



Dipartimento di Ingegneria

Corso di Laurea in Ingegneria Informatica

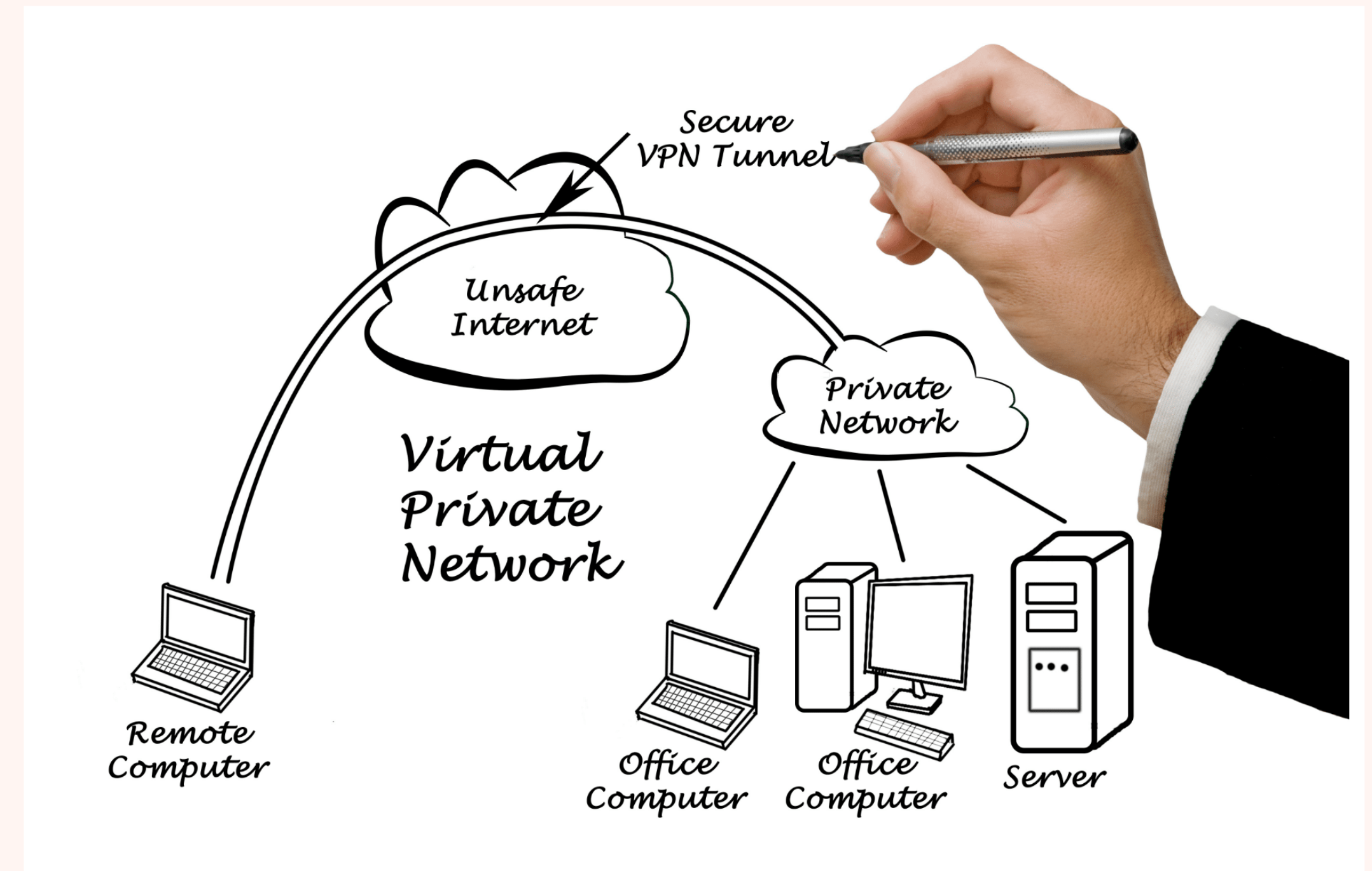
REALIZZAZIONE DI UN SISTEMA DI CYBER-DEFENCE:

ANALISI DI SOLUZIONI VPN

INTRODUZIONE

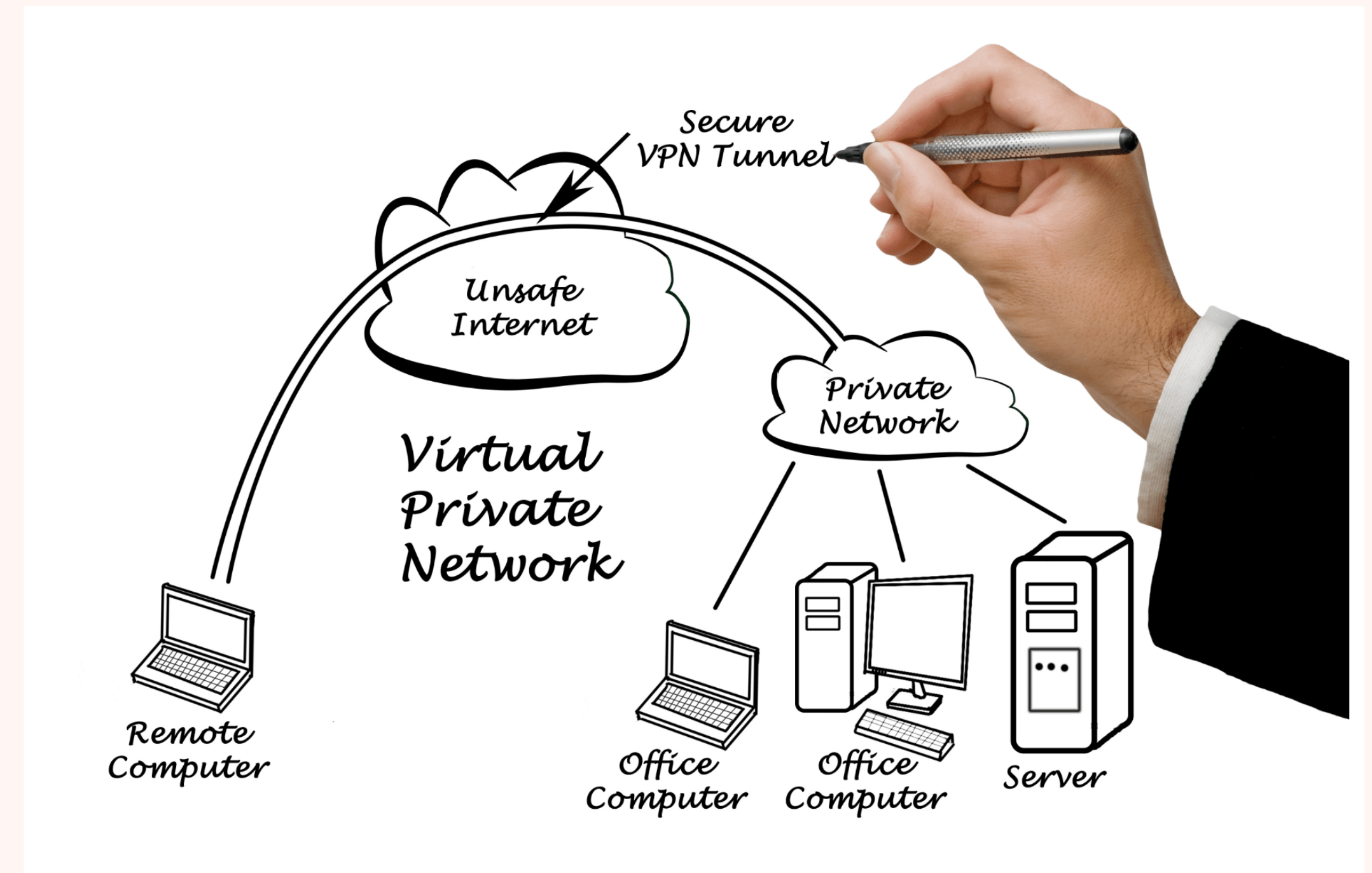
VIRTUAL PRIVATE NETWORK

- **Si costruisce su una rete di calcolatori preesistente**
- **Protegge la connessione e la privacy**
- **Crea un tunnel cifrato per i dati**
- **Permette accesso da remoto a reti private**



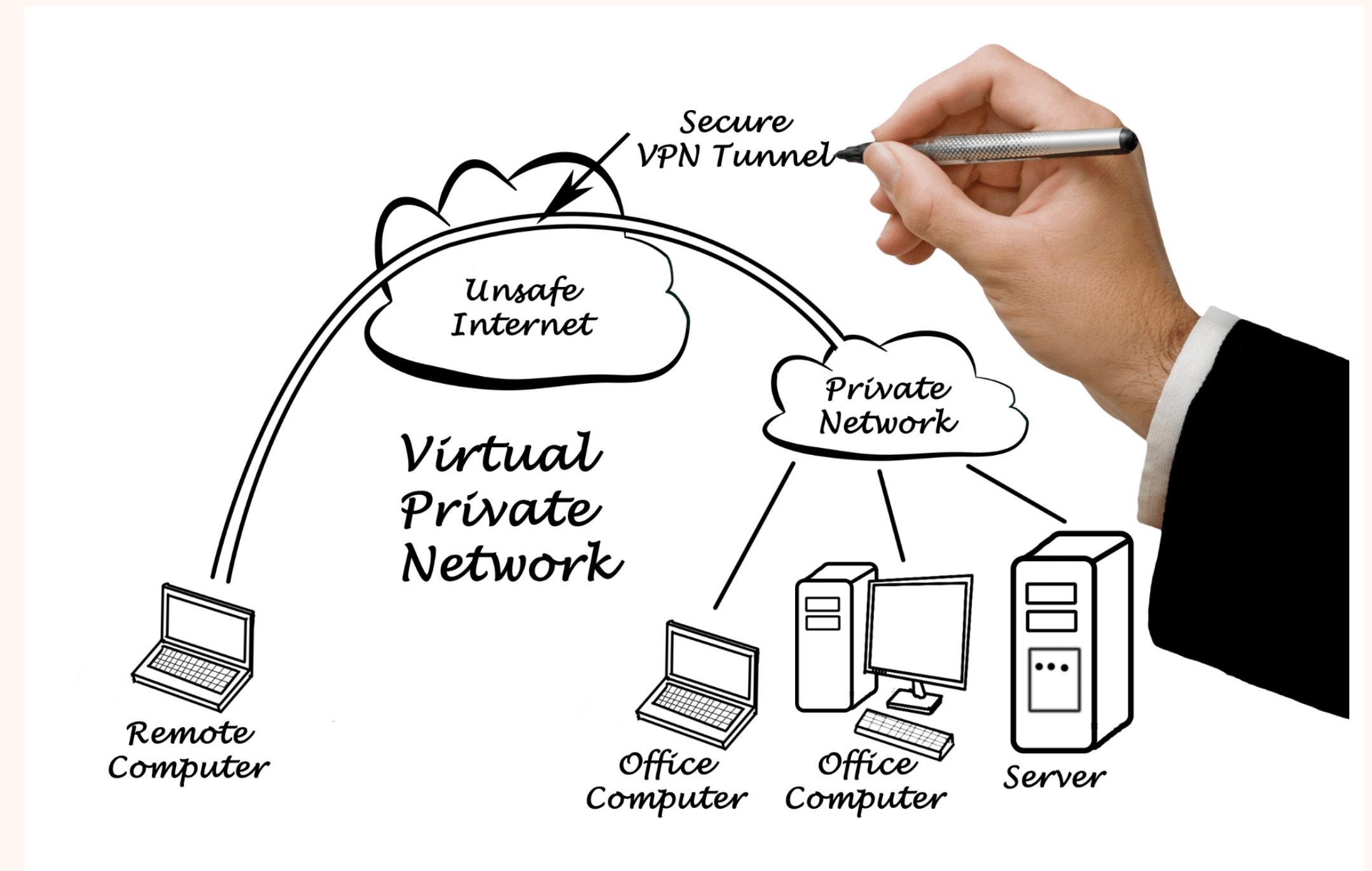
VIRTUAL PRIVATE NETWORK

- **autenticazione**
- **controllo degli accessi**
- **confidenzialità**
- **integrità**
- **non-repudiation**



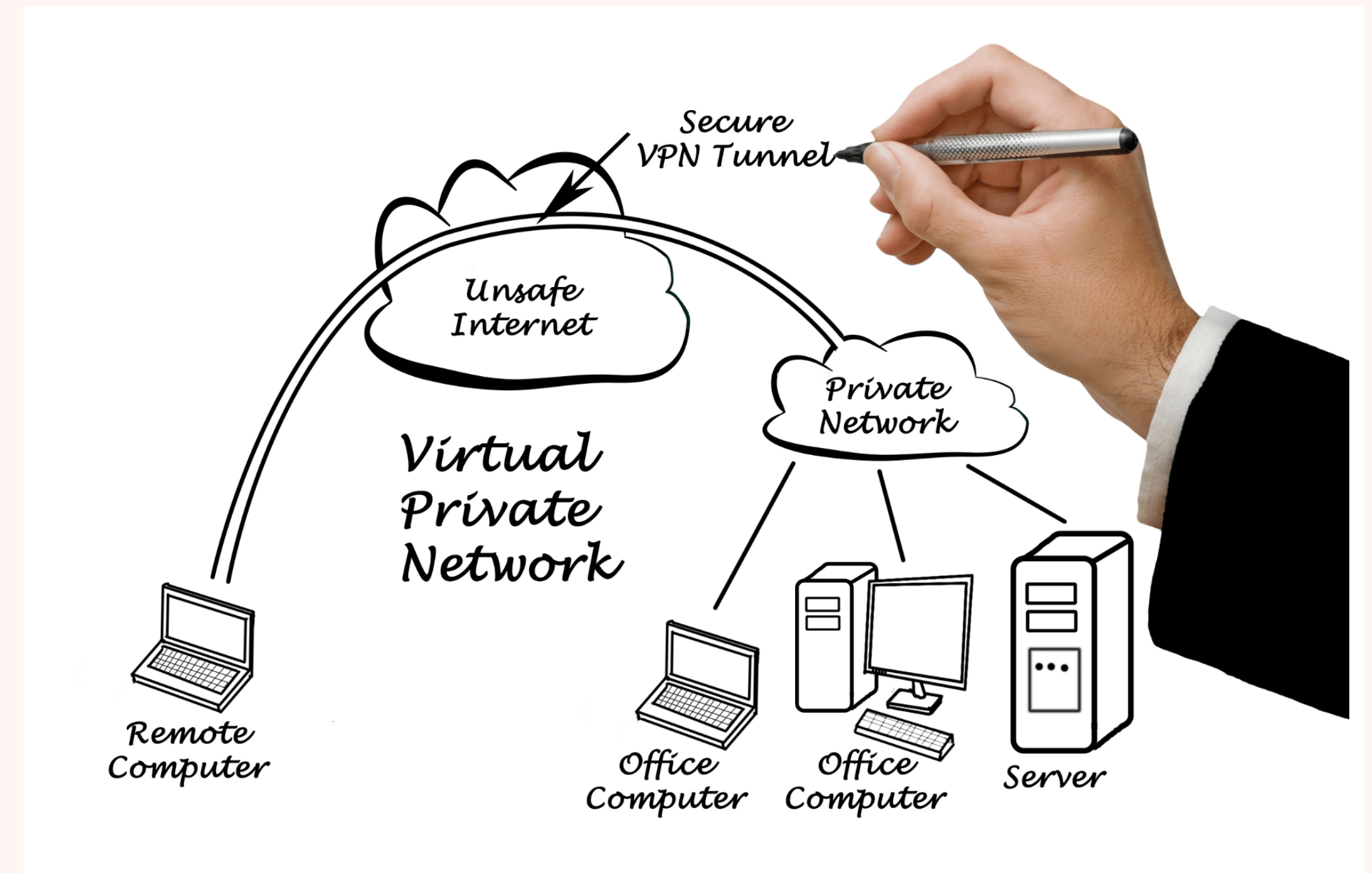
VIRTUAL PRIVATE NETWORK

- **autenticazione** - il servizio di autenticazione verifica l'identità di un utente o di un sistema
- **controllo degli accessi**
- **confidenzialità**
- **integrità**
- **non-repudiation**



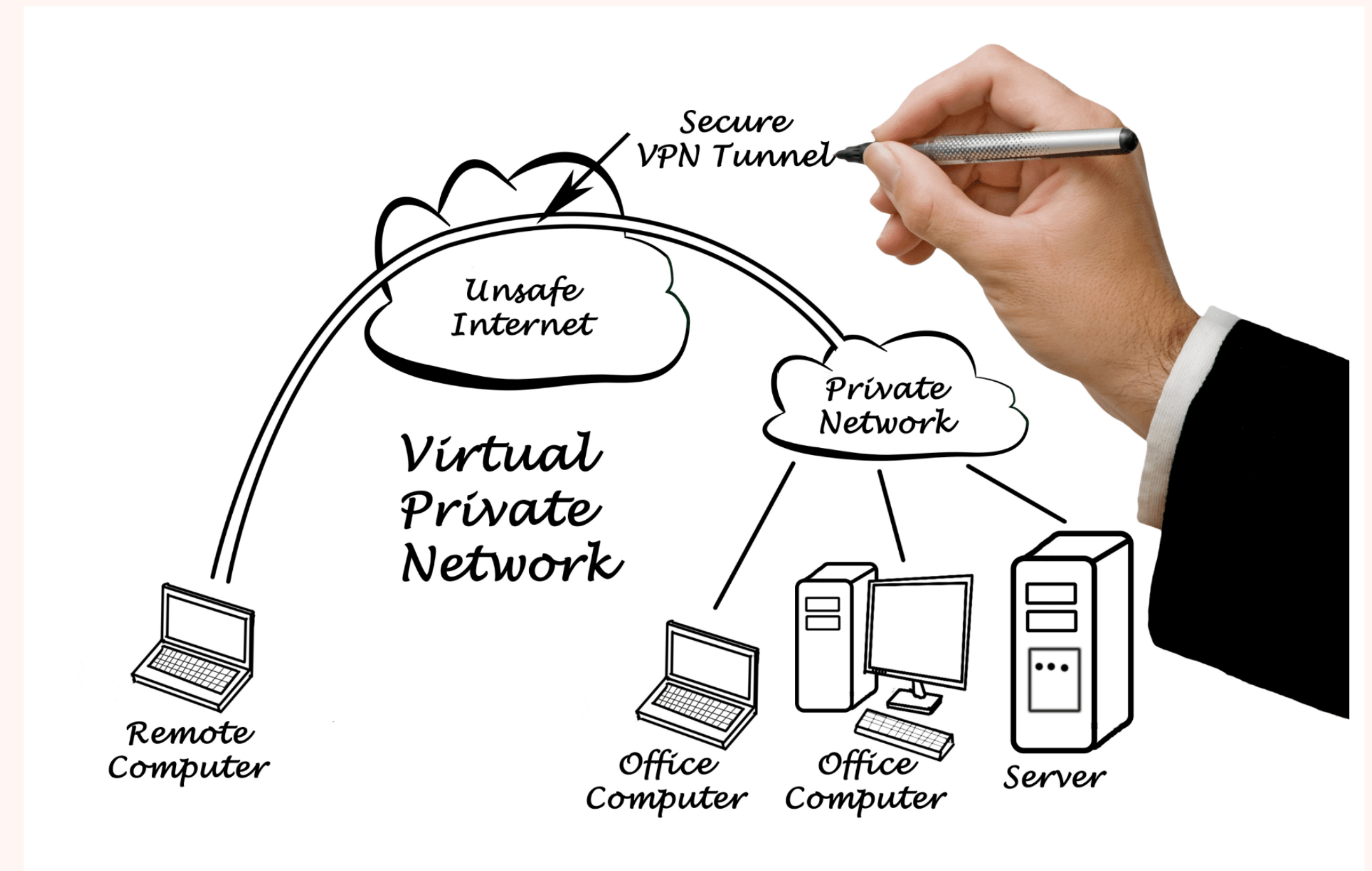
VIRTUAL PRIVATE NETWORK

- **autenticazione**
- **controllo degli accessi - il servizio protegge le risorse di sistema da utenti non autorizzati**
- **confidenzialità**
- **integrità**
- **non-repudiation**



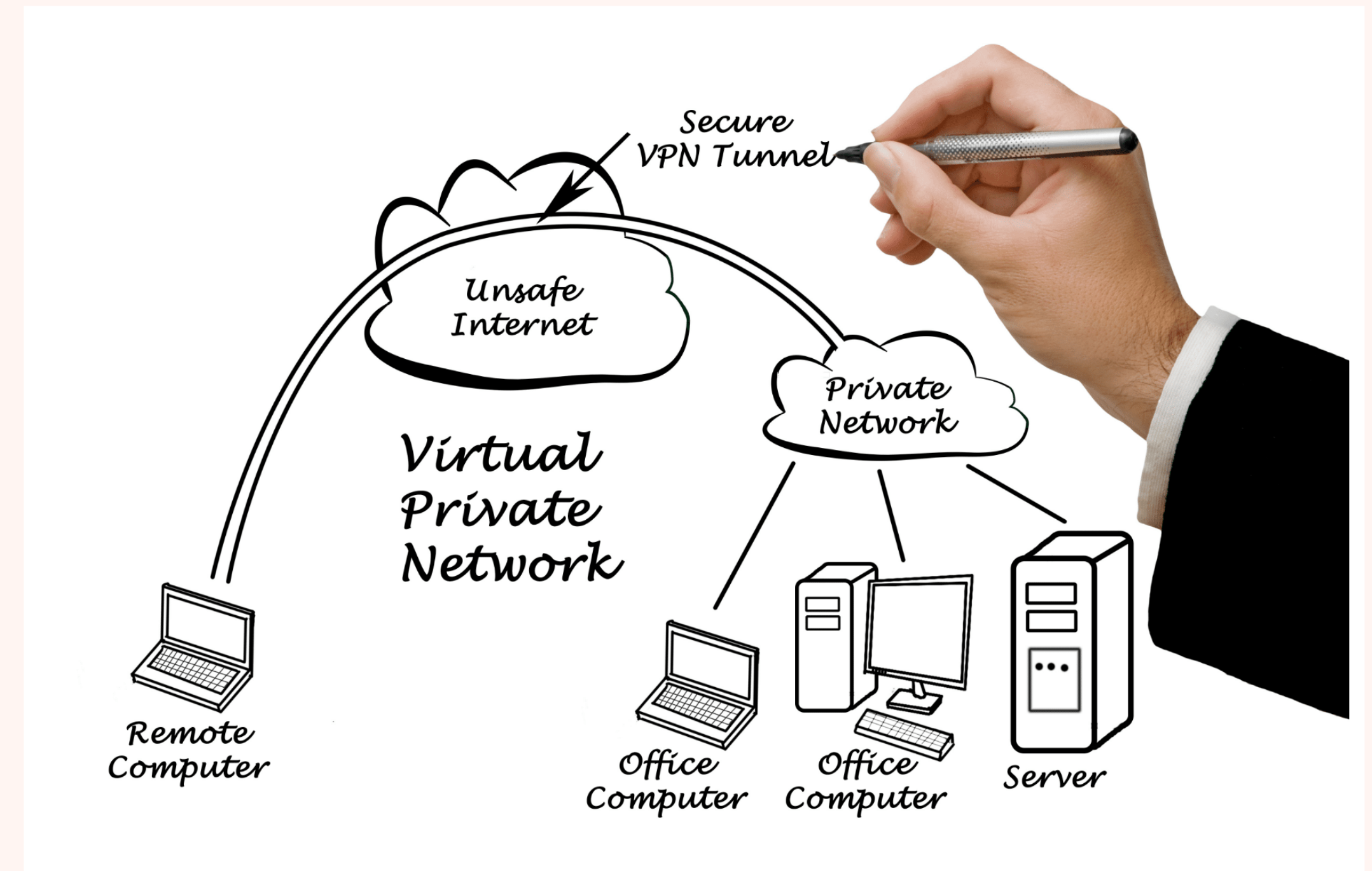
VIRTUAL PRIVATE NETWORK

- **autenticazione**
- **controllo degli accessi**
- **confidenzialità - il servizio protegge i dati da rivelazioni non autorizzate**
- **integrità**
- **non-repudiation**



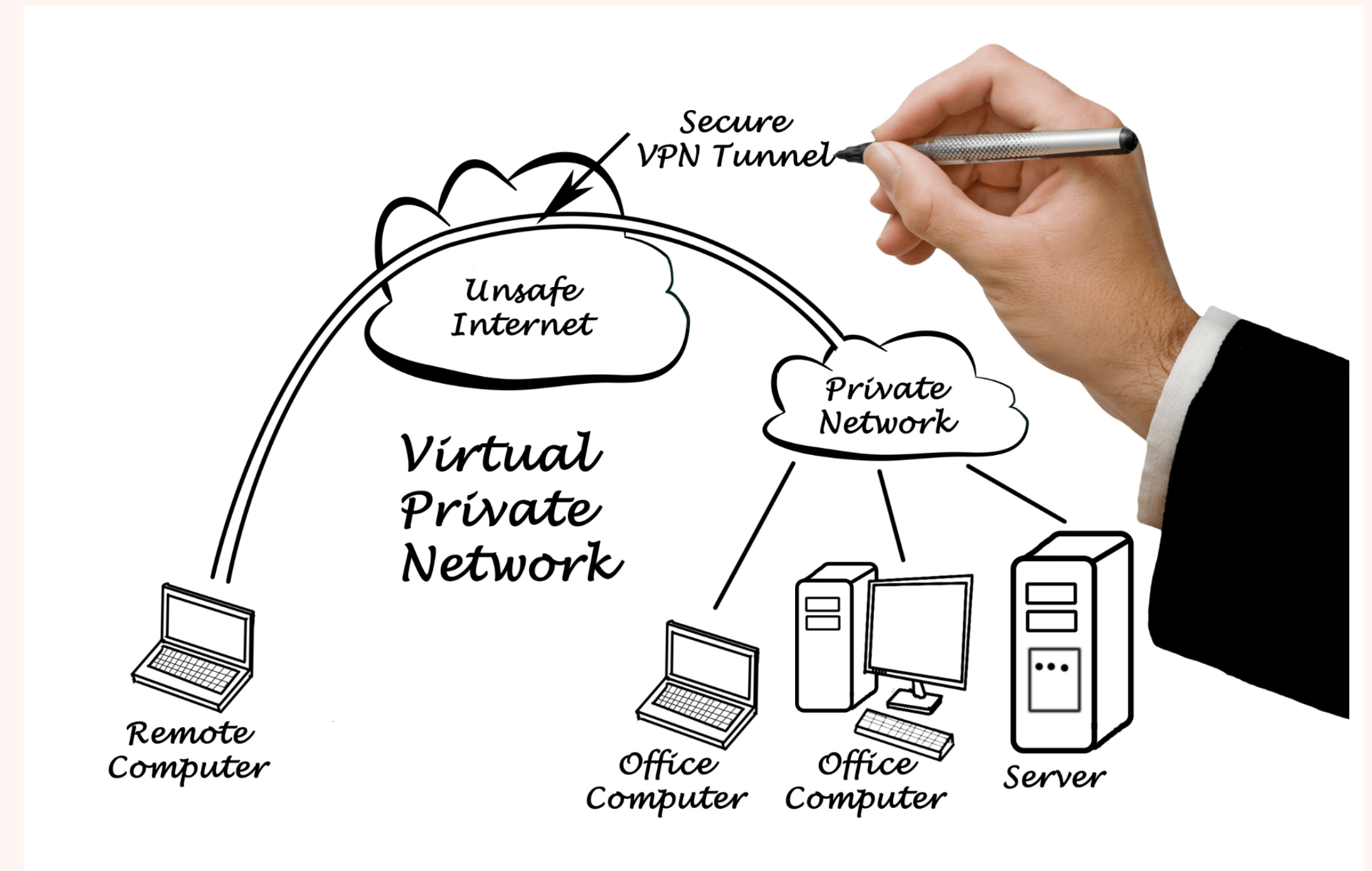
VIRTUAL PRIVATE NETWORK

- **autenticazione**
- **controllo degli accessi**
- **confidenzialità**
- **integrità - il servizio protegge i dati da modifiche, aggiunte o rimozioni non autorizzate**
- **non-repudiation**



VIRTUAL PRIVATE NETWORK

- **autenticazione**
- **controllo degli accessi**
- **confidenzialità**
- **integrità**
- **non-repudiation** - il servizio assicura che né il mittente né il destinatario possano successivamente negare di aver processato tali dati



IPSec



IPSec



- **Open source**
- **Supportano elevati standard di sicurezza**
- **Rispettano i requisiti minimi richiesti**

IPSec



- **Definita dalle RFC 2401-2412**
- **Tunnel a L3**
- **Integrato nel sistema operativo**
- **Totalmente personalizzabile**



IPSec



- **20 anni di storia la rendono una soluzione matura**
- **Tunnel a L7**
- **Richiede di installare un software aggiuntivo per funzionare**



IPSec



- **Codebase estremamente ridotta**
 - **Promette performance eccellenti**
 - **Soluzione molto recente**
 - **Tunnel a L3**
 - **Potrebbe richiedere di installare un software aggiuntivo per funzionare**
-

MISURAZIONE DELLE PERFORMANCE

OBIETTIVO:
SICUREZZA ED EFFICIENZA

MISURAZIONE DELLE PERFORMANCE

tramite iPerf3 e mtr

MISURAZIONE DELLE PERFORMANCE

tramite iPerf3 e mtr

1. Throughput medio



MISURAZIONE DELLE PERFORMANCE

tramite iPerf3 e mtr

- 1. Throughput medio**
- 2. Latenza media**



MISURAZIONE DELLE PERFORMANCE

tramite iPerf3 e mtr

- 1. Throughput medio**
- 2. Latenza media**
- 3. Packet loss**

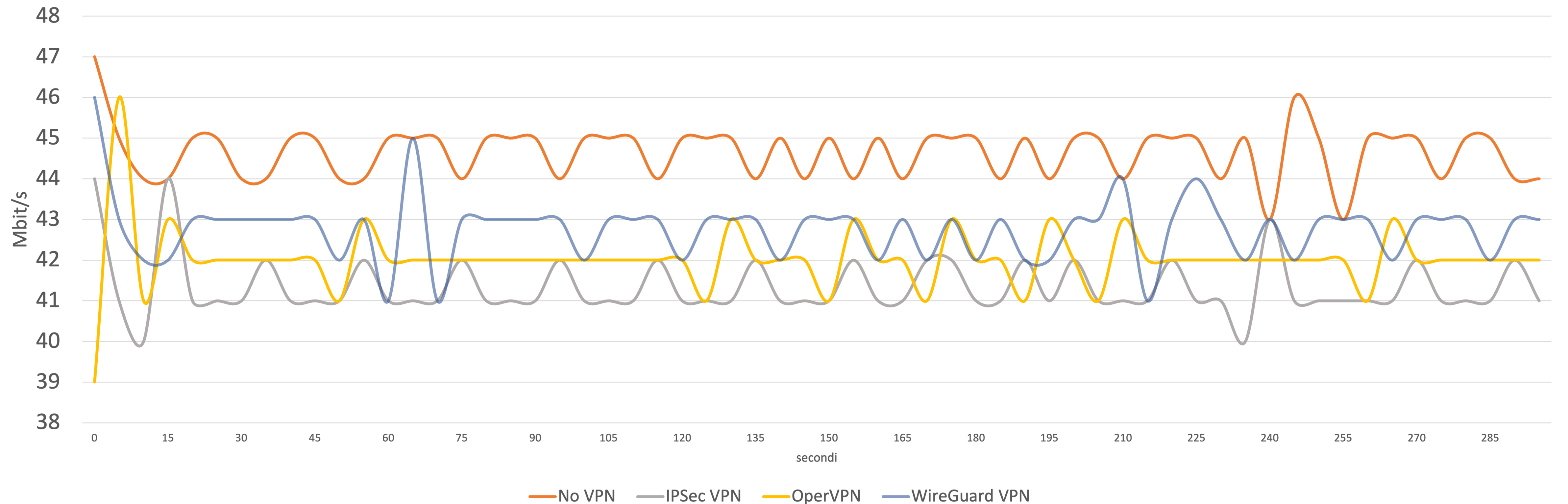


THROUGHPUT

- **Definito come la** quantità di dati **trasferiti con successo da un host all'altro in un determinato** periodo di tempo **(1 secondo)**.
- **Misura la capacità *effettiva* di un canale di telecomunicazione, in** bit al secondo.
- *Non* **va confuso con la larghezza di banda, che misura la *massima* capacità *teorica* di un canale di telecomunicazione.**



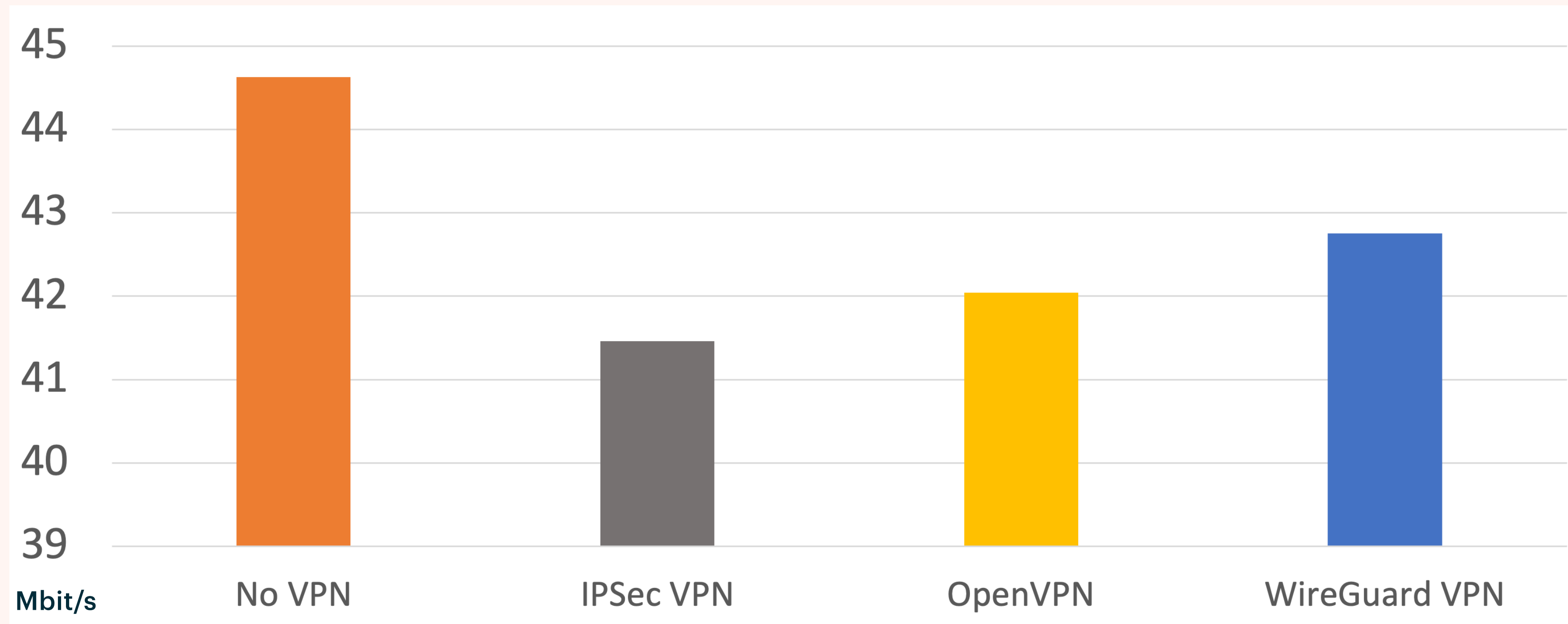
THROUGHPUT



su 300 secondi, con rilevazioni ogni 5 secondi

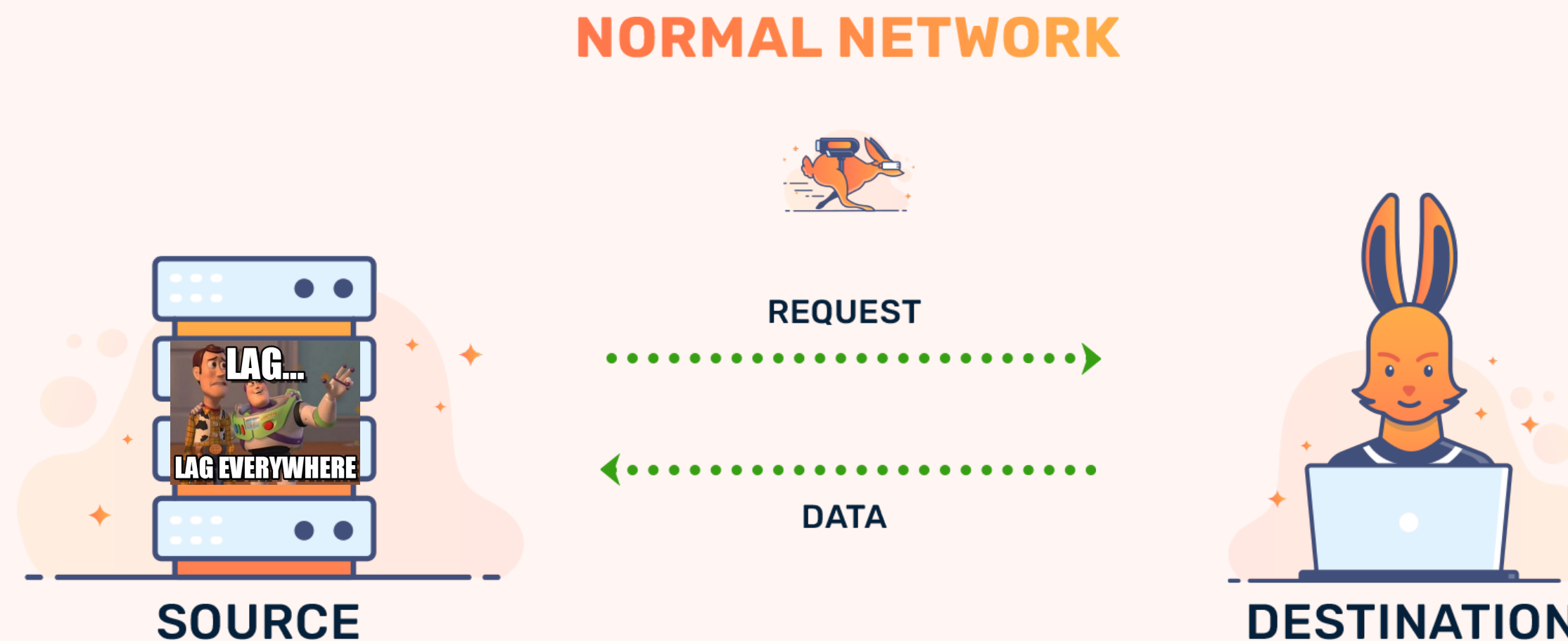
THROUGHPUT MEDIO

higher is better



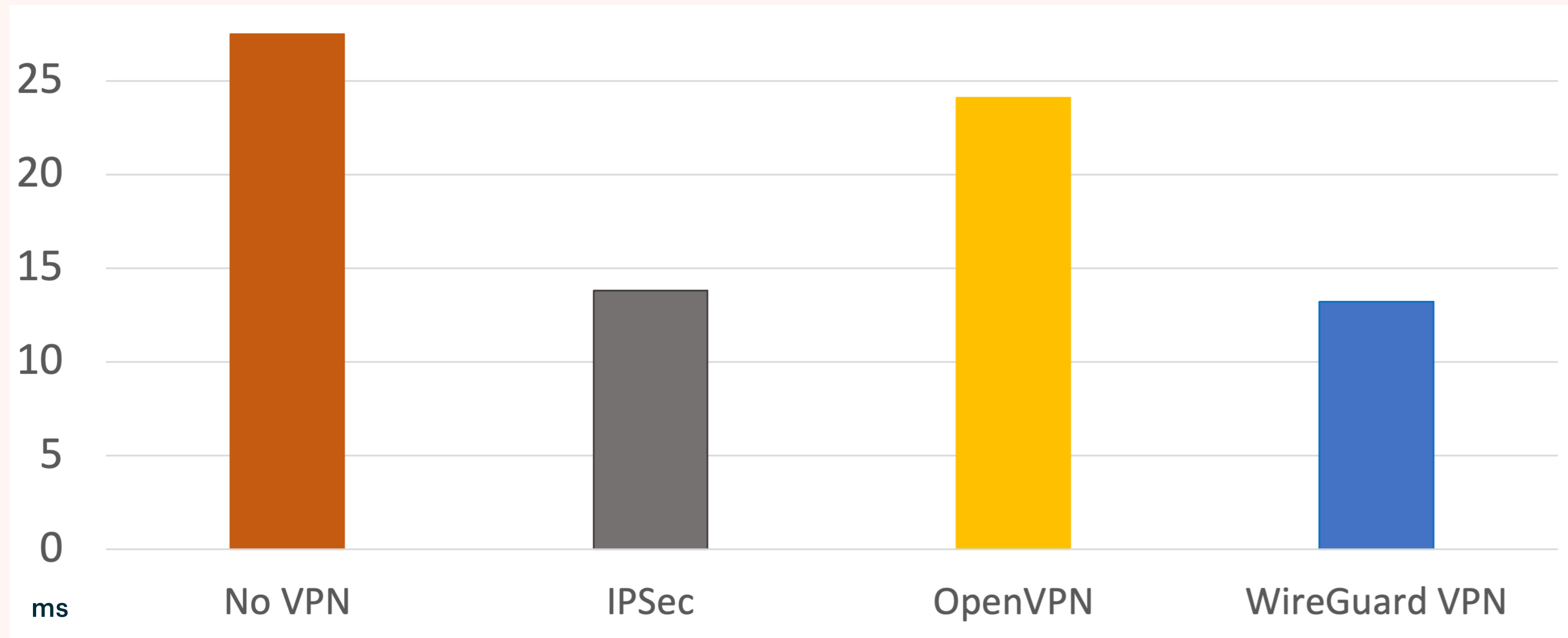
LATENZA MEDIA

- La latenza è la misura del tempo necessario affinché un bit raggiunga un altro dispositivo connesso in rete.
- Una latenza bassa corrisponde ad una connessione più “reattiva”



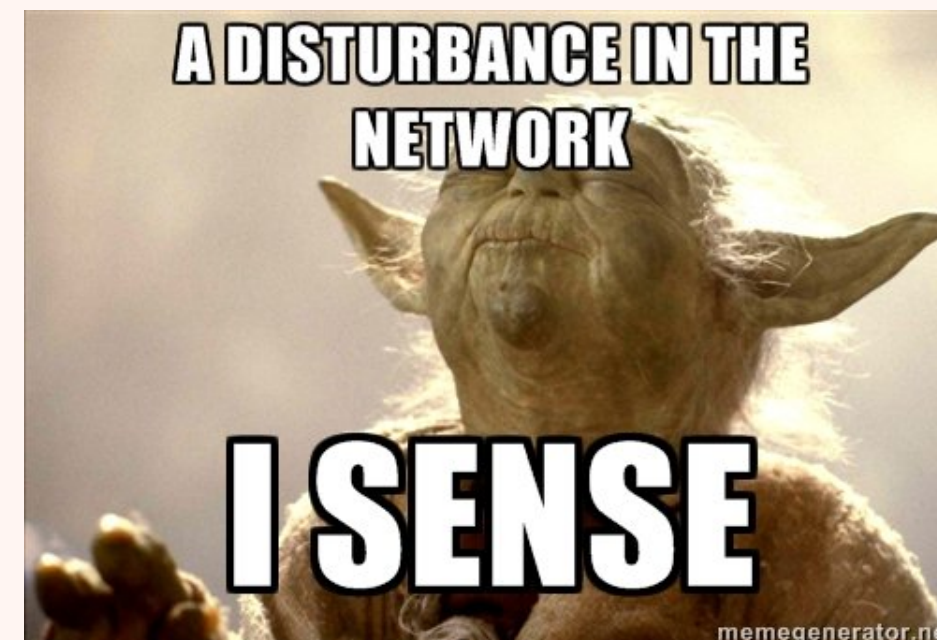
LATENZA MEDIA

lower is better



PACKETLOSS A DESTINAZIONE

- **La perdita di pacchetti si verifica quando dei dati non raggiungono la destinazione dopo essere stati trasmessi. Può essere dovuta a congestione della rete, problemi hardware, problemi software, etc...**
- **Si manifesta all'utente come una qualità di connessione scadente, o una perdita di connettività.**
- **Per gli utenti domestici, è un'esperienza sgradevole.
Per le attività commerciali, potrebbe arrivare ad impedire il corretto svolgimento delle attività.**



PACKETLOSS A DESTINAZIONE

lower is better



CONCLUSIONI

42,5 MBIT/s

Miglior throughput medio — WireGuard

~13 ms

Migliore latenza media — IPSec e WireGuard

RISULTATI

Performance → WireGuard

RISULTATI

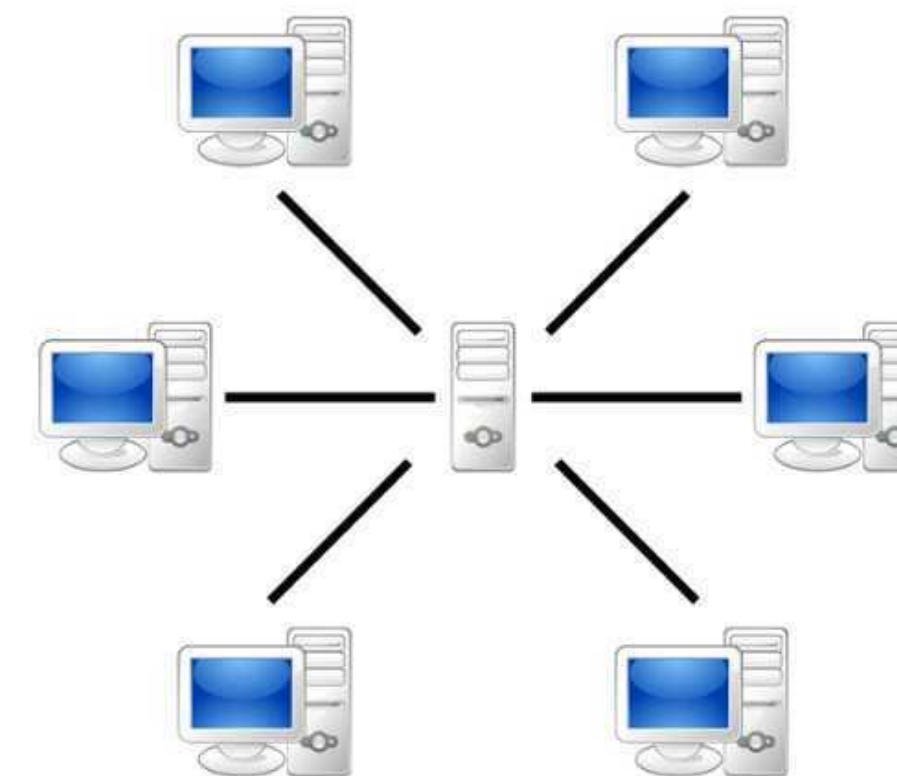
Performance → WireGuard

Personalizzazione → IPSec

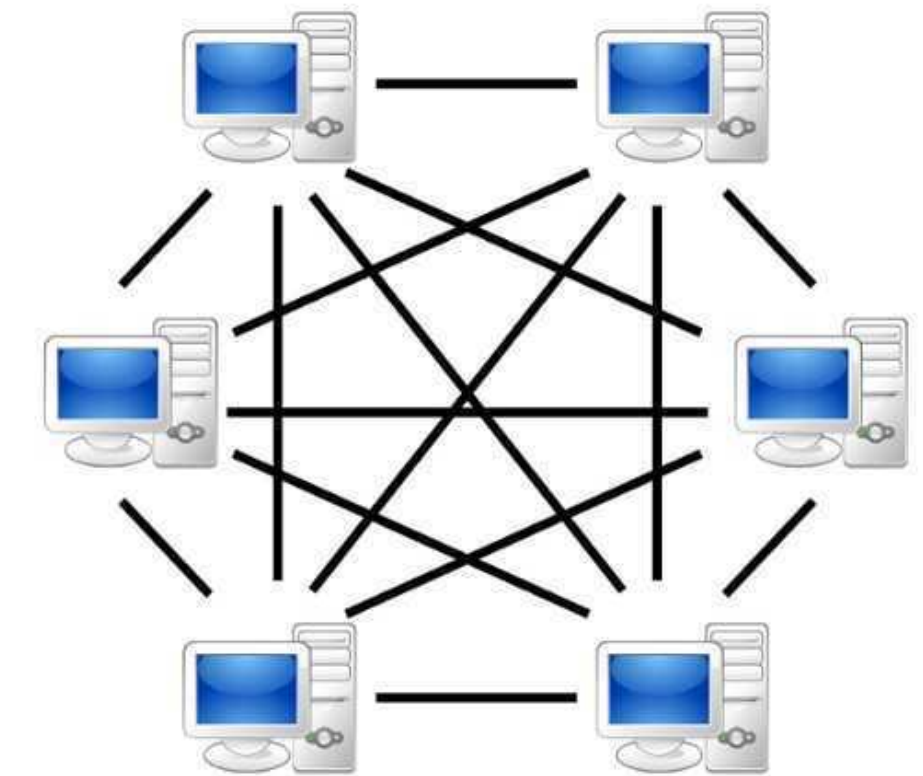
SVILUPPI FUTURI

VPN PEER-TO-PEER

- **Implementa livelli 1 e 2 virtuali al di sopra di una rete Peer-To-Peer cifrata**
- **Le comunicazioni non passano attraverso un nodo centrale**
- **Non è necessario il port-forwarding verso internet**
- **e.g.: ZeroTier**



Server-based



P2P-network

PRIVILEGED ACCESS MANAGEMENT

- **Insieme di strumenti e strategie per un controllo più granulare dei permessi concessi ai singoli utenti**
- **Tracciare con precisione le attività nella rete**
- **Permette di intervenire tempestivamente**



GRAZIE PER L'ATTENZIONE
