| **IIS Costanzo”**  **Istituto Tecnico Informatico**  **Soveria Mannelli (CZ)**  **LABORATORIO DI SISTEMI E RETI**  **ESERCITAZIONE N° \_\_5\_\_\_\_ ANNO SCOLASTICO 2024/2025** | **Allievo Colosimo Pietro Salvatore**  **Classe e Sez. 5 H**  **Data \_\_\_12/03/2025\_\_\_** |
| --- | --- |
| **TEMA DELL’ESERCITAZIONE**  **Reti e VPN** | |
| **RELAZIONE**  1. **Introduzione**  2. **Concetti Fondamentali**  2.1 Definizione di VPN  2.2 Storia ed evoluzione delle VPN  2.3 Principi di sicurezza e privacy  3. **Tipologie di VPN**  3.1 VPN Remote Access  3.2 VPN Site-to-Site  3.3 VPN Mobile  3.4 VPN Peer-to-Peer  4. **Protocolli e Tecnologie**  4.1 PPTP (Point-to-Point Tunneling Protocol)  4.2 L2TP/IPsec (Layer 2 Tunneling Protocol)  4.3 OpenVPN  4.4 WireGuard  4.5 SSL/TLS VPN  5. **Funzionamento delle VPN**  5.1 Creazione del Tunnel VPN  5.2 Processo di autenticazione  5.3 Crittografia dei dati  5.4 Routing del traffico  6. **Vantaggi e Svantaggi**  6.1 Protezione della privacy e anonimato  6.2 Accesso a contenuti geolocalizzati  6.3 Sicurezza nelle reti Wi-Fi pubbliche  6.4 Impatti sulle prestazioni della rete  6.5 Possibili vulnerabilità e rischi  **1. Introduzione**  Le VPN (Virtual Private Network) sono strumenti fondamentali per garantire comunicazioni sicure, mascherando il traffico di dati, sia in azienda ma anche in ambito personale, utili a proteggerci da determinate minacce informatiche.  **2. Concetti Fondamentali**  **2.1 Definizione di VPN**  Una Virtual Private Network (VPN) è una tecnologia che consente di creare una connessione sicura e criptata attraverso una rete pubblica (come Internet). Questo "tunnel" virtuale permette di trasmettere dati in modo sicuro, proteggendo la comunicazione da intercettazioni non autorizzate.  **2.2 Storia ed Evoluzione delle VPN**  - **Origini e necessità:** Le VPN sono nate per rispondere alla necessità di collegare in sicurezza sedi remote, consentendo lo scambio di informazioni sensibili senza dover ricorrere a costosi collegamenti dedicati.  - **Evoluzione tecnologica:** Con l’aumentare delle minacce informatiche e la diffusione di Internet, le VPN si sono evolute passando da protocolli iniziali, come PPTP, a soluzioni più sicure come L2TP/IPsec, OpenVPN e WireGuard.  - **Adattamento alle nuove esigenze:** La crescita del lavoro da remoto e la necessità di accedere in sicurezza alle risorse aziendali hanno reso le VPN uno strumento imprescindibile sia per le aziende che per i singoli utenti.  **2.3 Principi di Sicurezza e Privacy**  - **Crittografia:** Le VPN impiegano algoritmi crittografici per proteggere i dati durante il transito, rendendoli illeggibili a eventuali intercettatori.  - **Autenticazione:** Processi che verificano l’identità degli utenti e dei server, prevenendo accessi non autorizzati.  - **Integrità dei dati:** Meccanismi che garantiscono che i dati non vengano alterati durante il trasferimento, assicurando l’affidabilità della comunicazione.  - **Privacy degli utenti:** Le VPN offrono un ulteriore livello di privacy mascherando l’indirizzo IP e consentendo una navigazione più anonima, contrastando il tracciamento da parte di terzi.  **3. Tipologie di VPN**  Le VPN possono essere suddivise in diverse categorie in base alla loro configurazione e al tipo di connessione che offrono. Ogni tipologia risponde a esigenze specifiche e presenta vantaggi e svantaggi distinti.  **3.1 VPN Remote Access**  Le VPN di accesso remoto consentono agli utenti di connettersi a una rete privata da una posizione remota attraverso Internet. Vengono spesso utilizzate per accedere in sicurezza a risorse aziendali o per proteggere la navigazione in reti pubbliche.  - **Vantaggi:** Facile configurazione, sicurezza nelle connessioni da remoto.  - **Svantaggi:** Rallentamenti dovuti alla crittografia, necessità di un client VPN dedicato.  **3.2 VPN Site-to-Site**  Le VPN site-to-site collegano intere reti locali (LAN) attraverso Internet, creando un’unica rete estesa (WAN). Sono comunemente usate per connettere sedi aziendali distanti tra loro.  - **Vantaggi:** Maggiore sicurezza rispetto a connessioni dirette, gestione centralizzata.  - **Svantaggi:** Configurazione complessa, necessità di hardware dedicato.  **3.3 VPN Mobile**  Progettate per dispositivi mobili, queste VPN ottimizzano le connessioni in movimento, adattandosi ai cambiamenti di rete tra Wi-Fi e dati mobili.  - **Vantaggi:** Continuità della connessione, sicurezza in ambienti pubblici.  - **Svantaggi:** Maggiore consumo energetico, possibili problemi di stabilità.  **3.4 VPN Peer-to-Peer**  Questa tipologia di VPN sfrutta la tecnologia peer-to-peer (P2P), connettendo direttamente i dispositivi degli utenti senza passare per un server centrale.  - **Vantaggi:** Maggiore decentralizzazione, riduzione del carico sui server.  - **Svantaggi:** Rischi di sicurezza, possibile instabilità della rete.  **4. Protocolli e Tecnologie**  Le VPN si basano su diversi protocolli per garantire la sicurezza e la trasmissione efficace dei dati. Ogni protocollo offre un diverso livello di crittografia, velocità e compatibilità.  **4.1 PPTP (Point-to-Point Tunneling Protocol)**  Uno dei primi protocolli VPN sviluppati da Microsoft, ormai considerato obsoleto a causa della scarsa sicurezza.  - **Vantaggi:** Elevata compatibilità, facile configurazione.  - **Svantaggi:** Vulnerabilità note, crittografia debole.  **4.2 L2TP/IPsec (Layer 2 Tunneling Protocol)**  Combinazione tra L2TP e IPsec, offre un buon livello di sicurezza grazie alla crittografia avanzata.  - **Vantaggi:** Maggiore sicurezza rispetto a PPTP, compatibilità diffusa.  - **Svantaggi:** Prestazioni inferiori a causa della doppia incapsulazione.  **4.3 OpenVPN**  Uno dei protocolli più utilizzati grazie alla sua flessibilità, sicurezza e supporto per connessioni SSL/TLS.  - **Vantaggi:** Open-source, elevata sicurezza, altamente configurabile.  - **Svantaggi:** Configurazione complessa per utenti non esperti.  **4.4 WireGuard**  Un protocollo moderno e leggero, progettato per offrire velocità e sicurezza superiori rispetto ai protocolli tradizionali.  - **Vantaggi:** Codice snello, elevata efficienza e prestazioni.  - **Svantaggi:** Supporto relativamente recente, compatibilità ancora limitata su alcuni sistemi.  **4.5 SSL/TLS VPN**  Basate sul protocollo SSL/TLS, queste VPN permettono di stabilire connessioni sicure senza necessità di software client dedicati.  - **Vantaggi:** Accesso tramite browser, facilità d’uso.  - **Svantaggi:** Sicurezza dipendente dalla configurazione del server.  **5. Funzionamento delle VPN**  Le VPN operano creando un tunnel sicuro tra il dispositivo dell’utente e un server remoto, garantendo privacy e sicurezza nelle comunicazioni. Questo processo coinvolge diversi passaggi tecnici.  **5.1 Creazione del Tunnel VPN**  Il tunnel VPN è il percorso criptato attraverso cui viaggiano i dati. Viene stabilito tramite protocolli di tunneling che incapsulano i pacchetti di rete per proteggerli da intercettazioni.  - **Tecnologie utilizzate:** GRE, SSL/TLS, IPsec, OpenVPN, WireGuard.  - **Obiettivo:** Assicurare che il traffico dati non possa essere letto da terzi.  **5.2 Processo di Autenticazione**  Per garantire che solo utenti autorizzati possano accedere alla VPN, vengono utilizzati diversi metodi di autenticazione.  - **Autenticazione a due fattori (2FA):** Combina password e codice temporaneo.  - **Certificati digitali:** Utilizzati nelle VPN aziendali per una maggiore sicurezza.  - **Credenziali utente:** Username e password tradizionali.  **5.3 Crittografia dei Dati**  La crittografia è il cuore della sicurezza VPN, proteggendo i dati in transito da eventuali intercettazioni.  - **AES-256:** Standard di crittografia avanzato utilizzato in molte VPN.  - **ChaCha20:** Alternativa più leggera, impiegata da WireGuard.  - **RSA e Diffie-Hellman:** Utilizzati per lo scambio sicuro delle chiavi crittografiche.  **5.4 Routing del Traffico**  Una volta stabilita la connessione VPN, il traffico dell’utente può essere instradato attraverso il server VPN.  - **Split Tunneling:** Permette di instradare solo parte del traffico attraverso la VPN.  - **Full Tunneling:** Tutto il traffico passa attraverso la VPN, garantendo massimo anonimato.  - **Politiche di logging:** Alcuni provider VPN mantengono registri del traffico, mentre altri adottano una politica "no-log".  Con queste sezioni, abbiamo esplorato le diverse tipologie di VPN, i protocolli utilizzati e il loro funzionamento tecnico. Nelle prossime sezioni, approfondiremo vantaggi, svantaggi e applicazioni pratiche delle VPN.  **6. Vantaggi e Svantaggi**  L'uso delle VPN comporta numerosi vantaggi, ma presenta anche alcuni svantaggi, a seconda delle esigenze dell'utente e del contesto di utilizzo.  **6.1 Vantaggi delle VPN**  **- 6.1.1 Maggiore Sicurezza**  Le VPN proteggono i dati trasmessi su reti pubbliche grazie alla crittografia, prevenendo intercettazioni e attacchi man-in-the-middle.  **- 6.1.2 Privacy e Anonimato**  Utilizzando una VPN, l'indirizzo IP dell'utente viene mascherato, riducendo la tracciabilità online da parte di ISP, governi e inserzionisti pubblicitari.  **- 6.1.3 Accesso a Contenuti Georestritti**  Le VPN permettono di aggirare le restrizioni geografiche imposte su alcuni siti e servizi di streaming, consentendo l'accesso a contenuti disponibili solo in determinate regioni.  **- 6.1.4 Protezione nelle Reti Pubbliche**  L'uso di una VPN in reti Wi-Fi pubbliche (es. aeroporti, caffè) impedisce a eventuali malintenzionati di intercettare dati sensibili, come credenziali di accesso e informazioni bancarie.  **- 6.1.5 Bypass della Censura**  In alcuni paesi con restrizioni sulla libertà di navigazione, le VPN consentono agli utenti di accedere a Internet senza limitazioni imposte dal governo.  **6.2 Svantaggi delle VPN**  **- 6.2.1 Rallentamenti della Connessione**  A causa della crittografia e dell'instradamento del traffico attraverso server remoti, le VPN possono ridurre la velocità di navigazione e streaming.  **- 6.2.2 Costo del Servizio**  Le VPN gratuite spesso presentano limitazioni e rischi per la privacy, mentre i servizi premium possono avere un costo mensile o annuale elevato.  **- 6.2.3 Compatibilità e Configurazione**  Non tutte le VPN funzionano con ogni dispositivo o sistema operativo. Alcuni servizi richiedono configurazioni avanzate per un utilizzo ottimale.  **- 6.2.4 Possibili Restrizioni da Parte dei Servizi Online**  Alcuni siti web e piattaforme di streaming rilevano e bloccano le connessioni VPN, impedendo l'accesso ai loro contenuti. | |

| **VALUTAZIONE**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **DOCENTI**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| --- | --- |