Esame di Stato 2026 – Sistemi e Reti

Possibile soluzione e relazione di progetto

Infrastruttura digitale multi-Cantiere con architettura distribuita, storage ibrido e indirizzamento di classe C

Salvatore Capolupo, Docente di Sistemi e Reti

Sessione Ordinaria 2026

1 Premessa

Questa soluzione nasce da osservazioni, scambi di opinioni, appunti e riflessioni sviluppate nel periodo in cui stavo lavorando all'esame di maturità. Si ricorda che:

- la soluzione proposta è volutamente più corposa / dettagliata di quanto sia richiesto ad uno studente;
- serve a fornire spunti di approfondimento e riflessione sulle nuove tecnologie;
- non è vincolante per l'esito o la correzione dell'esame;
- potrebbe contenere errori o imprecisioni.

2 Introduzione (Prima Parte - Punto 1)

Il progetto richiede di definire l'architettura di rete, i dispositivi, i protocolli e la struttura di sicurezza di un sistema interconnesso , composto da una infrastruttura multi-cantiere scalabile.

Per usare le parole delle traccia, si dovrà predisporre *"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"*.

In accordo con i vincoli e le specifiche fornite dalla traccia, il sistema si basa sinteticamente sui seguenti aspetti:

- **Vincoli:** Trattandosi di cantieri - dotati tipicamente della sola energia elettrica - non sarà possibile sfruttare dispositivi cablati (ethernet). Tuttavia la traccia preveda la possibilità di farne uso in maniera ibrida, e per alcune sotto-categorie di dispositivi.
- **Scala della rete:** Il sistema si estende su un numero di cantieri geograficamente distribuiti sul territorio, che assumiamo pari a N. Essi saranno operanti in simultanea. Si assume, inoltre, che ogni cantiere disponga di M edifici, e che il progetto sia replicabile su ognuno di essi. Per semplicità progetteremo solo (si fa per dire...) l'i-esimo cantiere del j-esimo edificio, una sola volta per tutte.
- **Nodo di coordinamento:** Esiste una Sede Centrale (adibita al coordinamento tecnico, amministrativo e direzionale) e un (ipotizziamo) SaaS (Software as a Service) a supporto, deputato alla ricezione dei backup asincroni, alla sincronizzazione dei modelli BIM globali e all'erogazione di servizi analoghi / futuri.

- **Canale di interconnessione:** Il mezzo trasmissivo pubblico è la rete Internet, che non potrà essere utilizzato senza accorgimenti e protocolli di sicurezza. Come minimo useremo HTTPS come protocollo, ad esempio con certificato gratuito Let's Encrypt, e VPN con supporto a IP Sec.

2.1 Sede centrale

Alla sede centrale, i software BIM elaborano nuvole di punti (file di svariati GB), un formato di file con cui i candidati potrebbero non avere familiarità. Ovviamente non rileva il tipo di file ma solo - si fa per dire - la dimensione dello stesso. Il backbone (la dorsale) della LAN andrà realizzata ad esempio in fibra monomodale, per sopperire alle distanze tra rack/piani, alla larghezza di banda richiesta.

2.2 I cantieri

I cantieri sono ambienti in cui chiaramente cablare come in ufficio è impraticabile. ci sono pertanto varie soluzioni di connettività alternativa disponibili:

- connettività satellitare (ad esempio VSAT)
- connettività mobile 4G/5G (con SIM dati) per i tablet rugged + router / AP con SIM;
- Wi-Fi 6 / Wi-Fi 6E Wi-Fi 7 Reti MESH industriali

In questo contesto, se usiamo VPN con IPsec in modalità tunnel posso comunicare in modo sicuro tra i cantieri e la sede centrale. Standard da citare potrebbero essere IKEv2, crittografia AES-256, autenticazione con certificati X.509. È plausibile aggiungere dei firewall di cantiere per la sicurezza dati e un accesso controllato / limitato ai tablet (in modo che non possano accedere liberamente su internet, ma solo sui servizi autorizzati).

Si può anche ipotizzare che i tablet abbiano una - o addirittura due - SIM fisica/fisiche (ma nulla vieta di valutare l'installazione di eSIM aziendali).

2.3 I dispositivi

Ogni singolo cantiere presenta una densità di endpoint suddivisa in tre specifiche tipologie:

1. **Fascia IoT (Internet of Things) – Sensori Ambientali e di Sicurezza (assumiamo 100 unità):** Dispositivi dislocati capillarmente per il monitoraggio di parametri critici (monossido di carbonio, polveri sottili, vibrazioni strutturali, micro-movimenti dei ponteggi). Generano flussi costanti ma a bassissimo bit-rate.
2. **Fascia Video – Fotocamere Timelapse (assumiamo 10 unità):** Dispositivi ad alta risoluzione posizionati in punti strategici per la documentazione visiva dell'avanzamento dei lavori e per la sorveglianza perimetrale. Generano traffico pesante di tipo multimediale (immagini ad alta definizione e flussi video a scatti).
3. **Fascia Mobile – Tablet Rugged (ipotizziamo 5 unità):** Terminali mobili in dotazione ai direttori dei lavori e ai topografi per la consultazione e la modifica in loco delle nuvole di punti e del modello BIM. Questi dispositivi saranno **già connessi tramite SIM cellulare nativa 4G/5G**, consentendo una duplice o multipla modalità di connessione.

Per quello che riguarda i sensori, dovranno inviare e ricevere payload piccoli e frequenti (pochi byte alla volta), ma dovranno funzionare anche in condizioni ambientali non agevoli. MQTT (publish/subscribe, broker centrale, QoS 0/1/2) è lo standard de facto per l'IoT industriale. Si doterà pertanto il data center di un broker MQTT (es. Eclipse Mosquitto); Per una connessione sicura si può adottare MQTT over TLS (porta 8883).

I sensori si associano all'AP più vicino tramite Wi-Fi; il traffico MQTT over TLS (porta 8883) transiteranno nel tunnel VPN IPsec verso il broker Mosquitto in sede centrale.

2.4 LAN / Topologia / Access Point / Router con SIM

Per ovviare alle problematiche di attenuazione elettromagnetica tipiche degli ambienti edili (dovute a gabbie di Faraday, cemento armato e barriere di altro genere), si adotta una topologia di distribuzione perimetrale degli Access Point (AP).

Si assume inoltre che gli access point siano wireless, con distribuzione radiale del segnale, e che sia opportuno collocarli in alto e negli angoli del cantiere. Questo dovrebbe garantire, almeno sulla carta - e in assenza di ostacoli - una copertura più uniforme / completa dell'area di lavoro.

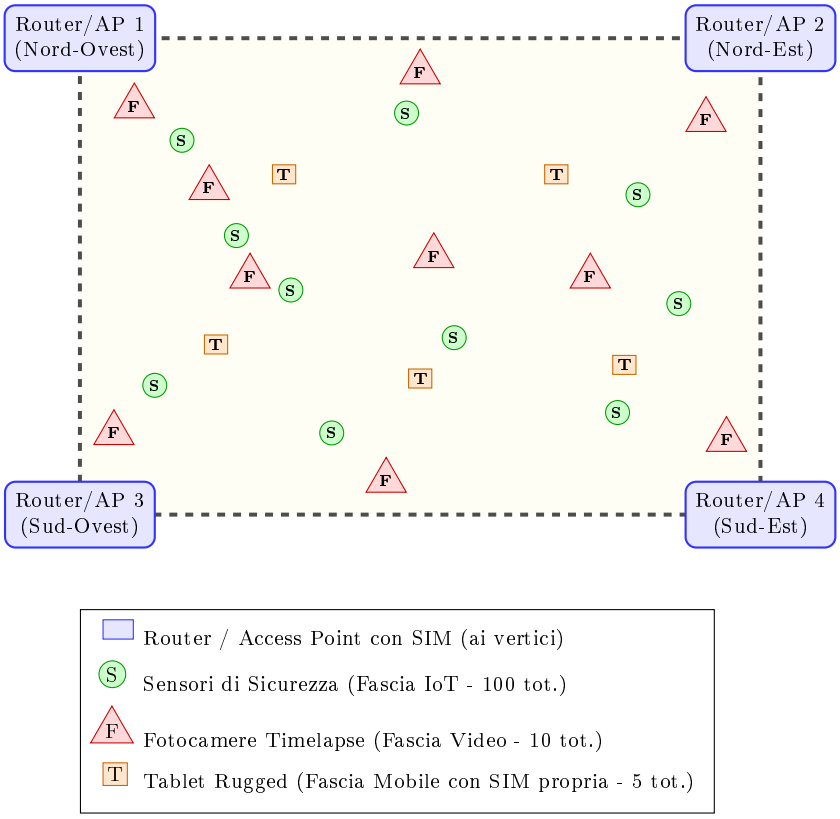
Per ogni edificio M_i verranno installati: **4 Access Point operanti come router, con SIM integrata**, posizionati agli **angoli (vertici) del cantiere**. Tale scelta permette:

- **Ridondanza WAN:** Ciascun angolo dispone di un uplink cellulare indipendente (4G/5G). I quattro router cooperano tramite protocolli di routing dinamico o architetture SD-WAN locali, garantendo che il cantiere resti online anche in caso di guasto hardware fino a tre dei quattro moduli radio.
- **Diversificazione degli Operatori:** Sarà possibile installare SIM di operatori differenti nei diversi angoli al fine di massimizzare la resilienza alle fluttuazioni di segnale delle stazioni radio base (SRB) locali.
- **Copertura Incrociata:** La disposizione ai quattro angoli permetterà di coprire l'intera area di cantiere, riducendo le "zone d'ombra" o prive di connettività.

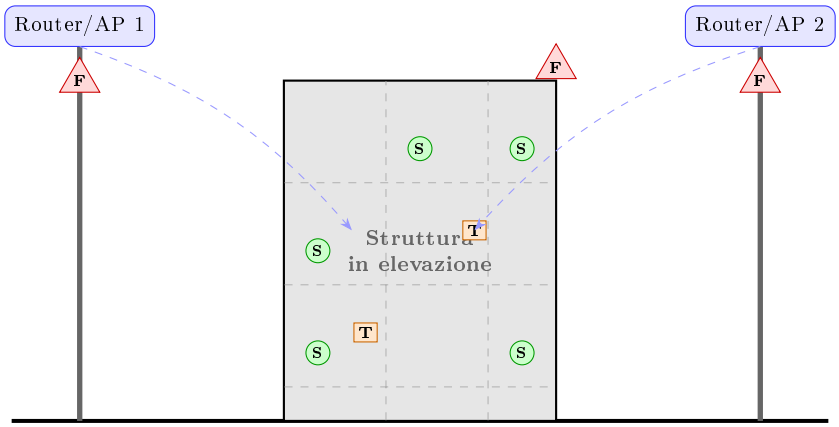
2.5 Schema del cantiere

Di seguito si riporta la modellazione grafica del cantiere, evidenziando la distribuzione dei dispositivi dislocati sul campo.

La mappa mostra il perimetro rettangolare del lotto, i 4 moduli Router/AP ai vertici e la distribuzione casuale dei sensori, delle fotocamere e dei tablet all'interno dell'area di lavoro.



Lo schema in sezione che segue mostra lo sviluppo verticale dello scavo e del fabbricato in corso d'opera. Evidenzia come gli AP/Router siano montati su pali telescopici perimetrali per superare l'altezza degli ostacoli strutturali, garantendo la connettività ai vari piani.



2.6 Piano di Indirizzamento IP Manuale (Classe C)

Come da specifica opzione progettuale, si adotta uno schema di indirizzamento **manuale** basato su indirizzi privati di **Classe C** (specificamente estratti dal blocco `192.168.0.0/16` previsto dalla RFC 1918). Questa scelta garantisce facilità di manutenzione e previene potenziali conflitti di instradamento (*overlapping*) all'interno dei tunnel VPN che collegano i cantieri alla Sede Centrale e al cloud.

Il modello è strutturato assegnando **un intero blocco di classe C (maschera fissa /24) per ogni cantiere**, per semplicità di trattazione. All'interno di ciascun cantiere, lo spazio di 254 indirizzi assegnabili verrà suddiviso manualmente in segmenti dedicati alle singole fasce di dispositivi. Si sarebbe potuto fare lo stesso, chiaramente, usando subnetting classico oppure VLSM (Variable Length Subnet Masking) al fine di ottimizzare l'assegnamento di IP.

Lo spazio viene gerarchicamente distribuito associando il terzo ottetto all'identificativo binario dell'infrastruttura:

- **Sede Centrale (LAN):** `192.168.0.0/24`
- **Cantiere 1:** `192.168.1.0/24`
- **Cantiere 2:** `192.168.2.0/24`
- **Cantiere N:** `192.168.N.0/24` (fino a un massimo di $N = 253$ cantieri distinti).

Prendendo come riferimento il Cantiere 1 (`192.168.1.0/24`), lo spazio di indirizzamento viene strutturato come segue::

Intervallo IP	Sotto-Maschera	Destinazione Fascia	Modalità Configurazione
`192.168.1.1` – `192.168.1.4`	/24 (Nativo)	Infrastruttura di Rete (I quattro AP/Router)	**Manuale** / **Statica** (IP fissi sui moduli d'angolo)
`192.168.1.10` – `.109`	/24 (Nativo)	**Fascia IoT:** 100 Sensori ambientali	**Manuale** (Pre-configurata a bordo firmware del sensore)
`192.168.1.120` – `192.168.1.129`	/24 (Nativo)	**Fascia Video:** 10 Fotocamere Timelapse	**Manuale** (Mappatura statica per NVR/Storage)
`192.168.1.140` – `192.168.1.144`	/24 (Nativo)	**Fascia Mobile:** 5 Tablet Rugged	**DHCP con Reservation** (Legati al MAC-address via Wi-Fi)
`192.168.1.200` – `192.168.1.252`	/24 (Nativo)	Area di Riserva Espansioni Future	–
`192.168.1.253`	/24 (Nativo)	Switch di Cantiere Intermedio	**Manuale** / **Statica**

2.7 Connettività mobile

Un'attenzione particolare merita l'integrazione dei 5 tablet rugged. Essendo dotati di SIM propria, essi possiedono un indirizzo IP assegnato dall'operatore mobile (tipicamente un IP pubblico dinamico aziendale).

A partire dalle reti **LTE/4G** fino al **5G Standalone**, la mobilità geografica pura è gestita nativamente e in modo trasparente dall'infrastruttura Core dell'operatore telefonico. Grazie a questi meccanismi di rete, l'IP pubblico / nattato assegnato alla SIM del tablet rimane lo stesso per tutta la durata della connessione, indipendentemente dagli spostamenti che facciamo.

Avendo 4 router distribuiti ai quattro angoli del cantiere, l'instradamento del traffico viene gestito secondo una logica di **Default Gateway Virtuale** tramite protocolli di ridondanza hardware come VRRP (*Virtual Router Redundancy Protocol*).

- I quattro router configurano un IP virtuale comune (es. `192.168.1.254`) che funge da gateway predefinito per tutti i sensori e le fotocamere.
- Il router posizionato sull'angolo con le migliori condizioni di ricezione cellulare assume il ruolo di *Master*, prendendosi carico del traffico in uscita e mantenendo attivo il tunnel VPN principale verso la Sede Centrale.
- Gli altri tre router rimangono in stato di *Backup*. In caso di saturazione della banda o di caduta della cella radio del router Master, il protocollo commuta istantaneamente il traffico sul vertice alternativo senza interruzioni di servizio (*session persistence*).

Il modello BIM centralizzato risiede fisicamente su un cluster di NAS (*Network Attached Storage*) installato nella Sede Centrale, operando in modalità On-Premise per garantire la massima velocità di elaborazione ai progettisti interni alla LAN aziendale.

3 (Prima Parte - Punto 2)

In questa seconda parte si fa riferimento alla richiesta della "*descrizione della ipotetica struttura della rete pre-esistente in sede centrale, con proposte di integrazione e potenziamento necessarie per l'adozione del sistema BIM*".

Possiamo ipotizzare che la Sede Centrale (SC) disponga di una rete LAN cablata con topologia a stella, basata su switch gigabit e router/firewall per l'accesso a Internet. La rete interna supporta già servizi di condivisione file, posta elettronica e accesso remoto tramite VPN (ad esempio aziendale).

Dobbiamo inoltre mettere a disposizione un file server e/o una serie di NAS per l'archiviazione dei modelli BIM e dei dati di progetto, magari distinguendoli sulla base della provenienza (se da cantiere C_1, C_2, ...). Tale file server dovrà avere un indirizzo IP privato, ad esempio di classe A, e si potrà ad esempio collocare dentro una DMZ (zona demilitarizzata) per garantire l'accesso sicuro dai cantieri remoti. Per realizzarla, porremo due firewall in serie, uno perimetrale e uno interno, con regole di filtraggio specifiche per i protocolli utilizzati (HTTPS, SFTP, VPN) in modo da limitare il rischio di intrusioni.

Sarà inoltre disponibile una sottorete per l'amministrazione, uno per la gestione dei backup e uno per i backup incrementali (dei dati raccolti dai cantieri).

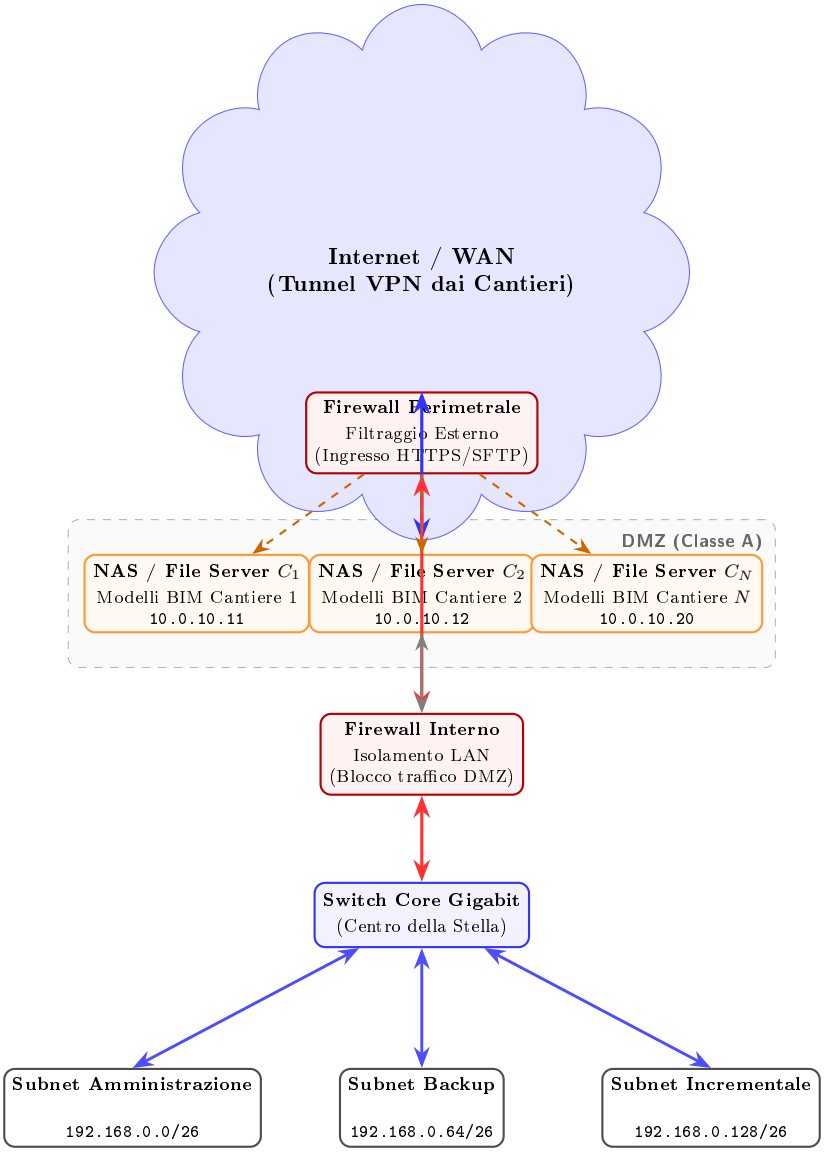
A livello grafico potremmo avere pertanto qualcosa del genere, pronta da interfacciare con l'esterno (e sebbene la traccia presupponga di averla a disposizione, non di doverla progettare):

La Sede Centrale (SC) funziona da centro di coordinamento per l'intera infrastruttura multi-cantiere. In conformità con i requisiti di massima sicurezza e segregazione dei compiti, la rete interna è strutturata tramite una topologia a stella protetta da un'architettura DMZ (Demilitarized Zone) con doppio firewall (Back-to-Back).

La comunicazione tra i cantieri e la sede centrale avviene mediante tunnel VPN sicuri basati su SSL / IPSec, garantendo la cifratura end-to-end dei dati trasmessi.

Dato che la rete funziona con ADSL, è ragionevole ipotizzare che possa essere rimpiazzata - o affiancata, al limite - da una seconda rete mobile 4G/5G, da una connessione in fibra ottica FFTH oppure, ancora, da un collegamento satellitare.

Di seguito viene riportato lo schema logico e strutturale dei flussi di rete e della segmentazione interna della SC.



L'infrastruttura rispetta i seguenti vincoli progettuali:

1. **Separazione dello Storage BIM in DMZ:** Il cluster di NAS/File Server è configurato con indirizzi IP privati su SD-WAN di classe A (es. all'interno del blocco `10.0.0.0/8` come già nella traccia del 2024). Lo storage sarà fisicamente diviso in volumi logici o macchine indipendenti $(V_1, V_2, \ldots, V_N)$, associate univocamente al cantiere di provenienza $(C_1, C_2, \ldots, C_N)$.
2. **Firewall:**
   - **Firewall Perimetrale:** Isola la DMZ da Internet. Permette esclusivamente le connessioni in ingresso originate dai router perimetrali dei cantieri remoti tramite protocolli crittografati HTTPS (porta 443) per l'interfaccia web BIM, SFTP (porta 22) per il caricamento dei file pesanti e i tunnel VPN (IPsec/WireGuard).
   - **Firewall Interno:** Isola la LAN aziendale dalla DMZ. Impedisce qualsiasi connessione originata dalla DMZ verso la LAN interna (se un server in DMZ venisse compromesso, l'attaccante non potrebbe accedere alla rete centrale).

3. **LAN a Stella:** Lo Switch Core serve a smistare il traffico interno su tre sotto-reti separate:
    - **Sottorete Amministrazione:** Si occupa della gestione dei terminali e degli apparati di rete;
    - **Sottorete Gestione Backup:** Si occupa sia dei backup che dei log
    - **Sottorete Backup Incrementali:** Riceve, elabora e crea lo storico dei flussi asincroni di micro-dati ambientali (MQTT) e immagini (Timelapse) provenienti dai cantieri.

4 (Prima Parte - Punto 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"

- **Mezzo trasmissivo:** connettività mobile 4G/5G tramite router/AP con SIM integrata (uno per vertice del cantiere); in alternativa o come fallback, collegamento VSAT (standard DVB-S2/DVB-RCS2) per cantieri in zone prive di copertura cellulare adeguata.
- **Protocollo di sicurezza:** tunnel VPN IPsec in modalità tunnel, IKEv2, cifratura AES-256, autenticazione con certificati X.509; HTTPS (Let's Encrypt) come strato applicativo aggiuntivo.
- **Ridondanza WAN:** 4 router perimetrali ai vertici del cantiere operanti in VRRP; IP virtuale comune (es. `192.168.1.254`); il router Master gestisce il tunnel VPN principale, gli altri tre in Backup con failover automatico.
- **Stima della capacità trasmissiva:**
    - Fascia IoT (100 sensori MQTT): traffico trascurabile, pochi byte/messaggio, aggregato < 1 Mbps;
    - Fascia Video (10 fotocamere timelapse 4K/8K): upload asincrono di fotogrammi, stimabile in $\sim$10–20 Mbps per sessione;
    - Fascia Mobile (5 tablet rugged, sync nuvole di punti): file da svariati GB, upload programmato fuori orario di punta, banda richiesta $\sim$20–50 Mbps per sessione.
    - **Totale stimato per cantiere:** $\sim$50–100 Mbps garantiti in uplink; 4G/5G (tipicamente 50–300 Mbps in upload con SIM aziendale) è sufficiente; VSAT Ka offre 20–50 Mbps in upload come fallback accettabile.
- **Apparati da adottare:**
    - 4 router industriali 4G/5G con doppia SIM (operatori diversificati), Wi-Fi integrato, supporto IPsec/IKEv2, montaggio su palo telescopico perimetrale;
    - 1 terminale VSAT (antenna + modem DVB-S2/RCS2) per cantieri remoti;
    - Firewall perimetrale in sede centrale per la terminazione dei tunnel VPN in ingresso dai cantieri.

5 (Prima Parte - Punto 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."

- **In sede (LAN locale):** autenticazione centralizzata tramite protocollo **RADIUS** (RFC 2865) con backend **LDAP/Active Directory**; credenziali username+password con obbligo di **2FA** (TOTP, es. Google Authenticator).

- **Da remoto (cantieri):** accesso ai sistemi della sede centrale esclusivamente *dentro* il tunnel VPN IPsec già attestato; autenticazione operatore via **SSH** con coppia di chiavi RSA/Ed25519 (no password) oppure via **HTTPS** con certificato client X.509 emesso dalla CA aziendale.
- **Servizi coinvolti:**
  - **LDAP/AD** – gestione centralizzata di utenti, ruoli e permessi;
  - **RADIUS** – autenticazione di rete per accesso a switch, AP e VPN;
  - **PKI interna** – emissione e revoca certificati X.509 per apparati e utenti;
  - **SSH** (porta non standard, es. 2222) – accesso amministrativo ai server con port forwarding se necessario.

1 (Seconda Parte - Punto 1)

"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."

Le soluzioni **on premise** (NAS/cluster in sede) garantiscono latenza minima, controllo totale dei dati e indipendenza dalla connettività, ma richiedono investimento hardware iniziale e manutenzione interna. Le soluzioni **cloud-based** (SaaS/IaaS) offrono scalabilità immediata, accesso multi-cantiere e backup automatico, al costo di dipendenza dalla banda WAN e da fornitori terzi per la sovranità del dato.

2 (Seconda Parte - Punto 2)

"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."

Nella sede centrale si adotta un'architettura **DMZ a doppio firewall** (perimetrale e interno) con regole ACL restrittive per i protocolli ammessi (HTTPS, SFTP, IPsec).

Nei cantieri i router perimetrali applicano **NAT** e filtrano il traffico in uscita limitandolo ai soli servizi autorizzati, impedendo ai dispositivi di campo l'accesso libero a Internet. La continuità trasmissiva è garantita dalla ridondanza **VRRP** sui quattro router d'angolo con SIM di operatori diversificati e, come fallback, dal collegamento **VSAT**. Tutti i log di sicurezza (firewall, IDS, MQTT broker) sono centralizzati in sede su un sistema **SIEM** per correlazione degli eventi e conservazione dello storico.

3 (Seconda Parte - Punto 3)

"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."

Il problema è posto in un contesto scolastico e presenta diverse possibili soluzioni che possono essere adottate. Questo vale sia in modalità software che hardware, ed eventualmente con un ibrido o combinazione di più tecniche tra loro.

Il modo più semplice, in prima istanza, è quello di bloccare l'accesso a tali piattaforme stilando una blacklist di domini e/o indirizzi IP noti, come ad esempio: chatgpt.com, openai.com, gemini.google.com, copilot.microsoft.com, ...

Come impostare una lista di domini bloccati in una rete scolastica? Un modo potrebbe essere quello di utilizzare un firewall o un router con funzionalità di filtraggio dei domini, ad esempio tramite DNS filtering o URL filtering. Sui modelli TP-link ad esempio è possibile impostare una lista di domini bloccati direttamente nell'interfaccia di amministrazione del router, come ad esempio HomeShield sui router TP-Link. In alternativa, si può utilizzare un server DNS locale che filtra le richieste DNS verso i domini bloccati, e un esempio in tal senso è NextDNS. La funzionalità blacklist blocca un dominio e tutti i sottodomini, per cui potrei impostarlo su:

```
chatgpt.com
openai.com
gemini.google.com
copilot.microsoft.com
```

La lista può essere aggiornata dinamicamente a livello applicativo, ad esempio tramite uno script che scarica periodicamente un file di testo con i domini da bloccare, seguendo la stessa falsariga con cui vengono aggiornate le liste di blocco dei contenuti pubblicitari o spam (disponibili in genere su github.com e simili).

Questo approccio ha un limite: gli studenti potrebbero aggirare il blocco mediante VPN o proxy. Questo suggerisce che sia altresì fondamentale l'uso di sistemi operativi adeguatamente configurati, e che non trapelino le password di amministratore o di root. Solo in questo modo i ragazzi non potranno installare nulla in autonomia. MA anche questo non basta: la traccia è uno spunto di riflessione considerevole, in tal senso, per capire il mondo in cui viviamo e le difficoltà di alcuni problemi di informatica.

Si potrebbero combinare le tecniche precedenti con l'uso di una regola ACL (Access Control List) per bloccare un ipotetico server di un'IA su un router/firewall tradizionale, ammesso che una certa IA si trovi sull'IP 104.17.33.154 e agisca sulla porta 443 (HTTPS):

```
deny tcp any host 104.17.33.154 eq 443
```

ovvero: blocca/rifiuta tutto il traffico TCP proveniente da qualsiasi origine e diretto verso l'indirizzo IP 104.17.33.154 sulla porta HTTPS 443.

L'uso di un Next-Generation Firewall (NGFW) o un filtro basato su DNS (come NextDNS) può compensare ulteriormente i limiti degli approcci standard. I firewall NGFW a Deep Packet Inspection (DPI) / filtraggio dei domini consentono di bloccare la categoria "Generative AI" o i domini specifici con una semplice regola testuale (es. block *openai.com* o block *claude.ai*), indipendentemente dall'indirizzo IP che utilizzano in quel momento.

La schedulazione del blocco può essere realizzata tramite regole temporizzate sul firewall (per orario e VLAN di laboratorio) oppure tramite un task pianificato (`cron`) sul server DNS locale, che attiva e disattiva le blacklist negli orari di lezione stabiliti.

Altre soluzioni, qui non approfondite solo per brevità, potrebbero coinvolgere l'uso di firewall con blocco dei contenuti a pacchetto, sistemi di autenticazione a due fattori, o l'uso di software di monitoraggio e controllo delle attività degli studenti sui computer scolastici (NetSupport).

In generale non sembra poter esistere una soluzione definitiva e sicura al 100gli IP e i domini possono cambiare nel tempo, e potrebbero uscire nuove IA non considerate o non note all'amministratore.

4 (Seconda Parte - Punto 4)

"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."

Il comando da terminale remoto:

```
ssh -p 25500 administrator@200.1.1.1
```

permette di accedere al server identificato dall'indirizzo IP 200.1.1.1 come amministratore sulla porta 25500. Poichè è attiva una regola di reindirizzamento verso un secondo dispositivo identificato da 172.16.1.100, questo comando è utile per consentire l'accesso ad un terminale remoto con privilegi di administrator su quest'ultimo dispositivo, usando 200.1.1.1 come gateway perimetrale, router o firewall..

Nel contesto descritto, l'operazione effettuata è un classico esempio di **Port Forwarding** (nello specifico, *Destination NAT* o *Port Mapping*).

Effetti del comando

- **Richiesta iniziale:** Il client SSH avvia una connessione verso l'IP pubblico `200.1.1.1` sulla porta non standard `25500`.
- **Reindirizzamento:** Il dispositivo perimetrale (`200.1.1.1`) intercetta il traffico e, in base alla regola configurata, ne modifica l'IP di destinazione inoltrando i pacchetti verso l'host interno `172.16.1.100` (generalmente sulla porta standard SSH `22`).
- **Risultato:** Il candidato effettua il login come `administrator` direttamente sul dispositivo della rete privata (`172.16.1.100`), pur avendo digitato l'indirizzo del gateway pubblico.

Finalità di utilizzo

- **Accessibilità:** Permette di raggiungere da remoto un host con IP privato (non instradabile su Internet).
- **Sicurezza:** L'uso di una porta non standard (`25500` invece di `22`) riduce l'esposizione a scansioni automatizzate e attacchi brute-force.
- **Ottimizzazione delle risorse:** Consente di esporre molteplici servizi interni utilizzando un unico indirizzo IP pubblico, differenziandoli unicamente tramite la porta d'ingresso.

Allegato: Traccia Originale dell'Esame

Sessione ordinaria 2026
Seconda prova scritta

Ministero dell'Istruzione e del Merito

A038 - ESAME DI MATURITÀ

Indirizzo ITIA - INFORMATICA E TELECOMUNICAZIONI ARTICOLAZIONE "INFORMATICA"
(Testo valevole anche per gli indirizzi quadriennali IT32)

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 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.

[1] I tablet "rugged" sono progettati per funzionare in modo affidabile in condizioni di lavoro difficili, con resistenza a urti e cadute, impermeabilità, resistenza alla polvere, batterie a lunga durata e/o sostituibili, porte per vari supporti e connettività avanzate, display più facilmente leggibili all'aperto.

Sessione ordinaria 2026
Seconda prova scritta

Ministero dell'Istruzione e del Merito

A038 - ESAME DI MATURITÀ

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:

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.

Sessione ordinaria 2026
Seconda prova scritta

Ministero dell'Istruzione e del Merito

A038 - ESAME DI MATURITÀ

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.

Durata massima della prova: 6 ore.
È consentito l'uso di manuali tecnici e di calcolatrici scientifiche o grafiche purché non siano dotate della capacità di elaborazione simbolica algebrica e non abbiano la disponibilità di connessione a Internet.
È consentito l'uso del dizionario bilingue (italiano-lingua del Paese di provenienza) per i candidati di madrelingua non italiana.
Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla consegna della traccia.