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.

Progettazione di rete per filiale aziendale

Piano di indirizzamento IP

Per soddisfare i requisiti della nuova filiale, propongo il seguente schema di indirizzamento IP:

- **Subnet principale filiale**: 192.168.0.0/24
  - Gateway: 192.168.0.1 (router ISP)
  - Range dispositivi: 192.168.0.2-192.168.0.254

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

Architettura di rete

L'architettura proposta prevede:

1. **Router perimetrale** (già fornito dall'ISP)
   - Interfaccia WAN: 84.23.67.121/29
   - Interfaccia LAN: 192.168.0.1/24
2. **Firewall/UTM** posizionato tra il router ISP e la rete interna
   - Interfaccia esterna: 192.168.0.2/24
   - Interfaccia interna: 192.168.0.3/24
3. **Switch Layer 3 core** per gestione VLAN e routing interno
   - Interfaccia di gestione: 192.168.0.4/24
   - Implementazione delle VLAN 10 e 20
4. **Switch di accesso** per la connessione dei dispositivi terminali

Servizi di rete

1. **DHCP**: Configurato sul firewall/UTM per assegnare indirizzi IP dinamici ai client
   - Pool VLAN 10: 192.168.10.100-192.168.10.254
   - Prenotazioni statiche per computer e stampanti
2. **DNS interno**: Implementato sul firewall/UTM
   - Risoluzione nomi per risorse interne (fileserver.azienda.local, intranet.azienda.local)
3. **Servizio VPN IPSec**: Configurato sul firewall per connessioni sicure dalla sede centrale
   - Tunnel IPSec tra 84.23.67.121 (filiale) e IP pubblico sede centrale
4. **Web server intranet**:
   - Non accessibile da Internet (bloccato a livello firewall)
   - Autenticazione integrata con Active Directory
   - HTTPS obbligatorio
5. **File server**:
   - Protocolli SMB/CIFS con crittografia abilitata
   - Backup automatizzato

Standard di sicurezza

1. **Firewall UTM** con:
   - Ispezione pacchetti stateful
   - IPS/IDS per rilevamento intrusioni
   - Filtro contenuti web
   - Antivirus perimetrale
2. **Segmentazione VLAN** per limitare la propagazione di attacchi
3. **Policy di accesso** basate sul principio del minimo privilegio
4. **Crittografia** per tutti i servizi di rete (HTTPS, SMB con crittografia)
5. **Monitoraggio centralizzato** con invio log a server SIEM nella sede centrale

Seconda parte: Risposte teoriche

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

Questi attributi formano il nucleo di qualsiasi framework di sicurezza informatica e costituiscono i pilastri su cui si fondano le politiche di sicurezza aziendali.