swisscom

Frequently Asked Questions
Progetto «Scuole in Internet»

FAQ

Queste FAQ sono destinate ai servizi cantonali di coordinamento e in parte alle scuole che, nell'ambito dell'iniziativa «Scuole in Internet» di Swisscom, usufruiscono del servizio supplementare URL Filtering SecurePoP® WCS. Vi invitiamo a chiedere al vostro servizio cantonale di coordinamento se e in che misura avete a disposizione questo servizio come scuola.

Problemi generali

Se la mia scuola passa da una rete scolastica a un'altra rete (dalla rete della scuola dell'obbligo a Open Net): L'indirizzo IP pubblico esistente può continuare ad essere utilizzato?
No. Ad ogni migrazione verso un'altra rete, l'indirizzo IP cambia.
Passando a Open Net non necessitiamo di un modulo di richiesta separato.

È possibile allacciare tramite SAI l'infrastruttura dell'edificio?
Nell'ambito dell'iniziativa «Scuole a Internet» si collegano le scuole a Internet a fini formativi.
Poiché nel quadro di tale programma non si possono garantire SLA (larghezza di banda, disponibilità), non è possibile allacciare l'infrastruttura dell'edificio (ad es. impianti antincendio ecc.) al collegamento Internet tramite SAI.

Server FTP
In rari casi è stato constatato che i server FTP meno recenti non sempre rispettano i formati definiti secondo RFC 959.
Poiché il SecurePoP® di Swisscom controlla il protocollo, in questi casi non viene stabilita alcuna connessione dati.
Con un aggiornamento del server del cliente alla versione attuale è possibile risolvere il problema.

Problemi di performance

Il collegamento a Internet è disponibile?
Eseguite un «ping 164.128.36.36» dal prompt dei comandi PC DOS.
Se non ricevete alcuna risposta significa che non si tratta di un problema legato alla portata e che il collegamento a Internet è sostanzialmente disturbato.

Sussiste un problema esplicito anche su altri PC a) nella stessa scuola b) in altre scuole?
In caso negativo si tratta di un problema dell'host/del PC in questione. Nel caso a) la causa del disturbo potrebbe risiedere nella rete locale all'interno della scuola o eventualmente nel router LAN-I di quest'ultima. Nell'eventualità b) si tratta invece di un problema centrale, da segnalare all'helpdesk di Swisscom tramite l'ufficio di coordinamento cantonale.

Esiste un problema con determinati host/siti Internet e/o servizi?
Quale sito/host di servizi (http, https, ...) avete tentato di raggiungere? Appare un messaggio di errore?
Per escludere che il problema sia circoscritto a un unico sito visitatene altri quali
www.swisscom.com, www.cisco.com, quindi valutatene la reperibilità e la velocità.

Il problema interessa e-mail/SMTP?
La procedura varia a seconda che si tratti della rete di livello 1 o 2 e va concordata con l'ufficio di coordinamento cantonale.
Andate su http://www.anti-abuse.org e inserite l'indirizzo IP pubblico del firewall SecurePoP o eventualmente della scuola (livello 2). L'indirizzo è stato registrato in una blocking list (ad es. RBL/CBL) in seguito a SPAM o abusi?
In caso affermativo, in quale?

Versione 2.0: Aprile 2018

Si tratta di un problema riguardante DNS?
Potete aprire http://www.swisscom.com e http://138.190.35.25 con il browser?
Nel caso in cui funzioni solamente la seconda variante, si tratta di un problema locale di impostazione.

La connessione è lenta?
Ai seguenti URL sono disponibili file da 1 MByte, 5 MByte ecc. che si possono scaricare per verificare la velocità.

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

Misurando il tempo di download è possibile determinare la velocità e confrontarla con la larghezza di banda del router della scuola. Controllare il modello del router e le impostazioni della porta (sull'apparecchio allacciato direttamente al router) – se 10 Mbit/s Half Duplex, segnalarlo all'ufficio di coordinamento cantonale.

Qualora i test di cui sopra non dovessero rivelare la presenza di un problema locale, è possibile aprire un SecurePoP Case presso l'helpdesk di Swisscom tramite l'ufficio di coordinamento cantonale. Vi preghiamo di comunicare i risultati della presente lista di controllo completi di data, ora ed indirizzi IP di origine e destinazione.

SecurePoP® Web Content Screening (WCS)

Quali categorie WCS sono bloccate?
www.securepop.ch – Service Options – Web Content Screening – Categories

Come faccio a bloccare o riabilitare altre categorie?
www.securepop.ch – Service Options – Web Content Screening – Categories

Dove è disponibile una descrizione delle categorie WCS?
www.securepop.ch – Service Options – Web Content Screening – Categories – Description of the Categories
Link diretto: https://www.securepop.ch/global/smartfilter_xl_category_set_german.pdf

In quale categoria si trova il sito in questione?
www.securepop.ch – Service Options – Web Content Screening – Look up a Sites Category
Questo link porta al sito di McAfee (è necessario registrarsi).

Questa pagina è consultabile anche direttamente:
http://www.trustedsource.org/TS?do=feedback&subdo=url&action=checksingle&subdo=product&action=4-xl
Selezionate il prodotto «McAfee Web Gateway (Webwasher)» per impiegare il database aggiornato.

Dove è possibile modificare l'attribuzione dei siti alle categorie?
Le proposte di modifica della banca dati devono essere inviate al seguente indirizzo:
http://www.trustedsource.org/en/feedback/url
Possono essere proposte fino a 3 categorie.

Perché un sito è consultabile nonostante faccia parte di una categoria bloccata?
Internet è estremamente dinamico. I siti sospetti, in particolare, cambiano spesso l'URL o il nome di dominio, per cui risultano temporaneamente inseriti in una categoria errata. Ogni settimana, inoltre, si aggiungono migliaia di nuovi siti che devono essere inseriti nelle varie categorie.

Filtro contenuti per traffico criptato

Qual è la differenza tra traffico Internet non criptato (traffico http) e criptato (traffico https)?
Se viene richiamata una pagina tramite comunicazione criptata, i browser comuni la visualizzano con il simbolo del lucchetto nella barra degli indirizzi. Oggi gran parte dei siti web è raggiungibile tramite https. In questo modo la comunicazione tra applicazione locale e server viene criptata. Con la criptazione però non è più possibile un filtro contenuti.

Google?
Dal 2012 Swisscom offre alle scuole la possibilità di interrompere le Request a Google se vengono inviate tramite protocollo https. In questo modo si possono filtrare i risultati della ricerca di Google o i contenuti rilevanti per la protezione dei minorenni. Ai cantoni è lasciata la facoltà di avvalersi di questa possibilità. Affinché questo meccanismo funzioni occorre installare un determinato certificato sull'applicazione locale, che si può scaricare qui:
https://www.swisscom.ch/de/schulen-ans-internet/internet-services.html.

Swisscom quindi interrompe il mio traffico criptato di utente?
Sì. Swisscom tuttavia lo fa soltanto su ordine delle amministrazioni cantonali e soltanto per le categorie di contenuti che il cantone vuole controllare tramite il filtro contenuti. Il cantone tuttavia è libero di fare inserire nelle Whitelist voci come ad esempio: e-banking, Health, etc.

Nei tunnel IPsec come classificazione viene impiegato anche l'IP di destinazione. Non essendo possibile una classificazione univoca, questo viene classificato come Varie. Se un cantone non vuole interrompere questa categoria, in sé non problematica, i contenuti indesiderati ivi presenti non vengono più rilevati.

Un attacco man-in-the-middle (così si definisce la procedura in cui il traffico criptato viene interrotto, analizzato in base ai parametri di un filtro e reimmesso di nuovo criptato) è una possibilità ancora attuale?
Sì. È una procedura comune per poter filtrare unilateralmente il traffico Internet in modalità criptata. L'attacco man-in-the-middle necessita di un proprio certificato specifico noto per poter criptare nuovamente il traffico dopo averlo filtrato. Oggi nelle scuole viene impiegato un certificato generico di ZScaler. I cantoni però possono anche impiegare un proprio certificato specifico per la rete.

Non desidero che il mio traffico criptato della scuola venga interrotto. Come devo procedere?
L'infrastruttura di protezione è localizzata dietro la rete di formazione cantonale. In tal modo il relativo traffico passa attraverso le regole che il cantone ha implementato per questa rete di formazione, questa infrastruttura (Firewall ed eventualmente Content Filter). Se, in base a queste regole anche il traffico https (o solo determinate categorie di tale traffico) deve essere filtrato secondo i contenuti rilevanti per la protezione della gioventù dai rischi dei media, occorre un certificato.

Come singola scuola potete rinunciare al servizio di filtro (Migrazione a «Open Net», una rete senza filtro contenuti). In questo modo, secondo le disposizioni del cantone, siete responsabili di stabilire una protezione adatta della gioventù dai rischi dei media. Il mercato offre molte alternative, più o meno divergenti per affidabilità e prezzo.

Cosa fa Swisscom con i dati che riceve tramite la suddivisione del traffico?
Con la suddivisione del traffico deve visionare questi dati:
a) applicazione locale (indirizzo IP del dispositivo che ha trasmesso la Request)
   Se viene utilizzato un NAT è noto solo l'IP del collegamento della scuola.
   In questo modo è praticamente impossibile risalire all'utente
b) risorse richieste (URL)
c) Timestamp
d) decisione del filtro software (contenuto consentito, contenuto da bloccare)

Questi dati vengono salvati da Swisscom nei propri centri di calcolo secondo gli obblighi di legge per un periodo di tempo minimo e massimo.