

Reloaded internet Safe Kit

« solution OpenSource de contrôle parental facile et accessible »



Plan

- **Partie 1** (10mn)
 - Tour d'horizon
 - Les solutions existantes
 - Les atouts de RISK



- **Partie 2** (30mn)

- Les fonctionnalités
- Installation



- **Partie 3** (10mn)

- Les améliorations à venir
- Les échéances

WHAT'S
NEXT ™

 Tour d'horizon 

Tours d'horizon

Quel est le public concerné ?

Fonctionnalités	Enfants (2-6)	Enfants (>6 ans)	Adultes (tout public)	Adultes (geeks)
Liste verte	✓			
Listes rouges contenu adultes		✓		
anti-pub		✓	✓	✓
anti-tracker		✓	✓	✓
anti-worm		✓	✓	✓
Recherche sécurisée		✓		
Navigation anonyme	✓	✓	✓	✓
Accès au darknet				✓

Contrôle parental (C.P)



WiFi Tours d'horizon

Comment ça marche (version hotspot wifi)?

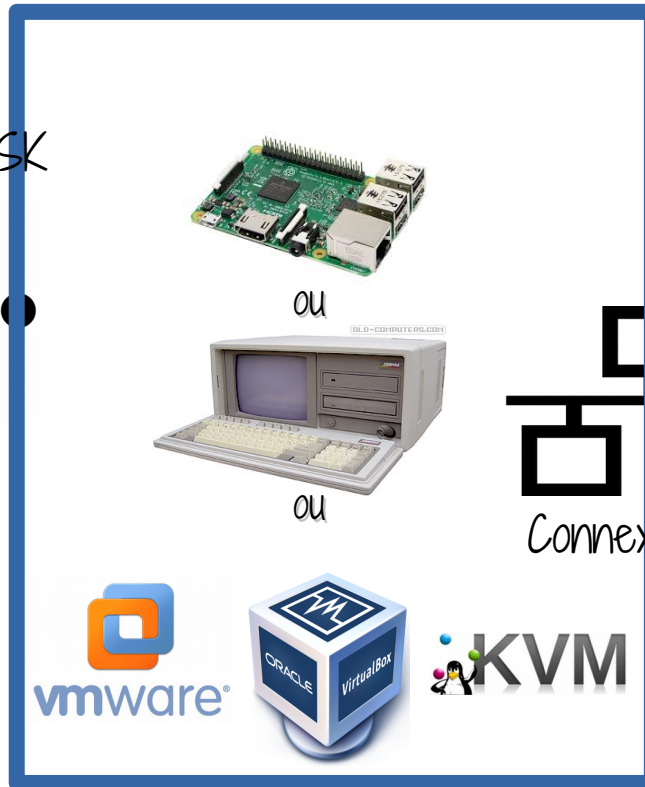


Appareils protégés

Hotspot RISK

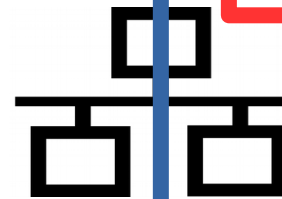


reloaded internet Safe kit



ou

ou



Connexion filaire

Appareils non protégés



Hotspot box



reloaded internet Safe kit

 Les solutions existantes
de C.P 

Les solutions existantes de C.P

1ere approche: les applications "clientes"

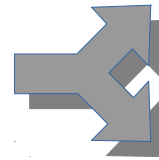
- Elles s'installent sur chaque appareil
- Avantages :
 - Simples à installer
- Inconvénients :
 - Nécessite de passer sur tous les appareils
 - Pas nécessairement compatibles avec tous les appareils
 - Boîtes noires (exfiltration de données possible)
- plugins de navigateurs ou applications complètes fonctionnant éventuellement avec les droits d'administrateur.



Les solutions existantes de C.P



2e approche: les proxy HTTP
comment ça marche ?



Interception des requêtes

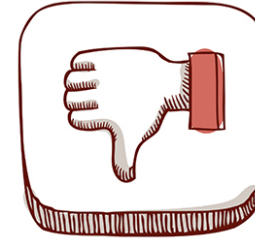
```
66.82.9.16 - [10/Aug/2004:01:12:27 +0000] "GET /images/main_nor.gif HTTP/1.1" 200 73797 "http://www.utilites.his.ru/feu
66.82.9.16 - [10/Aug/2004:01:13:56 +0000] "GET /images/main_nor.gif HTTP/1.1" 200 73797 "http://www.utilites.his.ru/feu
66.82.9.16 - [10/Aug/2004:01:14:19 +0000] "GET /images/main_nor.gif HTTP/1.1" 200 73797 "http://www.utilites.his.ru/feu
80.170.104.145 - [10/Aug/2004:01:18:13 +0000] "GET /download.htm HTTP/1.1" 200 7901 "http://celebsager.01net.com/windows
80.170.104.145 - [10/Aug/2004:01:18:15 +0000] "GET /windows.htm HTTP/1.1" 200 3466 "-" Mozilla/5.0 (Windows; U; Windows I
80.170.104.145 - [10/Aug/2004:01:18:15 +0000] "GET /images/search.gif HTTP/1.1" 200 874 "http://www.coolfilesearch.com
80.170.104.145 - [10/Aug/2004:01:18:16 +0000] "GET /images/search.gif HTTP/1.1" 200 874 "http://www.coolfilesearch.com
80.170.104.145 - [10/Aug/2004:01:18:16 +0000] "GET /index.html HTTP/1.1" 200 1193 "http://www.coolfilesearch.com/download
80.170.104.145 - [10/Aug/2004:01:18:18 +0000] "GET /images/main.gif HTTP/1.1" 200 873 "http://www.coolfilesearch.com/cu
61.238.163.75 - [10/Aug/2004:01:22:06 +0000] "HEAD / HTTP/1.1" 200 0 "-" InternetSec.com coolfilesearch.com text/html
11.20.121.21 - [10/Aug/2004:01:22:25 +0000] "GET /images/main.gif HTTP/1.1" 200 2378 "http://www.gnomies.com/menu
81.241.83.239 - [10/Aug/2004:01:19:06 +0000] "GET /download.htm HTTP/1.1" 200 7901 "http://celebsager.01net.com/windows/
81.241.83.239 - [10/Aug/2004:01:19:06 +0000] "GET /images/search.gif HTTP/1.1" 200 215 "http://www.coolfilesearch.com/
81.241.83.239 - [10/Aug/2004:01:19:06 +0000] "GET /images/search.gif HTTP/1.1" 200 215 "http://www.coolfilesearch.com/
81.241.83.239 - [10/Aug/2004:01:19:06 +0000] "GET /images/search.gif HTTP/1.1" 200 874 "http://www.coolfilesearch.com
81.241.83.239 - [10/Aug/2004:01:19:10 +0000] "GET /screen_shot.htm HTTP/1.1" 200 7918 "http://www.coolfilesearch.com/dam
81.241.83.239 - [10/Aug/2004:01:19:14 +0000] "GET /images/main_nor.gif HTTP/1.1" 200 3345 "http://www.coolfilesearch.com
81.241.83.239 - [10/Aug/2004:01:19:21 +0000] "GET /images/main_nor.gif HTTP/1.1" 200 73797 "http://www.coolfilesearch.com
```

Les solutions existantes de C.P



2e approche: les proxy HTTP

Avantages/inconvénients



- ✓ Le contenu exact des pages visitées est intercepté
- ✓ Sur des bandes passantes limitées améliore la navigation

- ✗ En cas de fortes sollicitations demande beaucoup de ressources (CPU)
- ✗ Fonctionne mal avec HTTPS

Les solutions existantes de C.P



3e approche : les DNS
C'est quoi un DNS?

- Il s'agit de l'annuaire IP de l'internet
- fait le lien site ↔ adresse IP.

Je veux me rendre sur google.fr

Mon navigateur demande au DNS quelle est l'IP de google.fr

Le DNS répond au navigateur → **216.58.209.227**

Le navigateur contacte google.fr sur l'IP **216.58.209.27** et me renvoi sa page web

Je suis connecté à google.fr

Les solutions existantes de C.P

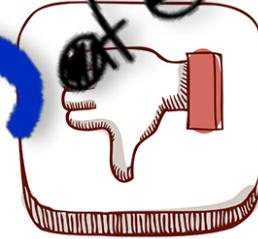


✓ Performant même en cas de fortes sollicitations

✓ Compatible avec HTTPS sans alerte de sécurité



3^e approche: les DNS
Avantages/inconvénients









✗ Seul le nom du site visité est répertorié

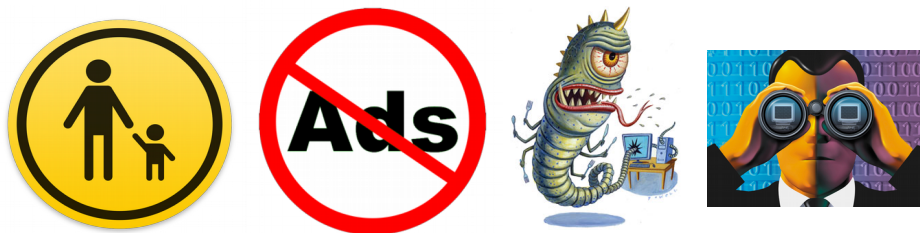
✗ Le contenu précis de la navigation n'est pas connu



Les atouts de RISK

- Gratuit et opensource 
- Interface web d'administration grand public 
- Plug'n play (liveCD, clé USB, carte SD) 
- Contrôle non intrusif (Pas de proxy) 
- Pas de configuration à faire sur les appareils 
- Navigation anonyme et Tor Box intégré 

Fonctionnalités



Fonctionnalités

Fonctionnement par listes rouges

- Par défaut tous les sites sont accessibles et seuls les sites en listes rouges ne sont pas accessibles.
- Les listes adultes, pubs, trackers sont pré-chargées avec plus de 1 million de sites issues de <https://dsi.ut-capitole.fr/blacklists/> (licence CC)
- Elles sont personnalisables
- Elles sont désactivables
- Son efficacité dépend de la richesse des listes et de leur actualisation

Reloaded Internet Safe Kit

Liste rouge

Activé / Désactivé

Liste rouge Liste verte

porn

Sites	bloquage du site	bloquage des sous-sites
0-0-7-hardcoresex.dk	Bloqué	Bloqués
0-fightingshaving.da.ru	Bloqué	Bloqués
0-bondage.dk	Bloqué	Bloqués
0-foodwarez.da.ru	Bloqué	Bloqués
0-...	Bloqué	Bloqués
0-...	Bloqué	Bloqués
0-...	Bloqué	Bloqués
0-sex.dk	Bloqué	Bloqués
0-ass-cinema-newsp.da.ru	Bloqué	Bloqués

475691 résultats trouvés.

Demo time



WiFi Fonctionnalités

Fonctionnement par liste verte

- Par défaut l'accès à tous les sites est interdit et seuls les sites de la liste verte sont accessibles à la navigation.
- Il s'agit du mode qui convient le mieux pour les plus jeunes enfants.

✓ 100 % fiable

✗ Plus difficile à maintenir que l'approche par listes rouges



Sites en liste verte	
passageenseine.fr	Autorisé
google.com	Autorisé
...	Autorisé
...	Autorisé
...	Autorisé



- Permet de connaître les sites consultés ainsi que les horaires de consultation.
- Aperçu rapide des sites bloqués
- Permet d'autoriser ou bloquer un site (ou ses sous-sites) directement depuis le tableau.

📶 Fonctionnalités

Connaître l'historique de navigation

The screenshot displays the 'Liste rouge' (Red List) interface. At the top, there is a navigation menu with options like 'Suivi des connexions', 'Gestion des listes', 'Recherche sécurisée', 'Paramètres wifi', and 'Autres paramètres'. The main area shows a table of connections with columns for time, status (red or green dot), and domain name. A large 3D 'Demo time' watermark is overlaid on the table.

Time	Status	Domain
14:22:07	Red	tmgr.cmbg.com
14:22:07	Green	dpm.lefigaro.fr
14:22:06	Green	p.crm4d.com
14:22:06	Red	idsync.rlcdn.com
14:22:06	Green	...
14:22:05	Red	t4.liverail.com
14:22:04	Red	rtb-csync.smartadserver.com
14:22:04	Red	js.revsci.net
14:22:03	Red	ad.360yield.com
14:22:03	Red	pixel.rubiconproject.com
14:22:03	Red	cm.g.doubleclick.net
14:22:03	Red	ib.adnxs.com
14:22:03	Green	usermatch.krx.net
14:22:02	Green	dpm.zebestof.com
14:22:02	Green	cdn.zebestof.com
14:22:02	Red	staticxx.facebook.com



WiFi Fonctionnalités

Safe search (Recherche sécurisée)

- Force le filtrage des contenus pour adultes dans les moteurs de recherche
- Disponible pour google, youtube et bing





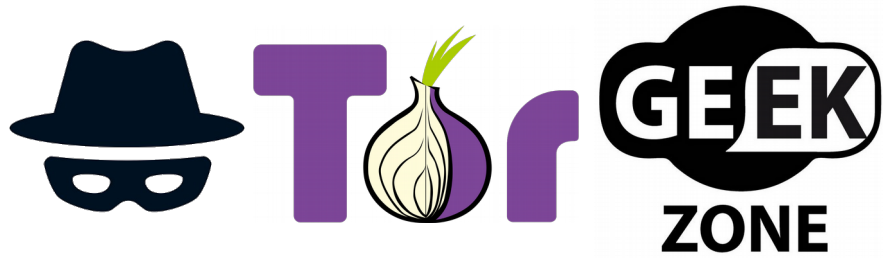
WiFi Fonctionnalités

Navigation anonyme

- Votre adresse IP est masquée
- Des limitations à connaître:
 - ne vous affranchit pas d'activer le mode navigation anonyme du navigateur (fuite des métadonnées du navigateur et des cookies)
 - Faille webRTC
 - Lenteur liée au re-routage des paquets réseau dans le réseau ONION

The screenshot displays the Reloaded Internet Safe Kit interface. At the top, there is a navigation menu with options like 'Liste rouge', 'Suivi des connexions', 'Gestion des listes', 'Recherche sécurisée', 'Paramètres wifi', and 'Autres paramètres'. The main area shows a table of connection logs for the date '25-Jun-2017'. The table has columns for time, status (red or green dot), and domain name. A large 3D watermark 'Démotime' is overlaid on the screenshot.

Time	Status	Domain
14:22:07	Red	tmgr.ccmbg.com
14:22:07	Green	dpm.lefigaro.fr
14:22:06	Green	p.crm4d.com
14:22:04	Green	ads.yahoo.com
14:22:04	Red	t4.liverail.com



📶 Fonctionnalités

Accès au darknet - TOR box

- Il s'agit du mode navigation anonyme précédent
- Les sites en .onion sont désormais accessibles
- Utiles pour les geeks (mais pas que... 😞)

Reloaded Internet Safe Kit

📶 Activé
🔒 Activé(+TOR)

⚙️ Liste rouge ▾

👁️ Suivi des connexions
☰ Gestion des listes
🔍 Recherche sécurisée
📶 Paramètres wifi
⚙️ Autres paramètres

☑️ Connexions par liste rouge ☑️ Connexions par liste verte

25-Jun-2017 🔄

Liste des dernières connexions 📄

14:22:07	🔴	tmgr.ccmbg.com
14:22:07	🟢	dpm.lefigo.fr
14:22:04	🟢	sync.ligadx.com
14:22:04	🟢	ads.yahoo.com
14:22:04	🔴	t4.liverail.com

🔍 Recherche

Démo time

Les topologies d'installation



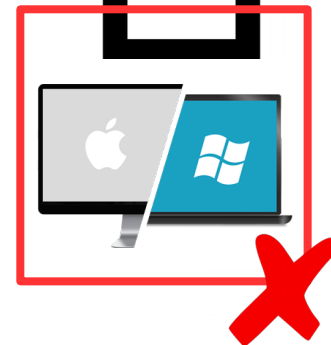
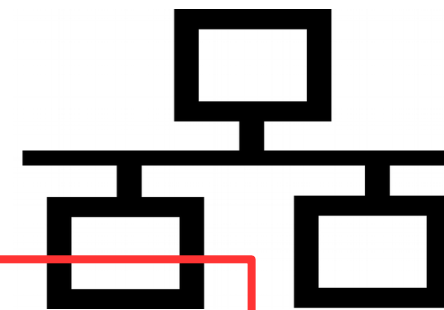
Les topologies d'installation

en hotspot WiFi uniquement

- Il s'agit de l'intention première de RISK
- RISK est connecté à une Box ou un routeur en filaire
- Il crée un hotspot wifi sécurisé
- Les appareils qui se connectent à ce hotspot sont automatiquement sécurisés via RISK sans configuration.
- Le principal inconvénient est que les appareils filaires et ceux connectés au wifi de la Box ne bénéficient pas de la sécurisation de RISK



Reloaded Internet Safe Kit



Hotspot Box



Reloaded Internet Safe Kit



Les topologies d'installation

Le serveur DNS uniquement

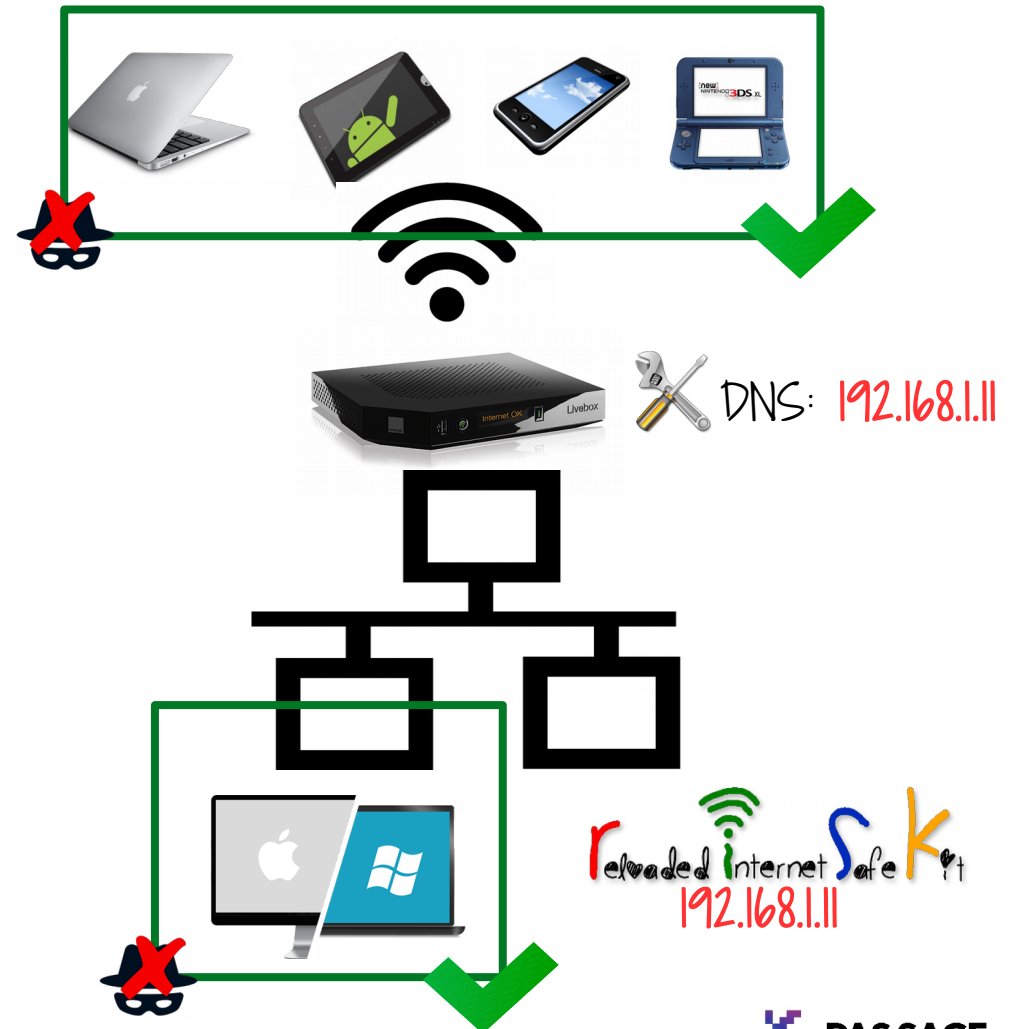
- Risk est relié à la Box en filaire
- Le serveur DNS de la box est configuré sur l'IP de Risk

✓ Appareils filaires et wifi connectés à la box sont protégés par Risk

✗ Navigation anonyme non disponible

✗ Pas toutes les box permettent de configurer leur DNS

✗ Le DNS peut-être re-paramétré sur chaque appareil pour court-circuiter Risk (admin requis)



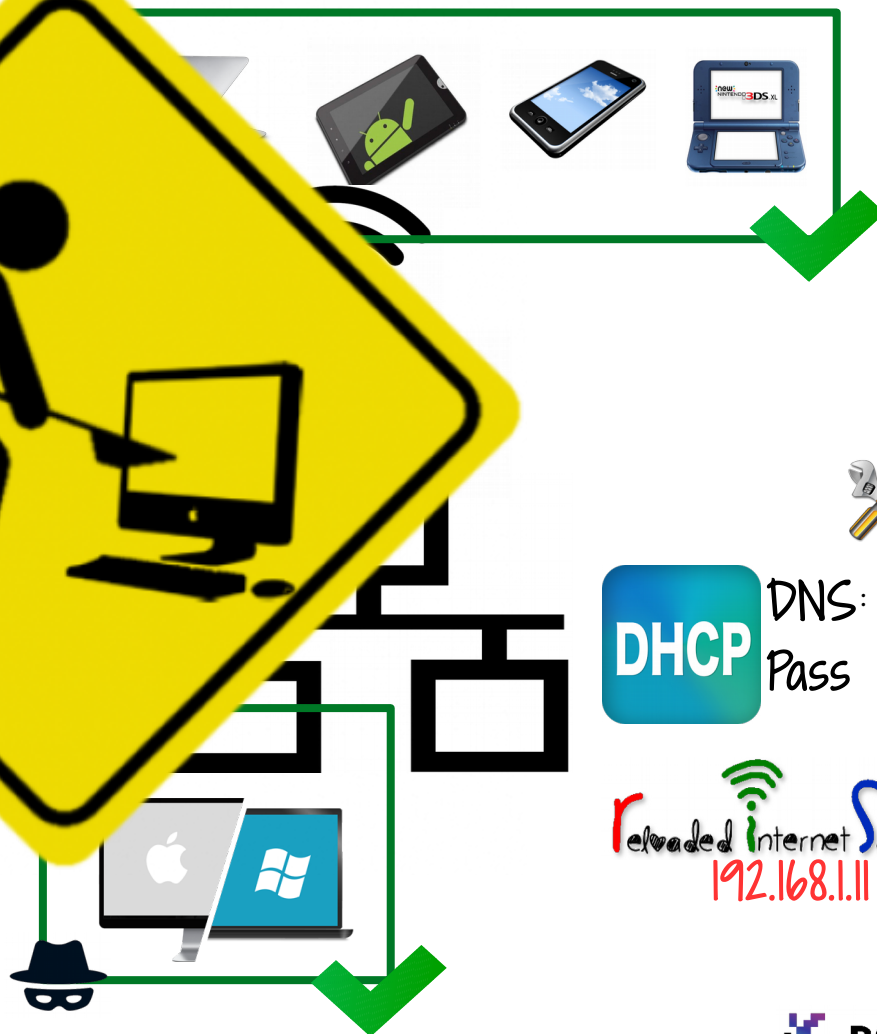


Les topologies d'installation

Un serveur DHCP: un bon compromis

- RISK est relié à la Box en filaire
- Le serveur DHCP de RISK est paramétré pour envoyer aux appareils connectés la même configuration déclarant l'ordinateur comme passerelle réseau

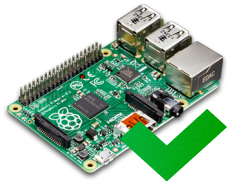
- ✓ Appareils filaires et wifi de la box sont protégés par RISK
- ✓ Navigation anonyme possible pour les appareils filaires et wifi
- ✗ Le DNS peut-être re-paramétré sur chaque appareil pour court-circuiter RISK (admin requis)



DNS: 192.168.1.11
 Pass : 192.168.1.11

Reloaded Internet Safe Kit
 192.168.1.11

 Autres considérations 
sur l'installation

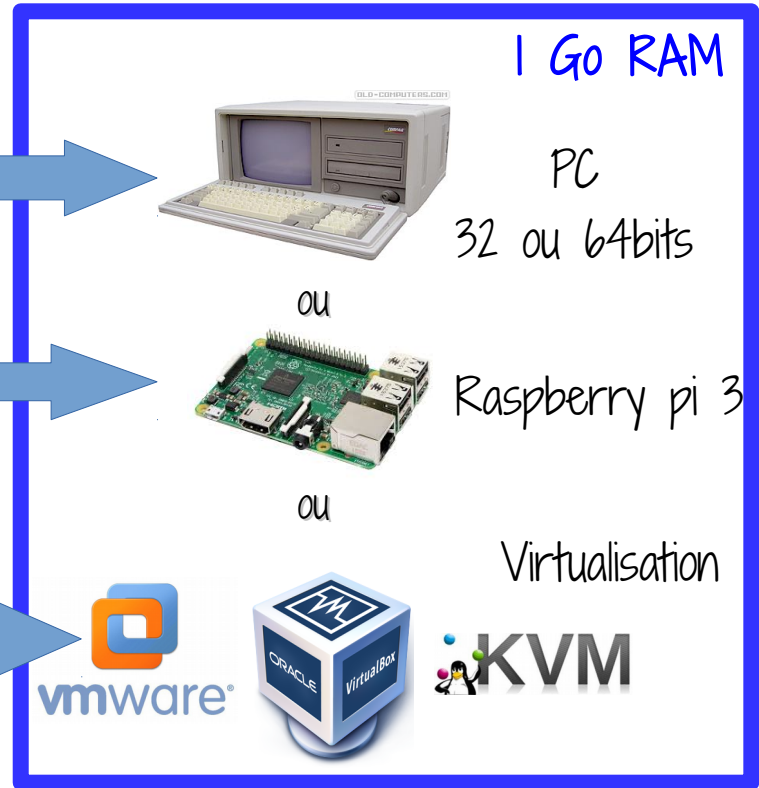


Autres considérations sur l'installation



Matériel et supports d'installation

reloaded internet safe kit



reloaded internet safe kit



Autres considérations sur l'installation

Live



Live
persistant



Modalités d'exécution

- ✓ Plug'n play
- ✓ Intéressant pour tester la compatibilité matérielle
- ✓ Intéressant pour un usage nomade

- ✗ Les modifications ne sont pas sauvegardées
- ✗ Lenteur dans le chargement des listes (sauf...)



Persistant



- ✓ Plug'n play
- ✓ Les modifications sont sauvegardées
- ✓ Intéressant pour un usage nomade

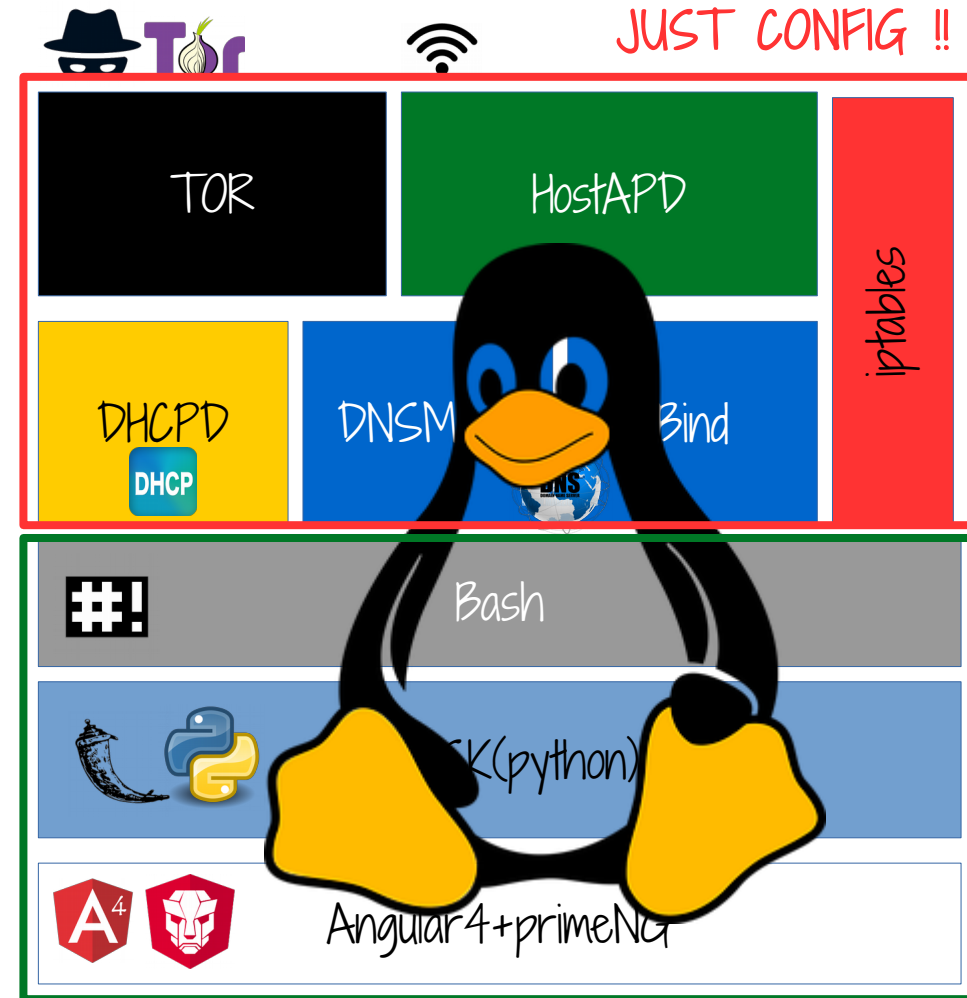
- ✗ Lenteur dans le chargement des listes

- ✓ Les modifications sont sauvegardées
- ✓ Rapidité optimale d'exécution

- ✗ Nécessite d'y dédier un appareil

Composants techniques de RISK

- **Hostapd** :Création du hotspot WIFI
- **DNSMasq** : gestion des listes vertes
- **Bind** : Gestion des listes rouges
- **DHCPD** :Distribution des configurations réseaux sur le LAN
- **Iptables** : Routage des paquets
- **Tor** : Navigation anonyme et accès au darknet
- **Bash**: contrôle des services
- **Flask**(python) : exposition de l'API d'admin web (Rest)
- **Angular4+PrimeNG** :interface web d'administration




Composants RISK
(seules nouveautés!)

📶 Passé, présent, futur 📶

Passé, présent, futur

Génèse et historique de RISK

- 
- L'idée est née d'un besoin exprimé par le maître d'école (Florian) de mon fils de mettre en place un contrôle parental par liste verte sans avoir à configurer chaque machine de la classe.
 - Quelques mois plus tard, il y a 1 an environ, j'ai réalisé un premier prototype sur raspberry pi 3 (sans interface WEB) qui continue de fonctionner avec environ 4 appareils connectés en permanence.
 - Les développements sur l'interface WEB datent de 2 mois
 - La version 0.9 de RISK à Passage en Seine 2017!

Aujourd'hui

Passé, présent, futur

Feuille de route Version 1.0

- La sortie officielle de RISK (1.0) est programmée pour octobre 2017
- A sa sortie, l'entièreté du code source sera disponible en téléchargement sous licence GPL V2
- D'ici là, de nombreux chantiers doivent être finalisés :
 - Documentation de RISK (utilisateurs et développeurs)
 - Retravailler le vocabulaire pour le rendre moins technique
 - Sécurisation des entrées dans le code
 - Sécurisation de l'interface d'administration
 - Travailler sur la topologie d'installation utilisant un serveur DHCP dans RISK
 - Paramétrage de plages horaires pour l'usage du wifi RISK
 - Retravailler l'ergonomie pour la rendre plus intuitive
 - Optimiser les performances de RISK et réduire son empreinte mémoire

C'est fini,
vous pouvez vous réveiller !

