eritel
passione per l'ICT

Connessioni da remoto
in modo sicuro

eritel.it

REMOTE WORKING


MacBook Pro
Jessica Garson
esc
tab
caps lock

REMOTE WORKING

ATTIVITÀ COMUNI

Accesso a gestionale aziendali

Consultazione documenti

Aggiornamento CRM

Posta elettronica aziendale

Collegamento al centralino telefonico

Collaboration (chat, videomeeting, etc.)

REMOTE WORKING

ATTIVITÀ COMUNI

Accesso a gestionale aziendali

Consultazione documenti

Aggiornamento CRM

Posta elettronica aziendale

Collegamento al centralino telefonico

Collaboration (chat, videomeeting, etc.)

COLLEGAMENTO DA REMOTO

ERRORI COMUNI

1

Collegamento via RDP (Remote Desktop Protocol) tramite Internet

1 **Collegamento via RDP (Remote Desktop Protocol) tramite Internet**

2 **Collegamento ai server aziendali tramite IP pubblico**

1. Collegamento via RDP (Remote Desktop Protocol) tramite Internet

2. Collegamento ai server aziendali tramite IP pubblico

3. Basso livello di sicurezza (password deboli, assenza 2FA, nessun firewall, etc.)

VPN

VIRTUAL PRIVATE NETWORK

VPN

COS'È?

Una VPN può essere paragonata ad una **estensione** geografica della **rete locale** privata (LAN) e permette di collegare tra loro, in maniera sicura, le **sedi aziendali** e gli **utenti remoti**, distribuiti sul territorio.

VPN

TUNNELING

Viene creato un "tunnel" **sicuro** tra due entità remote.

Le due estremità del tunnel, anche se distanti e collegate attraverso molti nodi intermedi, diventano **virtualmente** adiacenti.

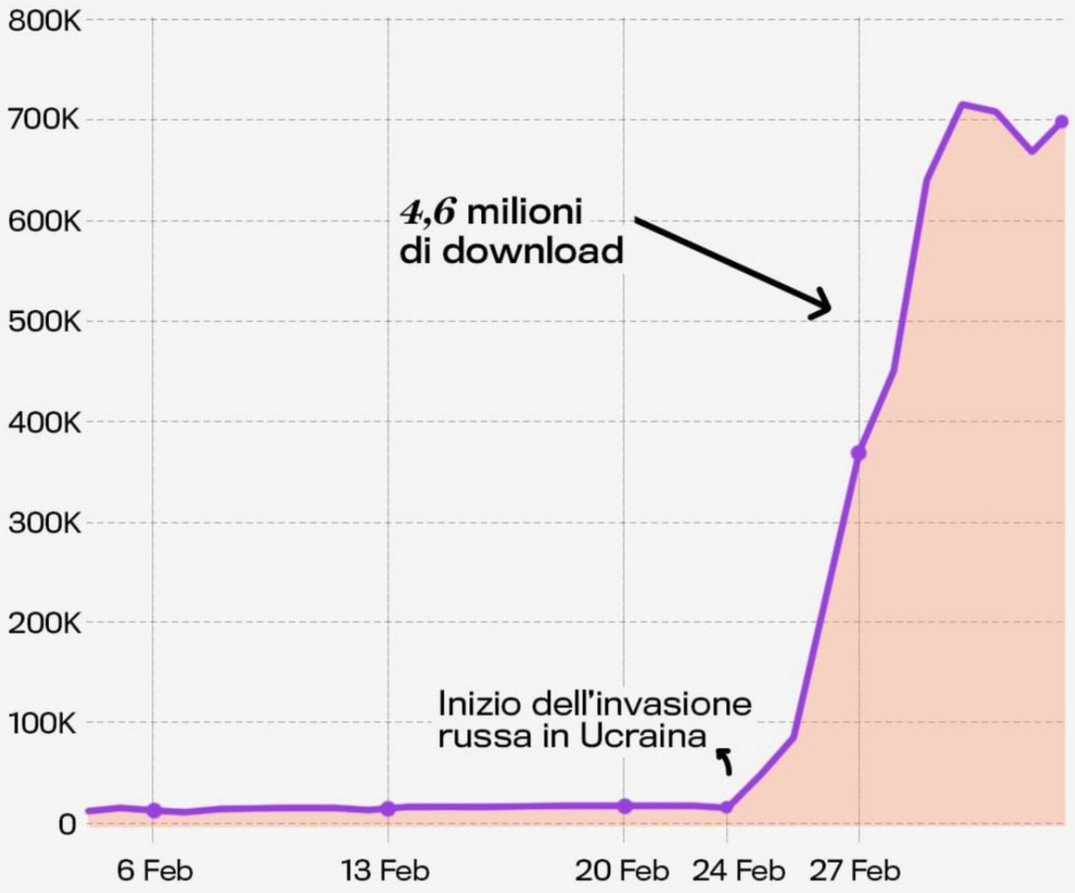
I pacchetti di dati, all’ingresso del tunnel, vengono **criptati** e spediti sulla rete verso l’uscita del tunnel, dove, dopo avere rimosso la crittografia, raggiungono la **destinazione**.

VPN

PROTOCOLLI

Esistono diversi protocolli per creare una VPN, la cui scelta d’utilizzo dipende dalle **necessità** e dai **requisiti** desiderati. Tra i protocolli più comuni si possono citare PPTP, L2TP, IPSEC, SSL/TLS e HTTPS.

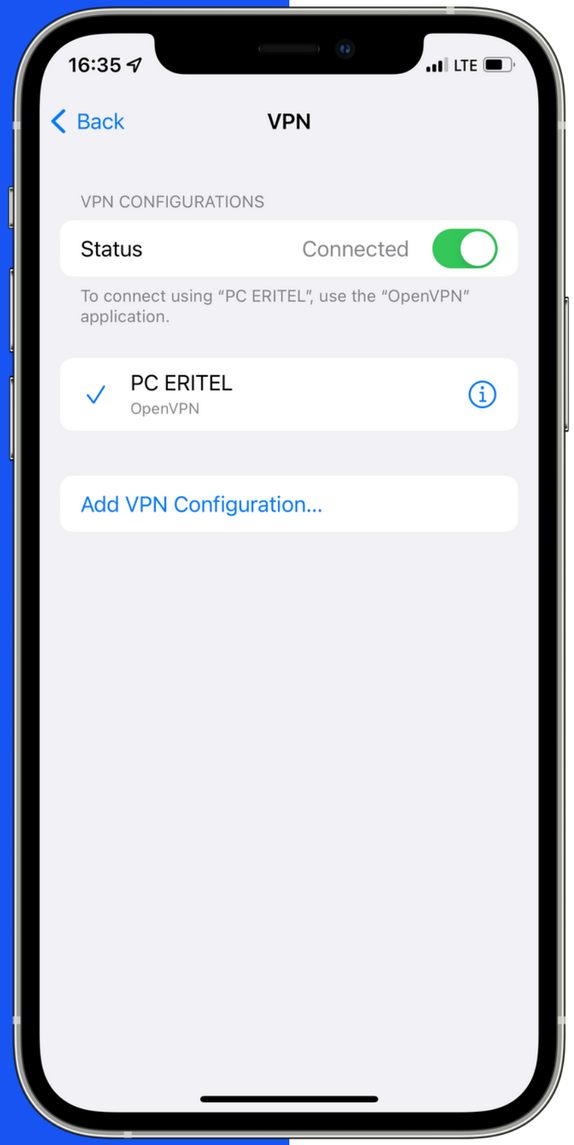
Download di servizi VPN* da App Store e Google Play



*i Virtual Private Network permettono di nascondere l'identità della propria connessione ad Internet

Fonte: Appfigures e Surfshark

Gli utenti accedono ad una rete privata tramite la rete Internet.



TIPOLOGIE DI VPN

Connessione VPN ad accesso remoto

Questo tipo di connessione può essere visto come un collegamento tra un dispositivo **client VPN** e il **server** dell’azienda.

Ogni sede avrà un router dedicato che instraderà i pacchetti dati verso i destinatari.

TIPOLOGIE DI VPN

Connessione VPN site-to-site

Utilizzata per connettere **uffici dislocati** geograficamente in una rete privata, consentendo il **routing** ed una **comunicazione** sicura.

COLLEGAMENTO TRA SEDI

INTERNET VS. PROVIDER

INTERNET VS. PROVIDER

INTERNET

Per definizione, Internet è una rete **best effort**, ovvero la banda disponibile e i tempi di consegna dipendono dal **carico di rete**.

A seconda della disponibilità di risorse, il traffico verrà **consegnato** o **scartato**.

INTERNET VS. PROVIDER

PROVIDER

La rete Vianova costituisce la portante di tutti i servizi dell’azienda e permette di erogare servizi di telecomunicazione e IT con i più alti livelli di **affidabilità**, **sicurezza** e **bassa latenza**.

Il traffico voce e dati è instradato su **distinti** circuiti dedicati, configurati con banda minima garantita e **controllata** per assicurarne la **qualità** del servizio.

vianova

Controllo della rete

Se non puoi misurarlo, non puoi migliorarlo

Un avanzato sistema di monitoraggio rileva **ogni minuto** i volumi di traffico e lo stato delle linee di ogni singolo Cliente.

Il controllo dei parametri delle linee in “quarantena” è rilevato **ogni secondo**.

Il traffico Internet viene automaticamente analizzato e suddiviso in tipologie con differenti **livelli di priorità**.

In caso di presenza di traffico, un operatore **contatta telefonicamente** il Cliente per gli eventuali accertamenti.

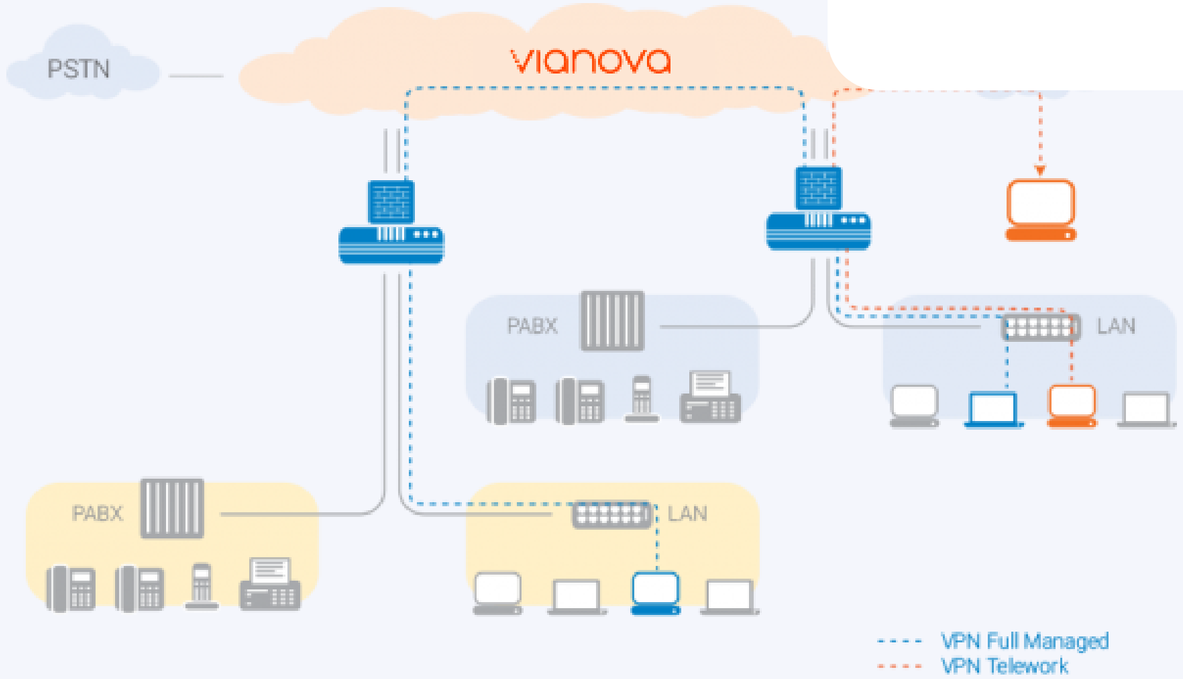
12.511

sono le VPN gestite tra le sedi dei Clienti

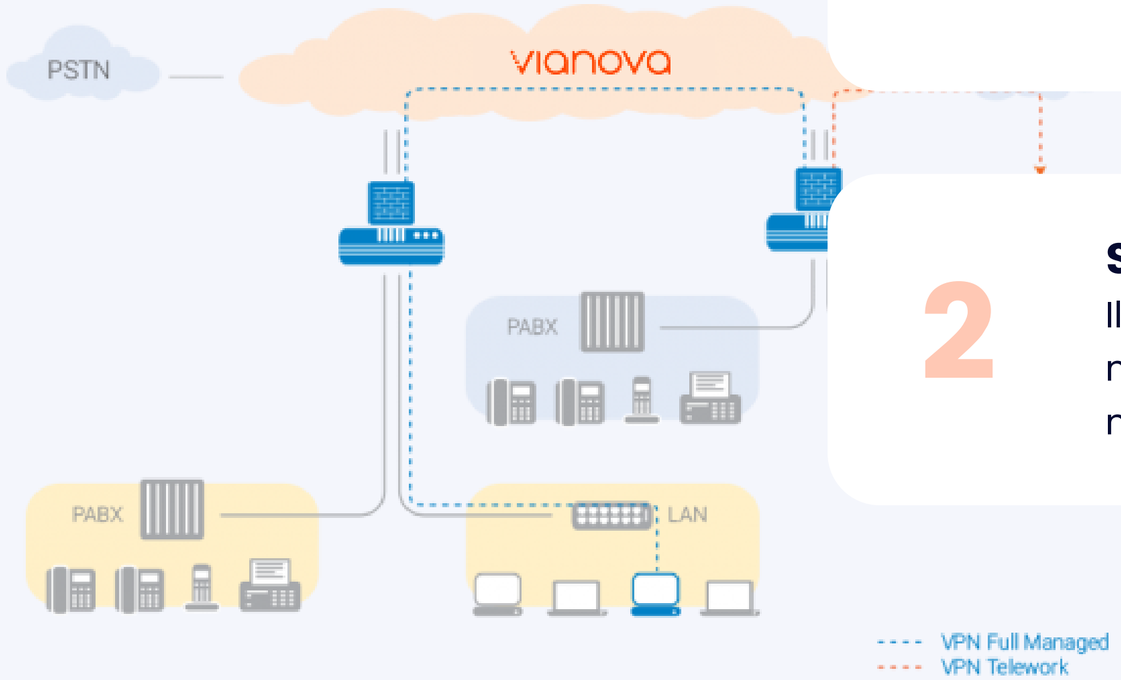
1

Prestazioni garantite

Latenza minore di 40 millisecondi, numero di **hop max** uguale o minore di 4, **packet loss** minore di 0,1% al mese.



vianova



1

Prestazioni garantite

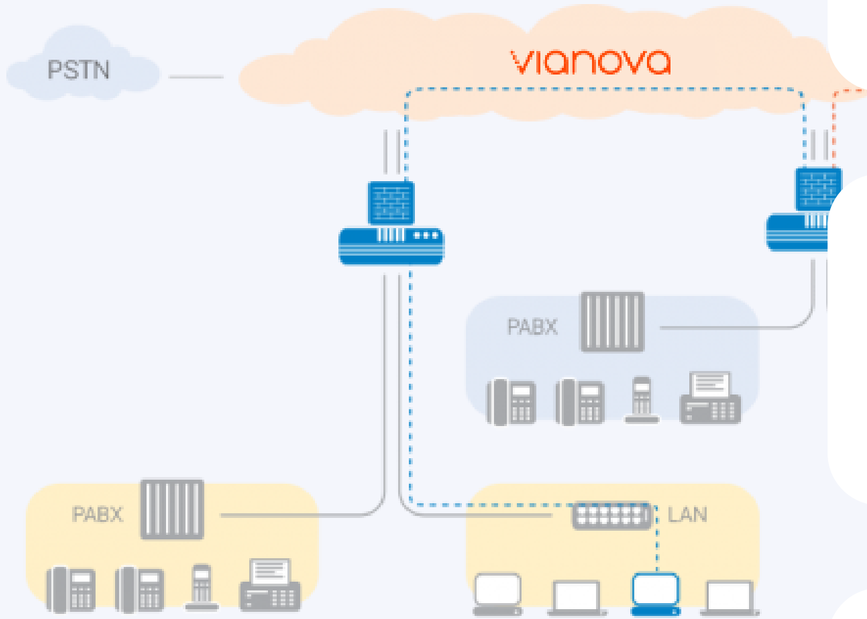
Latenza minore di 40 millisecondi, numero di **hop max** uguale o minore di 4, **packet loss** minore di 0,1% al mese.

2

Sicurezza elevata

Il traffico tra sedi è effettuato all'interno della **rete Vianova** e non passa "attraverso internet". Gli indirizzi **IP privati** utilizzati non sono "visibili" dall'esterno.

vianova



1

Prestazioni garantite

Latenza minore di 40 millisecondi, numero di **hop max** uguale o minore di 4, **packet loss** minore di 0,1% al mese.

2

Sicurezza elevata

Il traffico tra sedi è effettuato all'interno della **rete Vianova** e non passa "attraverso internet". Gli indirizzi **IP privati** utilizzati non sono "visibili" dall'esterno.

3

Garanzia della qualità

La qualità del **traffico voce** è garantita dall'applicazione dei parametri di **QoS** tra PBX satelizzati.

vianova

Servizio Clienti

Chiama il 145, ti rispondiamo in tre squilli.

Lavorare al tuo fianco significa **ascoltare direttamente** le tue richieste e prendersi carico delle tue necessità **senza** farti **perdere tempo** con messaggi registrati.

Il nostro Servizio Clienti opera esclusivamente con personale dipendente e garantisce i tempi di risposta più rapidi del mercato: solo tre squilli di telefono, con **risposta diretta** di un **Operatore** e senza risponditori automatici.

92,5%

percentuale di chiamate a cui abbiamo risposto in 3 squilli

6 regole per una VPN affidabile

1 **Scegliere un provider affidabile** e non affidarsi ai molti servizi gratuiti o low cost disponibili sul web.

1. **Scegliere un provider affidabile** e non affidarsi ai molti servizi gratuiti o low cost disponibili sul web.

2. **Informarsi sul tipo di servizio VPN** che si sta acquistando e sui protocolli di sicurezza utilizzati.

1. **Scegliere un provider affidabile** e non affidarsi ai molti servizi gratuiti o low cost disponibili sul web.

2. **Informarsi sul tipo di servizio VPN** che si sta acquistando e sui protocolli di sicurezza utilizzati.

3. **Seguire le indicazioni di sicurezza** fornite dal provider ed applicare gli aggiornamenti e le patch consigliate.

1. **Scegliere un provider affidabile** e non affidarsi ai molti servizi gratuiti o low cost disponibili sul web.

2. **Informarsi sul tipo di servizio VPN** che si sta acquistando e sui protocolli di sicurezza utilizzati.

3. **Seguire le indicazioni di sicurezza** fornite dal provider ed applicare gli aggiornamenti e le patch consigliate.

4. **Scegliere un fornitore con una rete proprietaria** ad elevate prestazioni e sicura.

1. **Scegliere un provider affidabile** e non affidarsi ai molti servizi gratuiti o low cost disponibili sul web.
2. **Informarsi sul tipo di servizio VPN** che si sta acquistando e sui protocolli di sicurezza utilizzati.
3. **Seguire le indicazioni di sicurezza** fornite dal provider ed applicare gli aggiornamenti e le patch consigliate.
4. **Scegliere un fornitore con una rete proprietaria** ad elevate prestazioni e sicura.
5. **Verificare i livelli di assistenza e controllo delle prestazioni** forniti dal provider.

1. **Scegliere un provider affidabile** e non affidarsi ai molti servizi gratuiti o low cost disponibili sul web.
2. **Informarsi sul tipo di servizio VPN** che si sta acquistando e sui protocolli di sicurezza utilizzati.
3. **Seguire le indicazioni di sicurezza** fornite dal provider ed applicare gli aggiornamenti e le patch consigliate.
4. **Scegliere un fornitore con una rete proprietaria** ad elevate prestazioni e sicura.
5. **Verificare i livelli di assistenza e controllo delle prestazioni** forniti dal provider.
6. **Formare i collaboratori sulla sicurezza informatica:** gran parte degli attacchi che avvengono sono dovuti a errori o imprudenze di collaboratori.

eritel
passione per l'ICT

Michele Bucciarelli

eritel.it