TRACCIA ORIGINALE (link)

SIMULAZIONE SECONDA PROVA SCRITTA ESAME DI STATO

Indirizzo: INFORMATICA E TELECOMUNICAZIONI

Articolazione: INFORMATICA

Disciplina: SISTEMI E RETI

Il candidato svolga la prima parte della prova e due tra i quesiti proposti nella seconda parte.

PRIMA PARTE

Una grande società di ingegneria ha deciso di avvalersi di nuove tecnologie ed infrastrutture digitali per la realizzazione di alcune importanti opere edilizie, acquisendo presso la propria sede centrale un sistema BIM, acronimo di Building Information Modeling (in italiano: Modellazione informativa delle costruzioni). Si tratta di un "metodo per l'ottimizzazione della pianificazione, realizzazione e gestione di costruzioni tramite un processo codificato, attraverso il quale tutti i dati rilevanti di una costruzione possono essere raccolti, combinati e collegati digitalmente. La costruzione virtuale è visualizzabile inoltre come un modello geometrico tridimensionale" (fonte: Wikipedia.org).

L'utilizzo di un sistema BIM consentirà alla società il monitoraggio dell'avanzamento dei lavori nei cantieri edili, la riduzione di errori, la velocizzazione dei tempi e, su edifici esistenti, faciliterà la rilevazione dello stato di fatto dell'edificio e la progettazione degli interventi di recupero. Per il conseguimento di tali obiettivi, la società dovrà avvalersi di apparecchiature digitali da utilizzare in cantiere:

a) diversi tablet rugged 1 corredati di laser scanner 3D o sensore Lidar;
b) alcune fotocamere timelapse;
c) numerosi sensori di sicurezza (ad es. vibrazioni, gas e fumi, umidità, temperatura o altre proprietà chimico-fisiche).

I tablet rugged saranno utilizzati per i cosiddetti "rilevamenti BIM", operazioni di scansione effettuate con strumenti basati su tecnologia Laser Scanner 3D (alta precisione) o Lidar (bassa/media precisione). Questi strumenti di scansione possono essere interfacciati ai tablet attraverso varie tipologie di porte wired/wireless o possono essere anche integrati negli stessi tablet (come nel caso del sensore Lidar). In un rilevamento BIM, quando il raggio laser dello scanner colpisce la superficie di un oggetto anche molto irregolare, viene registrata la posizione (X, Y, Z) di un insieme denso di punti campione di tale superficie. L'insieme di tutti questi punti campionati, che darà origine alla visualizzazione 3D dell'oggetto, è chiamato "nuvola di punti". Al termine dei rilevamenti, i dati di ogni nuvola di punti acquisiti con le scansioni sono poi trasformati in un modello geometrico tridimensionale parametrico (oggetto BIM) che costituisce una rappresentazione digitale precisa dell'edificio o di una sua parte (ad esempio una facciata, una scala, un impianto, etc.). Ogni

mappedsa.it

vietata la condivisione

oggetto BIM viene solitamente integrato con altri dati informativi quali, ad esempio, dati relativi a misure chimico-fisiche, dati tecnici e immagini digitali provenienti dalla fotocamera degli stessi tablet.

Per quanto riguarda le fotocamere timelapse, queste sono invece dispositivi fotografici automatici progettati per scattare foto a intervalli di tempo regolari e prestabiliti. Garantiscono normalmente alta risoluzione (es. 4K/8K), e offrono, in generale, connettività sia wired (es. via porta USB) che wireless. Le immagini delle foto scattate da una fotocamera timelapse sono utilizzate per assemblare video che "accelerano" il tempo, allo scopo di mostrare in pochi secondi processi lunghi e lenti. La società utilizzerà queste fotocamere per monitorare e documentare l'avanzamento dei lavori e/o creare video promozionali; esse verranno pertanto installate in punti strategici di ciascun cantiere in corso. Per quanto riguarda infine i sensori per la sicurezza del cantiere, la società ha acquisito sensori interfacciabili a varie tipologie di moduli di trasmissione dati sia wired che wireless.

Con l'adozione del sistema BIM, per l'apertura di ogni nuovo cantiere la società dovrà quindi dotarsi di una infrastruttura di comunicazione che possa di volta in volta essere messa temporaneamente in campo al fine di consentire:

- Il trasferimento, dal cantiere alla sede centrale, dei dati grezzi delle nuvole di punti derivanti dai rilevamenti BIM, che verranno utilizzate in software specialistici per le successive operazioni di modellazione 3D. Il modello finale verrà gestito in condivisione dati tra i vari uffici della sede per il coordinamento tra i tecnici che lavorano al progetto.
- La trasmissione e la raccolta dei fotogrammi provenienti dalle fotocamere in un opportuno sistema di repository presso la sede centrale, per costruire i video in timelapse.
- La trasmissione dei dati provenienti dai sensori di sicurezza, sia internamente al cantiere verso i sistemi locali per l'eventuale attivazione di notifiche ed allarmi in tempo reale, sia verso i sistemi remoti in sede centrale per le segnalazioni, le ulteriori elaborazioni e per mantenere un registro di log storico.

Tutte le operazioni di comunicazione locale (nei cantieri e nella sede centrale) e remota (tra singolo cantiere e sede) dovranno avvenire mediante idonee misure di sicurezza ed autenticazione sia a livello di singoli apparati che degli operatori. La società dispone già di una infrastruttura di rete locale presso la sede a cui afferiscono i computer degli uffici tecnici per l'accesso condiviso ai sistemi che conterranno i software BIM specialistici; tale rete locale è provvista di accesso ad internet mediante router con un collegamento WAN datato basato su tecnologia ADSL.

Il candidato, analizzata la realtà di riferimento e formulate le opportune ipotesi aggiuntive, incluse ipotesi di dimensionamento del numero degli apparati correlato alla complessità di ciascun cantiere e del numero massimo dei cantieri contemporaneamente attivi, sviluppi i seguenti punti:

vietata la condivisione

mappedsa.it

1. un progetto generale dell'infrastruttura di rete da realizzare in un cantiere, anche supportato da uno schema grafico, indicando tipologia e caratteristiche dei canali locali, apparati, protocolli, schemi di indirizzamento e servizi da adottare;
2. una descrizione della ipotetica struttura della rete pre-esistente in sede centrale, con proposte di integrazione e potenziamento necessarie per l'adozione del sistema BIM;
3. la scelta della tipologia e delle caratteristiche dei canali di comunicazione da realizzare tra cantieri e sede centrale, inclusa una stima della capacità trasmissiva sufficiente a supportare il traffico dati, individuando gli apparati da adottare;
4. le modalità, i protocolli e i servizi con cui consentire agli operatori di autenticarsi presso i sistemi in sede centrale sia nella sede stessa che dai cantieri da remoto.

SECONDA PARTE

I. In relazione al tema proposto nella prima parte, per quanto riguarda le finalità di archiviazione dei dati (scansioni, immagini, dati da sensori, etc.) si individuino e descrivano, illustrandone anche vantaggi e svantaggi, le differenze tra possibili soluzioni tecnologiche "on premise" e soluzioni cloud-based, da adottare ed integrare nel progetto.

II. In relazione al tema proposto nella prima parte, per quanto riguarda le operazioni di comunicazione locale e remota, si individuino e si descrivano, oltre alle modalità di autenticazione già discusse al punto 4 della prima parte, le ulteriori misure di sicurezza informatica da adottare nella sede centrale e nei cantieri, incluse quelle idonee a garantire la continuità trasmissiva del canale tra i singoli cantieri e la sede centrale.

III. Il candidato ipotizzi di essere l'amministratore della rete didattica di un istituto ad indirizzo informatico. Dall'analisi dei log dei sistemi e da osservazioni dirette effettuate dai docenti, è stato riscontrato che diversi studenti, in modo non autorizzato, fanno sviluppare da piattaforme di Intelligenza Artificiale il codice dei programmi delle tracce proposte dai docenti per le attività in laboratorio. Il candidato illustri e dettagli con esemplificazioni le possibili misure e tecniche da attuare per impedire l'accesso a tali piattaforme. Proponga inoltre eventuali modalità per schedulare tale blocco (ed il successivo sblocco) in specifici momenti dell'orario scolastico e/o da specifici laboratori.

IV. In relazione al protocollo SSH, il candidato immagini di impartire il comando ssh -p 25500 administrator@200.1.1.1 Sapendo che sul dispositivo con indirizzo 200.1.1.1 è configurata una regola che reindirizza il traffico, in ingresso sulla porta 25500, ad un altro dispositivo con indirizzo 172.16.1.100, il candidato esponga gli effetti del comando impartito e le finalità del suo utilizzo.

mappedsa.it

vietata la condivisione

SOLUZIONE PROPOSTA (SOGGETTIVA)

PRIMA PARTE

La grande società di ingegneria ci ha commissionato la progettazione e l'adeguamento dell'infrastruttura tecnologica e di rete necessaria a supportare l'adozione del sistema BIM (Building Information Modeling). L'obiettivo è quello di digitalizzare la gestione dei cantieri edili e di connetterli in modo sicuro alla sede centrale, così da consentire il monitoraggio dell'avanzamento dei lavori, la raccolta delle scansioni 3D (le cosiddette nuvole di punti) effettuate tramite i tablet rugged, l'acquisizione dei fotogrammi delle fotocamere timelapse e la gestione in tempo reale degli allarmi provenienti dai sensori di sicurezza.

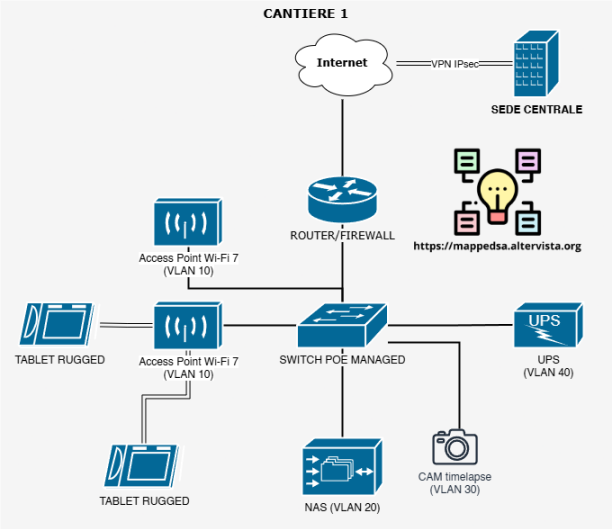
Essendo i cantieri degli ambienti temporanei, ostili e in continua evoluzione, è stato deciso di progettare una infrastruttura locale (on premise) robusta, tollerante ai guasti e capace di gestire la congestione dei canali di comunicazione. La sede centrale, invece, dovrà essere potenziata per poter centralizzare il controllo e l'archiviazione della grande mole di dati in arrivo da tutti i cantieri.

Di seguito viene dettagliato il progetto generale dell'infrastruttura. Come ipotesi di dimensionamento è stato previsto un numero massimo di dieci cantieri attivi contemporaneamente sul territorio nazionale, ciascuno dotato in media di quattro o cinque tablet rugged, due o tre fotocamere timelapse e una decina di sensori di sicurezza, valori che possono crescere nei cantieri più complessi.

mappedsa.it

1. Infrastruttura del cantiere (rete locale)

Ogni cantiere sarà dotato di una infrastruttura on premise alloggiata all'interno di un armadio rack compatto, blindato e con protezione stagna (IP65), posizionato nel box ufficio del cantiere. Per garantire l'accesso a Internet anche in mobilità, l'hardware principale di connessione sarà un router industriale 4G/5G ad alta affidabilità, affiancato da una connessione satellitare usata in modalità bilanciata o di backup nei cantieri situati in zone geograficamente isolate.



vietata la condivisione

Il primo apparato della rete locale è il router/firewall 4G/5G. Esso svolge le funzioni di NAT, di instradamento e di firewall di frontiera e funge inoltre da terminatore dei tunnel VPN verso la sede centrale. A valle del router è stato previsto uno switch PoE (Power over Ethernet) di tipo managed, ovvero gestito, in grado di alimentare direttamente tramite il cavo di rete gli apparati distribuiti sul campo, come gli access point e le telecamere, semplificando così il cablaggio.

Per la copertura wireless sono stati scelti più access point outdoor con standard Wi-Fi 7, perché un cantiere edile si estende su migliaia di metri quadri e le strutture metalliche, le gru, i container e i macchinari in movimento creano forti zone d'ombra che un solo apparato non riuscirebbe a coprire. Tutti gli access point trasportano la stessa VLAN 10, che resta una sola rete logica indipendentemente dal loro numero, e diffondono lo stesso SSID con il supporto del roaming veloce 802.11r, così che un operatore che si sposta nel cantiere passi da un access point all'altro senza perdere la connessione. Per configurarli in modo coerente e tenerli sotto controllo viene impiegato un controller wireless, anche in versione software o gestita dal cloud. La scelta del Wi-Fi 7 è motivata dal fatto che introduce l'uso della banda a 6 GHz e di canali radio più ampi, riducendo in modo sensibile la latenza, le interferenze e l'affollamento dello spettro, particolarmente critici in un ambiente come quello di cantiere.

Per quanto riguarda i rilevamenti, ogni laser scanner 3D o sensore Lidar viene interfacciato al proprio tablet rugged. Nel caso del Lidar il sensore è spesso già integrato nel tablet, mentre gli scanner esterni si collegano tramite porta USB di tipo C oppure, quando il produttore lo prevede, in modalità wireless tramite Wi-Fi Direct o Bluetooth. Il tablet acquisisce così la nuvola di punti e, una volta rientrato in copertura, la carica sul NAS di cantiere attraverso l'access point.

Per ridurre i rischi di congestione, sullo switch e sugli access point è stato configurato il QoS (Quality of Service). Al traffico dei tablet rugged dedicato al caricamento delle nuvole di punti sul NAS viene assegnata la priorità più alta, limitando in modo preventivo la banda destinata all'eventuale navigazione web o alle comunicazioni non prioritarie del personale.

Le fotocamere timelapse generano immagini ad altissima risoluzione (4K/8K) che occupano molta banda. Per questo motivo è stato deciso di non collegarle in modalità wireless, evitando di saturare le frequenze radio, ma di cablarle direttamente alle porte dello switch PoE isolandole in una VLAN dedicata.

Le scansioni laser producono file di dimensioni molto grandi e la banda della WAN è a consumo e potenzialmente lenta durante il giorno, perciò l'invio diretto in sede congestionerebbe la linea. Tutti i dati grezzi e i fotogrammi timelapse vengono quindi salvati in locale sul server NAS di cantiere durante le ore lavorative e trasferiti verso la sede centrale soltanto di notte, tramite una operazione pianificata e schedulata. Per ottimizzare i tempi di trasferimento ed evitare di saturare la linea, il NAS locale confronta i file con quelli già presenti in sede, calcola le differenze (il cosiddetto delta) e invia soltanto i blocchi di dati

mappedsa.it

vietata la condivisione

nuovi o modificati, applicando inoltre una compressione alla fonte e riducendo così in modo deciso il traffico sulla WAN. Il trasferimento vero e proprio avviene tramite rsync incapsulato in una sessione SSH, in modo che il confronto dei file, il calcolo dei blocchi modificati e il loro invio siano gestiti dallo stesso strumento in forma cifrata. In alternativa può essere impiegato il protocollo SFTP, anch'esso basato su SSH.

All'interno del rack viene installato anche un UPS (gruppo di continuità) intelligente. In un cantiere i blackout e gli sbalzi di tensione sono frequenti e l'UPS non solo protegge l'hardware dai guasti elettrici, ma è collegato direttamente al NAS locale. In caso di mancanza prolungata di corrente, l'UPS invia un comando al NAS per avviare una procedura di spegnimento sicuro, impedendo la corruzione dei dati e la perdita delle scansioni effettuate durante la giornata.

La rete dei sensori di sicurezza (indipendente)

I sensori di sicurezza, come quelli per gas, fumi, umidità e vibrazioni, richiedono la massima affidabilità. Per questo saranno alimentati da batterie a lunga durata e comunicheranno via wireless tramite protocolli a lungo raggio e a basso consumo come Zigbee o LoRa. È importante sottolineare che questi sensori non faranno capo alla rete principale del cantiere, ma comunicheranno con una centralina separata e indipendente, dotata di una propria scheda SIM di un operatore telefonico diverso, scelto per ridondanza, e di un proprio pacco batterie tampone. In questo modo, anche in caso di blackout totale del cantiere o di guasto del router principale, la centralina sarà sempre in grado di trasmettere le segnalazioni di emergenza sia in locale sia verso la sede remota.

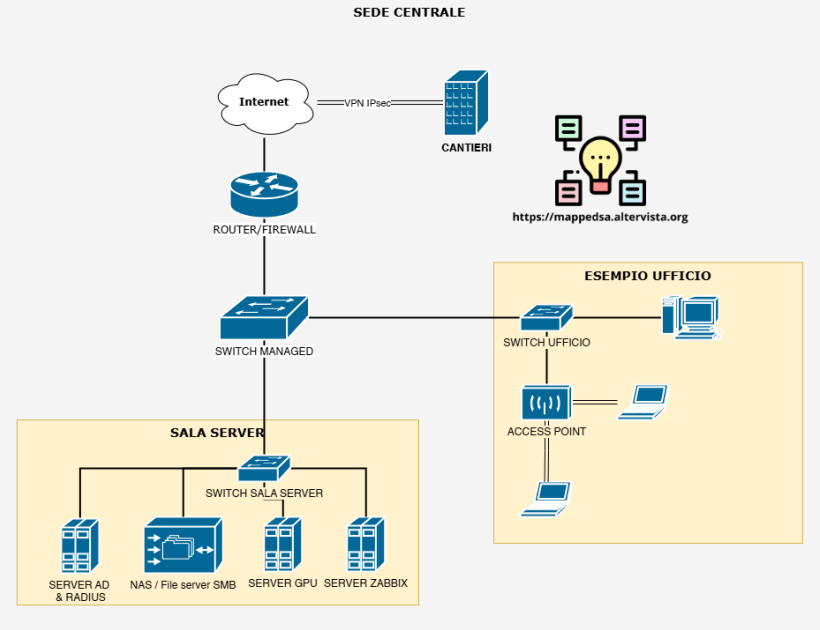
2. Infrastruttura della sede centrale

L'attuale rete della sede centrale è basata su una vecchia connessione ADSL e su un router datato a cui afferiscono i computer degli uffici tecnici. Si ipotizza che questa rete sia oggi una semplice LAN piana, priva di segmentazione e con un unico dominio di broadcast, adatta alla sola navigazione e alla condivisione di file tra gli uffici. Una struttura di questo tipo non è in grado di gestire i flussi BIM simultanei provenienti da più cantieri attivi e deve quindi essere potenziata in modo deciso.

Come primo intervento si prevede l'attivazione di una linea in fibra ottica dedicata (FTTH o FTTO) con banda minima garantita, simmetrica e ad alta capacità, ad esempio 1 Gbps, protetta da una seconda linea di backup (FTTC o FWA) per garantire la continuità del servizio. Il vecchio router verrà sostituito da un router/firewall perimetrale di fascia enterprise che gestirà il NAT, le politiche di sicurezza e la terminazione di tutti i tunnel VPN provenienti dai cantieri.

mappedsa.it

vietata la condivisione



La rete interna verrà segmentata tramite switch managed e suddivisa in VLAN distinte per gli uffici tecnici, per i server e per la gestione degli apparati, così da ridurre i domini di broadcast e isolare i sistemi più critici. Nel dettaglio la rete della sede viene organizzata su tre reti logiche. La VLAN degli uffici tecnici raccoglie i computer dei progettisti, la VLAN dei server ospita lo storage e i servizi interni, la VLAN di gestione è riservata alle interfacce di amministrazione degli apparati. Il firewall perimetrale regola il traffico tra queste reti applicando il principio del privilegio minimo, così che gli uffici raggiungano i server soltanto sulle porte necessarie e la rete di gestione resti isolata dal resto.

Il modello finale deve poter essere gestito in condivisione tra i vari uffici tecnici. Per questo nella VLAN dei server viene predisposto un file server o NAS con condivisioni di rete in protocollo SMB, affiancato da un ambiente di condivisione dati dedicato al BIM, che gestisce i permessi e le versioni del modello evitando sovrascritture tra i tecnici. La trasformazione delle nuvole di punti in modello 3D parametrico è una elaborazione molto pesante dal punto di vista del calcolo, perciò la sede viene dotata di workstation ad alte prestazioni con GPU dedicate oppure di un server di elaborazione con GPU condiviso a cui i progettisti accedono da remoto, in modo da non dover spostare file enormi su ogni singolo computer.

Nella sala server verrà installata una infrastruttura di storage enterprise composta da NAS rack dotati di alcuni Terabyte di cache veloce su SSD NVMe. Questa cache è fondamentale durante la fase di ricezione massiva notturna, perché quando tutti i cantieri avviano nello stesso momento la sincronizzazione dei dati la cache assorbe i picchi di scrittura senza rallentare i sistemi, riversando poi i dati sui dischi meccanici di grande capacità nelle ore successive.

Per supervisionare l'intera infrastruttura distribuita sul territorio nazionale, nella sala server verrà installata la piattaforma di monitoraggio Zabbix. Sfruttando i protocolli standard SNMP e Syslog, Zabbix interrogherà di continuo tutti i nodi remoti e metterà a disposizione degli amministratori una dashboard centralizzata in

vietata la condivisione

tempo reale. Attraverso questa dashboard sarà possibile controllare lo stato e la raggiungibilità di router e switch nei singoli cantieri, il livello di carica delle batterie degli UPS e la presenza di anomalie elettriche, la temperatura interna dei rack industriali, l'eventuale saturazione della banda o la disconnessione degli access point e infine il corretto completamento della sincronizzazione notturna dei dati BIM.

La rete della sede centrale viene suddivisa in VLAN, secondo lo schema seguente, con un piano di indirizzamento basato sullo spazio privato 192.168.0.0/16.

VLAN ID	Nome VLAN	Descrizione e apparati connessi	Politica di accesso
100	VLAN_UFFICI	Computer e workstation dei progettisti	Accesso ai server solo sui servizi BIM e navigazione web controllata
200	VLAN_SERVER	NAS/file server SMB, server GPU di elaborazione e server Zabbix.	Isolata, raggiungibile dagli uffici solo sulle porte applicative previste e dalla rete di gestione
300	VLAN_MGMT	Interfacce di gestione di firewall, switch e access point	Massima restrizione, accesso riservato agli amministratori

Dispositivo	Indirizzo IP	Interfaccia o porta switch	DHCP	ID VLAN
Firewall perimetrale / router	192.168.1.1	Porta core in trunk	No	Trunk (tutte)
Switch core managed	192.168.3.2	Collegato al firewall in trunk	No	300
Switch sala server	192.168.3.3	Collegato al core in trunk	No	300
Switch uffici	192.168.3.4	Collegato al core in trunk	No	300
Workstation progettista	192.168.1.10	Porta switch uffici	Sì	100
Access point uffici	192.168.1.5	Porta switch uffici	No	100
NAS / file server SMB	192.168.2.10	Porta switch sala server	No	200
Server GPU di elaborazione	192.168.2.20	Porta switch sala server	No	200
Server Zabbix	192.168.2.30	Porta switch sala server	No	200
Server AD e RADIUS	192.168.2.40	Porta switch sala server	No	200

mappedsa.it

vietata la condivisione

Il firewall perimetrale funge da gateway per tutte le VLAN tramite sottointerfacce, ad esempio 192.168.1.1 per la VLAN degli uffici, 192.168.2.1 per quella dei server e 192.168.3.1 per quella di gestione. Le workstation degli uffici ricevono l'indirizzo via DHCP, mentre i server e gli apparati di rete hanno indirizzo statico per essere sempre raggiungibili.

3. Collegamento WAN, stima della banda e isolamento tra i cantieri

I canali di comunicazione tra i singoli cantieri e la sede centrale saranno realizzati attraverso reti pubbliche protette da VPN Site-to-Site basate sul protocollo IPsec, in grado di garantire autenticazione, integrità e confidenzialità dei dati grazie alla cifratura AES. La negoziazione delle chiavi e dei parametri di sicurezza avviene tramite IKEv2, versione più recente e sicura rispetto all'ormai deprecato IKEv1.

Per quanto riguarda la stima della capacità trasmissiva conviene distinguere il traffico in tempo reale da quello differito. Durante il giorno il singolo cantiere genera soprattutto traffico di gestione, di monitoraggio e di allarme dei sensori, oltre a un eventuale flusso di controllo, per un fabbisogno modesto nell'ordine di pochi Mbps. La parte più pesante è invece il trasferimento notturno delle scansioni. Ipotizzando che un cantiere produca in media circa 50 GB di dati grezzi al giorno e che la deduplicazione e la compressione riducano il volume effettivo a circa 15 GB, per trasferire questa quantità in una finestra notturna di otto ore servono in media poco più di 4 Mbps in upload per ogni cantiere. Con dieci cantieri che sincronizzano in contemporanea, la sede centrale deve quindi poter ricevere almeno 40 Mbps di traffico utile, valore ampiamente coperto dalla linea in fibra da 1 Gbps prevista, che lascia un buon margine per i picchi e per la crescita futura. Sul lato cantiere è sufficiente la banda in upload offerta da una buona connessione 4G/5G, mentre la connessione satellitare garantisce la continuità quando la copertura cellulare è scarsa.

Per evitare conflitti di instradamento, a ogni cantiere viene assegnato un blocco di indirizzi IP privati univoco, ad esempio 10.1.0.0/16 per il Cantiere 1 e 10.2.0.0/16 per il Cantiere 2. All'interno del blocco di ogni cantiere ciascuna VLAN occupa in pratica una sottorete /24, come 10.1.10.0/24 per la VLAN 10 o 10.1.20.0/24 per la VLAN 20. L'assegnazione di un intero /16 a ciascun cantiere è quindi una scelta di comodità che semplifica il routing e lascia un ampio margine di crescita, pur essendo nei fatti sovradimensionata rispetto al numero reale di apparati.

Grazie a politiche rigide configurate sul firewall della sede centrale e sui router remoti, tutti i cantieri saranno completamente isolati tra di loro. Un host del Cantiere 1 potrà comunicare soltanto con le risorse autorizzate della sede centrale, come il NAS centrale e il server Zabbix, e solo sulle porte applicative consentite, senza poter in alcun modo raggiungere o scansionare la rete del Cantiere 2. In questo modo si riduce la superficie di attacco in caso di furto o di compromissione di un dispositivo in cantiere.

4. Struttura delle VLAN all'interno del cantiere

mappedsa.it

vietata la condivisione

Per separare logicamente i domini di broadcast e ottimizzare le prestazioni della rete cablata e wireless del cantiere, lo switch PoE managed sarà configurato con le VLAN riportate nella tabella seguente.

VLAN ID	Nome VLAN	Descrizione e apparati connessi	Politica di accesso e QoS
10	VLAN_WIFI	Access point a cui accedono i tablet rugged degli operatori	Priorità alta con QoS e accesso a Internet limitato alla VPN verso la sede
20	VLAN_STORAGE	Server NAS locale di cantiere	Isolata, comunica solo con la VLAN 10 per ricevere i file dai tablet e con la sede centrale
30	VLAN_TIMELAPSE	Telecamere timelapse cablate su porta PoE	Banda controllata che isola i flussi video massivi dal Wi-Fi
40	VLAN_MGMT	Interfacce di gestione di router, switch e UPS intelligente	Massima restrizione, accessibile solo dalla sede centrale tramite VPN

Il servizio DHCP per la VLAN 10 dei tablet rugged è erogato direttamente dal router industriale, che assegna in automatico gli indirizzi nel range previsto. Tutti gli altri apparati, come NAS, telecamere, access point e interfacce di gestione, hanno invece indirizzo statico per garantirne una raggiungibilità costante.

Di seguito viene riportato un esempio pratico di indirizzamento IP per il Cantiere 1, basato sulla sottorete 10.1.0.0/16.

Dispositivo	Indirizzo IP	Interfaccia o porta switch	DHCP	ID VLAN
Router industriale	10.1.40.1	Porta LAN 1 in trunk	No	Trunk (tutte)
Switch PoE managed	10.1.40.2	Collegato al router in trunk	No	Trunk (tutte)
Access point 1 (Wi-Fi 7)	10.1.10.11	Porta 2	No	10
Access point *n* (Wi-Fi 7)	10.1.10.12	Porta 3	No	10
Tablet rugged *n* BIM	10.1.10.100	Connessione su AP 1	Sì	10

mappedsa.it

vietata la condivisione

NAS locale di cantiere	10.1.20.10	Porta 4	No	20
Cam timelapse *n* (PoE)	10.1.30.10	Porta 5	No	30
UPS intelligente	10.1.40.5	Porta 6	No	40

5. Autenticazione e accesso degli operatori

Tutte le operazioni di comunicazione, sia locali sia remote, devono avvenire con idonee misure di autenticazione a livello di singolo apparato e di singolo operatore. Per questo motivo nella sede centrale verrà installato un server AAA basato sul protocollo RADIUS, integrato con un servizio di directory centralizzato come Active Directory o LDAP, nel quale sono registrate le identità di tutti gli operatori e i relativi permessi.

A livello di apparati, l'accesso alla rete cablata e wireless del cantiere viene controllato tramite lo standard 802.1X. In pratica un tablet o un computer che si collega alla porta dello switch o all'access point non riceve subito un indirizzo, ma deve prima autenticarsi presentando le proprie credenziali, che lo switch o l'access point inoltrano al server RADIUS della sede attraverso il tunnel VPN. Soltanto dopo l'esito positivo il dispositivo viene ammesso nella VLAN corretta. In questo modo un dispositivo rubato o non autorizzato non riesce a entrare nella rete.

A livello di operatori, l'accesso ai sistemi e ai software BIM della sede centrale avviene tramite le stesse credenziali aziendali gestite dalla directory centralizzata, con un meccanismo di Single Sign On che permette di usare un'unica identità per i diversi servizi. Per aumentare la sicurezza viene richiesta l'autenticazione a più fattori (MFA), ad esempio una password unita a un codice temporaneo generato da una app sullo smartphone.

Quando un operatore lavora dalla sede centrale si autentica direttamente sulla rete locale. Quando invece lavora da remoto, ad esempio da un cantiere o da casa, deve prima stabilire una VPN di tipo Remote Access verso il firewall della sede, autenticandosi sempre con credenziali aziendali e secondo fattore. Solo a quel punto, e nei limiti dei permessi assegnati al suo ruolo, potrà accedere alle risorse condivise. Il server AAA si occupa anche della parte di accounting, registrando in un log chi ha effettuato l'accesso, da dove e quali risorse ha utilizzato, una informazione utile sia per la sicurezza sia per l'analisi a posteriori.

mappedsa.it

vietata la condivisione

SECONDA PARTE

Quesito 1. Soluzioni on premise e soluzioni cloud per l'archiviazione

Per l'archiviazione dei dati prodotti dal progetto, ovvero le scansioni, le immagini e i dati dei sensori, si possono seguire due strade principali, la soluzione on premise e la soluzione cloud, che spesso vengono combinate in un modello ibrido.

La soluzione on premise prevede che i dati siano conservati su server e NAS fisici di proprietà della società, collocati nella sala server della sede centrale. Il principale vantaggio è il controllo totale sui dati, che non escono mai dal perimetro aziendale, con benefici in termini di riservatezza e di rispetto della normativa sulla protezione dei dati. Le prestazioni in lettura e scrittura all'interno della LAN sono inoltre molto elevate e i dischi dei server e dei NAS vengono configurati in RAID, una tecnica che distribuisce le informazioni su più dischi così che, in caso di guasto di una singola unità, i dati non vadano persi e restino disponibili. Ad esempio una configurazione RAID 1 crea una copia speculare dei dati su due dischi, mentre il RAID 5 e il RAID 6 garantiscono la tolleranza al guasto rispettivamente di uno e di due dischi mantenendo un buon compromesso tra spazio utile e sicurezza. È bene ricordare però che il RAID protegge dal guasto fisico dei dischi ma non sostituisce un vero backup. Gli svantaggi di questa soluzione sono i costi iniziali alti per l'acquisto dell'hardware, la necessità di personale specializzato per la manutenzione e la difficoltà di ampliare lo spazio in fretta quando la mole di dati cresce. In caso di guasto grave o di disastro nella sede, inoltre, il rischio di perdita dei dati ricade interamente sulla società.

La soluzione cloud prevede invece di affidare l'archiviazione a un fornitore esterno come Amazon Web Services (AWS), Google Cloud o Microsoft Azure, attraverso servizi di tipo storage as a service. Questi provider mettono a disposizione diverse classi di archiviazione in base alla frequenza con cui si accede ai dati. Per i dati usati di frequente esistono servizi come Amazon S3 o Google Cloud Storage in classe Standard, mentre per lo storico e per i dati a cui si accede di rado si usano le classi di tipo archivio, molto più economiche, come Amazon S3 Glacier e Glacier Deep Archive, dove il costo di conservazione è bassissimo a fronte di tempi di recupero più lunghi. I vantaggi sono la scalabilità quasi illimitata, perché lo spazio si amplia in pochi minuti pagando solo ciò che si usa, l'assenza di costi iniziali per l'hardware e la presenza di copie ridondanti e geograficamente distribuite gestite dal fornitore, che migliorano la resistenza ai disastri. Gli svantaggi sono la dipendenza dalla connessione Internet, i costi che a lungo termine e con grandi volumi possono diventare elevati, e soprattutto il fatto di affidare a terzi dati riservati, con possibili vincoli normativi sulla loro collocazione geografica. A questi si aggiungono i costi di egress, ovvero le tariffe che i provider applicano allo scaricamento dei dati verso l'esterno, che con i volumi del progetto BIM, nell'ordine di decine di Terabyte, possono incidere in modo notevole ogni volta che occorre recuperare grandi quantità di dati dal cloud. Considerando la grande mole di dati del progetto BIM, la scelta più ragionevole è una soluzione ibrida. I dati di lavoro più recenti e più richiesti, sui quali i tecnici operano ogni giorno, vengono mantenuti on premise su

vietata la condivisione

NAS configurati in RAID per garantire prestazioni elevate e pieno controllo, mentre lo storico, le copie di backup e i dati a cui si accede di rado vengono spostati nel cloud nelle classi di tipo archivio come Amazon S3 Glacier o Google Cloud Storage Archive, sfruttandone la scalabilità e la ridondanza a costi molto contenuti.

Quesito 2. Ulteriori misure di sicurezza e continuità trasmissiva

Oltre alle modalità di autenticazione già descritte nella prima parte, l'infrastruttura deve essere protetta con un insieme di misure di sicurezza sia nella sede centrale sia nei cantieri.

Nella sede centrale il punto di ingresso è protetto da un firewall perimetrale che filtra tutto il traffico in entrata e in uscita e applica il principio del privilegio minimo, consentendo solo le comunicazioni strettamente necessarie. Sulla rete viene affiancato un sistema IDS/IPS per rilevare e bloccare i tentativi di intrusione, mentre la segmentazione in VLAN limita i danni nel caso un singolo apparato venga compromesso. I sistemi operativi e i firmware degli apparati vengono mantenuti aggiornati per chiudere le vulnerabilità note, gli accessi sono registrati nei log e raccolti in modo centralizzato e dei backup periodici, conservati secondo la regola del 3 2 1, permettono di ripristinare i dati in caso di attacco, ad esempio di tipo ransomware.

Nei cantieri valgono gli stessi principi, adattati a un ambiente più esposto. Poiché un dispositivo può essere rubato, è importante che le credenziali siano gestite a livello centrale e revocabili da remoto e che i dati sensibili presenti sui NAS e sui tablet siano cifrati a riposo, così che un eventuale furto non comprometta le informazioni. Il traffico verso la sede viaggia comunque sempre all'interno del tunnel VPN cifrato. Per autenticare in modo forte i router di cantiere, le VPN non si basano soltanto su nome utente e password ma anche su certificati digitali installati su ciascun apparato, così che solo i dispositivi realmente autorizzati possano stabilire il tunnel verso la sede.

Un aspetto fondamentale richiesto dalla traccia è la continuità trasmissiva del canale tra cantiere e sede. Per garantirla è stata prevista una doppia connettività, con il router industriale che utilizza in via principale la rete 4G/5G e passa automaticamente alla connessione satellitare in caso di assenza di copertura o di guasto, secondo una logica di failover. Le VPN possono essere configurate in modalità ridondante, in modo che la caduta di un canale non interrompa la comunicazione, e la rete dei sensori di sicurezza, come già visto, è del tutto indipendente, con una propria SIM di un altro operatore e batterie tampone, così da continuare a trasmettere gli allarmi anche quando il resto del cantiere è fuori uso. Gli UPS, infine, garantiscono il funzionamento degli apparati durante i blackout e ne permettono lo spegnimento ordinato quando l'autonomia sta per esaurirsi.

mappedsa.it

vietata la condivisione

Quesito 3. Blocco delle piattaforme di Intelligenza Artificiale nella rete didattica

Come amministratore della rete didattica dell'istituto, l'obiettivo è impedire agli studenti di accedere in modo non autorizzato alle piattaforme di Intelligenza Artificiale durante le attività di laboratorio. Nessuna singola tecnica è risolutiva da sola, perciò conviene combinare più livelli di blocco.

Il primo livello agisce sul DNS. Configurando i computer del laboratorio affinché usino soltanto un server DNS interno gestito dalla scuola, è possibile inserire in una lista nera i nomi di dominio dei principali servizi di IA, ad esempio chat.openai.com e simili, facendo in modo che la loro risoluzione fallisca o venga reindirizzata a una pagina di avviso. Questa misura è semplice da gestire ma da sola è aggirabile, perché uno studente esperto potrebbe impostare manualmente un DNS pubblico come 8.8.8.8.

Per questo si aggiunge un secondo livello sul firewall e sul proxy. Sul firewall perimetrale si bloccano gli indirizzi IP e i domini delle piattaforme di IA e si impedisce l'uso di DNS esterni, costringendo tutto il traffico a passare dal DNS interno. Inserendo poi un proxy con funzionalità di content filtering si può analizzare il traffico web, anche quello cifrato HTTPS tramite ispezione SSL, e bloccare per categoria tutti i siti riconducibili all'Intelligenza Artificiale, intercettando anche eventuali nuovi domini non presenti nella lista nera. Per riconoscere il traffico verso le piattaforme di IA anche quando queste cambiano dominio o si appoggiano a reti di distribuzione dei contenuti, si può ricorrere alla Deep Packet Inspection, che analizza il contenuto dei pacchetti e non solo l'indirizzo di destinazione.

Poiché gli studenti potrebbero tentare di aggirare i blocchi con VPN o servizi proxy esterni, è importante bloccare sul firewall anche le porte e i protocolli tipici delle VPN e i siti che offrono questi servizi, oltre a impedire l'installazione di software non autorizzato sui computer del laboratorio tramite policy di sistema e account privi di privilegi di amministratore.

Per quanto riguarda la schedulazione del blocco e del successivo sblocco in determinati momenti o in determinati laboratori, la soluzione più ordinata è sfruttare le regole del firewall basate sul tempo, le cosiddette time based ACL, che attivano o disattivano automaticamente i filtri in fasce orarie prestabilite, ad esempio durante le ore di laboratorio. In alternativa o in aggiunta si possono usare degli script schedulati, tramite cron su un sistema Linux oppure l'Utilità di pianificazione su Windows Server, che a un orario preciso modificano le regole di filtraggio o spostano le postazioni di un certo laboratorio in una VLAN con politiche più restrittive. Associando le regole a gruppi di indirizzi IP corrispondenti ai singoli laboratori, il blocco può essere applicato in modo selettivo solo dove e quando serve, lasciando liberi gli altri ambienti, ad esempio quando l'uso dell'IA è invece previsto dalla lezione.

mappedsa.it

vietata la condivisione

Quesito 4. Effetti del comando SSH con reindirizzamento di porta

Il comando ssh -p 25500 administrator@200.1.1.1 avvia una connessione SSH verso l'host con indirizzo pubblico 200.1.1.1, contattando però la porta 25500 al posto della porta standard 22, e chiede di autenticarsi come utente administrator.

Sul dispositivo 200.1.1.1, che svolge il ruolo di router o firewall di frontiera, è configurata una regola di port forwarding, ovvero di NAT di destinazione (DNAT), che reindirizza tutto il traffico in ingresso sulla porta 25500 verso la porta SSH di un altro dispositivo interno, quello con indirizzo privato 172.16.1.100. L'indirizzo 172.16.1.100 appartiene infatti a una rete privata e non sarebbe raggiungibile direttamente da Internet.

L'effetto pratico del comando è quindi che l'amministratore, pur scrivendo l'indirizzo pubblico 200.1.1.1, apre in realtà una sessione SSH sicura e cifrata con il dispositivo interno 172.16.1.100, sul quale potrà eseguire comandi da remoto. Il dispositivo 200.1.1.1 fa semplicemente da tramite e si limita a inoltrare i pacchetti. È importante notare che la sessione resta cifrata da un capo all'altro, perciò il dispositivo 200.1.1.1 non è in grado di leggere il contenuto dei comandi scambiati ma vede soltanto i pacchetti TCP che provvede a reindirizzare.

La finalità di questo tipo di configurazione è permettere la gestione remota e sicura di un apparato che si trova all'interno di una rete privata, senza esporlo direttamente su Internet. L'uso di una porta diversa da quella standard, la 25500 al posto della 22, è inoltre una misura di sicurezza per offuscamento che riduce il numero di tentativi di accesso automatici da parte dei bot, i quali in genere cercano la porta 22. Una configurazione simile è tipica per amministrare un server o un dispositivo collocato dietro a un NAT, ad esempio uno dei NAS o dei router presenti nei cantieri del progetto.

mappedsa.it

vietata la condivisione