VPN

UN Virtual Private Network(VPN) è una tecnologia che consente una connessione sicura e crittografata tra una rete privata e un dispositivo remoto. Ciò consente alla macchina remota di accedere direttamente alla rete privata, fornendo un accesso sicuro e riservato alle risorse e ai servizi della rete.

Esistono diversi motivi per cui gli amministratori utilizzano le VPN. Le VPN crittografano la connessione tra il dispositivo remoto e la rete privata, rendendo molto più difficile per gli aggressori intercettare e rubare informazioni sensibili. Con questo, l'intera comunicazione è più sicura.

Un altro motivo è che le VPN consentono ai dipendenti di accedere alla rete privata e alle sue risorse in remoto da qualsiasi luogo, purché dispongano di una connessione Internet. Ciò è particolarmente utile per i dipendenti che devono lavorare in remoto, come quelli che viaggiano o lavorano da casa. Inoltre, le VPN possono essere più convenienti rispetto ad altre soluzioni di accesso remoto, come linee affittate o connessioni dedicate, poiché utilizzano la rete Internet pubblica per connettere gli utenti remoti alla rete privata.

Requisiti	Descrizione
VPN Client	Viene installato sul dispositivo remoto e viene utilizzato per stabilire e mantenere una connessione VPN con il server VPN. Ad esempio, questo potrebbe essere un client OpenVPN.
VPN Server	Si tratta di un computer o dispositivo di rete responsabile dell'accettazione delle connessioni VPN dai client VPN e dell'instradamento del traffico tra i client VPN e la rete privata.
Encryption	Le connessioni VPN sono crittografate utilizzando una varietà di algoritmi e protocolli di crittografia, come AES e IPsec, per proteggere la connessione e proteggere i dati trasmessi.
Authentication	Il server e il client VPN devono autenticarsi a vicenda utilizzando un segreto condiviso, un certificato o un altro metodo di autenticazione per stabilire una connessione sicura

Il client e il server VPN utilizzano queste porte per stabilire e mantenere la connessione VPN. A livello TCP/IP, una connessione VPN utilizza in genere il protocollo Encapsulating Security Payload (ESP) per crittografare e autenticare il

traffico VPN. Ciò consente al client e al server VPN di scambiare dati in modo sicuro su Internet pubblico.

1.1 IPSec

Internet Protocol Security (IPsec) è un protocollo di sicurezza di rete che fornisce crittografia e autenticazione per le comunicazioni Internet largamente utilizzato e funziona crittografando il carico utile di dati di ciascun pacchetto IP e aggiungendo un authentication header che viene utilizzato per verificare l'integrità e l'autenticità del pacchetto. IPsec utilizza una combinazione di due protocolli per fornire crittografia e autenticazione:

- Intestazione di autenticazione (AH): questo protocollo fornisce integrità e autenticità per i pacchetti IP ma non fornisce la crittografia. Aggiunge un'intestazione di autenticazione a ciascun pacchetto IP, che contiene un checksum crittografico che può essere utilizzato per verificare che il pacchetto non sia stato manomesso.
- Encapsulating Security Payload (ESP): fornisce crittografia e autenticazione facoltativa per i pacchetti IP. Crittografa il carico utile dei dati di ciascun pacchetto IP e, facoltativamente, aggiunge un'intestazione di autenticazione, simile a AH.

IPsec può essere utilizzato in due modalità:

- Transport Mode: crittografa e autentica il payload di dati di ogni pacchetto IP ma non crittografa l'intestazione IP. (utilizzato per proteggere la comunicazione end-to-end tra due host).

- Tunnel Mode: crittografa e autentica l'intero pacchetto IP, inclusa l'intestazione IP. (utilizzato per creare un tunnel VPN tra due reti).

1.2 PPTP

Point-to-Point Tunneling Protocol (PPTP) è anche un protocollo di rete che consente la creazione di VPN e funziona stabilendo un tunnel sicuro tra il client e il server VPN e quindi incapsulando i dati trasmessi all'interno di questo tunnel.
È un'estensione del PPTP ed è implementato in molti sistemi operativi. A causa di vulnerabilità note, PPTP non è più considerato sicuro oggi. PPTP può essere utilizzato per eseguire il tunneling di protocolli come IP, IPX o NetBEUI tramite IP. A causa di

vulnerabilità note, il PPTP non è più considerato sicuro ed è stato ampiamente sostituito da altri protocolli VPN come L2TP/IPsec, IPsec/IKEv2o OpenVPN. Dal 2012, però, PPTP non è più considerato sicuro perché il metodo di autenticazione MSCHAPv2 utilizza il dusty DES e può quindi essere facilmente craccato con hardware speciale.