Esercizio di sistemi e reti: fare una lettura del testo proposto e immaginare una possibile soluione.

Un'azienda decide di aprire una filiale in una città vicina. Nella nuova sede dovranno essere installati e configurati circa 30 nuovi computer e 3 stampanti di rete. In questa nuova succursale dovranno inoltre essere installati 1 file server per l'archiviazione e 1 web server per il sito intranet aziendale che non deve essere accessibile però da Internet.
Nella sede centrale i dispositivi sono configurati con indirizzi IP del tipo 192.168.1.0/24 e dovranno poter accedere al file server e al sito intranet sviluppato e pubblicato nella rete della nuova sede.
L'ISP ha già consegnato in questa nuova sede il router per il collegamento ad Internet pre configurato con indirizzo IP privato 192.168.0.1/24 e indirizzo pubblico 84.23.67.121/29.

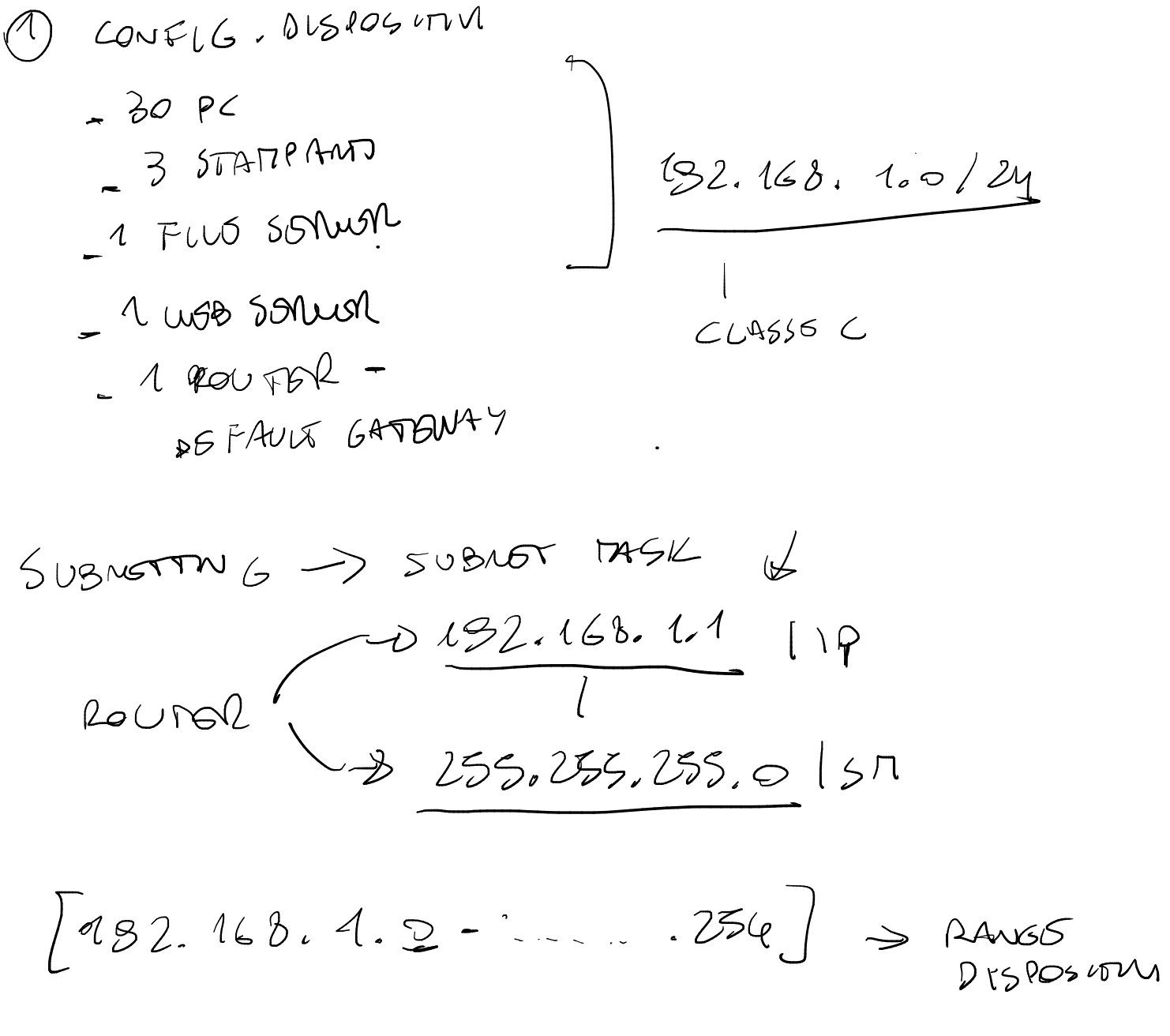
L'azienda richiede:

1. una configurazione dei dispositivi semplice da gestire
2. una configurazione di rete che preveda alti standard di sicurezza
3. una documentazione dell'architettura di rete comprensiva degli indirizzamenti utilizzati
4. una documentazione che riporti i servizi di rete previsti e la loro configurazione

Il sito intranet aziendale, previa autenticazione, permette agli utenti di specificare i lavori svolti durante la giornata al fine di consuntivare a fine mese le attività suddivise per utente o suddivise per cliente.

***Seconda parte:***

1. Spiegare i vantaggi ed il funzionamento del TCP/IP.
2. Spiegare cos'è una VPN basata sul protocollo IPSec, quali sono le sue caratteristiche e le problematiche specifiche.
3. Scrivere la definizione di sicurezza informatica (ISO) e descriverne gli specifici attributi.



Per facilitare la gestione e garantire alti standard di sicurezza, implementerei la segmentazione della rete attraverso VLAN:

- **VLAN 10 (Uffici)**: 192.168.10.0/24
  - Computer (30): 192.168.10.2-192.168.10.31
  - Stampanti (3): 192.168.10.50-192.168.10.52
- **VLAN 20 (Server)**: 192.168.20.0/24
  - File server: 192.168.20.2
  - Web server intranet: 192.168.20.3

PC + STAMPANTI

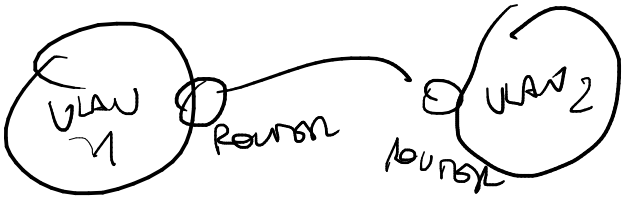
SERVER

VLAN 2 DIVISIONI IN 2 SOTTORETI

→ ARCHITETTURA DI RETE

- 30 PC
- 3 STAMPANTI
- 1 FILE SERVER
- 1 WEB SERVER
- 1 ROUTER - DEFAULT GATEWAY

- SWITCH PER LE VLAN (2)
- ROUTER PERIMETRALE




- FIREWALL

→ SICUREZZA DI RETE

- SERVER → SOFTWARE ENTERPRISE
- DHCP →
- INTRANET → DNS INTERNO
  NAT
  MASCHERA IP PRIVATI
- VPN → TUNNELING TRA HOST
- POLICY DI ACCESSO

- MONITORAGGIO CON LOG SENSOR

***Seconda parte:***

1. Spiegare i vantaggi ed il funzionamento del TCP/IP.
2. Spiegare cos'è una VPN basata sul protocollo IPSec, quali sono le sue caratteristiche e le problematiche specifiche.
3. Scrivere la definizione di sicurezza informatica (ISO) e descriverne gli specifici attributi.

1. TCP → MODULO A STRATI → SUITE DI PROTOCOLLI
   - AFFIDABILE
   - INTEROPERABILE

## TCP/IP: Vantaggi e funzionamento

Il TCP/IP (Transmission Control Protocol/Internet Protocol) è un modello di comunicazione a strati che standardizza l'interoperabilità di rete. I principali vantaggi sono:

- **Interoperabilità**: Consente comunicazione tra dispositivi eterogenei
- **Scalabilità**: Supporta reti di qualsiasi dimensione
- **Robustezza**: Tolleranza ai guasti e ritrasmissione dei pacchetti persi
- **Indipendenza dall'hardware**: Funziona su qualsiasi infrastruttura fisica

Il TCP/IP opera su quattro livelli:

1. **Livello di accesso alla rete**: Gestisce l'hardware di rete e la trasmissione fisica
2. **Livello Internet (IP)**: Indirizzamento logico e instradamento dei pacchetti
3. **Livello di trasporto (TCP/UDP)**: Affidabilità (TCP) o velocità (UDP) della connessione
4. **Livello applicazione**: Implementa protocolli di alto livello (HTTP, FTP, ecc.)

## VPN IPSec: Caratteristiche e problematiche

Una VPN basata su IPSec (Internet Protocol Security) è un sistema che crea canali di comunicazione cifrati attraverso reti non sicure.

**Caratteristiche principali**:

- **Sicurezza a livello IP**: Opera al livello 3 (rete) del modello OSI
- **Autenticazione** tramite certificati digitali o chiavi pre-condivise
- **Integrità dei dati** garantita da hash crittografici
- **Confidenzialità** tramite algoritmi di cifratura (AES, 3DES)
- **Modalità tunnel** (incapsula l'intero pacchetto IP) o **trasporto** (solo payload)

**Problematiche specifiche**:

- **Complessità di configurazione** rispetto ad altre soluzioni VPN
- **Overhead di elaborazione** dovuto alla crittografia
- **Problemi con NAT** (Network Address Translation)
- **Difficoltà con firewall** che bloccano protocolli IPSec (ESP/AH)
- **Gestione delle chiavi** complessa in ambienti di grandi dimensioni

## Sicurezza informatica (ISO): Definizione e attributi

La sicurezza informatica, secondo l'ISO/IEC 27001, è definita come la protezione dell'informazione e dei sistemi informativi da accessi, utilizzi, divulgazioni, interruzioni, modifiche o distruzioni non autorizzate.

**Attributi specifici**:

1. **Confidenzialità**: Garanzia che le informazioni siano accessibili solo a chi è autorizzato
2. **Integrità**: Protezione dell'accuratezza e completezza dei dati durante l'intero ciclo di vita
3. **Disponibilità**: Assicurazione che le risorse siano accessibili quando necessario
4. **Autenticità**: Verifica che un'entità sia effettivamente chi dichiara di essere
5. **Non ripudio**: Impossibilità di negare di aver eseguito un'azione
6. **Responsabilità** (Accountability): Tracciabilità delle azioni svolte sui sistemi