**Prova di simulazione (si omettono tutti gli eventuali approfondimenti sulle varie tecnologie)**

**Ipotesi aggiuntive:**

* Nell’ipotesi che sia biblioteca che APT disponessero solo di una dotazione informatica minimale, si attua una riprogettazione completa della rete relativa
* La rocca sede della biblioteca è soggetta a vincoli di integrità, pertanto sono da escludere opere murarie, ad eccezione dell’**Entrance Facility** per Internet.
* Il municipio risulta dotato di PC ancora adeguati alle esigenze dell’utenza e non si attueranno nuovi acquisti.
* Gli apparati di rete verranno acquistati per l’occasione
* La zona risulta servita da un WISP che fornisce collegamenti business a larga banda
* Il numero di dipendenti/postazioni-fisse risulta essere:
  + 2 presso l’APT
  + 2 per i dipendenti + 2 per gli utenti in biblioteca
  + 15 in Municipio
* La dimensione della rete non sarà soggetta a significative variazioni nel prossimo futuro
* Il flusso di dati generato dagli utenti rientra in un profilo “attività d’ufficio” che non prevede il trasferimento di dati multimediali o la telefonia voip.
* L’amministrazione gestisce anche dati personali e sensibili ( ragion per cui verranno intraprese adeguate misure per la loro protezione)

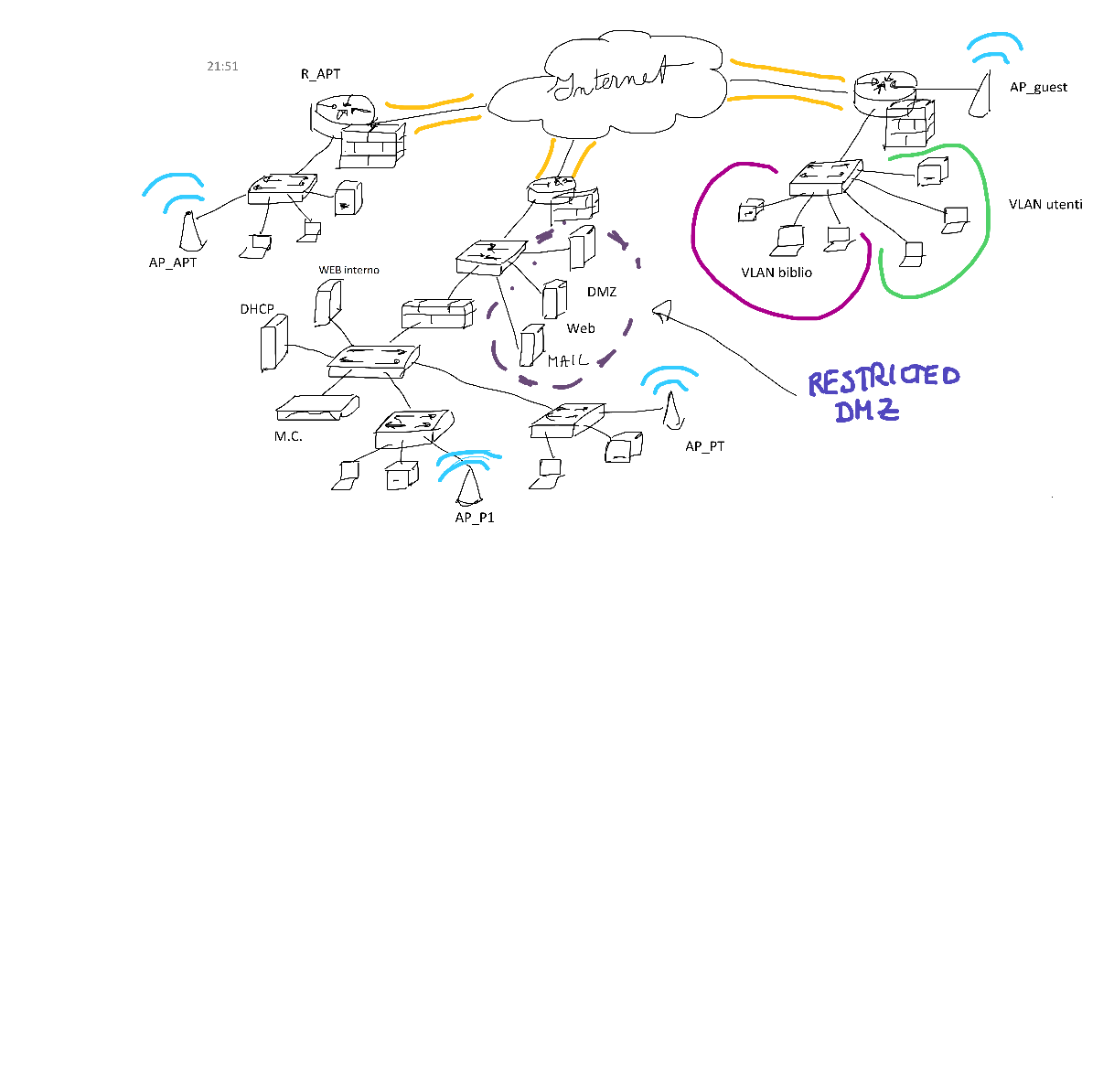
**Prima parte**

1. Il tema proposto prevede la realizzazione (esplicita) di 3 LAN, dislocate, come si desume dalla piantina allegata, alla distanza di poche centinaia di metri.

* La LAN del Municipio sarà basata su tecnologia ethernet (802.3 FE e GE), come pure quella dell’APT.
* Il cablaggio presso la sede APT e Municipio sarà realizzato tramite UTP cat 6 (velocità massima 10GE fino a 55m) e rispetterà gli standard ISO/IEC 11801
* Nella biblioteca si utilizzerà lo standard 802.11n che offre prestazioni confrontabili a FE (o superiore, quale 802.11ac a 800 Mbps nominali).
* Per le LAN cablate e non, sarà necessario acquisire un router con funzione di firewalling incorporata. I router avranno una porta WAN e una porta LAN di tipo FE. Nel caso della biblioteca, dovremo disporre di un’interfaccia FE aggiuntiva per connetterci ad un AP (Access Point) per la rete Guest. La funzionalità di Fail over è richiesta per attivare una connessione a Internet di backup in caso di malfunzionamento di quella primaria.
* Un firewall come appliance separata servirà da ulteriore protezione alla rete del Municipio, con regole di filtraggio più stringenti
* Gli switch di accesso di APT e Municipio (collegati direttamente agli End System) avranno porte GE, in numero di 8 e non occorrerà il Management. Lo switch della biblioteca supporterà le VLAN con standard 802.1q (tagging) per separare il traffico dei dipendenti da quello degli utenti della biblioteca. Il core switch del Municipio sarà managed e con supporto per VLAN per evenienze future (separazione ufficio-tributi da anagrafe o sindaco…).
* L’access point per la biblioteca fornirà l’accesso ad una rete guest, abilitata alla sola navigazione Internet tramite opportuna regola sul router. Si prevedono due (scelta arbitraria) AP anche presso la sede del Municipio per consentire (nell’ottica della modalità BYOD) l’utilizzo di dispositivi mobili a scopo lavorativo. L’autenticazione dell’accesso prevede l’uso di un server RADIUS che, basandosi su accesso certificato dell’utente, risulta molto più sicuro dell’uso di password, per WPA2 che possano essere.
* Un mobility controller permetterà il roaming dei dispositivi mobili del Municipio
* Di nuova acquisizione risulteranno i server, che saranno collocati in apposito locale presso la sede del Municipio, soggetto a restrizioni d’ingresso e adeguatamente climatizzato. Verrà acquistato un armadio rack nel quale troveranno posto:
  + UPS
  + Router del Municipio
  + Core switch del Municipio
  + Server web esterno
  + Server …
  + Firewall
  + Switch di DMZ
  + Mobility Controller
* L’interconnessione tra le tre LAN, che devono condividere un archivio di materiali centralizzato, potrebbe essere realizzato in alternativa tramite:
* Collegamento fisico dedicato tra le sedi (tramite fibra, considerando finanziamenti per l’Italia digitale, opere di manutenzione periodica del fondo stradale, nonché la progressiva e capillare diffusione del collegamento in fibra ottica da parte di carrier Internet), con realizzazione di un’unica LAN, sostituendo i router con altrettanti switch con management e supporto VLAN;
* Utilizzando Internet come veicolo del traffico di rete locale. Ciò è realizzabile tramite l’implementazione di VPN di tipo site-to-site, con l’applicazione di adeguata cifratura.

La modesta mole di dati soggetta a scambio tra le sedi e le caratteristiche di flessibilità, fanno preferire la seconda soluzione. La funzione di end-point delle VPN verrà associata ai router.

* Gli indirizzi usati saranno di classe C privati (192.168.0 per il Municipio, 192.168.1.0 per APT, 192.168.2.0 per biblioteca e 192.168.11.0 per rete guest). I server e le stampanti di rete, nonché le interfacce con ruolo di DG avranno IP statico. I router svolgeranno funzione di NAT con overload. Il port forwarding riguarderà il sito web comunale.



Schema LAN

1. Particolare attenzione dovrà essere posta nella scelta della tipologia (e del provider) di accesso a Internet, in quanto il traffico di interVLAN sarà a suo carico. Dal momento che è previsto un sito web, anche in questo caso dovrà essere operata una scelta tra soluzioni tecniche differenti: ospitarlo in sede oppure ricorrere ai servizi di un esterno in hosting, oppure ricorrere ad una soluzione in housing. Il fatto di dover avviare una connessione a Internet performante, avendo scelto una connettività tra LAN basata sulle VPN, la scarsa variabilità di flussi di accesso al sito web e la modesta mole di dati prevedibile in esso, fanno optare per una soluzione interna alla rete. La banda di accesso dovrà essere simmetrica per il Municipio ( no ADSL) e con valori minimi garantiti e tempi di downtime contenuti. Sarà opportuno individuare una soluzione di accesso secondaria (es ADSL) attivabile in caso di guasto della principale. (….)
2. La restrizione degli accessi alla rete locale viene demandata a…

(AD) ….

Alcune restrizioni verranno invece messe in atto attivando ACL sui router o firewall.

Es. ACE su firewall per consentire l’accesso al sito web interno agli host delle LAN APT e Biblioteca ….

Da non trascurare: la formazione del personale, che deve essere consapevole dei rischi per poter accettare le limitazioni…

1. Servizi di rete:

* DHCP
* ……

**Seconda parte**

**Il candidato esponga il concetto di difesa perimetrale di una rete di computer, analizzi i componenti necessari alla sua implementazione e le loro modalità di lavoro. Analizzi quindi differenti configurazioni di rete che prevedano anche l’uso di DMZ, e motivi poi la loro adozione a seconda delle differenti esigenze di sicurezza della rete e dei servizi da essa offerti.**

La difesa perimetrale di una rete consiste nell’individuazione dei confini di una rete definita *trusted* e la messa in atto di adeguate strategie per evitare la penetrazione all’interno di tali confini di utenti non autorizzati o, peggio ancora, malintenzionati.

In passato, quando l’utilizzo degli accessi wireless alla WAN globale era più limitato, la delimitazione dell’area trusted risultava più semplice e stabile di quanto lo sia oggi, con la sempre più massiccia presenza di dispositivi mobili utilizzati a scopo professionale.

Il dispositivo principale per il mantenimento dell’integrità perimetrale rimane tuttavia il firewall.

In una rete wired deve essere collocato in posizione tale che tutto il traffico da monitorare passi attraverso di esso. I firewall possono agire a differenti livelli di dettaglio:

Personal firewall (…)

Network firewall:

* + Cut through ….
  + Stateful inspection…
  + Application gateway…
  + UTM…

Un principio base su cui si fonda il funzionamento di un firewall è rappresentato dalle “regole di filtraggio” ….

Accanto ai firewall possono essere utilizzati dispositivi di Intrusion Detection e Prevention (IDS e IPS) con le seguenti funzioni…..

All’interno di una infrastruttura di rete può essere necessario implementare servizi cui devono poter accedere utenti esterni alla rete gestita. Permettere l’accesso alla rete trusted potrebbe essere fonte di pericolo, perciò tali servizi (bastion host con sito web o altro) vengono posizionati in una zona a minor livello di protezione, soggetta a regole di filtraggio più lasche e denominata zona demilitarizzata (DMZ). Tale DMZ può essere collocata tra due dispositivi firewall oppure associata ad una interfaccia del router appositamente predisposta.

**Le informazioni che viaggiano attraverso la rete Internet riguardano, sempre di più, aspetti rilevanti e delicati della vita degli individui e delle aziende. Tale mole di dati necessita di sistemi che garantiscano l’identità dei soggetti, l’integrità dei dati e la loro confidenzialità.**

**Il candidato descriva le caratteristiche dell’infrastruttura di sicurezza basata sulle chiavi pubbliche (PKI) evidenziando il ruolo delle Autorità di Certificazione.**

La tecnica che garantisce l’integrità dei dati trasmessi e l’identità del mittente, fornendo anche la riservatezza, è la crittografia a chiave asimmetrica. …..

Con questa tecnica è infatti possibile realizzare uno scambio di dati, anche reciproco utilizzando solo la chiave pubblica ( e pertanto non occorre la sua segretezza). In uno scambio unidirezionale, se i dati necessitano di autenticazione e riservatezza avverrà quanto segue:…

Se occorre la sola autenticazione, il documento verrà firmato digitalmente tramite i seguenti passaggi:….

L’apposizione della firma digitale avverrà tramite un apposito kit (ad esempio smart card o chiavetta USB).

L’elenco delle chiavi pubbliche rappresenta una potenziale fragilità per la sicurezza del sistema. Esiste infatti un grave rischio per la verifica dell’autenticità: un malintenzionato potrebbe pubblicare la propria chiave a nome di un altro e utilizzarla per impersonarlo. Per sopperire a questo punto debole, si ricorre ad una terza parte, ossia alle Certification Authority, che si fanno garanti dell’autenticità delle chiavi (pubbliche) da esse pubblicizzate (X.509). Gli enti certificatori accreditati sono rintracciabili anche sul sito dell’agenzia per l’Italia digitale. (vedi pdf)

Oltre alla firma digitale, gli Enti Certificatori forniscono la PEC (Posta Elettronica Certificata) e lo SPID (Sistema Pubblico di Identità Digitale)

**Negli ultimi anni lo sviluppo tecnologico ha portato ad una maggiore apertura delle infrastrutture informatiche, ormai ampiamente interconnesse. La sicurezza dei dati è diventata, di conseguenza, un aspetto fondamentale nell’ambito del trattamento delle informazioni. Il candidato descriva i possibili tipi di minacce alla sicurezza di un sistema informatico.**

I concetti cardine relativi alla sicurezza delle informazioni sono: Disponibilità, Segretezza e Integrità (CIA: Confidentiality, Integrity, Availability) e per “minaccia” si intende tutto ciò che è potenzialmente in grado di arrecare danno; dunque andiamo ad esaminare tutto ciò che può compromettere disponibilità, segretezza e integrità. Per prima cosa, in una infrastruttura informatica, occorre tenere conto delle condizioni ambientali e delle eventualità quali fenomeni meteo, guasti, disastri accidentali, che possono compromettere la disponibilità dei dati, ma tutto ciò sarà stato considerato in fase di valutazione dei rischi e saranno stati presi provvedimenti di disaster recovery, concernenti, in particolare, procedure di backup sia locale che remoto (anche su cloud) protetti, se si ritiene, con tecniche crittografiche. Considerando invece minacce informatiche deliberate, andiamo ad elencare le principali tipologie, riportando a cosa rappresentano una minaccia tra parentesi:

spyware (confidenzialità), cryptolocker (disponibilità), DoS e DDos (disponibilità), Phishing e social engineering (confidenzialità/disponibilità/integrità)

Da ultimo vorrei citare come grave tipo di minaccia alla sicurezza la mancanza di informazione da parte degli utenti del sistema: la formazione sulle tecniche di prevenzione (hardening delle password, applicazione consapevole delle misure di sicurezza) rappresenta forse la contromisura più importante.