Aperçu technique

Projet «Internet à l'école» (SAI)

CONTENU

1 Objectif

Swisscom (Suisse) SA propose aux cantons, à des conditions uniques, un réseau de formation reliant tous les LAN (réseaux locaux) des écoles en une seule infrastructure de communication avec des bandes passantes / temps de réponse garantis, ainsi qu'un raccordement central à Internet à haut débit.

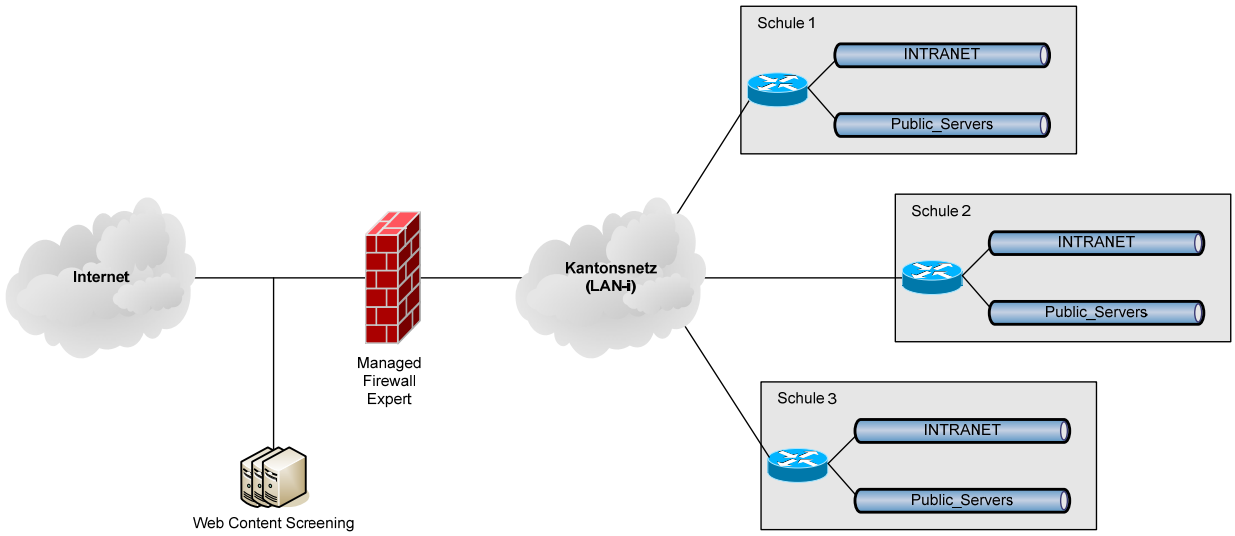
Une fois leur école connectée, les élèves et le personnel enseignant peuvent utiliser Internet sans limite de volume ni de temps et gratuitement. La sécurité est assurée par un pare-feu central qui protège le réseau de formation contre les attaques et accès non autorisés de et vers l'extérieur.

La présente directive porte sur les conditions-cadres techniques et organisationnelles du raccordement des écoles au sein du canton.

Offre «Standard»
> SecurePopManaged Firewall, qui empêche les accès extérieurs non autorisés.
> Web Content-Screening, filtre de contenu qui bloque l'accès aux contenus Internet inappropriés.

Offre «Extra» et **«Spécial»**
> VDSL Business Access entry (jusqu'à 30/10 MBit/s)
> Office Access fibre optique (jusqu'à 50/10 Mbits/s)
> Business Enterprise-Access (dès 2/2 MBit/s jusqu'à 200/200 MBit/s)

Pour les raccordements dont la bande passante est plus élevée (**«Extra»** et **«Spécial»**), c'est au canton de décider quelle solution de sécurité utiliser.



2 Principes

Le réseau de formation pour le raccordement des écoles à Internet est conçu de manière totalement **séparée** des réseaux administratifs des différents cantons. Les communications avec les services cantonaux internes (hors écoles) et les autres réseaux de formation cantonaux passent exclusivement par le **pare-feu** Internet central sur le réseau de formation cantonal (un pare-feu par réseau de formation cantonal).

Swisscom SA gère un **helpdesk** pour chaque réseau de formation.
Les dérangements ne peuvent être signalés que par le service cantonal de coordination à Swisscom SA. Les écoles sont tenues de s'adresser au service cantonal de coordination en cas de dérangement.

Les **frais d'installation** par des électriciens concessionnaires pour les câblages internes aux écoles en vue du raccordement au réseau de formation sont pris en charge par les écoles (resp. les cantons). Les écoles assurent les conditions appropriées en termes de locaux et de température (MODEM, routeur) dans leurs bâtiments.

3 Résumé de la solution

Le réseau implémenté et exploité par Swisscom SA est basé sur les services LAN-I et le service Managed Firewall *expert* de Swisscom SA.

Les écoles raccordent leurs terminaux (ordinateur, imprimante) via un LAN Ethernet, qu'elles raccordent au routeur CISCO propre à Swisscom SA sur place. Tous les routeurs constituent entre eux, par canton, un réseau à 3 couches fermé avec connectivité «any-to-any», qui possède une seule passerelle – centrale et sécurisée – vers Internet. La protection est assurée par un pare-feu (Managed Firewall *expert*), dont le dispositif juridique («Policy») est valable pour toutes les écoles raccordées.

Un Web Content Screening est disponible en option. Il est possible de définir par réseau cantonal quelles catégories disponibles sont autorisées ou bloquées. Les filtres peuvent être adaptés aux besoins spécifiques via un nombre limité de listes noires et blanches.

4 Adressage IP

Swisscom SA élabore le **concept d'adressage IP** , afin que chaque école reçoive une **plage d'adresses** IP précise.
Les adressages IP existants doivent être **modifiés** par les écoles en fonction du nouvel adressage.

Les **terminaux** des écoles doivent être adressés soit de manière fixe, soit via le DHCP interne de l'école. La fonctionnalité DHCP n'est pas comprise dans la solution Swisscom. Pour ce faire, il faut utiliser la plage d'adresses attribuée pour chaque école. Les cinq premières adresses IP (par sous-réseau) sont réservées pour Swisscom SA et ne peuvent pas être occupées.

5 Politique de sécurité

Le dispositif juridique (policy) concernant le pare-feu central de chaque réseau de formation cantonal est applicable **pour toutes** les écoles raccordées.

Le dispositif juridique mis en place est défini de manière **ouverte** à la demande des responsables de formation et ne répond pas aux dispositifs de sécurité habituellement restrictifs pour les pare-feu du segment de la clientèle commerciale. Des risques accrus en termes de sécurité peuvent donc survenir. Le pare-feu central n'effectue ni une authentification des utilisateurs, ni un scan antivirus.

6 Mise en réseau Inhouse LAN

Le LAN et donc les périphériques en réseau (ordinateurs, imprimantes) reçoivent des adresses IP privées selon le concept d'adressage de Swisscom SA. Les écoles/cantons doivent se procurer et gérer eux-mêmes d'éventuels moyens auxiliaires pour l'administration des réseaux, tels que serveurs DNS ou DHCP.

7 Organisation et exploitation

Dans chaque canton, un **service de coordination central** est désigné pour le réseau de formation cantonal. Ses tâches vis-à-vis de Swisscom SA et des écoles raccordées sont les suivantes:

- Traitement et transmission des demandes des écoles cantonales.
- Traitement des modifications de configuration sur le pare-feu central à l'attention de Swisscom SA.
- **Interlocuteur unique** pour les écoles en cas de dérangements techniques ou liés à l'exploitation dans le réseau de formation cantonal.
- Interface cantonale **unique** avec le helpdesk SAI dédié de Swisscom SA.

Un **interlocuteur technique** doit être désigné par école. Les dérangements dans le réseau de formation cantonal ne sont signalés aux services cantonaux de coordination que par les interlocuteurs techniques.

Informations techniques

8 Messageries hébergées chez ISP

Normalement, les fournisseurs de messagerie n'autorisent l'envoi d'e-mails via leurs serveurs que depuis la propre plage d'adresses IP. Deux possibilités sont disponibles pour pouvoir également envoyer des mails depuis les réseaux SAI à partir de comptes de messagerie externes:

Authentification SMTP

Actuellement, la plupart des fournisseurs de messagerie offrent une authentification SMTP, la méthode la plus simple pour envoyer des e-mails via un serveur SMTP externe.

Relais de messagerie IP-Plus

L'école configure sur les Clients le serveur de messagerie IP-Plus **mailhub.ip-plus.net** comme serveur SMTP pour l'envoi de messages électroniques (en lieu et place de mail.bluewin.ch). Spécialement mis à disposition pour «Internet à l'école», ce serveur remplace les deux indiqués auparavant:

- mailhost.ip-plus.net
- smtp.ip-plus.net

Les écoles qui utilisent encore l'un de ces deux serveurs devraient envisager de passer prochainement au nouveau serveur.

9 Serveur DNS

Pour autant que l'école n'exploite pas son propre serveur DNS, elle peut enregistrer les deux serveurs DNS IP-Plus ci-après sur les Clients et serveurs:

sdns1.ip-plus.net	164.128.36.36
sdns2.ip-plus.net	164.128.36.37

Les serveurs DNS standard d'IP-Plus ne sont plus disponibles pour SAI.

10 Plage d'adresses IP privée (zone INTRANET)

Le concept d'adressage IP de Swisscom prévoit, pour l'adressage d'ordinateurs de l'école, des adresses de la plage privée 10.x.x.x. Le pare-feu SecurePoP central autorise, par canton, pour cette plage d'adresses, tous les services courants dont un ordinateur a besoin (http, ftp, pop3, smtp, etc.). Sur demande, certains ports de la zone INTRANET sont ouverts à Internet. Les ouvertures de ports concernent toujours l'ensemble du réseau cantonal et ne peuvent pas être limitées à certaines écoles ou adresses IP.

L'accès à un serveur de la plage d'adresses 10.x.x.x depuis Internet n'est pas pris en charge. Vues d'Internet, ces adresses sont cachées derrière l'adresse publique du pare-feu (212.x.x.x) par Network-Address-Translation (NAT).

11 Plage d'adresses IP publique (zone Public_Servers)

Un nombre limité d'adresses IP publiques sont également mises à disposition pour les systèmes devant être directement adressables depuis Internet (appelés «Public_Servers»). Le pare-feu SecurePoP central autorise, par canton, pour cette plage d'adresses, tous les services courants. Sur demande, des ports spécifiques entre la zone «Public_Servers» et Internet sont ouverts dans les deux directions. Les ouvertures de ports concernent toujours l'ensemble du réseau cantonal et ne peuvent pas être limitées à certaines écoles ou adresses IP.

Remarque: La plage d'adresses pour la zone «Public_Servers» est configurée sur le même raccordement que la zone INTRANET («Multi-Netting»). Il ne s'agit dès lors pas d'une DMZ sur une interface de pare-feu dédiée.

12 Pare-feu propre à l'école

Swisscom exploite, dans le cadre de l'initiative «Internet à l'école», un pare-feu dédié par réseau cantonal. Les pare-feu propres aux écoles ne sont pas pris en charge (à l'exception d'OpenNet). Si une école utilise son propre pare-feu ou Proxy Gateway, Swisscom ne peut pas apporter son aide pour les interruptions de service et les pertes de performances qui en résultent.

Support Web Content Filtering

Caractéristiques du service de Web Content Filtering

- Chaque réseau cantonal a son propre Content Filtering. Par conséquent, aucune personnalisation pour chaque école n'est possible.
- Filtrage de contenus Web dans 30 catégories principales et 120 sous-catégories, listes blanches et noires.
- Protection contre les contenus dangereux tels que les virus, logiciels malveillants, sites d'hameçonnage, notamment avec la banque de données actuelle
- Activation de la fonction SafeSearch pour les recherches (implique une inspection de trafic SSL si le cryptage est actif par défaut)
- Catégories à bloquer sélectionnables par le service cantonal de coordination (KKS) via www.securepop.ch.
- Possibilité de consulter l'appartenance d'une URL définie à une catégorie et de demander une nouvelle catégorisation

Filtrage de contenus Web cryptés SSL
Il est possible de filtrer également le trafic de contenus cryptés SSL. Cela est par exemple nécessaire pour solliciter la fonction SafeSearch pour certains moteurs de recherche. Dans ce cas, l'installation sur tout le territoire d'un certificat client est nécessaire sur tous les appareils terminaux correspondants.

Anonymizers Proxy
Sur Internet, certains serveurs (Anonymizing Proxies) ne servent qu'à contourner un filtre URL et donc à permettre l'accès à des pages normalement bloquées. En principe, il est possible
de bloquer de tels proxys anonymes.

Recatégorisation de contenus Web
La banque de données de filtrage web comporte des valeurs continuellement actualisées pour des milliards de sites Internet dans le monde entier. Cependant, elle n'est pas parfaite. Par conséquent, il est possible que certains sites Internet soient mal catégorisés. Dans ce cas, il est possible de procéder à une recatégorisation. Une recatégorisation est possible sur www.securepop.ch ou directement sur http://www.zscaler.com/sitereview/

Authentification basée sur les adresses IP
Pour diverses offres web, il est nécessaire de s'identifier à l'aide de l'adresse IP source. Si l'accès à ces offres se fait via le filtrage, les domaines d'adresse IP suivants doivent être signalés aux prestataires correspondants.

195.65.152.0/24
195.65.154.0/24

Remarque: cela s'applique si l'accès effectif à l'offre se fait via Web Security Proxy.