

Technische Richtlinien Projekt "Schulen ans Internet" (SAI)

INHALT

1. ZWECK	2
2. GRUNDSÄTZE.....	2
3. ZUSAMMENFASSUNG DER LÖSUNG.....	2
4. IP-ADRESSIERUNG	3
5. SECURITY POLICY, DMZ (DEMILITARIZED ZONE)	3
6. ANSCHLUSS VON SCHULEN.....	3
7. MIGRATION BESTEHENDER ANSCHLÜSSE BEI INTERNET SERVICE PROVIDERN (ISP)	4
8. MIGRATION BESTEHENDER WEB-, FTP- UND MAILSERVER.....	4
9. ORGANISATION UND BETRIEB.....	4



1. Zweck

Swisscom AG offeriert den Kantonen zu einmaligen Konditionen ein Bildungsnetz, das alle LANs (lokale Netzwerke) der Schulen zu einer einzigen Kommunikationsinfrastruktur mit garantierten Bandbreiten/Antwortzeiten untereinander verbindet und einen zentralen Internetanschluss mit grosszügiger Bandbreite bietet.

Ist eine Schule erst einmal am Netz, können Schülerinnen und Schüler sowie Lehrkräfte unbeschränkt ohne Volumenbegrenzung und kostenlos rund um die Uhr das Internet nutzen. Für die Sicherheit sorgt eine zentrale Firewall, die das Bildungsnetz gegen unberechtigte An- und Zugriffe von und nach aussen schützt.

Diese Richtlinie zeigt weiter die technischen und organisatorischen Rahmenbedingungen für den Anschluss der Schulen innerhalb des Kantons auf.

Mit dem erweiterten **Angebot «Extra» (ab 01.01.2010)**, bietet Swisscom den Schulen zudem folgende Technologien/Bandbreiten:

- > VDSL Branch Access (bis 24/6 MBit/s)
- > Glasfaser Office Access (bis zu 50/10 MBit/s)

2. Grundsätze

Das Bildungsnetz für den Anschluss der Schulen ans Internet wird völlig **getrennt** von den administrativen Netzen der einzelnen Kantone aufgebaut. Kommunikationsbeziehungen zu internen kantonalen Stellen (nicht Schulen) sowie zu den anderen kantonalen Bildungsnetzen erfolgen ausschliesslich über die zentrale Internet **Firewall** am kantonalen Bildungsnetz (pro kantonales Bildungsnetz eine Firewall).

Für die einzelnen Bildungsnetze betreibt Swisscom AG ein **Helpdesk**. Störungen können ausschliesslich via die kantonale Koordinationsstelle Swisscom AG gemeldet werden. Die Schulen sind verpflichtet, sich bei allfälligen Störungen an die kantonale Koordinationsstelle zu wenden.

Die **Installationskosten** durch konzessionierte Elektriker für schulinterne Verkabelungen für den Anschluss ans Bildungsnetz werden durch die Schulen (resp. die Kantone) übernommen. Die Schulen sorgen in ihren Gebäuden für geeignete räumliche und klimatische Bedingungen (MODEM, Router).

Sind die neuen Technologien verfügbar, können die Schulen ohne zusätzliche Kosten profitieren (Angebot «Extra»).

- > Sind die Technologien nicht verfügbar, offeriert Swisscom die Anschlussarbeiten unter Kostenbeteiligung von Schule oder Kanton und unter Vorbehalt der Realisierbarkeit zu einem Spezialpreis.
- > Ungeachtet der Verfügbarkeit stehen Anschlüsse auf der Glasfaser-Technologie erst ab Herbst 2010 zur Verfügung.

3. Zusammenfassung der Lösung

Das von Swisscom AG implementierte und betriebene Netzwerk basiert auf dem eigenen LAN-I over IPSS Service sowie dem SecurePoP®*expert* Service.

Die Schulen erschliessen ihre Endgeräte (PC, Drucker) über ein Ethernet LAN/10BaseT/RJ45 und schliessen dieses an einem Swisscom AG eigenen CISCO-Router vor Ort an. Alle Router stellen untereinander pro Kanton ein geschlossenes Layer-3-Netzwerk mit any-to-any-Konnektivität dar, das einen einzigen zentralen und gesicherten Übergang zum Internet besitzt. Für den Schutz wird eine Firewall (SecurePoP®*expert*) eingesetzt, deren Regelwerk ("Policy") gilt für alle angeschlossenen Schulen.

Während einer Übergangsfrist wird für den Anschluss **bestehender** SMTP & POP3 Mailserver sowie von Web- und FTP-Servern bei einigen Schulen parallel dazu ein weiterer (DMZ-) Router installiert. Dies ist nur dort nötig, wo die Schule ausdrücklich einen eigenen Server vor Ort in ihren Lokalitäten betreibt. An dessen Ethernetschnittstelle schliesst die Schule ein **separates** LAN an und stellt dadurch die Konnektivität zu den erwähnten Servern sicher. Details für die Migration werden zwischen Swisscom AG und den Schulen direkt besprochen.

Bei vorhandenen speziellen Bedürfnissen, vor allem bei Schulen der Sekundarstufe II (z. B. Berufsschulen) kann durch Swisscom AG zusammen mit diesen Schulen und dem Kanton eine dedizierte Lösung erarbeitet werden. Diese Lösung unterscheidet sich vor allem bei der installierten Policy der Firewall und der IP-Adressierung von der üblichen Lösung. Dazu sind durch alle betroffenen Schulen, die dies wünschen, weitreichende schriftliche Zusagen zu Handen Swisscom AG nötig.

4. IP-Adressierung

Swisscom AG erstellt ein übergreifendes **IP-Adressierungskonzept** (über alle kantonalen Bildungsnetze) und sorgt damit dafür, dass innerhalb und zwischen den Kantonen jede Schule, die einen Anschluss an das jeweilige kantonale Bildungsnetz bestellt, einen eindeutigen **IP-Adressbereich** für die Schule erhält. Bestehende IP Adressierungen müssen durch die Schulen **umgestellt** werden.

Das Konzept nimmt in angemessener Weise auf bestehende grössere schulinterne IP-Adressierungen (insbesondere auf offiziell registrierte IP-Adressen, die für Web-, FTP- und Mailserver produktiv im Einsatz stehen) Rücksicht.

Die **Endgeräte** der Schulen müssen entweder fix oder via schuleigenes DHCP adressiert werden. Dazu ist der pro Schule zugeteilte Adressbereich zu verwenden. Die ersten fünf IP-Adressen (pro Subnetz) sind für Swisscom AG reserviert und dürfen nicht belegt werden.

5. Security Policy, DMZ (demilitarized Zone)

Die Policy an der zentralen Firewall des jeweiligen kantonalen Bildungsnetzes gilt **für alle** angeschlossenen Schulen. Den Schulen ist es freigestellt ihrerseits weitergehende Sicherheitsmassnahmen (Virenschanning, eigene Firewall, Adressfilter, Userverwaltung, Proxyserver etc.) vorzunehmen.

Die implementierte Policy ist bewusst **sehr offen** definiert und entspricht auf Wunsch der Bildungsverantwortlichen der Kantone; nicht den üblichen restriktiven Securitypolicies für Firewalls im Geschäftskundenbereich. Dadurch können erhöhte Sicherheitsrisiken entstehen. Auf der zentralen Firewall erfolgt weder Benutzerauthentifizierung noch Virenscreening.

Die Firewall kann mit einer **DMZ** konfiguriert sein. Diese DMZ bietet den Schulen/Kantonen die Möglichkeit, an einem ausgewählten Standort z.B. zentrale kantonale Serverfarm für alle Schulen anzubieten (zentraler Fileserver FTP, zentraler Webserver, zentraler Mailserver etc.).

Für das Angebot «Standart» (bisher), bleibt die Sicherheitslösung für die bestehenden Standard-Anschlüsse über ADSL unverändert:

- > SecurePop: Managed Firewall, die unberechtigte Zugriffe von aussen abwehrt.
- > Web Content-Screening: Inhaltsfilter, der den Zugriff auf ungeeigneten Inhalt im Internet verhindert.

Für die Anschlüsse mit höherer Bandbreite (**«Extra»**) entscheidet der Kanton, wer die Sicherheitslösung zur Verfügung stellt.

6. Anschluss von Schulen

Das LAN und dadurch vernetzte Peripheriegeräte (PC, Drucker) werden mit inoffiziellen IP-Adressen gemäss Adressierungskonzept von Swisscom AG adressiert. Allfällige Hilfsmittel für die Administration der Netzwerke wie DNS Server oder DHCP Server müssen durch die Schulen/Kantone beschafft und betrieben werden.

In einer späteren Phase steht den Schulen der in einem separaten Projekt geplante und neu aufgebaute Bildungsserver der Schweiz (siehe: www.educa.ch) für Webauftritte und Mail zur Verfügung.

7. Migration bestehender Anschlüsse bei Internet Service Providern (ISP)

Vorgehen für:

- **Domain Name:**
Die bestehenden aktiven Domains können beibehalten werden. Sinnvollerweise wird das Domain Name Hosting vom bestehenden Internet Service Provider (ISP) zu IP-Plus migriert. Dies erfordert auch die Anpassung der Registrierung bei Switch. Das SecurePoP Team von Swisscom AG plant und führt zusammen mit der Schule diese Migration zeitlich synchron durch.
- **IP-Adressen:**
Server, die bisher bereits unter offiziellen IP-Adressen erreichbar sind, erhalten neue offizielle Adressen, die durch Swisscom AG zugeteilt werden.

Die entsprechenden DNS Records (A, MX) werden zusammen mit der DNS-Migration zu IP-Plus angepasst.

8. Migration bestehender Web-, FTP- und Mailserver

- WEB-, FTP- und andere vom Internet her erreichbare Server werden in die DMZ migriert, wo sie eine **neue öffentliche IP-Adresse** zugeteilt erhalten.
- Mail-Server (nur SMTP) werden grundsätzlich im Intranet Segment betrieben. Sie erhalten dort eine neue öffentliche IP-Adresse. Die Anordnung im Intranet Segment ist meist sinnvoll, da (z.B. MS Exchange Server) umfangreiche VerbindungsaufbauprozEDUREN zwischen Client und Server und systemspezifische Protokolle/Services verwendet werden. Diese Kommunikation sollte nicht über die Firewall geführt werden.

Die SecurePoP[®]*expert* Firewall nimmt die Mails aus dem Internet entgegen, speichert sie zwischen und liefert sie anschliessend an den internen Mail-Server aus. Dies stellt sicher, dass nie eine direkte Verbindung via SMTP vom Internet ins LAN möglich ist. Gleichzeitig ist durch die Zwischenspeicherung gewährleistet, dass bei einem vorübergehenden Ausfall des internen Mail-Servers keine Mails verloren gehen.

9. Organisation und Betrieb

Pro Kanton ist eine **zentrale Koordinationsstelle** für das kantonale Bildungsnetz bezeichnet. Deren Aufgaben gegenüber Swisscom AG und den angeschlossenen Schulen umfassen:

- Die Bearbeitung und Weiterleitung der Anträge der kantonalen Schulen.



swisscom

- Die Bearbeitung von Konfigurationsänderungen an der zentralen Firewall zu Handen Swisscom AG.
- Koordinationsstelle für wichtige und alle Schulen betreffenden (betrieblichen und organisatorischen) Mitteilungen von Swisscom AG.
- **Alleiniger Ansprechpartner** für die Schulen bei technischen oder betrieblichen Störungen im kantonalen Bildungsnetz.
- **Einzig**e kantonale Schnittstelle zum dedizierten SAI-Helpdesk bei Swisscom AG.

Pro Schule ist ein **technischer Ansprechpartner** zu bezeichnen. Störungen im kantonalen Bildungsnetz werden durch die technischen Ansprechpartner an die kantonalen Koordinationsstellen gemeldet.

Während der **Implementationsphase** stehen auf Seite Swisscom AG die folgenden Mitarbeitenden zur Verfügung:

- 1 Projektleiter Implementation inkl. Stellvertreter
- 1 Engineer für LAN-I over IPSS
- 1 Engineer für SecurePoP®*expert*
- 1 Mitarbeitender für Administration

Die Namen und Adressen etc. werden den Kantonen bei einem Kickoff Meeting nach dem offiziellen Projektstart bekannt gegeben.