swisscom

Frequently Asked Questions
Projekt «Schulen ans Internet»

FAQ

Diese FAQ richtet sich an die kantonalen Koordinationsstellen und auszugsweise an die Schulen, die im Rahmen der Swisscom Initiative «Schulen ans Internet» vom zusätzlichen URL Filtering SecurePoP® WCS Gebrauch machen. Bitte fragen Sie bei Ihrer kantonalen Koordinationsstelle nach, ob und inwieweit Ihnen als Schule diese Dienstleistung zur Verfügung steht.

Allgemeine Probleme

Wenn meine Schule von einem Bildungsnetz in ein anderes Netz (Volksschulnetz zu Open Net) wechselt: Kann die bestehende öffentliche IP-Adresse weiterhin genutzt werden?
Nein. Bei einer Migration in ein anderes Netz ändert die IP-Adresse immer.
Beim Wechsel in das Open Net benötigen wir dafür kein separates Antragsformular.

Kann Gebäude-Infrastruktur über SAI erschlossen werden?
Das Sponsoring «Schulen ans Internet» erschliesst den Schulen das Internet zu Unterrichtszwecken. Da bei Schulen ans Internet keine SLA's garantiert werden (Bandbreite, Verfügbarkeit), ist die Erschliessung der Gebäudeinfrastruktur wie Brandmeldeanlagen etc. über den Schulen ans Internet-Anschluss nicht möglich.

FTP Server
In seltenen Fällen wurde festgestellt, dass sich ältere FTP-Server zum Teil nicht an die gemäss RFC 959 definierten Formate halten. Da der SecurePoP® von Swisscom das Protokoll prüft, kommt in solchen Fällen keine Daten-Verbindung zustande. Durch einen Upgrade des Kundenservers auf die aktuelle Version kann das Problem behoben werden.

Performance

Ist die Verbindung zum Internet vorhanden?
Führen Sie ein «ping 164.128.36.36» von der PC DOS Eingabeaufforderung aus.
Falls Sie keine Antwort erhalten, handelt es sich nicht um ein Durchsatz Problem und die Verbindung ins Internet ist grundsätzlich gestört.

Besteht ein explizites Problem auch bei anderen PC's in a) derselben Schule b) anderen Schulen?
Falls nein, handelt es sich um ein Problem dieses Hosts/PCs. Im Fall von a) kommt als Fehlerquelle das lokale Netzwerk in der Schule oder allenfalls der LAN-I Router der Schule in Frage. Bei b) handelt es sich um ein zentrales Problem, das via kantonale Koordinationsstelle (KKS) an das Swisscom Helpdesk gemeldet werden muss.

Besteht ein Problem mit einzelnen Internet Sites/Hosts und/oder Services?
Welche Site/Host mit welchem Service (http, https, ...) haben Sie angesteuert? Gibt es eine Fehlermeldung?
Um ein Problem mit einer einzigen Site auszuschliessen, bitte mehrere Sites wie www.swisscom.com, www.cisco.com besuchen und die Erreichbarkeit und Geschwindigkeit beurteilen.

Ist es ein Email/SMTP Problem?
Abhängig davon, ob es sich um das Stufe 1 oder Stufe 2 Netz handelt, ist das Vorgehen unterschiedlich und muss mit der kantonalen Koordinationsstelle (KKS) abgesprochen werden. Browsen Sie auf http://www.anti-abuse.org und geben Sie die öffentliche IP-Adresse der SecurePoP Firewall oder evtl. der Schule (Stufe 2) ein. Ist die Adresse infolge von SPAM oder Missbrauch in einer Blocking List, zum Beispiel RBL/CBL registriert? Falls ja, in welcher?

Version 2.0: April 2018

Handelt es sich um ein DNS Problem?
Können Sie http://www.swisscom.com und http://138.190.35.25 mit dem Browser öffnen?
Falls nur die zweite Variante funktioniert, handelt es sich um ein lokales Einstellungsproblem.

Ist der Durchsatz langsam?
Unter folgenden URLs stehen 1 MByte, 5 MByte etc. grosse Dateien zum Herunterladen zur Verfügung.

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

Durch Messen der Downloadzeit kann die Geschwindigkeit bestimmt und mit der Router Bandbreite der Schule verglichen werden. Router-Modell und Port-Einstellungen (auf dem direkt am Router angeschlossenen Gerät) kontrollieren – falls 10 Mbit/s Half Duplex bitte bei der KKS melden.

Falls die obigen Tests kein lokales Problem zeigen, kann via kantonale Koordinationsstelle (KKS) beim Swisscom Helpdesk ein SecurePoP Case geöffnet werden. Bitte teilen Sie die Resultate dieser Checkliste sowie Datum, Zeit, Source- und Destination-IP-Adressen mit.

SecurePoP® und Web Content Screening (WCS)

Welche WCS Kategorien sind gesperrt?
www.securepop.ch – Service Options – Web Content Screening – Categories

Wie kann ich zusätzliche Kategorien sperren oder wieder erlauben lassen?
www.securepop.ch – Service Options – Web Content Screening – Categories

Wo findet man eine Beschreibung der WCS-Kategorien?
www.securepop.ch – Service Options – Web Content Screening – Categories – Description of the Categories
Direkter Link: https://www.securepop.ch/global/smartfilter_xl_category_set_german.pdf

In welcher Kategorie ist die betroffene Site?
www.securepop.ch – Service Options – Web Content Screening – Look up a Sites Category
Dieser Link führt auf die Seite von McAfee (Registrierung erforderlich).

Diese Seite ist auch direkt erreichbar:
http://www.trustedsource.org/TS?do=feedback&subdo=url&action=checksingle&subdo=product&action=4-xl
Wählen Sie Product «McAfee Web Gateway (Webwasher)» um die aktuelle Datenbank anzuwenden.

Wo kann die Zuordnung von Sites zu Kategorien geändert werden?
Änderungsvorschläge für die Datenbank werden unter folgender Adresse entgegengenommen:
http://www.trustedsource.org/en/feedback/url
Bis zu 3 Kategorien vorgeschlagen werden können.

Warum ist eine Seite erreichbar, obwohl sie eigentlich einer Kategorie angehört, die gesperrt ist?
Das Internet ist sehr dynamisch. Gerade fragwürdige Sites wechseln oft die URL oder den Domain-Namen und sind damit vorübergehend nicht korrekt kategorisiert. Auch kommen pro Woche tausende neuer Sites hinzu, die neu zu kategorisieren sind.

Content Filterung bei verschlüsseltem Traffic

Was ist der Unterschied zwischen unverschlüsseltem (http-Traffic) und verschlüsseltem (https-Traffic) Internet Verkehr?
Wird eine Seite via verschlüsselter Kommunikation aufgerufen, zeigen die heute gängigen Browser dies mit einem Schloss-Symbol in der Adress-Zeile an. Heute ist ein grosser Anteil von Websites über https erreichbar. Damit wird die Kommunikation zwischen Client und Server verschlüsselt. Durch die Verschlüsselung ist aber eine Content-Filterung nicht mehr ohne weiteres möglich.

Google?
Seit 2012 bietet Swisscom den Schulen an, Requests an Google aufzubrechen, wenn sie über das https-Protokoll versendet werden. Dadurch können die Suchergebnisse von Google bez. jugendschutzrelevanten Inhalten gefiltert werden. Es ist dem Kanton überlassen, von dieser Möglichkeit Gebrauch zu machen. Damit dieser Mechanismus funktioniert, muss auf dem Client ein bestimmtes Zertifikat installiert sein.

Dies steht hier: https://www.swisscom.ch/de/schulen-ans-internet/internet-services.html zum Download bereit.

Swisscom bricht also verschlüsselten Traffic von mir als User auf?
Ja. Swisscom tut dies jedoch lediglich auf Geheiss der kantonalen Verwaltungen. Und sie tut dies lediglich bei diesen Inhaltskategorien, die der Kanton via Content Filterung kontrollieren will. Es steht dem Kanton jederzeit frei, Einträge in Whitelists vornehmen zu lassen, wie zum Beispiel: e-Banking, Health, etc.

Bei IPsec-Tunneln wird die Destination IP ebenfalls als Kategorisierung herangezogen. Da eine eindeutige Kategorisierung nicht möglich ist, wird sie als Miscellaneous kategorisiert. Will ein Kanton diese an sich unbedenkliche Kategorie nicht aufbrechen, werden unerwünschten Inhalte in dieser Kategorie nicht mehr entdeckt.

Ist eine Man-in-the-Middle-Attack (so nennt sich das Vorgehen, wenn man verschlüsselten Traffic aufbricht, auf Filter-Parameter hin untersucht und wieder verschlüsselt weitergibt) überhaupt noch zeitgemäss?
Ja. Dies ist ein übliches Vorgehen, um einerseits den Internet-Traffic auch im verschlüsselten Modus filtern zu können. Die Man-in-the-Middle-Attack benötigt ein eigenes bekanntes Zertifikat, um den Traffic nach der Filterung wieder verschlüsseln zu können. Heute wird für die Schulen ein generisches Zertifikat von ZScaler eingesetzt. Die Kantone können aber auch ein eigenes, netz-spezifischer Zertifikat einsetzen.

Ich möchte nicht, dass mein verschlüsselter Traffic aus der Schule aufgebrochen wird. Wie muss ich vorgehen?
Die Sicherungs-Infrastruktur ist hinter dem kantonalen Bildungsnetz verortet. Damit passiert jeglicher Traffic die Regeln, die der Kanton für dieses Bildungsnetz implementiert hat, diese Infrastruktur (Firewall und allenfalls Content Filter). Soll gemäss diesen Regeln auch https-Traffic (oder lediglich bestimmte Kategorien solchen Traffics) nach jugendmedienschutzrelevanten Inhalten gefiltert werden, wird ein Zertifikat benötigt.

Sie können als einzelne Schule auf den Filter-Service verzichten (Migration ins «Open Net», ein Netz, ohne Content-Filterung). Damit sind Sie je nach Vorgaben des Kantons selbst in der Verantwortung, einen geeigneten Jugendmedienschutz zu etablieren. Der Markt bietet viele Alternativen, die mehr oder minder verlässlich und preislich divergent sind.

Was macht Swisscom mit den Daten, die sie durch die Aufschlüsselung des Traffics erhält?
Beim Aufschlüsseln des Traffics muss sie Einsicht in diese Daten erhalten:

a) Client-Gerät (IP-Adresse des Devices, das den Request abgesetzt hat)
   Kommt ein NAT zum Einsatz, ist lediglich die IP des Schulanschlusses bekannt.
   Dadurch ist ein Rückschluss auf den User praktisch unmöglich.
b) angefragte Ressource (URL)
c) Timestamp
d) Entscheid der Filtersoftware (erlaubter Inhalt, zu sperrender Inhalt)

Diese Daten werden bei Swisscom in ihren Rechenzentren entlang der gesetzlichen Verpflichtungen minimal und maximal lange gespeichert.