swisscom

Frequently Asked Questions
Projet «Internet à l'école»

FAQ

Cette FAQ est destinée aux responsables cantonaux et, sous forme d'extraits, aux écoles qui utilisent URL Filtering SecurePoP® WCS dans le cadre de l'initiative de Swisscom «Internet à l'école». Veuillez vous adresser à votre service de coordination cantonal pour savoir si ce service est disponible dans votre école.

Problèmes généraux

Si mon école passe d'un réseau de formation à un autre réseau (du réseau d'école primaire à Open Net): L'adresse IP publique existante peut-elle toujours être utilisée?
Non. En cas de migration vers un autre réseau, l'adresse IP change toujours.
Le passage à Open Net ne nécessite aucun formulaire de demande séparé.

L'infrastructure du bâtiment peut-elle être raccordée via SAI?
Le sponsoring «Internet à l'école» raccorde les écoles à Internet à des fins didactiques.
Comme aucun SLA (bande passante, disponibilité) ne peut être garanti avec les écoles, le raccordement de l'infrastructure du bâtiment (p. ex. installations de détection d'incendie) via la connexion Internet des écoles n'est pas possible.

Serveur FTP
Dans de rares cas, il a été constaté que d'anciens serveurs FTP ne respectent pas l'intégralité des formats définis selon RFC 959. Comme le SecurePoP® de Swisscom vérifie le protocole, il arrive dans de tels cas que les données ne soient pas transmises. Une mise à niveau du serveur du client à la version actuelle permet de régler le problème.

Problèmes de performance

La connexion à Internet est-elle disponible?
Exécutez un «ping 164.128.36.36» à partir de l'invite PC DOS.
Si vous ne recevez pas de réponse, il ne s'agit pas d'un problème de débit et la connexion à Internet est défaillante.

Y a-t-il un problème explicite sur d'autres ordinateurs dans a) la même école b) d'autres écoles?
Si non, il s'agit d'un problème sur cet hôte/ordinateur. Dans le cas a), l'origine du problème est liée au réseau local dans l'école ou, le cas échéant, au routeur LAN-I de l'école. Dans le cas b), il s'agit d'un problème central qui doit être signalé au helpdesk de Swisscom via le service cantonal de coordination (KKS).

Y a-t-il un problème avec certains sites/hôtes et/ou services Internet?
Quel site/hôte avez-vous activé avec quel service (http, https...)? Y a-t-il un message d'erreur?
Afin d'exclure un problème avec un site particulier, veuillez en visiter plusieurs, p. ex. www.swisscom.com, www.cisco.com, afin d'en évaluer l'accessibilité et la vitesse.

S'agit-il d'un problème de messagerie/SMTP?
Selon qu'il s'agit du réseau de niveau 1 ou 2, la procédure est différente et doit être définie avec le service cantonal de coordination (KKS). Rendez-vous sur http://www.anti-abuse.org et entrez l'adresse IP publique de SecurePoP Firewall ou évent. celle de l'école (niveau 2). L'adresse est-elle, suite à un SPAM ou d'une utilisation abusive, enregistrée dans une liste de blocage, par exemple RBL/CBL? Si oui, dans laquelle?

Version 2.0: Avril 2018

S'agit-il d'un problème DNS?
Parvenez-vous à ouvrir http://www.swisscom.com et http://138.190.35.25 avec le navigateur?
Si seule la deuxième variante fonctionne, il s'agit d'un problème de réglage local.

Le débit est-il lent?
Les URL ci-après mettent à disposition des fichiers de 1 Mo, 5 Mo, etc. à télécharger.

www.securepop.ch/benchmark
http://hsi.bluewin.ch/speedtest/

La mesure de la durée de téléchargement permet de définir la vitesse et de la comparer avec la bande passante du routeur de l'école. Contrôler le modèle de routeur et les réglages du port (sur l'appareil raccordé directement au routeur) – s'il est réglé sur 10 Mbit/s Half Duplex, veuillez le signaler au service cantonal de coordination (KKS).

Si les tests ci-dessus n'indiquent aucun problème local, un SecurePoP Case peut être ouvert via le service cantonal de coordination (KKS). Prière de communiquer les résultats de cette liste de contrôle ainsi que la date, l'heure et les adresses IP source et de destination.

SecurePoP® Web Content Screening (WCS)

Quelles catégories WCS le logiciel permet-il de bloquer?
www.securepop.ch – Service Options – Web Content Screening – Categories

Comment puis-je bloquer (ou débloquer) des catégories supplémentaires?
www.securepop.ch – Service Options – Web Content Screening – Categories

Où trouver une description des catégories WCS?
www.securepop.ch – Service Options – Web Content Screening – Categories – Description of the Categories
Lien direct: https://www.securepop.ch/global/smartfilter_xl_category_set_german.pdf

Dans quelle catégorie se trouve tel ou tel site?
www.securepop.ch – Service Options – Web Content Screening – Look up a Sites Category
Ce lien permet d'accéder au site de McAfee (enregistrement obligatoire).

Cette page est également accessible directement via
http://www.trustedsource.org/TS?do=feedback&subdo=url&action=checksingle&subdo=product&action=4-xl
Sélectionnez Product «McAfee Web Gateway (Webwasher)» pour utiliser la banque de données actuelle.

Où peut-on modifier l'affectation des sites dans les différentes catégories?
Vous pouvez faire part de vos propositions de modifications de la banque de données à l'adresse suivante:
http://www.trustedsource.org/en/feedback/url
Il est possible de proposer jusqu'à 3 catégories.

Pourquoi un site est-il accessible bien qu'il fasse partie d'une catégorie bloquée?
Internet est très dynamique. Les sites suspects changent souvent d'URL ou de nom de domaine, de sorte qu'ils n'entrent provisoirement plus dans la bonne catégorie. En outre, chaque semaine, des milliers de nouveaux sites qui doivent être classés par catégorie voient le jour.

Filtrage du contenu pour le trafic crypté

Quelle est la différence entre un trafic Internet non crypté (trafic http) et crypté (trafic https)?
Si une page est consultée via connexion cryptée, un cadenas s'affiche dans la barre d'adresse des navigateurs actuels. Aujourd'hui, un grand nombre de sites Web est accessible via connexion https. Ainsi, la communication entre le client et le serveur est cryptée. Le cryptage empêche toutefois un filtrage optimal du contenu.

Google?
Depuis 2012, Swisscom propose aux écoles d'intercepter les requêtes envoyées à Google par protocole https.
Ainsi, il est possible de filtrer les résultats de la recherche Google pour n'afficher que le contenu pertinent pour les élèves. Le canton choisit ensuite de faire usage ou non de cette possibilité. Pour que ce mécanisme fonctionne, un certificat spécifique doit être installé sur les appareils des utilisateurs.

Le certificat peut être téléchargé ici: https://www.swisscom.ch/fr/internet-a-lecole/internet-services.html.

Swisscom intercepte donc mon trafic crypté en tant qu'utilisateur?
Oui. Swisscom agit toutefois sur l'ordre des autorités cantonales. Et uniquement pour les catégories de contenu que le canton souhaite contrôler par filtrage. Le canton peut à tout moment ajouter des entrées à la liste autorisée, comme: l'e-banking, la santé, etc.

Pour les tunnels IPsec, l'adresse IP de destination est également classée par catégorie. Comme une catégorisation précise est impossible, cette dernière est attribuée à la catégorie Autres. Si un canton ne souhaite pas intercepter cette catégorie fiable, les contenus indésirables ne seront plus découverts dans cette catégorie.

Une attaque de l'homme au milieu (attaque qui a pour but d'interrompre le trafic crypté, d'identifier les paramètres de filtrage et de crypter de nouveau le trafic) est-elle encore d'actualité?
Oui. Il s'agit d'une méthode courante pour filtrer le trafic Internet, même crypté. L'attaque de l'homme au milieu nécessite un certificat connu afin de crypter de nouveau le trafic après le filtrage. Aujourd'hui, un certificat générique de ZScaler est utilisé pour les écoles. Toutefois, les cantons peuvent également utiliser leur propre certificat spécifique au réseau.

Je ne souhaite pas que mon trafic crypté à l'école soit intercepté. Comment dois-je procéder?
L'infrastructure de sécurité est localisée dans le réseau de formation cantonal. Ainsi, tous les trafics sont soumis aux règles de cette infrastructure, implémentées par le canton pour ce réseau de formation (pare-feu et Content Filter éventuel).
Si le trafic https (ou certaines catégories de ces trafics) doit également être filtré pour n'afficher que le contenu pertinent pour les élèves, un certificat est nécessaire.

Chaque école peut renoncer au service de filtrage (Migration vers «Open Net», un réseau sans filtrage de contenu).
Par conséquent, il relève de votre responsabilité d'établir une protection appropriée de la jeunesse conformément aux directives du canton. Le marché offre de nombreuses alternatives plus ou moins fiables et plus ou moins abordables.

Que fait Swisscom des données obtenues via la ventilation du trafic?
En cas de ventilation du trafic, elle doit obtenir un aperçu des données suivantes:
a) Client (adresse IP de l'appareil qui a envoyé la requête)
   Si un NAT est utilisé, seul l'IP du raccordement de l'école est connu.
   Ainsi, une identification de l'utilisateur est pratiquement impossible.
b) Ressource demandée (URL)
c) Horodatage
d) Décision du logiciel de filtrage (contenu autorisé, contenu à bloquer)

Ces données sont enregistrées pour une certaine durée dans les centres de calcul de Swisscom conformément aux dispositions légales.