SATELLITE

Wifi sur Cristor Atlas E

Nous savons que cet appareil est dépourvu d'un port USB, et c'est vraiment dommage que l'on ne puisse pas utiliser un réseau Wifi sur ce récepteur. Pour cette raison, le constructeur a mis, il y a peu de temps (voir nos précédentes éditions) un dispositif pour réparer cette «injustice». Ce dispositif fonctionne aussi bien sur cet appareil que sur un autre tel Dreambox 500s…

Pour utiliser ce dispositif et pouvoir l'installer, il est impératif de disposer d'un PC pour pouvoir activer votre code Wifi (sécurité de votre réseau). Si votre réseau n'est pas sécurisé vous pouvez l'utiliser directement. Le Cristor ne disposant pas de port USB, la deuxième difficulté consiste à avoir une alimentation électrique externe (12 V). Ce dispositif est constitué d'un boîtier avec un câble USB, un autre câble RJ45 (réseau) et pourvu d'une entrée pour alimentation électrique 12 V. il est fournit avec un CD d'installation.

Sur PC

Branchez le dispositif sur les ports RJ45 et USB de votre PC (d'autres préconisent de brancher la fiche RJ45 sur le modem, mais dans nos essais nous avons réussi à la faire fonctionner en la branchant à la carte réseau du PC).

Insérez le CD et suivez la procédure d'installation. Le logiciel vous demande de choisir votre réseau et d'insérer le code de sécurité. A la fin de la procédure, un message vous informe que votre dispositif est fonctionnel («Successfully associated to wireless network») et votre boîtier s'allume en bleu, signe que votre connexion est réalisée avec succès.

Sur le récepteur

Après avoir débranché le dispositif du PC, branchez-le au récepteur. Au port RJ45 et à l'aide de l'alimentation 12 V externe.

Allez au menu vous verrez que votre récepteur est connecté à Internet et que vos serveurs sont activés. Il ne vous reste plus que de vous installer confortablement et de zapper sur vos programmes préférés.

Nacer Aouadi

TNT sans internet et Sharing sur Forever

Cet article est destiné :

1- Aux personnes qui veulent faire fonctionner la TNTSAT, Canal digitaal, TV Vlaanderen, ORF Digital, ENTV et autres chaînes BISS... sans internet gratuitement.

2- Aux personnes qui veulent faire marcher leur abonnement CCcam ou Newcam sur le Forever (ou autres démos Fortis comme Kiowa ou Octagon) et profiter en même temps des chaînes décryptées sans internet par un softcam.key comme la TNTSAT, les chaînes BISS (ENTV...), ORF digital, Canal digitaal...et ceci sans coupures à l'inverse de Mcas.

Avantages de la méthode :

1- Si on a une coupure de la connexion internet, on n'a pas à changer de chaîne pour que l'image revienne avec Xcam (à l'inverse d'Oscam, CCcam).

2- Xcam est le plus rapide en zapping puisqu'il crée un fichier prio pour décrypter chaque chaîne ouverte le plus rapidement possible sans se fatiguer à créer un fichier CCcam.prio).

3- Xcam ne souffre pas du problème de freeze récurrents que connaît Mgcamd. Mgcamd peut fonctionner sans problème 10, 20 minutes, voire des heures mais s'il y a un problème de connexion/serveur, il y aura des freezes interminables chaque 20/50 secondes (Cherchez sur Google «mgcamd warning both cws changed»).

4- Les chaînes ouvertes par l'ému (TNT, BISS...) ne dépendent pas d'internet/sharing et sont ouvertes instantanément.

Maintenant si vous êtes convaincus, il vous faut deux plugins (à télécharger) : Xcam (Sharing) et Oscam (Utilisé comme simple emu dans notre cas):

1. Installez les plugins comme vous avez l'habitude de le faire (soit en copiant le dossier plugin dans une clé USB ou en copiant manuellement les fichiers par FTP/Partage de fichiers Windows).

2. Désactivez, voire supprimez les autres plugins (Mcas, coconut, Exsim, mgcam...) qui peuvent interférer avec le fonctionnement correct d'Xcam+Oscam (vous n'aurez plus besoin de Mcas+Coconut si vous utilisez Oscam lmod).

3. Changez le mode de démarrage des deux plugins (XcamClient et OScam-lmodv8) en auto ou bien d'Oscam seul si vous ne faites pas du sharing.

4. Si vous faites du sharing, démarrez le plugin XcamConfigure pour ajouter votre abonnement CCcam (Choisissez ccam2) ou Newcam. Vous pouvez aussi éditer directement le fichier "cardclient.conf" qui se trouve dans /var/etc pour faire ça (mais pensez à supprimer /var/etc/protect/cardclient.conf s'il existe). La syntaxe est simple :

cccam2:monserveur:port:0/0/0:username:password

newcamd:monserveur:port:0/0000/0000:username:password:01020304050607080910111213 14

5. Démarrez XcamClient et OScam-lmodv8 (Ou OScam-lmodv8 seul si vous ne faites pas du sharing).

6. C'est tout. Si vous voulez mettre à jour les clés, lancez le plugin Oscam-Key-Update et attendez qu'il télécharge le nouveau softcam.key (Ou bien vous pouvez éditez le fichier /var/keys/oscam.keys manuellement).

Remarque :

• Lorsque vous lancez Oscam Key-update, rien ne s'affichera à l'écran mais la mise à jour des clés s'effectue normalement (s'il n'y a pas de problème de connexion internet). Il vous faudra attendre une trentaine de secondes après avoir lancé le plugin «Oscam Key-update» pour redémarrer le plugin Oscam lmod et prendre en compte le changement des clés.

Source : DZSAT Forum

NEWS

REPORTERS SANS FRONTIÈRES

Liste des pays et entreprises «ennemis d'internet» en 2012

Reporters sans frontières (RSF) a rendu public, mardi 12 mars, son dernier rapport sur les "ennemis d'internet", dédié à la surveillance des internautes.

Contrairement aux années précédentes, l'organisation n'a pas édité de liste générale des pays «ennemis» du réseau ni de liste des Etats «sous surveillance» pour leurs mesures allant à l'encontre de la liberté sur internet.

La surveillance s'intensifie

Pour Reporters sans frontières, les pays ayant appliqué le contrôle le plus strict des réseaux en 2012 sont le Bahreïn, la Chine, l'Iran, la Syrie et le Viêtnam. Pour chaque pays, le rapport détaille les moyens de répression utilisés, notamment les logiciels espion, le vol de comptes sur les services internet ou la surveillance ciblée et le piratage de connexions.

Ces derniers mois, la Chine et l'Iran ont notamment attaqué les moyens de contournement de la censure. La première cible est les réseaux privés virtuels (VPN), qui permettent d'accéder à des sites bloqués par une connexion chiffrée, donc difficilement identifiable.

Guerre contre les VPN

«La Chine et l'Iran ont été très actifs en matière de sophistication et de maîtrise de l'outil, mais il y a aussi la Syrie», qui a d'ailleurs coupé l'accès à internet à ses habitants en novembre, ajoute Mme Morillon. «La lutte contre les VPN demande des moyens techniques et humains importants. Si ces trois pays sont arrivés à un tel niveau de sophistication et de volonté, il n'y a pas de raisons que ces compétences ne soient pas transférées à d'autres pays autoritaires», anticipe la responsable.

La France, elle, reste sous surveillance de RSF, notamment sur les questions de filtrage administratif ou sur la coupure de connexion internet par Hadopi. L'organisation de défense des libertés indique rester vigilante, notamment sur les résultats de la mission Lescure, qui donnera la direction à suivre pour l'avenir de la Hadopi et du contrôle des contenus «illicites» sur internet.

Des entreprises européennes

Cette liste de pays autoritaires s'accompagne, pour la première fois, de celles des entreprises leur fournissant les moyens de surveillance. Pour RSF, les sociétés américaines et européennes Amesys, Blue Coat, Gamma, Hacking Team et Trovicor sont les principaux alliés techniques de ces régimes, repérés dans les dispositifs de plusieurs pays «ennemis d'internet». Ces technologies, souvent présentées comme neutres, seraient ainsi utilisées contre les opposants.

La société française Amesys, filiale de Bull, est d'ailleurs sous le coup d'une enquête en France, étant accusée de complicité de torture en Libye par la Ligue des droits de l'homme (LDH) et la Fédération internationale des droits de l'homme (FIDH). La société française aurait fourni ses technologies de surveillance au régime de Mouammar Kadhafi, lui permettant d'identifier et d'arrêter des opposants, torturés par la suite.

Contrôler les exportations

Le contrôle de ces technologies de surveillance est d'ailleurs un sujet politique montant. «Des pays défendent publiquement la liberté d'expression et des dissidents, mais accueillent des entreprises qui fournissent des technologies de surveillance, explique Mme Morillon. «Depuis deux ou trois ans, il y a tout de même des exemples de dégâts concrets publiés, notamment dans les pays qui ont connu le printemps arabe. Désormais, on sent des initiatives politiques [pour limiter ces technologies et leur commercialisation], mais il faut que les mesures soient contraignantes, et non simplement des déclarations», argumente l'organisation.

En Allemagne, RSF indique que le parti vert a déposé un projet de loi pour contrôler l'exportation de ces technologies. Outre-Atlantique, «les Etats-Unis ont interdit l'export de ces matériels vers la Syrie et l'Iran... Mais il y a d'autres pays ! C'est pour ça que le Global Online Freedom Act [une proposition de loi destinée à empêcher aux entreprises américaines de collaborer avec les pays autoritaires] doit être adopté rapidement», déclare l'organisation.

Fin novembre, RSF a lancé We Fight Censorship, un site proposant notamment un «kit de survie», des outils et méthodes pour se protéger de la surveillance et de la censure numérique.

Source : *Le Monde*

Publicité

الجمهورية الجزائرية الديمقراطية الشعبية

DIRECTION DES TRAVAUX PUBLICS DE LA WILAYA DE SETIF - ADRESSE : CITE ADMINISTRATIVE AIN T'BINET WILAYA DE SETIF

NIF : 40.80.150.000.19.003

AVIS D'ATTRIBUTION PROVISOIRE DE L'APPEL D'OFFRES NATIONAL RESTREINT N° 036.62.10.69/036.62.12.82

Conformément aux dispositions de l'article 49 alinéa 02 du décret présidentiel n° 10/236 du 07/10/2010 modifié et complété portant réglementation des marchés publics, la Direction des travaux publics de la wilaya de Sétif informe l'ensemble des soumissionnaires ayant participé à l'appel d'offres national restreint n° ..../2013, que le projet indiqué ci-dessous est provisoirement attribué comme suit :

OBJET	ENTREPRISE	MONTANT EN TTC (DA)	DELAI DE REALISATION	NOTE TECHNIQUE	OBSERVATION
Réparation des glissements sur CW45 PK 08+000 - PK 11+200 Lot route	GARICI ZERROUG	21.428.117,10	06 Mois	82.33	Qualifiée techniquement moins-disante

Conformément à l'article 114 du décret présidentiel sus-cité, les soumissionnaires qui contestent ce choix peuvent introduire un recours auprès de la Commission des marchés de la wilaya de Sétif dans un délai de 10 jours à compter de la première date de publication du présent avis dans les quotidiens nationaux.

NIF de l'entreprise GARICI ZERROUG 16819410005251

Les soumissionnaires intéressés par les résultats de l'évaluation des offres peuvent se rapprocher de la Direction des travaux publics service de l'entretien et de l'exploitation dans les trois (03) jours qui suivent la première parution de cet avis dans les quotidiens nationaux, pour prendre connaissance des résultats détaillés de l'évaluation technique et financière des offres.

Anep N° 512 366 - Le Soir d'Algérie du 16/03/2013