ISP (y servidores como clarín.com) guardar quien tenía cada IP en cada instante. En Argentina los ISP tienen esta obligación, y estos datos se usan para responder oficios judiciales. No se guardan por tanto tiempo estos datos igual. Los países que no tienen estas regulaciones, se llaman "refugios digitales"



Los datos (como IP de pedidos) que los servidores guardan, las empresas lo usan para analizar de que países se conecta la gente, que buscan, etc para hacer marketing

EJ - www.clarin.com

Directory AUTHORITY Server

- El cliente (Tor Browser) tiene una lista de
 - Directory AUTHORITY Service
- Hoy son 9 servidores

Relay Search

flag:authority

Show 10 entries

Son los primeros servidores donde vas a buscar información sobre el resto de los servidores. El concepto es parecido a los Root DNS Servers. El cliente ya los tiene precargados, y cuando me conecte me van a dar una lista de todos los relays que están prendidos (que son las computadoras con el + en la slide anterior).

Nickname [†]	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
● dannenberg (1)	100 KiB/s	5d 19h		193.23.244.244	2001:678:558:1000::244			443	80	Relay
● Serge (3)	100 KiB/s	25d 17h		66.111.2.131	2610:1c0:0:5::131			9001	9030	Relay
● dizum (1)	88 KiB/s	17d 22h		45.66.35.11	-			443	80	Relay
● tor26 (1)	75 KiB/s	2d 10h		217.196.147.77	2a02:16a8:662:2203::1			443	80	Relay
● bastet (1)	50 KiB/s	11d 19h		204.13.164.118	2620:13:4000:6000::1000:118			443	80	Relay
● maatuska (3)	50 KiB/s	46d 18h		171.25.193.9	2001:67c:289c::9			80	443	Relay
● moria1 (1)	40 KiB/s	14d 1h		128.31.0.39	-			9201	9231	Relay
● gabelmoo (1)	40 KiB/s	14d 19h		131.188.40.189	2001:638:a000:4140::ffff:189			443	80	Relay
● longclaw (1)	38 KiB/s	3d 12h		199.58.81.140	-			443	80	Relay
Total	581 KiB/s									

Showing 1 to 9 of 9 entries

Relays

- De un Directory AUTHORITY Server el cliente se descarga la lista de relays de toda la red
- Con esa lista el cliente elige el PATH (sucesión de relays) que va a usar.
- El cliente crea un CIRCUITO (al menos 3 relays)

Cuando Alicia se baje la lista de relays del authority server, va a elegir 3 al azar y va a armar un circuito. Se va a conectar al primero, el primero al segundo, el segundo al tercero, y de ahí voy a llegar a clarin.com.

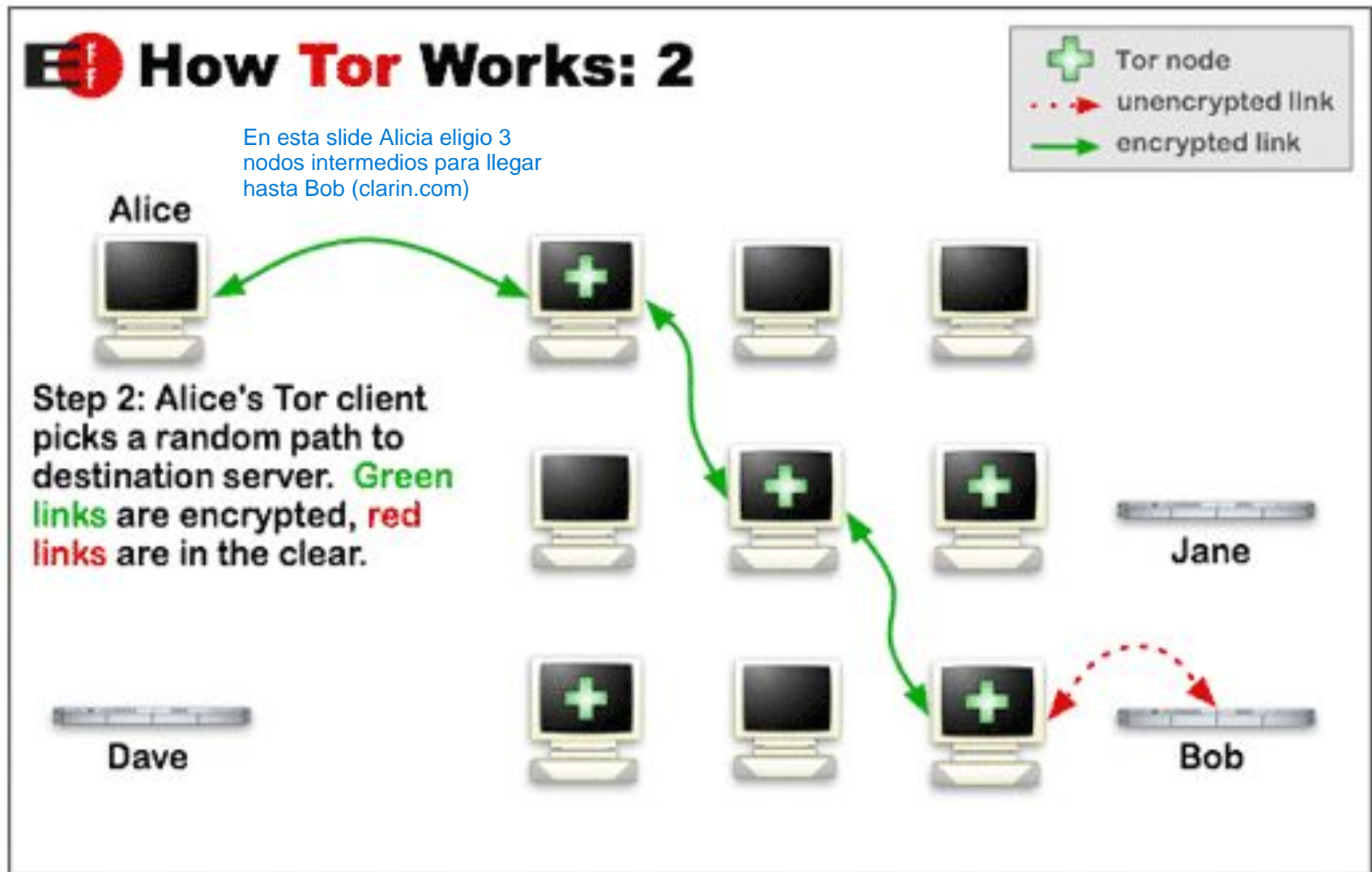
El objetivo es que el nodo 1 conoce a Alicia. El nodo 2 conoce al nodo 1 y al nodo 3. El nodo 3 conoce a clarin.com.

La idea es que ningún nodo puede asociar a Alicia con clarin.com. Si hacemos esto con menos de 3 nodos, se rompe. Si lo hacemos con más de 3 nodos, es mejor en seguridad pero la velocidad sigue decreciendo.

La única persona que conoce todo el camino es Alicia.

Notar que las conexiones a nivel TCP/IP son las mismas que internet normal. Lo distinto está en el esquema de nodos, en la cebolla y en el cifrado usado.

Cómo funciona TOR



Relay Servers

- Los relay servers:

- Solo conocen quien les habla y a quién hablan (un solo salto)

Solo alice sabe el camino completo

- Nunca saben el camino completo.

Este path tiene un timeout, que cambia la ruta cada cierto tiempo para sumar seguridad. Uno pensaria que si el path se cambia todo el tiempo entonces se pierden paquetes. Esto es verdad pero TCP detecta esta perdida de paquetes y pide su retransmision.

Notar que varios de los nodos estan hosteados en paises que obligan a los ISP a guardar logs de IPs usadas por cada cliente

No siempre el camino de ida es el mismo que el camino de vuelta

Una peligro es: si yo soy la CIA/FBI entonces tendria que levantar muchos nodos en la red TOR para trackear a la gente. Sin embargo, deberia alterar el software para que guarde las IPs de la gente. El problema es que con eso, estoy cambiando la firma de mi nodo, y los otros nodos no se van a conectar a mi porque tengo la firma cambiada.

Chequeo

<https://check.torproject.org/>



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **185.220.101.148**

Please refer to the [Tor website](https://www.torproject.org/) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Relay Search](#).

Podemos hacer click en “relay search” y buscar el nodo de salida que estamos usando

Cifrado

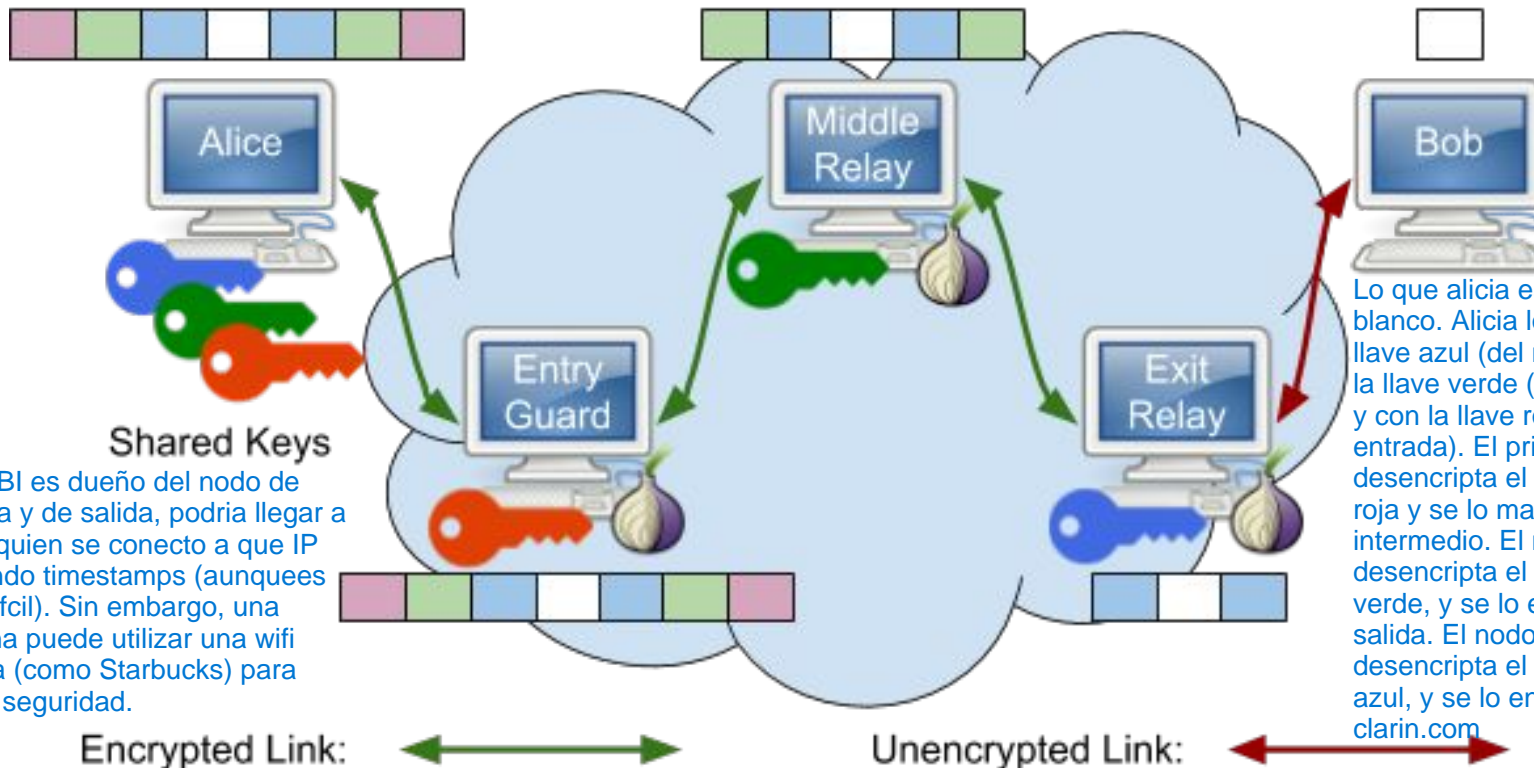
- El cliente negocia con cada relay la llave de cifrado simétrico.
- Existen llaves que se usan para cifrado y para autenticación

Cómo funciona el cifrado

Alicia obtiene las llaves de cifrado de cada relay cuando se comunica con el authority server. Estas claves son SIMETRICAS. Estas claves las comparto con cada nodo al inicio de la conexión.

Encrypted Message

Decrypted Message



Lo que termina pasando es que se hace una cebolla de encriptados.

Lo que alicia esta mandando es lo blanco. Alicia lo encripta con la llave azul (del nodo de salida), con la llave verde (del nodo del medio), y con la llave roja (del nodo de entrada). El primer nodo descripta el paquete con su llave roja y se lo manda al nodo intermedio. El nodo intermedio descripta el paquete con su llave verde, y se lo envia al nodo de salida. El nodo de salida descripta el paquete con su llave azul, y se lo envia descriptado a clarin.com

Si el FBI es dueño del nodo de entrada y de salida, podria llegar a inferir quien se conecto a que IP utilizando timestamps (aunquees muy difcil). Sin embargo, una persona puede utilizar una wifi publica (como Starbucks) para sumar seguridad.

Source: Alice	Source: Entry	Source: Middle	Source: Exit	Data	Dest: Bob	Dest: Exit	Dest: Middle	Dest: Entry
---------------	---------------	----------------	--------------	------	-----------	------------	--------------	-------------

Estas "capas de cebolla" de encriptaciones, consumen tiempo y agrandan el tamaño de los mensajes a enviar. Mientras mas nodos se sumen, mas lento anda.

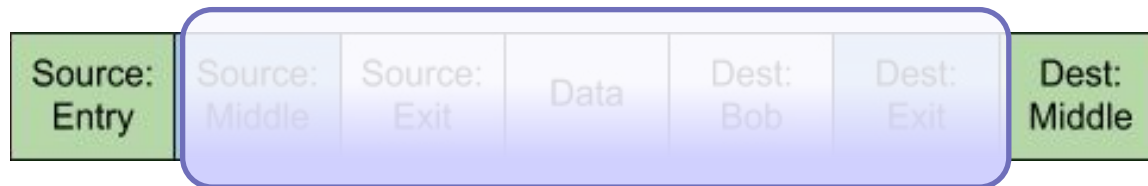
Notar que el nodo de salida puede ver la salida descriptada. Entonces lo que tiene que hacer alicia es usar TLS con clarin, para que solo clarin pueda ver el paquete. Entonces lo blanco tambien viajaria encriptado.

Cómo funciona el cifrado

Este es el paquete que prepara Alice para enviar a Bob



El primer nodo ve esto al descifrar con la llave “roja”:



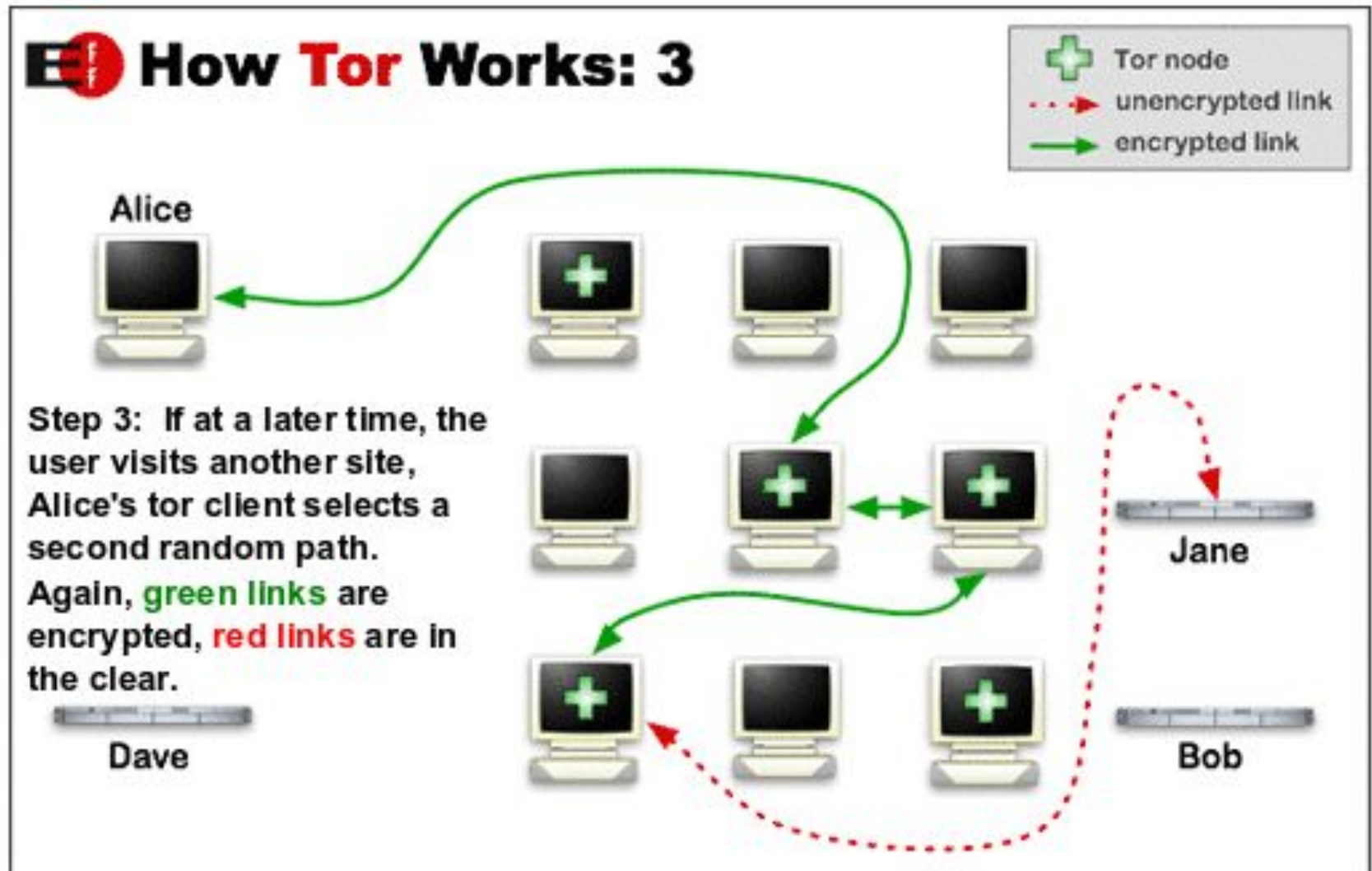
Pasa el paquete al próximo nodo

Cómo responde el servidor

- El servidor responde el paquete al EXIT NODE
 - (no sabe la IP del cliente inicial)
- El nodo de Exit busca en su tabla de asignación el Circuit ID y sabe que debe devolver el paquete al MIDDLE (por IP y puerto)
- Todos cifran con su clave pública.
- Alice tiene la clave privada para descifrar.

Cada nodo participa de multiples circuitos al mismo tiempo, pudiendo ser entry/middle/exit en cada uno de los distintos circuitos. Estos nodos guardan en una tabla de hash a quien le tienen que redirigir los paquetes que le van llegando.

Cómo funciona TOR - Conexiones



Conexiones

- Aproximadamente duran 10 minutos.
- Se puede forzar el cambio manual.
- “Exit Node” puede ver los paquetes entrantes y salientes. Por eso hay que encriptarlos utilizando TLS con el servidor destino
- Tor anonimiza el origen del tráfico. El servidor destino piensa que se esta comunicando con el EXIT NODE
- Si quiero mas privacidad debo usar “TLS /SSL”

Riesgos

- Si alguien ve tráfico del nodo entrante y del nodo de salida, por comparación de tráfico pueden llegar a determinar al cliente.
- No cifrar el mensaje (TLS, HTTPS)

(porque en este caso el EXIT NODE podría ver nuestro paquete en texto plano)

Ejemplo con Tor Browser

The screenshot shows the Tor Browser interface with the Google homepage in the background. A 'Site Information' popup is open for 'https://www.google.com'. The 'Tor Circuit' section displays a vertical list of nodes: 'This browser', 'Canada 198.245.49.191 Guard', 'United Kingdom 54.36.165.170', 'Netherlands 163.172.213.212', and 'google.com'. A blue button labeled 'New Circuit for this Site' is visible below the circuit. A blue annotation points to the circuit list with the text 'Aca se puede ver el circuito de los 3 nodos'. The background shows the Google logo and search bar.

Site Information for www.google.com

Connection secure

Tor Circuit

- This browser
- Canada 198.245.49.191 **Guard**
- United Kingdom 54.36.165.170
- Netherlands 163.172.213.212
- google.com

New Circuit for this Site

Your **Guard** node may not change. [Learn more](#)

Permissions

You have not granted this site any special permissions.

Aca se puede ver el circuito de los 3 nodos

Google

Google zoeken Ik doe een gok

Google aangeboden in: [Frysk](#) [English](#)

Tor cómo servicio

```
srv@srv-nb:~/Downloads/tor/tor-browser_en-US$ sudo service tor start
* Starting tor daemon...
srv@srv-nb:~/Downloads/tor/tor-browser_en-US$ netstat -an | grep 9050
tcp        0      0 127.0.0.1:9050      0.0.0.0:*           LISTEN
srv@srv-nb:~/Downloads/tor/tor-browser_en-US$
```

Levanta un servicio en localhost:9050

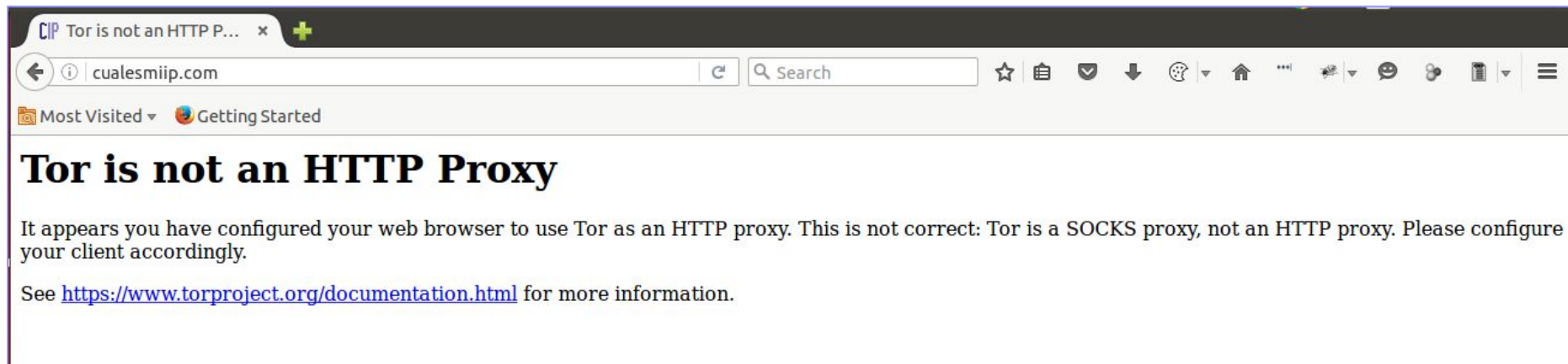
Puedo rutear cualquier aplicacion para que use ese servicio

Esto es si quiero usar la red de TOR sin TOR browser. Por ejemplo, para conectarme a pampetro por ssh utilizando la red de TOR.

Un navegador
Un escáner de puertos
Un cliente SSH
etc

Ejemplo con Firefox

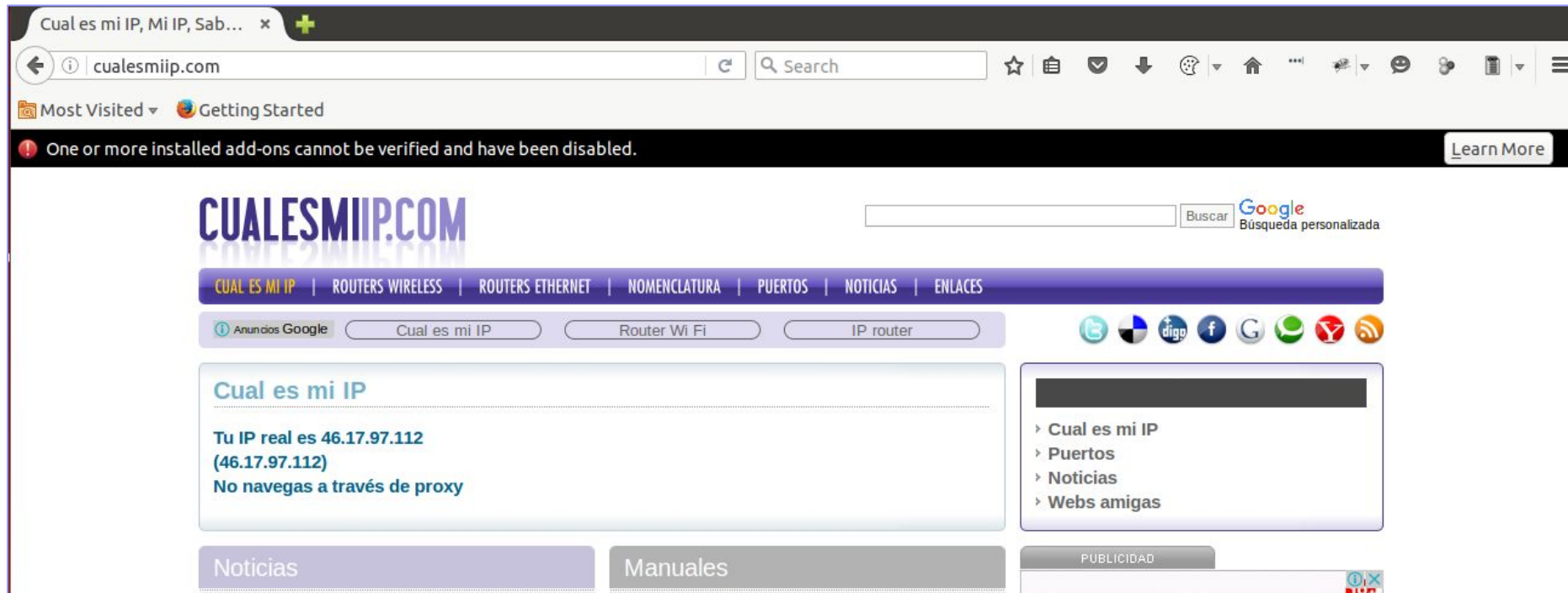
Configuramos en Firefox el proxy HTTP en localhost:9050 y al navegar.....



TOR NO es un proxy HTTP, es un proxy SOCKS

Ejemplo con Firefox - SOCKS

Configuramos solo SOCKS en Firefox localhost:9050 y al navegar.....



Ejemplo TOR en línea de comando

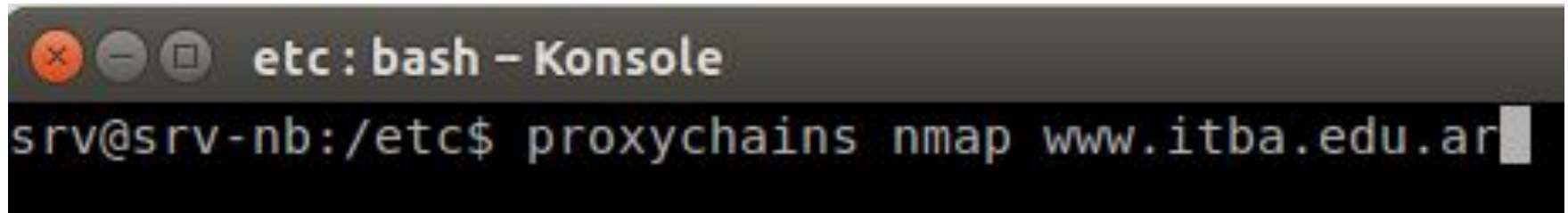
Usando curl sin y con TOR como proxy

```
[ec2-user@ip-172-31-42-40 ~]$ curl ipinfo.io
{
  "ip": "54.147.231.169",
  "hostname": "ec2-54-147-231-169.compute-1.amazonaws.com",
  "city": "Ashburn",
  "region": "Virginia",
  "country": "US",
  "loc": "39.0437,-77.4875",
  "org": "AS14618 Amazon.com, Inc.",
  "postal": "20149",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
```

```
[ec2-user@ip-172-31-42-40 ~]$ curl -s --socks5-hostname 127.0.0.1:9050 http://ipinfo.io
{
  "ip": "77.247.181.163",
  "hostname": "lumumba.torserver.net",
  "city": "Amsterdam",
  "region": "North Holland",
  "country": "NL",
  "loc": "52.3740,4.8897",
  "org": "AS43350 NForce Entertainment B.V.",
  "postal": "1012",
  "timezone": "Europe/Amsterdam",
  "readme": "https://ipinfo.io/missingauth"
```

Ejemplo TOR en línea de comando

Usando el programa “proxychains” se puede redireccionar fácilmente otras apps a TOR

A terminal window titled "etc : bash - Konsole" with standard window control buttons (close, minimize, maximize). The terminal shows a command being entered: "srv@srv-nb:/etc\$ proxychains nmap www.itba.edu.ar".

```
etc : bash - Konsole
srv@srv-nb:/etc$ proxychains nmap www.itba.edu.ar
```

Hidden services

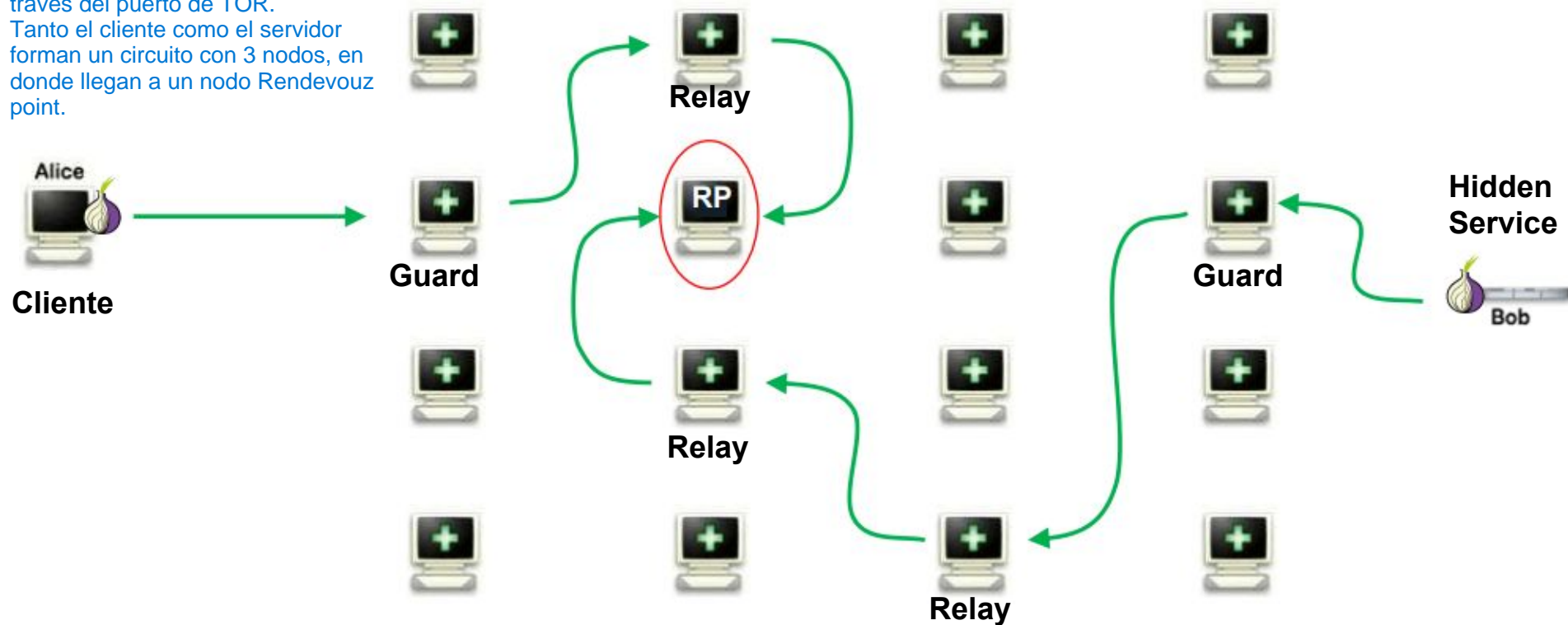
(como hago anonimo un servidor)

¿Cómo anonimizar servicios
(ej sitio web) si estamos
dentro de Internet con IP de
un ISP ?

Hidden services

Hacen dos circuitos (anonimizando al cliente y al servidor). Bob levanta un sitio web. En vez de escuchar en el puerto 90 o el 443, escucha solo a través del puerto de TOR.

Tanto el cliente como el servidor forman un circuito con 3 nodos, en donde llegan a un nodo Rendezvous point.

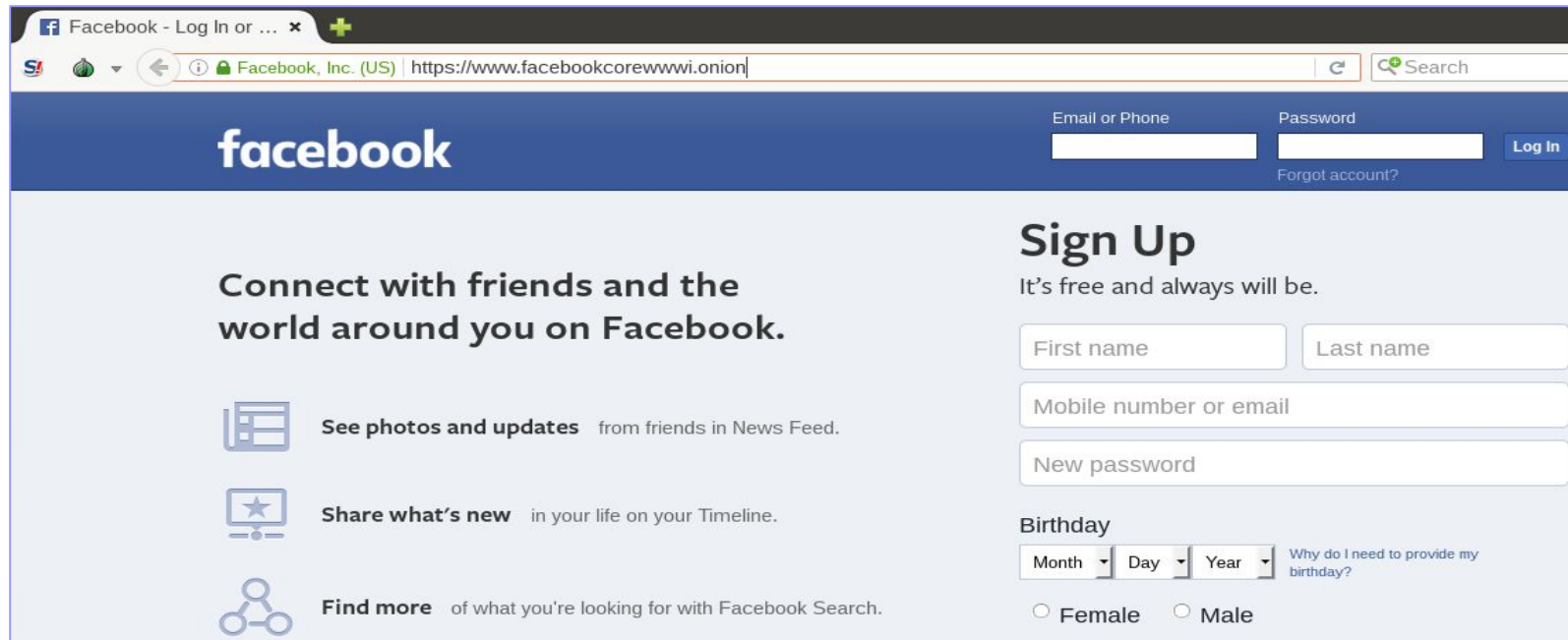


RP: Rendezvous point (punto de encuentro)

Alice y Bob crean circuito con RP (circuito = tres saltos)

Bob levanta un servicio, genera el URL .onion, y registro el hash en un servicio de directorio. Los nodos de la red, van a terminar armando el hash entre todos, sin que ninguno sepa el hash completo. Ni siquiera el ultimo puede saber el hash completo.

Facebook en la red Tor



Facebook - Log In or ...

Facebook, Inc. (US) | https://www.facebookcorewwwi.onion | Search

facebook

Email or Phone Password Log In

Forgot account?

Sign Up
It's free and always will be.

First name Last name

Mobile number or email

New password

Birthday
Month Day Year Why do I need to provide my birthday?

☐ Female ☐ Male

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

Nueva dirección

Muchas empresas "legales" ponen sus servidores tambien en la dark web. Estas empresas colaboran con la gente que quiere utilizar de manera anonima estos servicios, permitiendo esten a 6 nodos de distancia de mi servidor (dandome mas seguridad que si tuvieran solo 3).

facebookwkhpilnemxj7asaniu7vnjjbiltxjqhhye3mhbshg7kx5tfyd.onion

La pagina de la CIA y el FBI tambien tienen paginas en Dark Web.

De esta manera, si alguien quiere denunciar algo, estan tranquilos de que estan a 6 nodos de distancia de ser trackeados.

En TOR, las URL terminan en .onion

Estas direcciones NO se resuelven por DNS (porque sino el servidor no estaria anonimizado). La direccion es tan larga porque todos esos caracteres son parte de la llave publica del sitio .onion.

Facebook en la red Tor

Cuando quiero ver el CIRCUIT solo le muestra los 3 primeros “relays”

The screenshot shows a Tor browser window with a Facebook login page in the background. The address bar displays the URL: `https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion`. A Tor circuit overlay is visible, titled "Circuit for facebo...x5tfyd.onion". The circuit diagram shows the path from the browser through three relays: Finland (guard), United States, and Germany, followed by onion site relays and the destination site. A text box on the right explains that the circuit is shown up to the Rendezvous point, and that the user does not exchange keys with the onion site relays, thus anonymizing both the client and the server. At the bottom, it states "New Tor circuit for this site" and "Your guard node may not change".

Facebook - log in or sign up

← → ↻ https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion

Tor Circuit

Circuit for facebo...x5tfyd.onion

Tor Circuit

- This browser
- Finland (guard) 145.239.41.102
- United States 66.85.128.218
- Germany 185.207.107.98, 2a03:4000:1e:119::1
- Onion site relays
- facebo...x5tfyd.onion

Cuando entro a facebook.onion, me muestra los nodos de mi circuito hasta el Rendezvous, y luego me dice que vienen los "onion site relays", los cuales yo no conozco ni intercambio claves con ellos. De esta manera, logro anonimizar tanto el cliente como el servidor.

New Tor circuit for this site
Your guard node may not change

around you on Facebook.

Resolución de nombres

- .onion no es resuelto por el DNS tradicional
- La aplicación pasa el requerimiento del nombre a la red TOR. (por ejemplo con SOCKS)
- El nombre no corresponde a una IP (porque sino el servidor no estaria anonimizado)
- Los nombres son una combinación de llave pública del server, firmado con clave privada del servicio. Esto se registra en una tabla de hash distribuida. (Directory Server)

La idea de la tabla de hash distribuida es poder armar un hash con datos que estan distribuidos en distintas bases de datos. Entonces, los nodos relay tienen informacion parcial del hash en la URL. Ningun nodo tiene la informacion completa.

Hidden services

- Ejemplo

- Levanto un nginx en mi PC (que escucha en el puerto 80)
- Configuro servicio Tor (archivo Torrc) (le decimos que redirija el trafico a nuestro puerto 80)
- Se registra el servicio y se obtiene un nombre de 56 caracteres (parte de la clave pública del servidor)
- Se publica mi servicio en el directorio

Ejemplo

6zx6qma56jbl3qifk5rnta3zgbo4xf2d2q2vekt5r3yhwkwwig4q7j7id.onion/

Ningun nodo puede saber el hash completo del servidor.

1. El servidor se registra (armando una llave publica y subiendo el hash al directory service) y queda a la espera de conexiones. El servidor cambia constantemente en el directory service los nodos que se conectan al rendezvous.
2. Hay sitios que son foros que contienen listas de .onion. El dueño del servidor publica su .onion en este tipo de sitios. Los que cometen ilegalidades, van cambiando el .onion para que no los trackeen, pero las empresas como FBI/FACEBOOK generalmente no cambian su .onion.

Métricas

Permite buscar si una IP perteneció a TOR en un determinado día en un relay

Home » Services » ExoneraTor

ExoneraTor

La idea es que si alguien me ataca desde una IP en determinada fecha, yo le puedo preguntar a TOR si esa IP pertenecio a TOR (como un relay) en esa fecha. La unica respuesta es SI o NO, no me aportan mas informacion

Enter an IP address and date to find out whether that address was used as a Tor relay:

IP address	Date	
<input type="text" value="89.34.27.48"/>	<input type="text" value="24/05/2020"/>	<input type="button" value="Search"/>

Summary

Result is positive

We found one or more Tor relays on IP address 89.34.27.48 on or within a day of 2020-05-24 that Tor clients were likely to know.

Para buscar

Fue condenado a 3 cadenas perpetuas por el caso de SILK ROAD, que fue un sitio de venta de drogas que el gobierno de estados unidos trackeo por muchos años. Este sitio estaba publico en la dark web. Lo interesante es que aparentemente no pudieron averiguar quien era a traves de la red TOR, sino que hackearon el server donde estaba hosteado el sitio web (entrando por el .onion), por lo que el argumenta que el servidor fue hackeado (para resolver un delito uno no puede cometer un delito, entonces en teoria no lo pueden juzgar).

- Caso **SILK ROAD** (Ross Ulbricht)
- Proton Mail
- <https://protonirockerxow.onion/>
- DuckDuckGo
- <http://3g2upl4pq6kufc4m.onion/>

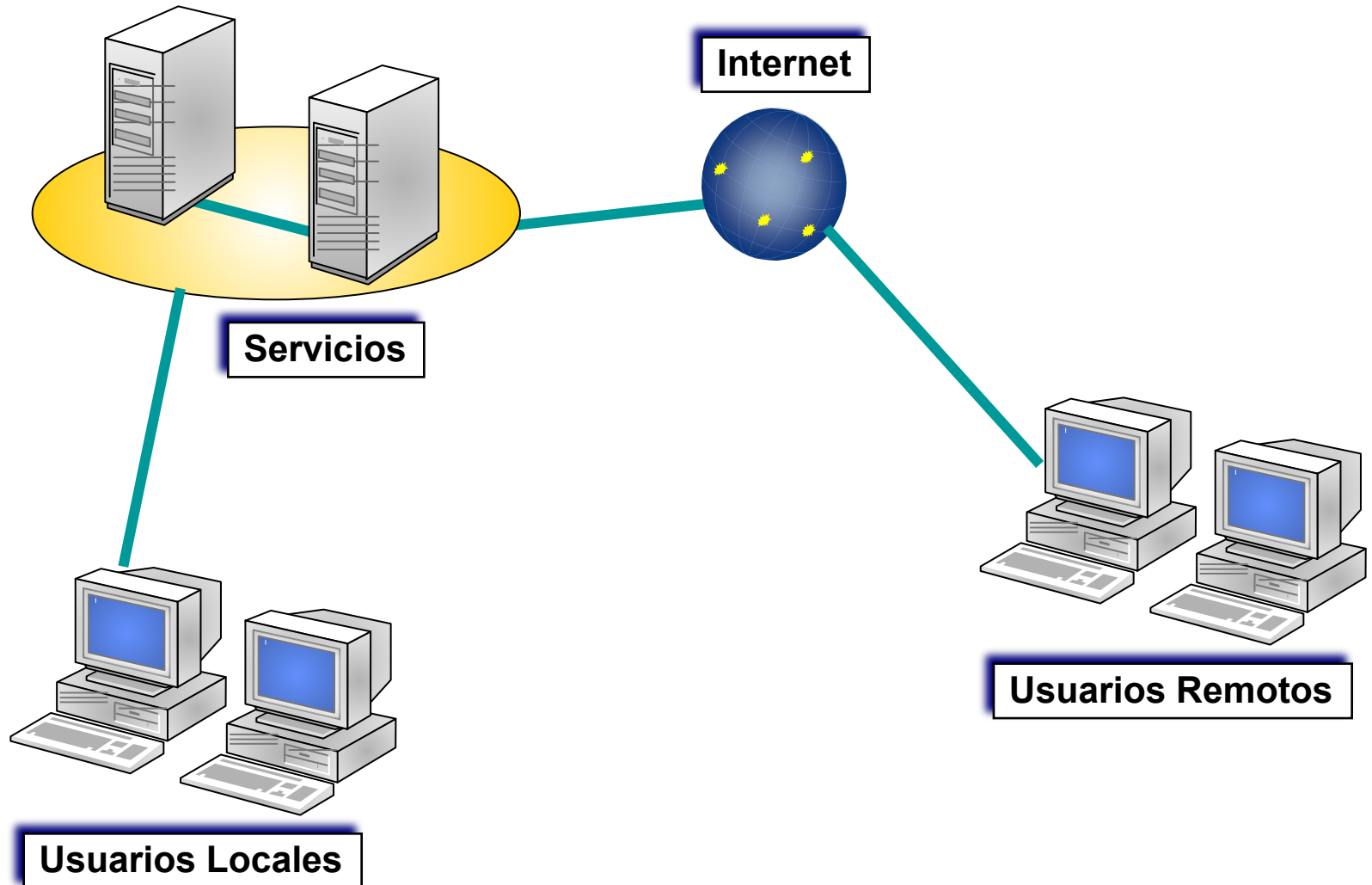


SEGURIDAD EN REDES

Lugares clásicos para aplicar seguridad

- Borde
- DMZ
- LAN

Topología clásica



Seguridad en capas

- Seguridad en capas
 - Seguridad en **estaciones** de trabajo
 - Seguridad en **red Interna**
 - Seguridad en **red de borde** La que se comunica a internet
 - **Seguridad física** de **centro de cómputos**
 - On-premises
 - En la nube
 - Veamos conceptos comunes para ambos.

Seguridad en Estación de trabajo

■ EPP

El menos seguro

- Endpoint Protection Platform

■ EDR

- Endpoint Detection and Recovery

■ XDR

- Extended Detection and Recovery

El mas seguro

Cuando nos dan una computadora de una empresa grande y no nos deja instalar nada.

No esta bueno para una empresa que el empleado haga lo que quiera con su compu, ya que esa compu se conecta luego a la red de la empresa (ya sea on-premise o VPN), entonces las empresas dan computadoras a los empleados con estos 3 productos: EPP, EDR, XDR (que es basicamente un antivirus).

Este software, no solamente escanea la maquina en busca de virus, sino que tiene firewall, controla la navegacion, controla las conexiones entrantes/salientes en distintos puertos, ven patrones de comportamiento (a que hora empiezo a trabajar, cuanto tipeo, que procesos corro) y cuando detectan un comportamiento anomalo accionan (ejemplo: si la maquina esta mandando 100 mails por minuto, tengo un problema)

Seguridad en Estación de trabajo

■ EPP

- Previene malware por firmas.
 - Filtro de contenidos al navegar.
 - Firewall local (IPS e IDS) y puertos
 - Control de periféricos escanea mouse/pendrive/etc
 - Control de aplicaciones No me deja instalar aplicaciones
 - Logs
-
- Orientado al chequeo luego de la acción del usuario o app

Seguridad en Estación de trabajo

■ EDR

- Consulta SQL al equipo para detectar anomalías.
- Detección de patrones de comportamiento.
- Aislamiento en Sandbox Antes de correr un software, lo corre primero en un sandbox para ver si tiene algun comportamiento raro
- Facilita el análisis de IOC (indicadores de compromiso)
- Orientado al monitoreo continuo en tiempo real.

Seguridad en Estación de trabajo

■ XDR

- Integra Endpoint, redes, nube, correo, etc
- Aplica Deep Learning para análisis
- El objetivo es mejorar los tiempos de detección y respuesta a incidentes globales.

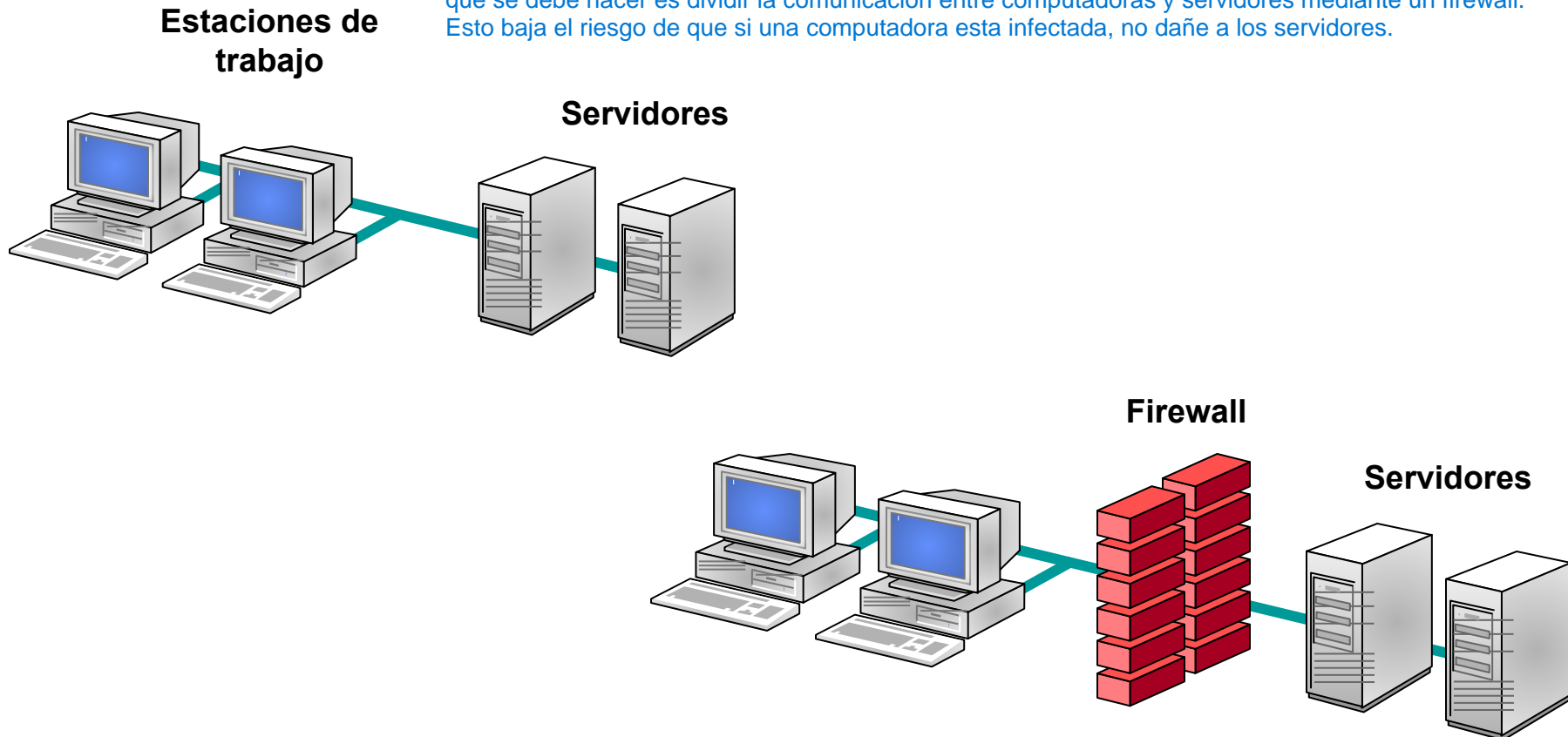
Seguridad en Redes LAN

- Los sistemas de seguridad apuntan a la capa 3 o superior
- Se confía en protocolos de capa 2
- Se debe tener acceso físico a la LAN
- La tendencia de ataques internos sube y la de externos baja.

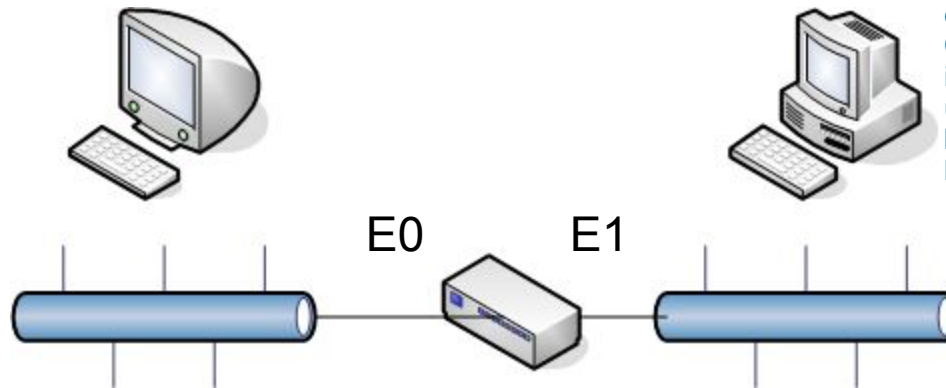
Seguridad en Redes LAN

- La conexión mas común on-premises es:
 - Los servidores y las estaciones de trabajo comparten la LAN

Esto puede suceder tanto on-premise como en la nube. En AWS hay que crear VPCs, subnets, etc. Lo que se debe hacer es dividir la comunicacion entre computadoras y servidores mediante un firewall. Esto baja el riesgo de que si una computadora esta infectada, no dañe a los servidores.



Recordemos Bridge



En las redes se suele usar el concepto de bridge, que es transparente en capa 2 y divide las redes en 2. Es indetectable porque un traceroute o cosas así no lo detectan. Cuando una computadora de la izquierda hace un ARP preguntando por una computadora de la derecha, el bridge le devuelve su MAC y no la del host de la derecha.

Ejemplo: en la red del ITBA, hay un firewall en modo bridge (que no lo vemos cuando salimos a internet). Traceroute no lo detecta porque no es a nivel IP (en capa 3), sino que es en capa 2.

NOTA: no es que se usan bridges en la actualidad, sino que se utilizan dispositivos (como routers/firewalls) en modo bridge

Interface	MAC
E0	33:44:55:00:00:01
E0	01:22:33:12:00:12
E1	33:44:55:00:00:21
E1	55:FF:33:00:00:10

Seguridad en Redes LAN

- Ataques comunes
 - ARP Poisoning/MAC Spoofing
 - IP Spoofing
 - DNS SPoofting
 - Ataque DHCP
- El objetivo final suele ser crear man in the middle

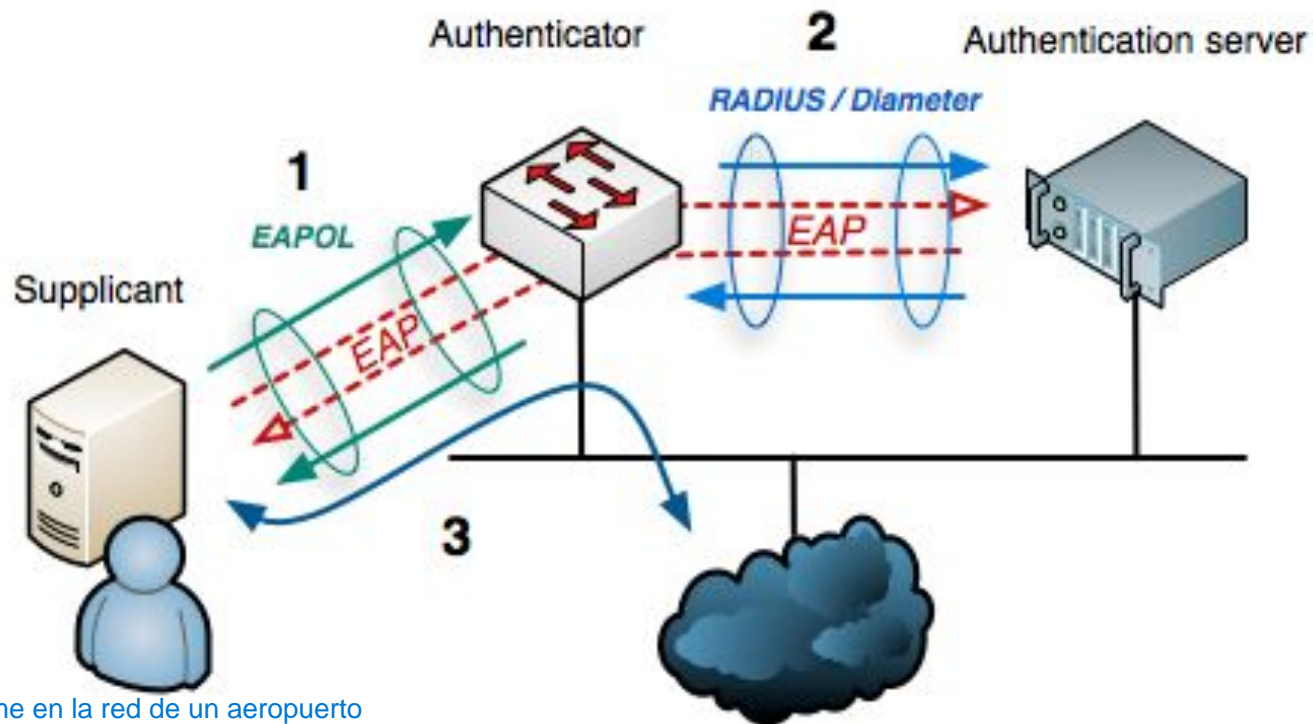
Seguridad en LAN - NAC

- NAC (Network Access Control)
- Permite el acceso físico a la red solo usuarios autenticados
- Se utiliza protocolo 802.1x y EAP El protocolo 802.1x es el estandar de la IEEE para que el switch y cualquier host puedan soportar NAC
- El switch y la estación de trabajo deben soportarlo

En ITBA, la wifi nos pide autenticarnos con nuestras credenciales. Esto se hace en muchas empresas, porque permiten autenticarnos para meternos en servidores de desarrollo/testing. No necesariamente las empresas dan wifi para conexion a internet.

NAC

■ NAC (Network Access Control)



Pasos para conectarme en la red de un aeropuerto

1) Me conecto a la wifi

2) Se empieza a ejecutar el protocolo EAP

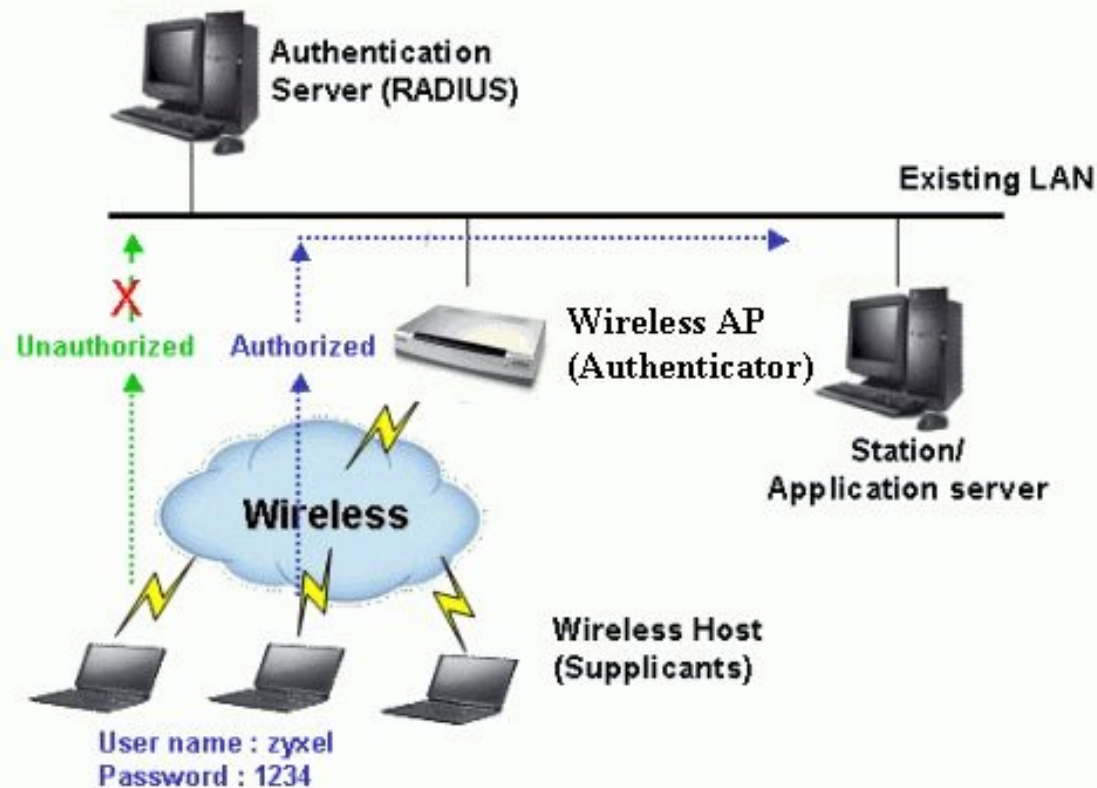
3) El access point (o switch) me da una IP en una VLAN que solo llega al servidor de autenticacion (que por ejemplo tiene hosteado en el puerto 80 una pagina web para que yo ingrese las credenciales). Algunos AP/switch ya vienen con un server para hacer esta autenticacion.

4) Le paso las credenciales al AP (o switch)

5) El switch me autentica y me pasa a otra VLAN que tiene conexion

NAC

- NAC (Network Access Control)
- BYOD (Bring your own device)



Seguridad en LAN

- Control de integridad de Estación de trabajo
- Host Integrity Check
- Se instala un software en la PC del cliente
- Puede ser un cliente permanente o disoluble
- Puede corroborar para la conexión:
 - Usuario Autenticado
 - Anti-virus actualizado
 - Firewall Activado
 - Actualizaciones de sistemas operativo
 - Aplicaciones instaladas
 - etc

BYOD es como NAC normal, pero antes de pasarme a la VLAN productiva, me obliga a bajar un software que puede hacer todos estos chequeos.

Tipos de Firewall

■ Software

- Netfilter/IPTables
- ISA Server/Forefront

■ Hardware

Un firewall era un equipo que te bloqueaba IP y puerto. Los equipos de ahora hacen muchas cosas mas, y se llaman UTM en vez de firewall.

- Solo Firewall
- Appliance de Seguridad (UTM)
 - Anti-Spam
 - Anti-virus
 - Content filter (puedo bloquear netflix en mi empresa)
 - IDS IDS e IPS: sistema de deteccion/prevencion de intrusos. Puede detectar/prevenir ataques como SQLi
 - IPS
 - VPN Para que la gente que trabaja remota se conecte a la LAN de la empresa

Firewalls de Hardware

- Sistema operativo dedicado (no multitarea) y propietario (cerrado)
- Sistema operativo versionado, con actualizaciones para resolución de bugs
- Marcas reconocidas
 - CISCO PIX/ASA
 - Juniper
 - Fortinet
 - Watchward
 - Sonicwall

Te venden "una caja" del tamaño de un servidor que trabaja en modo bridge y nos provee las funcionalidades de un UTM y un router. Son muy confiables y muy performantes (en vez de un SO tienen directamente un Firmware, que es un SO hecho por la empresa a medida). Son básicamente un CPU con RAM con un SO altamente optimizado.

Firewalls - CISCO



Firewall - Watchguard

(nombre de la empresa)

- Modelo Firebox X Peak E-Series
- Application proxy firewall, full-featured VPN (IPSec & SSL), IPS, URL filtering, spam blocking, anti-virus and anti-spyware
- 8 Interfaces



Firewalls - Comparación

- ¿Que parametros se utilizan para comparar un firewall ?

Parámetro	Valor Ejemplo
Firewall Throughput	300 Mbps
Máximas Conexiones	50.000
Sesiones por segundo	4000
VPN Throughput	40 Mbps
Máximas sesiones VPN	250
Puertos	5 NICs 10/100/1000 Mbps

Firewalls - Comparación

Funcionalidades
IDS
IPS
Filtros HTTP por contenidos
Anti-virus / Anti-spyware / Anti-Spam
Anti-phising
Bloqueo de archivos

Filtro de Contenidos (1)

Policy

URL List

Settings

Select Forbidden Categories

Tienen bases de datos en donde yo puedo
bloquear categorías de contenido

☐ Select all Categories

- | | |
|--|---|
| <input type="checkbox"/> 1. Violence/Hate/Racism | <input type="checkbox"/> 29. Search Engines and Portals |
| <input type="checkbox"/> 2. Intimate Apparel/Swimsuit | <input type="checkbox"/> 30. E-Mail |
| <input type="checkbox"/> 3. Nudism | <input type="checkbox"/> 31. Web Communications |
| <input type="checkbox"/> 4. Pornography | <input type="checkbox"/> 32. Job Search |
| <input type="checkbox"/> 5. Weapons | <input type="checkbox"/> 33. News and Media |
| <input type="checkbox"/> 6. Adult/Mature Content | <input type="checkbox"/> 34. Personals and Dating |
| <input type="checkbox"/> 7. Cult/Occult | <input type="checkbox"/> 35. Usenet News Groups |
| <input type="checkbox"/> 8. Drugs/Illegal Drugs | <input type="checkbox"/> 36. Reference |
| <input type="checkbox"/> 9. Illegal Skills/Questionable Skills | <input type="checkbox"/> 37. Religion |



If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click [here](#).

Filtro de Contenidos (2)

Policy

URL List

Settings

Select Forbidden Categories

☐ Select all Categories

19. Calendar Applications

☐ 20. Online Banking

☐ 21. Online Brokerage and Trading

☐ 22. Games

☐ 23. Government

☐ 24. Military

☐ 25. Political/Advocacy Groups

☐ 26. Health

☐ 27. Information Technology/Computers

☐ 28. Hacking/Proxy Avoidance Systems

10. Vehicles

☐ 47. Humor/Jokes

☐ 48. MP3/Streaming

☐ 49. Freeware/Software Downloads

☐ 50. Pay to Surf Sites

☐ 53. Kid Friendly

☐ 54. Advertisement

☐ 55. Web Hosting

☐ 56. Other

☐ 64. Not Rated

▲

▼

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click [here](#).

IDS/IPS (1)

#	Category ▼
	ACTIVEX
	APP-UPDATE
	BACKDOOR
	BACKUP-APPS
	BAD-FILES
	BUSINESS-APPS
	DATABASE-APPS
	DB-ATTACKS
	DNS
	DOS
	DOWNLOAD-APPS
	EMAIL-APPS
	EXPLOIT

FILE-TYPES-FTP
FILE-TYPES-HTTP
FORMAT-STRING
FTP
GAMING
ICMP
IM
IMAP
INFO
INFRASTRUCTURE
LDAP
MISC
MISC-APPS

IDS/IPS (2)

#	Name ▼	ID	Prevent	Detect	Priority	Direction
1	DabbleDB -- Data Access Attempt	320		✓	Low	Outgoing, to Server
2	DabbleDB -- Data Modification Attempt	321		✓	Low	Outgoing, to Server
3	DabbleDB -- Registration Attempt	319		✓	Low	Outgoing, to Server
4	DRDA -- Traffic	2301		✓	Low	Both, to Server
5	FileMaker Server -- Admin Console Connection Attempt	202		✓	Low	Incoming, to Server
6	FileMaker Server -- ODBC/JDBC Client Connection Attempt	203		✓	Low	Incoming, to Server
7	FileMaker Server -- TCP Client Connection Attempt	201		✓	Low	Incoming, to Server
8	GDS DB -- Connection Attempt	2319		✓	Low	Both, to Server
9	IBM DB2 -- Outbound Connection Handshake	197		✓	Low	Outgoing, to Server
10	IBM Informix -- Connection	283		✓	Low	Both, to Server
11	MS SQL Server -- Connection Attempt	206		✓	Low	Both, to Server
12	MS SQL Server -- Connection Attempt 2	839		✓	Low	Both, to Server
13	MS SQL Server -- sp_start_job Attempt 1	727		✓	Low	Incoming, to Server

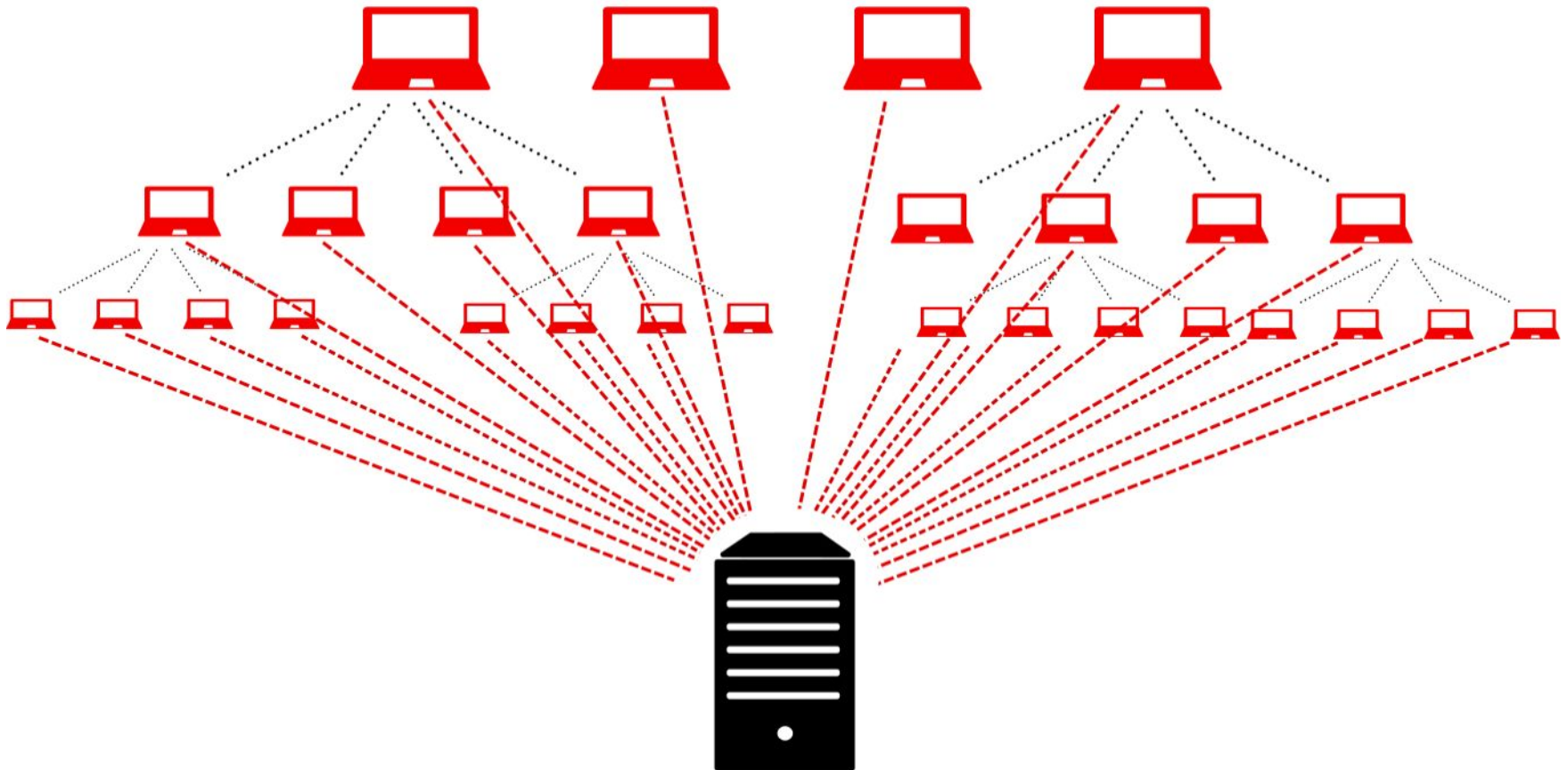


Demo

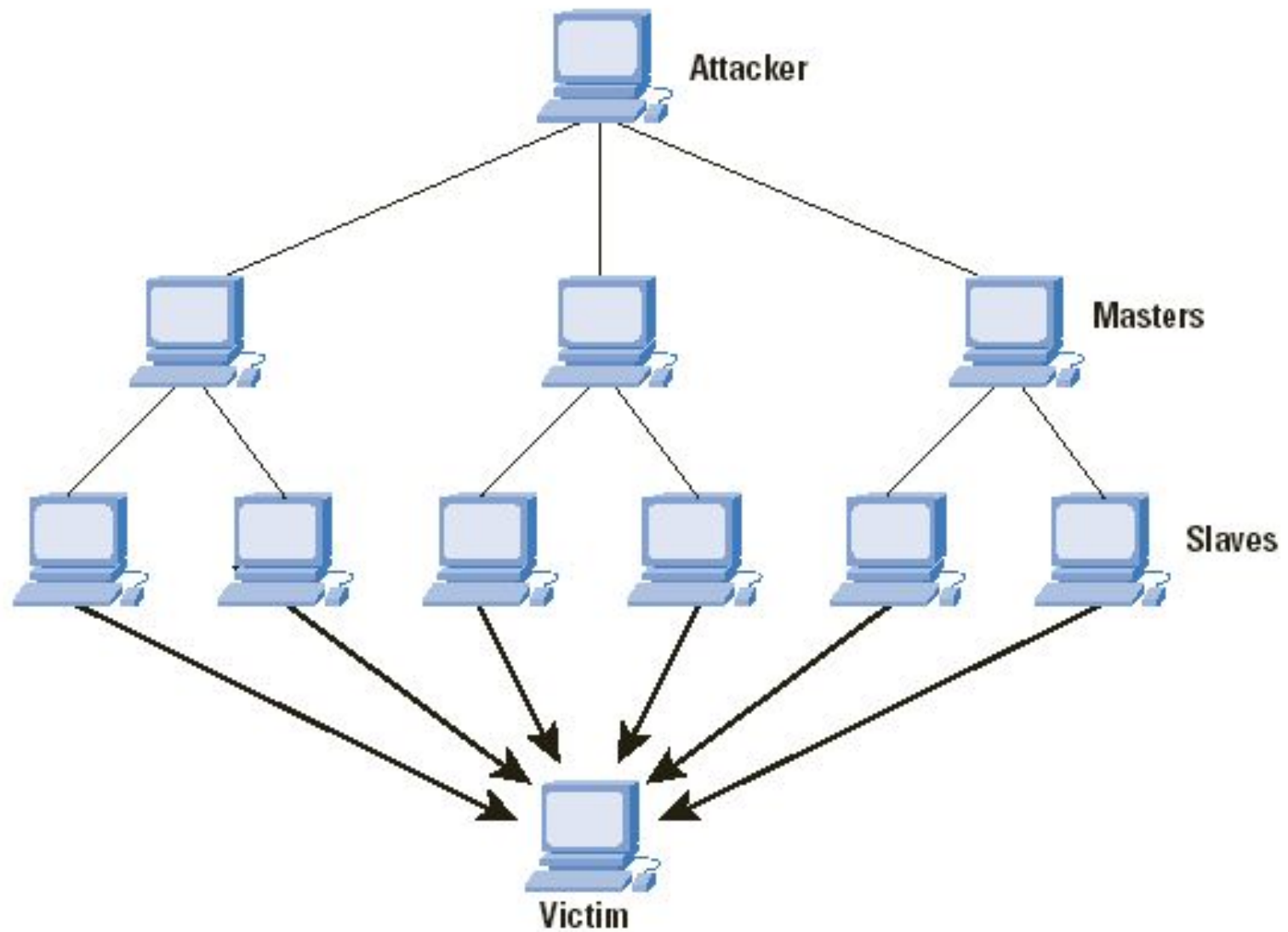
Veamos una demo de un UTM de marca SonicWall

<https://livedemo.sonicwall.com/>

DDoS



BotNet





Técnicas de DDoS

Por Volumen

UDP Flood, ICMP flood. El objetivo es saturar el ancho de banda de la víctima. Se mide en bps.

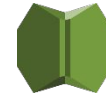
Por Protocolo

SYN Flood, paquetes fragmentados, ping de la muerte.
UDP Flood, ICMP flood. El objetivo es consumir recursos de los servidores, ó sistemas intermedios como firewalls o balanceadores de carga. Se mide en paquetes por segundo.

Por Aplicación

GET/POST Flood, ataque a Apache, Nginx, aplicación, etc.
El objetivo es saturar aplicaciones. Se mide en request por segundo.

Mitigación de DDoS



AWS Shield

Ejemplo AWS Shield

Capa Estándar

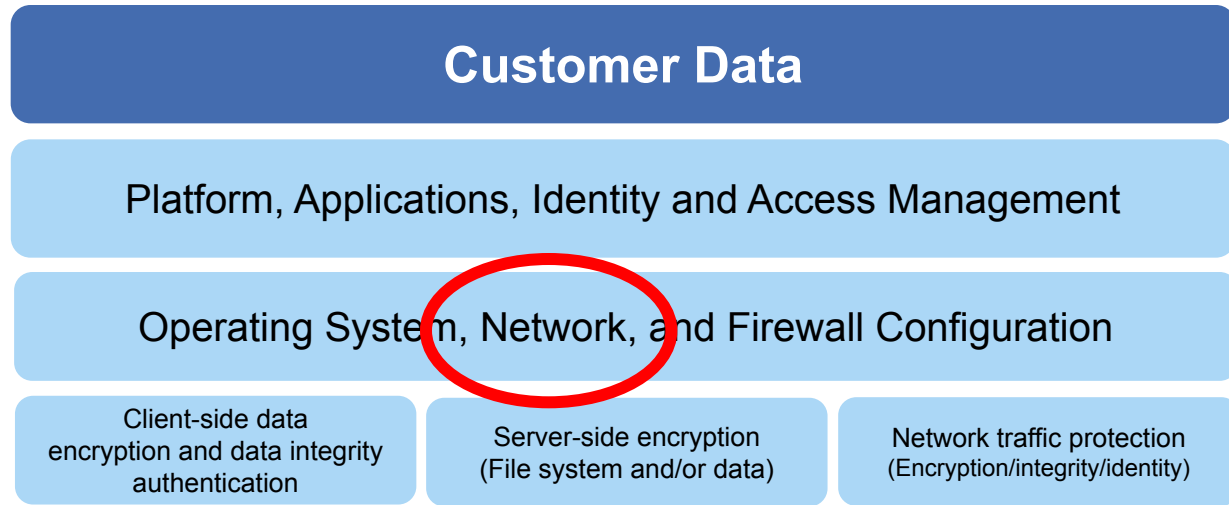
Para todos los clientes. Protege de ataques de DDoS comunes de capa 3 y 4. Ejemplo UDP Flood

Capa Advanced

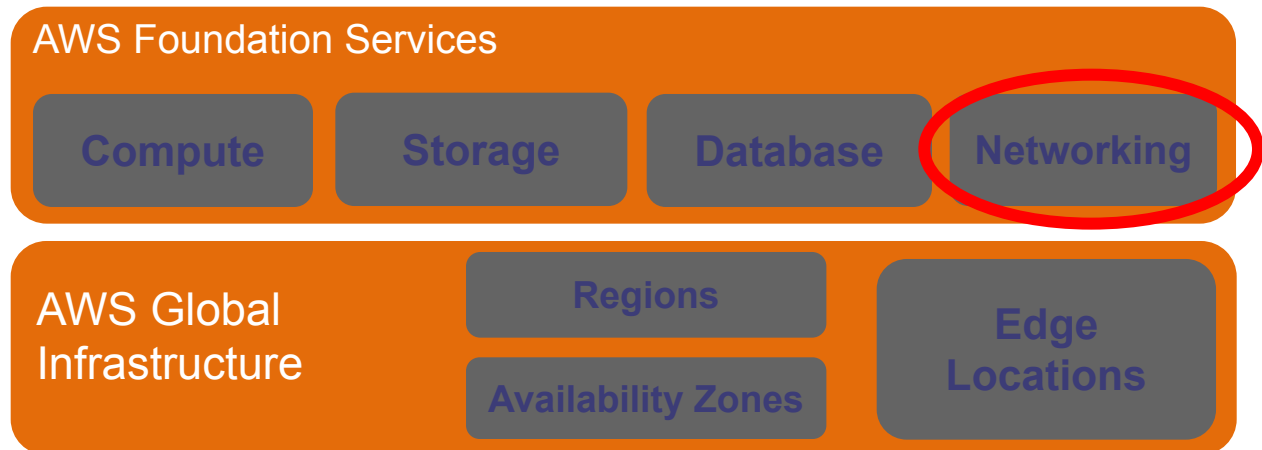
Protege servicios de AWS. EC2, CloudFront, Route 52, etc. Se integra con AWS WAF. Ej GET/POST Floods.

Ejemplo de Seguridad compartida en AWS

Customer Responsibility



AWS Responsibility



Seguridad en Centro de Cómputos

■ Control de acceso

- Tarjeta de acceso, clave, biométrico.
- Cámaras de seguridad con alertas.

■ Ambiente

- Piso técnico
- Aire acondicionado redundante
- Inhibidores de combustión con gas FM200
- Detector de partículas

■ Eléctrico

- UPS (Uninterruptible Power Supply)

