Aspetti tecnici

Progetto «Scuole in Internet» (SAI)

CONTENUTO

1 Scopo

Swisscom (Svizzera) SA offre ai Cantoni, a condizioni esclusive, una «rete scolastica» che integra le LAN (reti locali) delle scuole in un'unica infrastruttura di comunicazione con larghezze di banda e tempi di risposta garantiti e che consente l'accesso a un collegamento Internet centrale con un'elevata larghezza di banda.

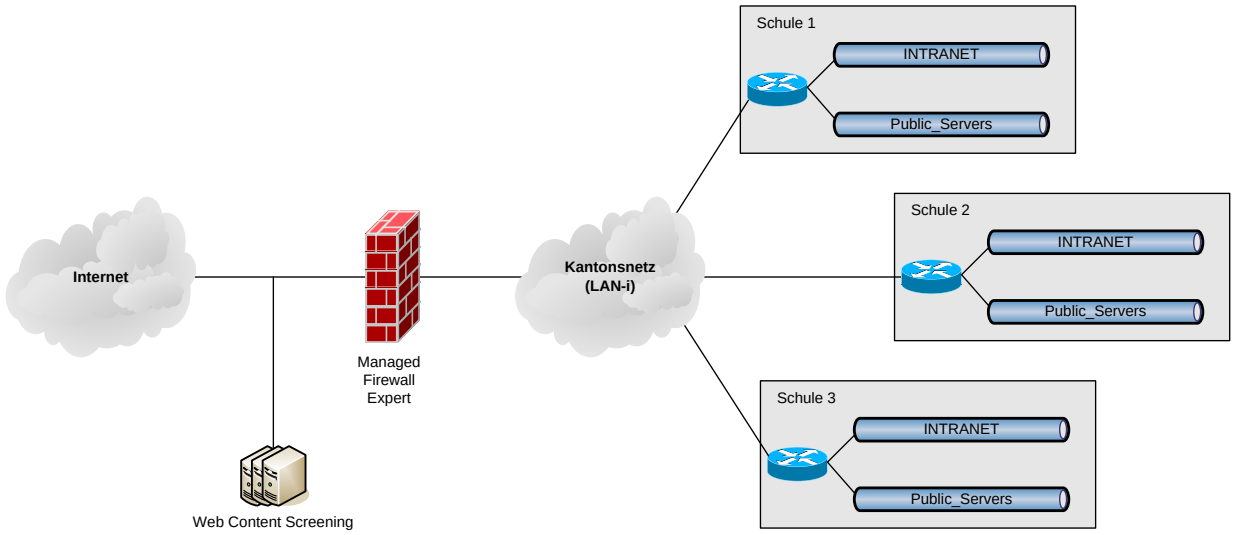
Una volta effettuato il collegamento in rete, le allieve e gli allievi nonché gli insegnanti della scuola possono navigare gratuitamente in Internet, senza limiti di tempo né di volume. La sicurezza è garantita da un firewall centrale che protegge la rete contro gli accessi e gli interventi da e verso l'esterno non autorizzati.

La presente direttiva contiene le condizioni quadro tecniche e organizzative da osservare per il collegamento delle scuole all'interno del Cantone.

Offerta «Standard»
> SecurePop Managed Firewall che protegge da accessi dall'esterno non autorizzati .
> Web Content Screening, filtraggio dei contenuti che impedisce l'accesso a contenuti inadeguati in Internet.

Offerta «Extra» e **«Special»**
> Business Access / light (xDSL)
> Business Access Low End Fibre (FTTH)
> Business Enterprise-Access (ab 2/2 MBit/s)

Per i collegamenti con larghezze di banda maggiori (**«Extra»** e **«Special»**) decide il Cantone chi mette a disposizione la soluzione di sicurezza.



2 Principi

La rete scolastica impiegata per collegare le suole a Internet è completamente **indipendente** dalle reti amministrative dei singoli Cantoni. Le comunicazioni con i servizi cantonali interni (non le scuole) e le altre reti cantonali del settore dell'insegnamento avvengono esclusivamente attraverso il **firewall** Internet centrale della rete scolastica cantonale (un firewall per ogni rete cantonale).

Swisscom SA gestisce un **helpdesk** per ognuna delle reti scolastiche.
I guasti possono essere segnalati a Swisscom SA unicamente dal servizio di coordinamento cantonale, al quale le scuole sono tenute a rivolgersi in caso di guasto.

I **costi d'installazione** relativi al cablaggio all'interno delle scuole, effettuato da elettricisti in possesso della concessione e necessario per il collegamento alla rete scolastica, sono a carico delle scuole (risp. dei Cantoni). Nei loro locali, le scuole devono garantire condizioni ambientali adeguate (MODEM, router).

3 Ricapitolazione della soluzione

La rete implementata e gestita da Swisscom SA verte sui suoi servizi LAN-I e Managed Firewall *expert*.

Le scuole allacciano i loro terminali (PC, stampanti) a una rete Ethernet LAN e collegano la rete al router CISCO di Swisscom SA sul posto. In ogni Cantone, l'insieme dei router interconnessi rappresenta una rete chiusa di livello 3 con interconnessione any-to-any che dispone di un unico accesso a Internet centrale e sicuro. Quale elemento di protezione viene impiegato un firewall (Managed Firewall *expert*) basato su una norma (policy) valida per tutte le scuole collegate.

A titolo facoltativo è disponibile un Web Content Screening. Per ogni rete cantonale si può definire quali categorie devono essere consentite o bloccate. Con l'ausilio di un numero limitato di voci in una black o white list è possibile adeguare i filtri a esigenze specifiche.

4 Indirizzi IP

Swisscom SA allestisce il **piano di indirizzamento IP** in virtù del quale ogni scuola riceve una **serie di indirizzi IP** univoca.
In seguito al nuovo piano di indirizzi, le scuole devono **adattare** gli indirizzi IP interni esistenti.

I **terminali** delle scuole devono essere indirizzati in modo fisso oppure attraverso il DHCP della scuola. La funzione DHCP non è parte integrante della soluzione Swisscom. A tal fine occorre impiegare la serie di indirizzi assegnata a ogni scuola. I primi cinque indirizzi IP (di ogni sottorete) sono riservati a Swisscom SA e non possono essere utilizzati.

5 Security Policy

La policy implementata nel firewall centrale di ogni rete scolastica cantonale vale **per tutte** le scuole collegate.

Su richiesta dei responsabili dell'istruzione è stata deliberatamente implementata una norma di sicurezza **meno restrittiva** di quelle solitamente impiegate per i firewall in ambito commerciale. Di conseguenza, i rischi a livello di sicurezza sono maggiori. Il firewall centrale non effettua né l'autenticazione degli utenti né la scansione dei virus.

6 Interconnessione LAN inhouse

Alla rete LAN e agli apparecchi periferici allacciati (PC, stampanti) vengono assegnati indirizzi IP privati conformemente al piano di indirizzi IP allestito da Swisscom SA. Eventuali mezzi ausiliari per l'amministrazione delle reti, come server DNS o server DHCP, devono essere procurati e gestiti dalle scuole/dai Cantoni.

7 Organizzazione e gestione

In ogni Cantone viene istituito un **servizio di coordinamento centrale** per la rete scolastica cantonale che è responsabile, nei confronti di Swisscom SA e delle scuole collegate, dei seguenti compiti:

- elaborare e inoltrare le richieste delle scuole cantonali;
- elaborare modifiche della configurazione del firewall centrale da sottoporre a Swisscom SA;
- fungere da **unico servizio di contatto** per le scuole in caso di guasti tecnici o interruzioni dell'esercizio della rete scolastica cantonale;
- assumere il ruolo di **unico** servizio cantonale che funge da interfaccia con l'helpdesk SAI di Swisscom SA.

Ogni scuola deve definire un **responsabile tecnico**. I guasti che si verificano all'interno della rete scolastica cantonale devono essere segnalati ai servizi di coordinamento cantonali dai rispettivi responsabili tecnici.

Informazioni tecniche

8 Mailbox con hosting presso ISP

Di solito i provider di posta elettronica consentono l'invio di e-mail tramite i loro server soltanto a partire dalla propria serie di indirizzi IP. Per poter inviare comunque delle e-mail a partire da account di posta elettronica esterni tramite le reti SAI esistono due possibilità:

Autenticazione SMTP

Oggi la maggior parte dei provider di posta elettronica offre l'autenticazione SMTP. È il metodo più semplice per inviare e-mail attraverso un server SMPT esterno.

IP-Plus Mail Relay

La scuola configura sui client il mail server IP-Plus **mailhub.ip-plus.net** come server SMTP per l'invio di e-mail (al posto ad es. di mail.bluewin.ch). Tale server è stato messo a disposizione appositamente per «Scuole in Internet» e sostituisce i due server indicati in passato:

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

Se nelle scuole viene ancora utilizzato uno di questi server, occorrerebbe pianificare al più presto un passaggio al nuovo server.

9 Server DNS

Se non gestisce un server DNS proprio, la scuola può inserire sui client e sui server i due seguenti server DNS IP-Plus:

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

I server DNS standard di IP-Plus non sono a disposizione per SAI.

10 Serie di indirizzi IP privata (zona INTRANET)

Il piano di indirizzi IP di Swisscom prevede indirizzi della serie privata 10.x.x.x per i computer nelle scuole. Il firewall SecurePoP centrale di ogni Cantone consente, per questa serie di indirizzi, tutti i servizi usuali di cui necessita un PC (http, ftp, pop3, smtp ecc.). Su richiesta vengono aperte specifiche porte dalla zona INTRANET a Internet. L'apertura di porte interessa sempre l'intera rete cantonale e non può essere limitata a singole scuole o singoli indirizzi IP.

Il raggiungimento di un server nella serie di indirizzi 10.x.x.x da Internet non è supportato. Questi indirizzi non sono visibili da Internet perché vengono nascosti tramite Network Address Translation (NAT) dietro l'indirizzo ufficiale del firewall (212.x.x.x).

11 Serie di indirizzi IP pubblica (zona Public_Servers)

Per i sistemi che devono essere indirizzabili direttamente da Internet (i cosiddetti «Public Servers») viene messo a disposizione un numero limitato di indirizzi IP pubblici. Il firewall SecurePoP centrale di ogni Cantone consente per questa serie di indirizzi tutti i servizi usuali. Su richiesta vengono aperte specifiche porte tra la zona «Public Servers» e Internet in entrambe le direzioni. L'apertura di porte interessa sempre l'intera rete cantonale e non può essere limitata a singole scuole o singoli indirizzi IP.

Nota: la serie di indirizzi per la zona Public Servers è configurata sullo stesso collegamento della zona INTRANET (cosiddetto multinetting). Non si tratta quindi di una DMZ su un'interfaccia firewall dedicata.

12 Firewall proprietari delle scuole

Nell'ambito dell'iniziativa dedicata alla scuole, Swisscom gestisce un firewall dedicato per ogni rete cantonale. I firewall proprietari delle scuole non vengono supportati (ad eccezione di OpenNet). Se una scuola si serve del proprio firewall o Proxy Gateway, Swisscom non può fornire alcun supporto per le interruzioni di servizio o i cali di performance che ne conseguono.

Support Cloud Security Services

Caratteristiche di Cloud Security Services

- Per ogni rete cantonale viene gestito un proprio Content Filtering. Pertanto, non è possibile un'individualizzazione per singole scuole.
- Filtraggio di contenuti web da 30 categorie principali e 120 sottocategorie nonché proprie whitelist e blacklist.
- Protezione da contenuti pericolosi quali virus, malware, siti di phishing, tra l'altro con una banca dati sempre aggiornata
- Attivare la funzione SafeSearch per domande di ricerca (richiede SSL Traffic Inspection dove la codifica è attiva per default)
- Le categorie da bloccare possono essere selezionate dall'ufficio cantonale di coordinamento tramite www.securepop.ch.
- È possibile richiedere la categoria di un determinato URL ed esigere una nuova classificazione delle categorie.
-

Filtering di contenuti web con codifica SSL
In linea di massima vi è la possibilità di filtrare anche il traffico con codifica SSL. Questo è necessario ad esempio per forzare la funzione SafeSearch nel caso di determinati gestori di motori di ricerca. In questo caso è necessaria l'installazione capillare di un certificato Client su tutti i rispettivi terminali.

Anonymizer Proxy
In internet ci sono server (Anonymizing Proxies) il cui scopo è quello di aggirare un filtro URL e quindi consentire l'accesso a pagine che in realtà sono bloccate. In linea di massima vi è la possibilità di bloccare questi proxy anonimi.

Nuova classificazione di contenuti web
La banca dati di Web Filtering contiene valori aggiornati costantemente per miliardi di siti web in tutto il mondo. Ma non è possibile evitare alcune lacune cosicché può succedere che singoli siti web vengano classificati erroneamente. In questo caso è possibile effettuare una nuova classificazione. Una nuova classificazione può essere effettuata tramite www.securepop.ch o direttamente via http://www.zscaler.com/sitereview/

Autenticazione basata su indirizzi IP
Per diverse offerte web è necessario identificarsi tramite l'indirizzo Source IP. Se l'accesso a tali offerte ha luogo tramite Web Filtering occorre informare il rispettivo operatore in merito all'autorizzazione dei seguenti ambiti dell'indirizzo IP.

195.65.152.0/24
195.65.154.0/24

Nota: questo vale nel caso in cui l'accesso all'offerta ha luogo effettivamente tramite Web Security Proxy.