Linee guida per la sicurezza informatica nelle scuole

Documento redatto dal SAIIT in collaborazione con la società Getronics

1. Premessa

Le istituzioni scolastiche italiane si trovano ad affrontare i riflessi dei notevoli cambiamenti che stanno interessando ed interesseranno il sistema informativo del MIUR. Da un paio di anni a questa parte le scuole rappresentano infatti i principali fruitori delle funzioni e dei servizi informatici del ministero, anche a seguito del decentramento operativo deciso dall'amministrazione che ha ridisegnato la stessa attività degli uffici periferici. Le applicazioni del sistema informativo sono ormai da diverso tempo disponibili via internet attraverso un'area riservata presente sul sito web dell'amministrazione, la quale diventerà presto l'unica modalità di fruizione, nel momento in cui sarà completato il dispiegamento di collegamenti internet ADSL presso ogni istituzione scolastica, in sostituzione delle vecchie linee ISDN.

Nella descrizione di questo scenario vanno inoltre considerate le iniziative di innovazione, anche collegate agli aspetti didattici, portate avanti autonomamente dalle scuole, che sono sempre più impegnate, attraverso un uso intelligente della tecnologia, nella messa a disposizione di servizi avanzati tramite la rete internet alla comunità dei propri utenti, che possono così sperimentare nuove modalità di interazione.

La situazione sin qui descritta, che vede l'esistenza, presso la scuola, di connessioni "always on", non può che porre l'accento sulle problematiche di sicurezza dei collegamenti e sulla protezione delle informazioni custodite all'interno dei sistemi. Questo aspetto, considerando l'ancora elevata eterogeneità di informatizzazione e di padronanza degli strumenti tecnologici da parte delle scuole italiane, merita un alto livello di attenzione e richiede la necessità di uno sforzo aggiuntivo, da parte dell'amministrazione, per fornire linee guida e strumenti che possano aiutare gli istituti scolastici a gestire le proprie esigenze di sicurezza. Alla prima realizzazione di un WBT sulla sicurezza informatica, a disposizione delle scuole e consultabile sul sito TRAMPI, (www.trampi.istruzione.it), fa seguito questo documento che ha lo scopo di fornire un set di concetti di base validi per ogni situazione, degli approfondimenti sugli strumenti tecnici disponibili, ed alcuni semplici casi di studio più direttamente legati alla realtà scolastica. Un sintetico elenco della normativa in materia ed un insieme di link a siti di riferimento completano il documento che si vuole caratterizzare come un agile strumento di consultazione.

2. La sicurezza delle informazioni

L'informazione è una componente fondamentale per l'attività di ogni istituzione e, conseguentemente, deve essere adeguatamente protetta. La sicurezza informatica protegge l'informazione nei confronti di un'ampia gamma di attacchi potenziali al fine di garantire la continuità dell'attività e minimizzare i danni e le interruzioni di servizio.

La sicurezza delle informazioni è caratterizzata dai seguenti aspetti:

- ✓ *Confidenzialità*: garantisce che l'informazione è accessibile solamente a coloro che hanno l'autorizzazione ad accedervi;
- ✓ *Integrità*: garantisce l'accuratezza e la completezza dell'informazione e dei metodi di elaborazione;
- ✓ *Disponibilità*: garantisce che gli utenti autorizzati possano accedere all'informazione quando vi è necessità.

La sicurezza delle informazioni è realizzata attraverso l'attivazione di politiche specifiche, strutture organizzative, procedure, funzionalità software ed è completata da un sistema di controlli.

E' importante sottolineare un principio che deve stare alla base della sicurezza di ogni organizzazione: la corretta separazione dei ruoli fra i responsabili della gestione della sicurezza e gli utenti operativi.

La definizione dei requisiti di sicurezza per un'organizzazione deriva da:

- ✓ valutazione del rischio cui possono essere esposti i beni dell'amministrazione con i potenziali danni che ne derivano; tale valutazione consiste in un'attività sistematica volta a considerare l'impatto sulle attività istituzionali, derivante da carenze o violazioni del sistema di sicurezza in termini di perdita di confidenzialità, integrità o disponibilità del sistema informativo. I risultati della valutazione portano a definire le azioni e le priorità di intervento nelle fasi di realizzazione dei sistemi di sicurezza e dei relativi controlli;
- ✓ quantificazione ed accettazione del cosiddetto "rischio residuo" cioè il rischio non coperto dai sistemi di sicurezza o da strumenti/sistemi non tecnologici (es. norme, assicurazioni, …);
- ✓ individuazione dell'insieme dei requisiti legali, regolamentari e contrattuali a cui l'istituzione ed i suoi fornitori devono far fronte.

3. Politiche di sicurezza

Una policy di sicurezza è una dichiarazione generale, prodotta dal responsabile della sicurezza che definisce le regole per la corretta gestione della stessa. Le politiche di sicurezza costituiscono il blocco di partenza da cui raggiungere qualsiasi obiettivo di information security che sia realmente efficace e rappresentano quindi un indispensabile strumento di supporto alla gestione. Le politiche di sicurezza sono usate come un punto di riferimento per una vasta varietà di attività di information security che includono: progettazione di controlli interni alle applicazioni, definizione delle regole per il controllo degli accessi, esecuzione dell'analisi del rischio, formazione degli utenti per un corretto utilizzo degli strumenti a disposizione ed altro.

3.1. Politiche di Sicurezza del Ministero per le scuole

Gli obiettivi che si vogliono conseguire sono di garantire, in accordo con le leggi e le regole interne:

a) per le risorse tecnologiche:

- la disponibilità del servizio in una forma adeguata, anche a fronte di eventi eccezionali, tramite la formulazione di appropriati piani di recupero delle funzionalità del sistema;
- la continuità del servizio a copertura delle esigenze operative della scuola.

b) per i dati:

- la riservatezza delle informazioni;
- l'integrità delle informazioni;
- la correttezza delle informazioni ritenute critiche per le eventuali conseguenze derivanti da una loro alterazione;
- la disponibilità delle informazioni e delle relative applicazioni.

Di seguito si riporta un elenco di regole che può essere adottato per garantire un livello di sicurezza modulabile:

- chiunque, dipendente o persona esterna, impieghi *risorse informatiche* della scuola deve essere espressamente autorizzato da un responsabile appositamente designato;

- le autorizzazioni devono garantire che sulle informazioni possano intervenire solo le persone abilitate e ciascuna nei limiti delle proprie competenze;
- le autorizzazioni vengono definite in accordo con le leggi, le norme interne e il livello di riservatezza e importanza delle informazioni;
- chiunque autorizzi un dipendente o una persona esterna all'impiego di *risorse informatiche* della scuola deve essere chiaramente individuabile;
- le informazioni sono protette in accordo con la loro criticità, sia nei sistemi ove risiedono, sia nei trasferimenti da un sistema ad un altro;
- le autorizzazioni per l'accesso ai dati e alle applicazioni sono di responsabilità del proprietario dell'informazione;
- le autorizzazioni per l'accesso alle risorse tecnologiche (hardware e software di base e di ambiente) sono in carico al responsabile dell'infrastruttura informatica all'interno della scuola;
- le modalità di gestione delle autorizzazioni sono concordate dallo stesso con il proprietario dell'informazione;
- è consentita la delega delle operazioni di gestione delle autorizzazioni a condizione che siano definite ed implementate procedure organizzative e modalità tecniche che impediscano che il raggiungimento degli obiettivi di sicurezza venga compromesso;
- sono predisposte opportune procedure tecniche ed organizzative per il sollecito ripristino del servizio a fronte di guasti o malfunzionamenti.

Per *risorse informatiche* da considerare nell'ambito della sicurezza, ci si riferisce a:

- dispositivi tecnologici (computer, terminali, linee di comunicazione, ...) il cui danneggiamento fisico può comportare l'interruzione del corretto funzionamento e la conseguente sospensione del servizio
- sistemi operativi o prodotti software la cui modifica, cancellazione o indisponibilità può comportare l'interruzione del funzionamento e la conseguente sospensione del servizio oppure può comportare la possibilità di accesso e manomissione di dati riservati da parte di personale non autorizzato
- programmi applicativi la cui modifica o cancellazione può compromettere l'esercizio di alcune funzioni del sistema informativo o alterarne le corrette caratteristiche di funzionamento
- dati per i quali si richiedono riservatezza, integrità e disponibilità.

3.2. Politiche di Sicurezza Fisica

La Sicurezza fisica si realizza attraverso la protezione delle aree dedicate agli strumenti, specifici o di supporto, per l'elaborazione, la conservazione e la distribuzione delle informazioni.

Gli obiettivi che si vogliono conseguire sono:

- -salvaguardare l'integrità fisica delle persone e l'integrità fisica e funzionale di apparati e locali;
- -evitare che un'operazione non ammessa provochi un danno significativo per la scuola o per i soggetti che interagiscono con essa.

Le Politiche di Sicurezza Fisica sono espresse dalle seguenti norme:

- le caratteristiche dei locali utilizzati devono essere commisurate all'importanza delle risorse da proteggere
- l'accesso ai locali deve essere limitato alle persone abilitate e deve esistere un sistema di monitoraggio degli accessi
- nessuno può utilizzare una attrezzatura critica per la sicurezza se non autorizzato
- nessuno può rimuovere od introdurre attrezzature o altri componenti informatici senza uno specifico documento di autorizzazione
- devono esistere procedure che descrivano l'uso degli impianti ausiliari (condizionamento, alimentazione elettrica, antincendio, etc.) in condizioni normali ed in condizioni di emergenza; il personale deve essere istruito al riguardo gli impianti ausiliari devono essere periodicamente sottoposti a collaudo.

3.3. Politiche di Sicurezza Logica

La sicurezza logica si realizza attraverso la protezione del patrimonio informatico mediante soluzioni, sia hardware che software, rese operative dal sistema informatico stesso.

Gli obiettivi che si vogliono conseguire sono:

- controllo degli accessi alle risorse informatiche a salvaguardia da intrusioni ed attacchi interni ed esterni, sicurezza nella memorizzazione e trasmissione
- disponibilità del servizio
- disponibilità di informazioni che consentano di indagare su possibili violazioni

- controllo del riutilizzo supporti.

Le Politiche di Sicurezza Logica sono espresse dalle seguenti norme:

- l'identità dell'utente deve essere certificata
- ogni servizio richiesto viene reso disponibile solo se previsto dalle autorizzazioni dell'utente
- si deve tenere opportuna traccia scritta delle operazioni individuate come critiche
- tutti i dati critici devono essere memorizzati e trasmessi in modo sicuro
- tutti i dati e le operazioni relativi alla gestione della sicurezza devono essere considerati critici
- tutti i supporti riutilizzabili su cui sono stati memorizzati dati riservati devono essere opportunamente trattati prima del loro rilascio in modo che non si possano da essi desumere informazioni significative
- il funzionamento delle applicazioni deve essere sempre ripristinabile a fronte di eventuali danneggiamenti.

3.4. Responsabilità generali

Le responsabilità, in termini di sicurezza, delle risorse informatiche sono suddivise nei seguenti termini generali:

- ✓ per quanto riguarda le strutture informatiche comuni (sistema di elaborazione centrale, reti di telecomunicazioni, server), le responsabilità fanno capo alla struttura deputata alla gestione dei sistemi informativi;
- ✓ per quanto riguarda le risorse informatiche che fanno capo alle singole unità operative (es. personal computer), il capo di ogni unità operativa è individuato come responsabile delle proprie risorse.

In entrambi i casi l'attuazione della protezione deve seguire le linee guida descritte negli specifici documenti di policy di sicurezza all'interno dell'organizzazione.

Ogni dipendente è responsabile dell'utilizzo delle risorse informatiche a lui assegnate ed utilizzate per l'espletamento della propria attività.

Le responsabilità nell'ambito della sicurezza dei sistemi informativi oltre che avere una valenza in termini di tutela del patrimonio ed in termini di tutela degli operatori e dei gestori, assume, alla luce del recente codice sulla privacy, anche una valenza giuridica.

3.5. Classificazione delle informazioni

La classificazione delle informazioni costituisce l'attività basilare per la valutazione del rischio e quindi del potenziale danno che un loro non corretto utilizzo può apportare al patrimonio informativo della scuola o di enti con cui essa interagisce.

La classificazione non deve essere riferita ai soli dati informatici, ma deve essere estesa a tutte le tipologie di informazioni e di documenti che li contengono oltre che ai programmi che li trattano indipendentemente dalla tipologia dei supporti su cui vengono memorizzati e registrati; per cui occorre prendere in considerazione anche le stampe, le linee di comunicazione, i documenti contenenti informazioni che non derivano direttamente da elaborazioni informatiche, ect. E perciò necessario prevedere un'opportuna classificazione delle informazioni sulla base del livello di riservatezza delle stesse.

3.6. Incidenti e violazioni

Ogni scuola deve attivare opportune procedure per minimizzare il rischio derivante da violazioni delle misure di sicurezza e per garantire un'adeguata e tempestiva segnalazione dei reali o sospetti incidenti o violazioni.

Un incidente, nell'ambito della sicurezza dei sistemi informativi, è un evento, un evento sospetto od una vulnerabilità tale da violare l'integrità, la confidenzialità o la disponibilità delle applicazioni o dei dati del sistema; nel caso di individuazione o di sospetto riguardante un incidente deve essere data immediatamente segnalazione alle strutture preposte.

3.7. Programmi e software pericolosi (virus informatici)

Per minimizzare i rischi derivanti dall'introduzione di programmi (virus informatici) e/o software pericolosi, devono essere attivate e strettamente seguite le opportune misure di sicurezza al fine di individuare tempestivamente infezioni virali, eliminarne gli effetti e bloccarne la diffusione. Data la natura del fenomeno è fondamentale, oltre che attenersi alle norme operative diramate, dare immediata

informativa alla struttura preposta alla gestione della sicurezza nel caso di individuazione o sospetto di casi relativi ad infezione da virus informatici.

4. Il nuovo Sistema Informativo e i rischi connessi all'accesso alla rete Internet

4.1. Premessa

In questo paragrafo vengono elencati rapidamente alcuni dei rischi indotti dalla presenza nelle scuole di collegamenti permanenti alla rete internet, come nel caso delle linee ADSL recentemente installate presso le segreterie scolastiche a carico del MIUR. Vengono quindi individuate le più comuni contromisure tecniche adottabili per garantire l'operatività delle infrastrutture informatiche ed assicurare il livello di sicurezza minimo ritenuto adeguato alle proprie esigenze. Uno dei principi basilari da tenere in mente, nella definizione delle politiche di sicurezza e nella scelta degli strumenti tecnologici di supporto è quello relativo alla proporzionalità dei costi. In generale infatti la spesa per assicurare il necessario livello di protezione dovrebbe essere inferiore al costo da sostenere per il recovery dei danni a seguito di un attacco subito. In altre parole, tenendo anche conto delle scarse risorse a disposizione della scuola per gli investimenti in tecnologie, la spesa per la sicurezza ed i meccanismi adottati dovranno sempre essere attentamente dimensionati, evitando il ricorso a tecnologie troppo sofisticate, costose e difficili da amministrare. Vale la pena ricordare che nella quantificazione del potenziale danno vanno considerati, oltre al valore economico, anche elementi a volte trascurati come, ad esempio, la reputazione, l'affidabilità ed in genere l'immagine dell'istituzione scolastica.

A questo proposito il MIUR, con il progetto FORTIC, ed in particolare con i docenti che supereranno con profitto i corsi relativi al profilo C, ha inteso supportare la formazione di figure che possano, con buona padronanza, affrontare questo tipo di problematiche all'interno della scuola, evitando, per quanto possibile, il ricorso alle prestazioni di professionalità esterne.

I rischi sono stati suddivisi molto semplicemente in esterni ed interni, a seconda della provenienza della minaccia. Contrariamente a quanto ci si potrebbe aspettare è stato dimostrato che molto spesso gli attacchi più seri e dannosi provengono dall'interno e sono opera di soggetti che conoscono la struttura della rete e dei servizi su di essa veicolati ed hanno avuto accesso, magari per le funzioni ricoperte, ai principali sistemi di elaborazione.

4.2 Rischi esterni

- Accessi non desiderati: la connessione permanente ad Internet sottopone alla possibilità di accessi alla rete interna da soggetti estranei e non autorizzati, esponendo le postazioni di lavoro e i dati in esse contenuti a rischio di manomissione o sottrazione;

- Virus: la navigazione Internet e ed il servizio di posta elettronica sono i principali veicoli di diffusione dei virus. I rischi connessi al contagio da virus informatico sono la perdita dei dati, l'accesso agli stessi da parte di soggetti estranei e non autorizzati, il blocco dei PC o di altri dispositivi connessi alla rete, il sovraccarico della stessa;
- E-MAIL Spamming: con questo nome si intendono le problematiche legate alla ricezione di un traffico di e-mail fasulle, non richieste e non sollecitate; tale rischio se non gestito può provocare :
    1. blocco dei server di posta elettronica
    2. aumento del traffico di rete e relativo sovraccarico con rallentamento delle applicazioni e relativi disservizi;
- Intercettazione dei dati: i dati trasmessi da un PC prima di giungere a destinazione attraversando la rete Internet, per definizione pubblica e non protetta, vengono gestiti da diversi apparati. Esiste quindi la possibilità che i dati vengano intercettati lungo il cammino e modificati oppure soltanto letti, con evidente violazione della privacy e dell'integrità degli stessi.
- Denial Of Service (DOS): utilizzando diverse tecniche, anche in coordinamento con altri soggetti attaccanti, è possibile per un malintenzionato far sì che un servizio, (come ad esempio il sito web istituzionale), divenga non più disponibile agli utenti autorizzati.

4.3 Rischi interni

- Trasmissione illecita di dati attraverso Internet: è possibile che chi ha ottenuto accesso a dati sensibili o riservati li possa trasmettere su Internet a soggetti non autorizzati a ricevere/manipolare quei dati;
- Navigazione su siti Internet con contenuti offensivi e/o forti o comunque non pertinenti con l'attività lavorativa: la navigazione libera su Internet dovrebbe essere sottoposta a filtraggio evitando che dalla rete interna si possano raggiungere siti con contenuti ritenuti non pertinenti;
- Traffico non consentito: la navigazione "libera" in Internet può interferire pesantemente con le attività istituzionali: lo scarico/scambio di immagini, di file musicali e video, (attraverso i così detti meccanismi di peer to peer), se non regolamentato finisce inevitabilmente col sovraccaricare la rete. Sono possibili politiche che vanno dal non consentire traffico al di fuori del necessario per l'attività lavorativa a politiche che restringano tali attività limitandole ad esempio a determinate fasce orarie o, più efficacemente adottando strumenti di partizionamento del traffico che, in modo automatico assegnano alle attività istituzionali la capienza di banda necessaria penalizzando gli accessi "liberi".

- Manomissione, danneggiamento di sistemi, apertura di back door. Qualora il personale deputato all'amministrazione dei sistemi lasci la scuola sarà necessario revocare immediatamente tutte le autorizzazioni e provvedere alla generazione di nuovi account. In caso contrario eventuali malintenzionati potrebbero sfruttare le conoscenze acquisite, nello svolgimento delle attività lavorative, per acquisire il controllo dei sistemi dall'esterno o in generale per provvedere al loro danneggiamento o manomissione, compromettendone anche le informazioni contenute al loro interno.

4.4 . L'organizzazione per la sicurezza

Prima di addentrarsi nell'esame degli strumenti tecnici a disposizione nell'ambito della sicurezza informatica è importante sottolineare, ancora una volta, la necessità di un cambiamento di tipo culturale e di un nuovo approccio alle problematiche poste dall'utilizzo di sistemi informativi connessi in rete. La consapevolezza dei rischi in gioco, ottenuta attraverso la sensibilizzazione ed il coinvolgimento di tutti gli utenti dei sistemi informativi, insieme con una corretta organizzazione che guardi prima ai processi e poi ai prodotti, costituiscono infatti le premesse indispensabili per ottenere buoni risultati. La tecnologia da sola non è sufficiente. Un importante punto di riferimento in materia è costituito dalla direttiva del Ministro per l'Innovazione del 16 gennaio 2002 in materia di sicurezza. Essa prevede e descrive le attività per posizionarsi su di un livello di sicurezza individuato come "base minima", da cui partire per ulteriori iniziative di miglioramento. La direttiva suggerisce inoltre un modello per la gestione della sicurezza, da adattare alla realtà di ogni amministrazione che prevede essenzialmente i seguenti passi:

- definizione delle strategie generali (politiche);
- formalizzazione delle procedure e delle regole;
- controllo del rispetto delle norme (auditing);
- gestione dei problemi di sicurezza (incident management);

4.5. Le contromisure di tipo tecnico

Al fine di minimizzare i rischi e gli effetti di attacchi informatici sono oggi a disposizione sul mercato svariate contromisure di tipo tecnico. Le contromisure sotto elencate sono coerenti con le politiche di sicurezza del Ministero.

La tecnologia offre una vasta gamma di strumenti di sicurezza informatica mirati a contrastare ciascuna delle vulnerabilità o dei rischi legati all'utilizzo di postazioni di lavoro in rete, (sia essa Intranet o Internet). Di seguito si indicano alcuni degli strumenti e delle tecnologie più comuni.

4.5.1 Firewall

Il Firewall e' un sistema che va posto al "confine" tra la rete locale interna e la rete Internet, in modo che tutto il traffico entrante ed uscente dalla rete interna sia costretto a transitare attraverso il firewall stesso. In tal modo le singole unità di traffico, i pacchetti, possono essere esaminate applicando la politica di sicurezza più adeguata. Il firewall realizza quindi una specie di 'barriera telematica' contro qualunque accesso non autorizzato in modo da proteggere il sistema locale da ogni indebita intrusione.

Una delle tipologie più comuni di firewall e quella così detta “Packet Filtering”. In questa configurazione il firewall controlla ogni pacchetto che transita e lo confronta con le regole che ha memorizzate per consentirne o meno il passaggio. Tale filtraggio viene effettuato specificando, protocollo per protocollo, le regole di accettazione o di rifiuto dei pacchetti associati. Le regole possono essere definite in modo molto flessibile. E’ ad esempio possibile inibire completamente il traffico proveniente da determinate sottoreti o soltanto da alcune macchine ben individuate; sarà possibile bloccare o abilitare singoli protocolli di rete scegliendo anche la direzione consentita.

Ad ogni modo la policy implementata sul firewall dovrebbe rispondere ai seguenti principi generali:

- Tutto il traffico deve essere proibito ad eccezione di quello esplicitamente permesso attraverso la compilazione delle rispettive regole;
- Il traffico permesso deve essere lo stretto necessario per permettere la normale operatività;
- Gli indirizzi di rete dei personal computer sulla rete interna devono essere mascherati e resi invisibili all’esterno della rete (NAT), al fine di garantirne maggiormente la sicurezza;
- deve esistere la possibilità di cifrare il traffico di rete, laddove necessario, mediante l’utilizzo di opportuni protocolli;

L’apparato firewall va posizionato nel segmento di rete tra il router di accesso ad Internet e la rete interna in modo che possa verificare tutto il traffico destinato o proveniente da reti esterne (Internet).

Il firewall deve essere configurato per tenere traccia del traffico analizzato, tramite file di log, per successive indagini.

4.5.2 Antivirus Gateway

Permette di esaminare il traffico generato dalla navigazione internet e dalla posta elettronica alla ricerca di eventuali Virus Informatici. Il server Antivirus Gateway si posiziona all’interno della LAN, ed opera, per il riconoscimento, sulla base di un archivio contenente le firme dei virus correntemente identificati. In caso di positività

viene in genere inviato un allarme all'amministratore della sicurezza e, opzionalmente, all'utente. In genere l'elemento pericoloso viene rimosso o, nel peggiore dei casi, il messaggio infetto viene cancellato.

L'aggiornamento delle firme dei virus o dei trojan deve poter essere effettuata in maniera automatica e preferibilmente senza la supervisione di un operatore.

4.5.3 Sistema Antivirus

Il sistema antivirus permette di contrastare l'infezione dei PC da parte di virus informatici e trojan. Il sistema, nella sua architettura più articolata, si compone di una componente software server e di una componente client. La parte server deve essere installata su hardware dedicato e permette la gestione centralizzata della parte client. La parte client deve essere installata sui PC della rete interna e deve proteggere lo spazio disco dei PC dall'infezione di virus conosciuti.

La postazione server dovrebbe permettere di individuare facilmente quali postazioni sono infette ed eventualmente tentare di rimuovere l'infezione. Inoltre deve essere possibile da questa postazione inviare in maniera automatica e programmata gli aggiornamenti alle stazioni di lavoro connesse in rete.

L'aggiornamento del database delle firme dei virus sul server centrale deve essere automatico e provenire direttamente dal sito del produttore.

4.5.4 URL Filtering

Si tratta di soluzioni software che consentono il filtraggio delle pagine web richieste dall'utente bloccando quelle che puntano a siti con contenuti ritenuti non idonei. L'elenco dei siti non permessi, la così detta "black list" di navigazione, viene generalmente suddiviso in categorie (ad es. cinema, news, contenuti per adulti, chat, ecc.) e deve essere aggiornato in maniera periodica.

Le categorie proibite o permesse potranno tener conto di diversi fattori legati alla sensibilità degli utilizzatori, all'utilità e alla pertinenza dei contenuti con l'attività svolta. Potrà essere lasciata facoltà a particolari gruppi di utenti di visitare categorie di siti proibite ad altri e viceversa. Questo meccanismo richiede quindi che il filtraggio sia basato anche sull'identificazione dell'utente che sta navigando.

4.5..5 VPN - (Virtual Private network)

Consente di cifrare e contrassegnare i messaggi in maniera elettronica in modo che siano inintelligibili a chi è estraneo alla comunicazione e che sia possibile rivelare eventuali manomissioni del messaggio. Grazie opportuni algoritmi è possibile identificare reciprocamente il mittente ed il destinatario della comunicazione. In generale non è difficile configurare una VPN tra due sistemi tramite l'utilizzo del protocollo IPSEC, che va opportunamente configurato su entrambi gli host. Un'alternativa all'utilizzo di tale protocollo può essere il ricorso a prodotti di terze parti, basati solitamente su protocolli proprietari e venduti sotto forma di pacchetti

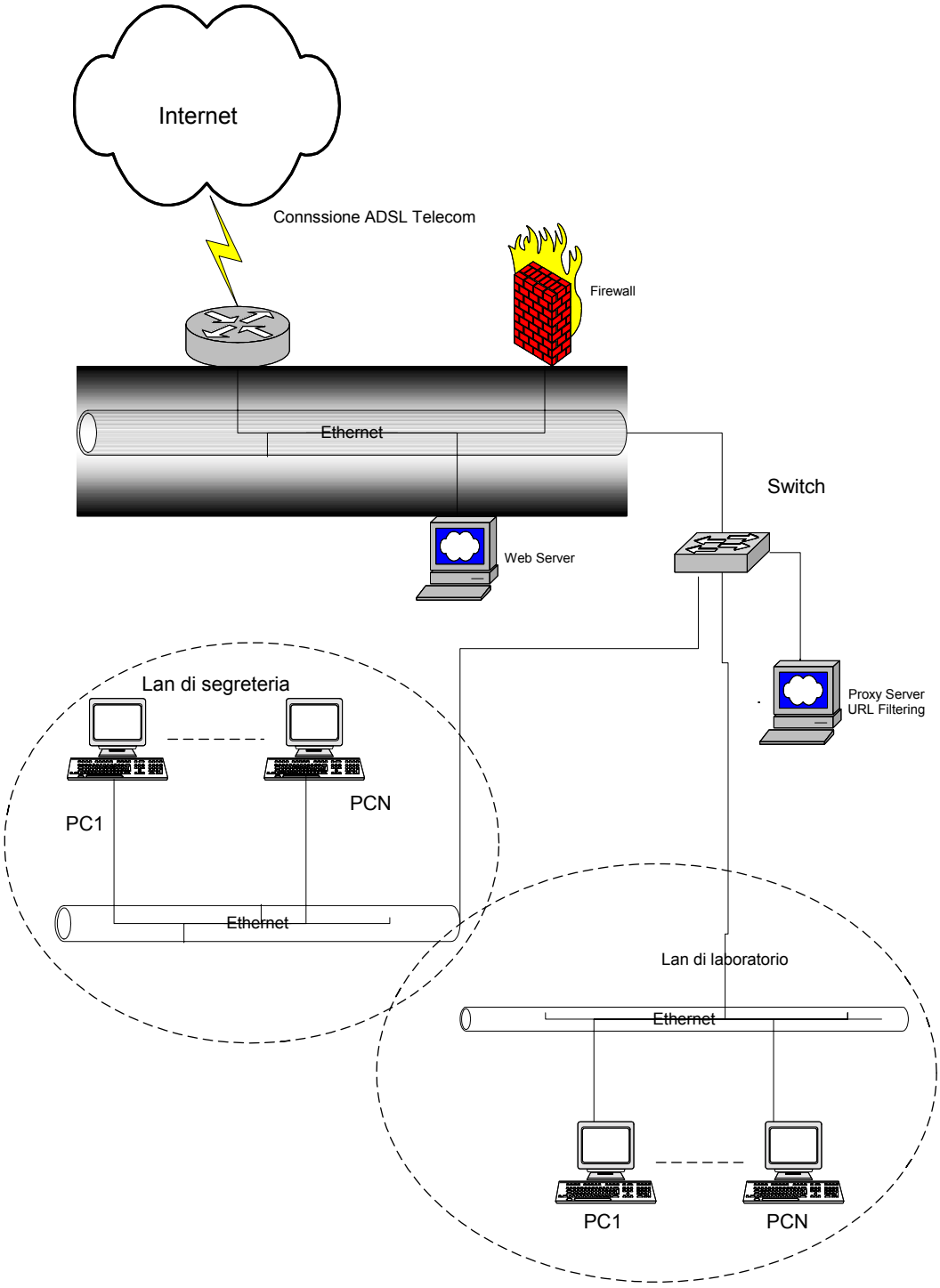
software da installare sulle entità che devono comunicare o come componenti hardware.

5. Casi di Studio

In questo paragrafo vengono riportati alcuni casi di studio con lo scopo di fornire indicazioni pratiche alle istituzioni scolastiche su come organizzarsi per garantire un livello minimo di sicurezza nell'ambito degli scenari ipotizzati. Gli esempi sviluppati si manterranno ad un livello di descrizione logica, senza entrare in dettagli tecnici approfonditi che richiederebbero una trattazione molto più complessa che esula dalle finalità di questo documento. Naturalmente visto la varietà delle situazioni e delle dotazioni tecnologiche presenti nelle scuole non si ha la pretesa di essere esaustivi, ma si intende fornire uno spunto di riflessione che faccia da base di partenza per determinare ed affinare la soluzione personalizzata sulla base delle esigenze della scuola.

Scenario N.1 – Scuola monosede collegata ad internet esclusivamente tramite la linea ADSL fornita dal MIUR

Questo scenario descrive una scuola che abbia limitate esigenze di connettività alla rete internet, interamente soddisfabili tramite il collegamento recentemente fornito dal MIUR in modalità ADSL o analogo collegamento già in dotazione alla scuola. Si suppone la connessione di una piccola Lan di segreteria ed opzionalmente di un laboratorio scolastico. La figura seguente riporta lo schema logico della rete:



E' possibile sulla base del precedente schema formulare alcune osservazioni:

- E' opportuno segmentare la rete sia per ragioni di prestazione che per separare il traffico ed evitare interferenze fra i due ambienti di segreteria e di laboratorio didattico. Questo può essere facilmente ottenuto con uno switch che dovrà essere dimensionato sulla base delle postazioni collegate in rete;
- L'utilizzo di un firewall a protezione della rete interna contribuisce anche alla creazione di una così detta "demilitarized zone" che può essere utilizzata dalla scuola per esporre su internet propri servizi come ad esempio un server

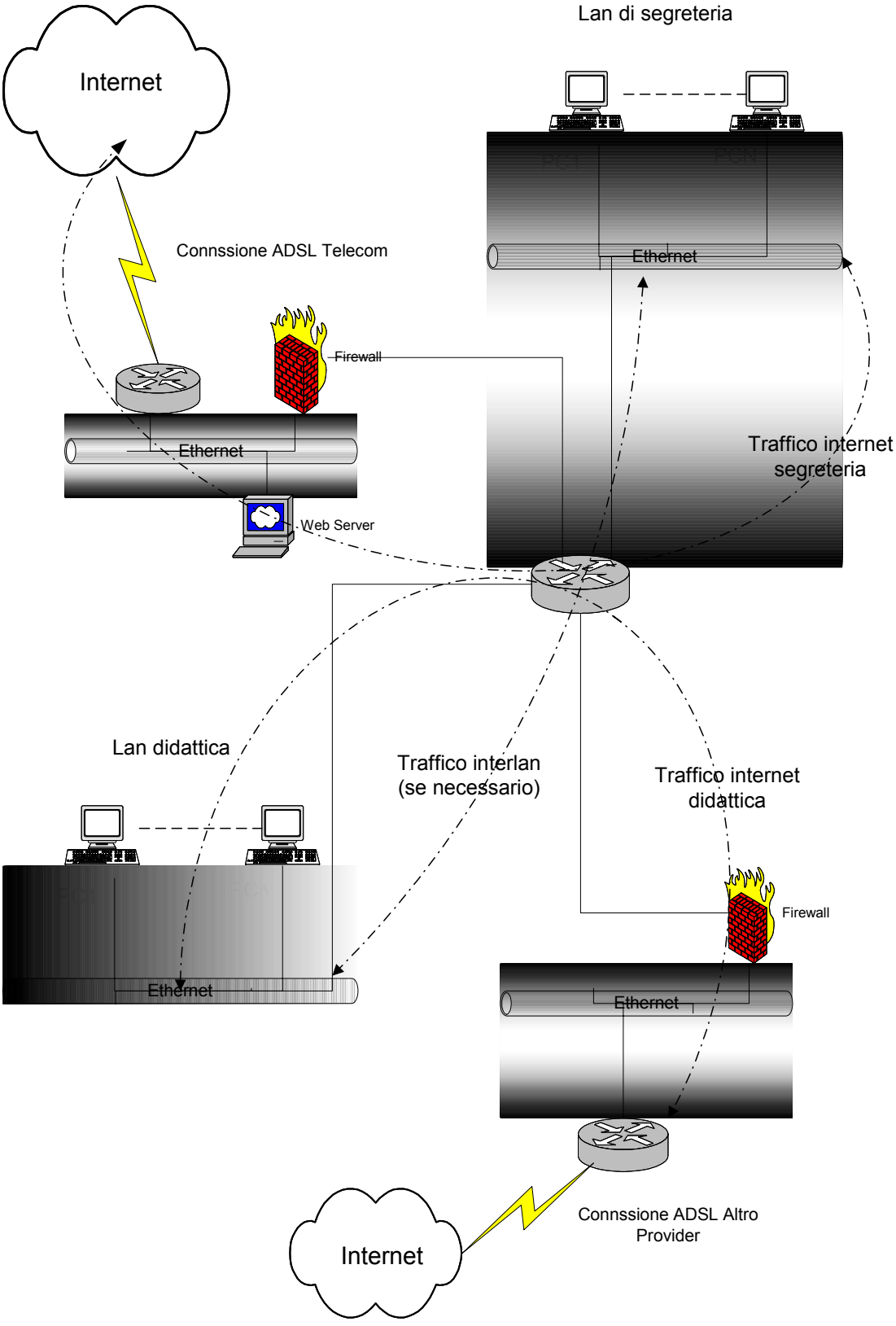
contenente il proprio sito web (allo stato attuale del progetto questo non è ancora possibile);

- Come principio generale è bene disabilitare tutti i protocolli non strettamente necessari; si può ipotizzare il transito dei protocolli http, https, ftp, smtp, nntp per garantire i principali servizi internet, così come l'abilitazione di particolari numeri di porta, oltre a quelli standard, che siano utilizzati da specifici servizi applicativi. Ogni altra esigenza dovrà essere espressamente valutata analizzando aspetti positivi e negativi;
- Da notare che i parametri relativi ai servizi di risoluzione degli indirizzi (DNS) e posta elettronica saranno forniti sulla base delle indicazioni del provider di connettività internet.

Una possibile variante allo schema proposto si può applicare prevedendo l'utilizzo di un proxy server che regoli l'accesso ai servizi internet. Si ricorda che un sistema del genere, funzionando anche da memoria cache per la navigazione web, contribuisce all'aumento della velocità di navigazione, potendo restituire all'utente le pagine richieste già presenti nella propria memoria senza necessità di richiederle all'esterno. Il server proxy può essere utilizzato anche in combinazione con un apposito software di filtraggio degli indirizzi internet, per la protezione della navigazione su siti a contenuto sconveniente.

Scenario N.2 – Scuola di grandi dimensioni con due o più uscite sulla rete internet con provider diversi

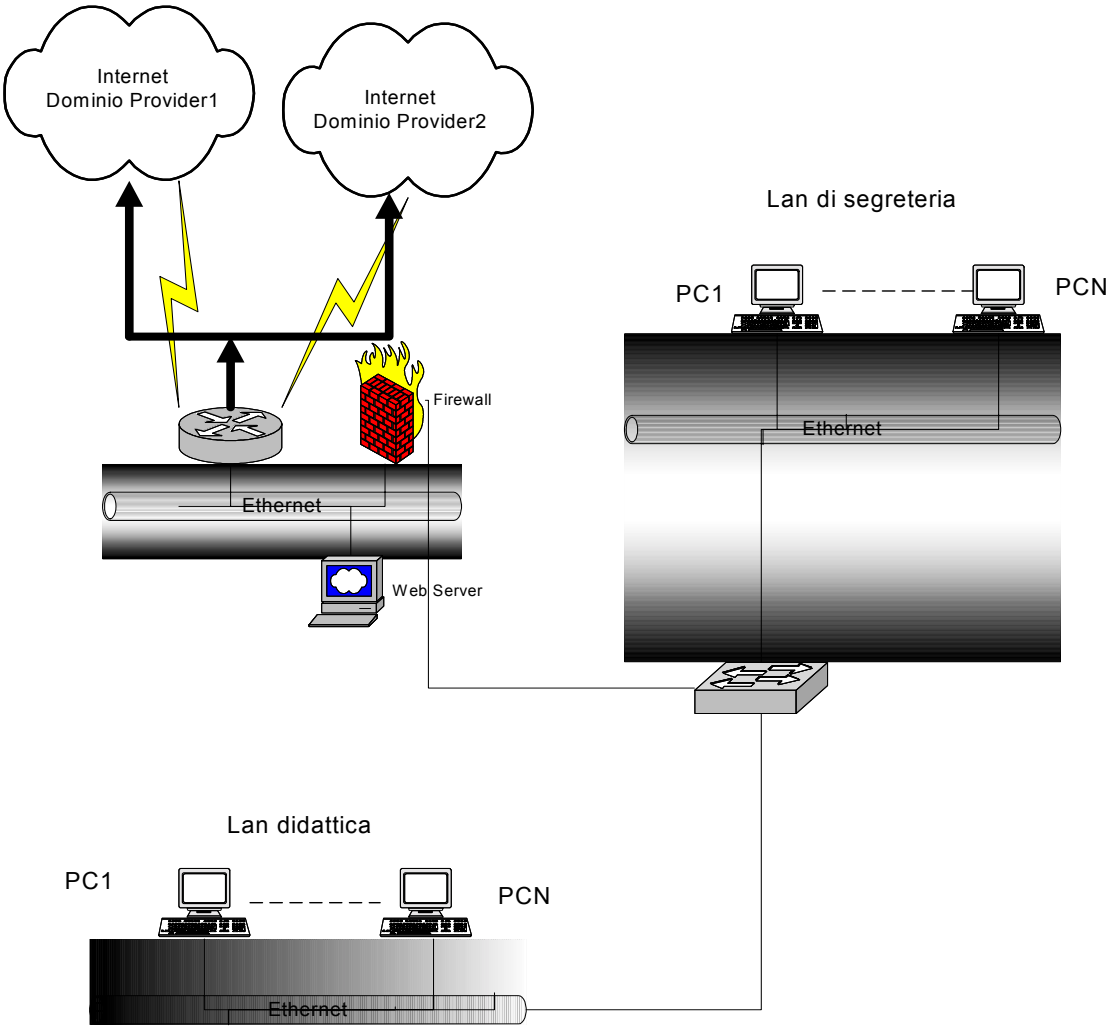
La distribuzione di linee ADSL internet per le segreterie scolastiche ad opera del MIUR si è inserita, in parecchi casi, in una situazione infrastrutturale che vede la presenza di ulteriori collegamenti alla rete, forniti da provider diversi, spesso messi a disposizione dagli enti locali. In questo caso, il mantenimento di entrambi i collegamenti pone problematiche non banali che devono essere correttamente indirizzate. Una prima ipotesi, descritta nella figura seguente prevede l'utilizzo separato delle due connessioni, riservandone una al traffico didattico, (quindi sostanzialmente dei laboratori o delle aule), una al traffico amministrativo (segreteria). Ipotizzando di voler mantenere gli stessi livelli di sicurezza sui due accessi si avrà la necessità di replicare la soluzione architetturale e tecnologica scelta, come indicato in figura:



E' evidente che la situazione descritta risulta onerosa e certamente richiede una gestione complessa. Al fine di minimizzare i costi, soprattutto per la parte firewall, si

può pensare al ricorso ad apparecchiature del tipo “security appliance” . Questo tipo di dispositivi presentano un’installazione semplificata e possono essere resi operativi con poco sforzo, essendo nella maggior parte dei casi configurabili e controllabili in remoto da un centro di controllo, sulla base delle esigenze della scuola stessa. Particolarmente problematica risulta in questo caso la gestione, a carico della scuola, di un proprio server di posta elettronica o del servizio di risoluzione degli indirizzi (DNS).

Un altro possibile approccio, inteso come variante allo scenario presentato è quello di utilizzare le due connessioni internet in bilanciamento di traffico, con selezione, per ogni connessione, del percorso più conveniente per raggiungere il server di destinazione. Questo tipo di scelta richiede comunque l’utilizzo di apparati di rete di fascia medio alta.

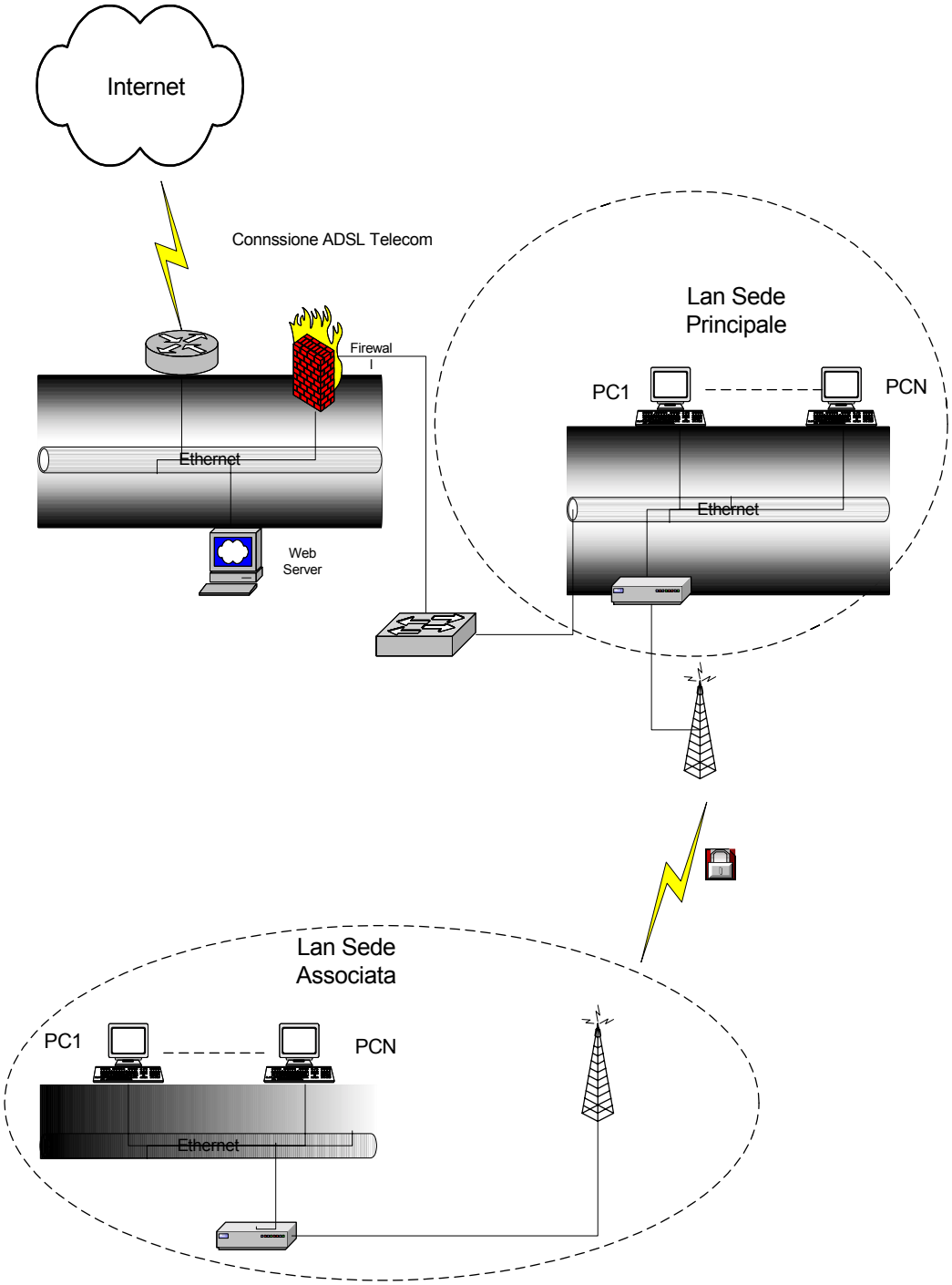


Scenario N. 3 - Scuola di grandi dimensioni costituita da più sedi associate collegate in LAN tra di loro

Una situazione del genere impone, fra le prime questioni da affrontare, la definizione delle modalità di connessione in rete fra le varie sedi, tenendo conto delle esigenze di connettività di ogni singolo plesso e dell'organizzazione dei principali servizi di rete (posta elettronica, file server, directory server ecc.). Tralasciando la possibilità di collegare le varie sedi tramite collegamento dedicato di tipo numerico (CDN), che risulta sicuramente onerosa e poco diffusa nell'ambito delle istituzioni scolastiche verranno esaminate due ipotesi:

- collegamento delle sedi secondarie alla principale tramite tecnologia wireless;
- collegamento di tutte le sedi in rete privata virtuale tramite internet;

La prima ipotesi è raffigurata dalla figura seguente:



In questo caso, qualora si mantenga la connettività verso internet esclusivamente presso la sede principale, valgono le considerazioni già fatte per i casi precedentemente descritti. Particolare accortezza occorre prestare nella protezione del collegamento wireless. Questo può essere facilmente individuato e sfruttato da potenziali aggressori per entrare nella rete dell'istituto scolastico e sfruttarne le risorse disponibili per attività illecite, (es. lanci di attacchi DOS, diffusione di virus e worm ecc.). E' buona regola predisporre in questi casi una comunicazione criptata fra le due sedi che renda estremamente difficile l'intercettazione di password e codici di accesso alle risorse di rete. E' particolarmente attiva in questo campo l'attività di

standardizzazione con l'introduzione di nuovi protocolli di interazione fra cui vale la pena di ricordare il WPA (Wi-Fi Protected Access).

La seconda ipotesi sopra formulata è il collegamento di tutte le sedi della scuola in VPN attraverso la rete internet. Si ricorda brevemente che la rete privata virtuale realizza una modalità di collegamento tra sedi, generalmente remote, che attraverso l'utilizzo di un mezzo intrinsecamente insicuro come la rete internet, mediante l'adozione di opportuni protocolli di comunicazione e di tecniche di cifratura, permette lo scambio di informazioni fra le varie sedi, come se si disponesse di una propria rete privata. Si tratta ovviamente di una modalità complessa di interazione che si giustifica nel caso di più sedi disperse geograficamente e dotata ognuna di collegamento alla rete internet. In questo caso la soluzione più semplice appare quella in cui le funzionalità di VPN siano implementate e configurate all'interno degli apparati di sicurezza adottati presso ciascuna sede e quindi in ultima analisi nei firewall o nei security appliances a seconda delle scelte. Si ricorda che una VPN può anche essere realizzata attraverso le funzionalità messe a disposizione dai moderni router.

6. Conclusioni

In questo documento sono stati forniti alcuni concetti di carattere generale relativi alla sicurezza informatica all'interno delle istituzioni scolastiche, arricchiti da un'analisi più dettagliata di alcuni possibili scenari, facilmente ipotizzabili nella variegata realtà delle scuole italiane. Le problematiche affrontate ed il livello di approfondimento non costituiscono ovviamente un esame esaustivo della varie fattispecie, ma rappresentano piuttosto uno spunto di riflessione ed una base di partenza per chi, all'interno della scuola, cura la gestione della sicurezza e più in generale delle infrastrutture informatiche. A tal proposito emerge in modo molto chiaro la necessità per la scuola di dotarsi di una o più figure di riferimento che, dotate di opportuna e costante formazione, siano in grado di padroneggiare le problematiche qui esposte, e nel contempo sappiano anche interfacciarsi in modo appropriato con i fornitori di soluzioni informatiche ai quali in genere ci si rivolge per l'implementazione delle soluzioni più complesse. L'amministrazione ha già intrapreso un primo significativo passo in questa direzione con il progetto FORTIC ed in particolare con la formazione di figure di profilo C che più si avvicinano alle esigenze di conoscenza ipotizzate. L'augurio è che anche la scuola possa autonomamente complementare queste iniziative valorizzando il personale a propria disposizione per un sempre più consapevole utilizzo delle enormi opportunità offerte dalle tecnologie dell'informazione e della comunicazione.

7. Normativa di riferimento e standards

- Testo Unico "**Codice in materia dei dati personali**" (DLgs 30.6.2003 n. 196, nel seguito T.U.) che ha riunito e semplificato tutta la vigente normativa sulla protezione dei dati personali, ad iniziare dalla Legge 675/96 e dal DPR 318/1999.

- Direttiva 16 gennaio 2002 del Dipartimento per l'innovazione e le tecnologie, sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni; **"Sicurezza nelle tecnologie dell'informazione e della comunicazione"(Direttiva Stanca).**

- Circolare Aipa/CR/32 del 22 giugno 2001 – I dati pubblici: linee guida per la conoscibilità, l'accesso, la comunicazione e la diffusione.

- Raccomandazione Aipa N.1/2000 – Norme provvisorie in materia di sicurezza dei siti internet delle amministrazioni centrali e degli enti pubblici

- Legge 23 Dicembre 1993 n. 547 – introduzione nel codice penale italiano dei crimini di natura informatica

- BS EN ISO17799 - Code of practice for information security management

8. Siti Web di riferimento

Centro Nazionale per l'Informatica	www.cnipa.it
Ministro per l'Innovazione e le Tecnologie	www.innovazione.gov.it
Clusit – Associazione Italiana per la Sicurezza Informatica	www.clusit.it
Osservatorio Tecnologico MIUR	www.osservatoriotecnologico.net
Polizia di Stato	www.poliziadistato.it
Garante della Privacy	www.garanteprivacy.it
Cert Coordination Centre (CERT/CC)	www.cert.org
Internet Security Glossary (RFC 2828)	www.ietf.org