

HYPERGRID®

HyperVPN Plus

Servizio VPN con accesso sicuro gestito da autenticazione forte a due fattori

La rete **HyperGrid** per progetti strategici comprende un servizio di fondamentale importanza quando per lavoro è necessario accedere alla rete aziendale dall'esterno. In ambito business la VPN diventa essenziale per gli utenti che lavorano fuori sede o in “smart working” e devono avere accesso alla rete inserendo le credenziali di accesso. Purtroppo, quando si entra in una LAN aziendale l'autenticazione con username e password non garantisce sufficiente protezione, anzi, può dimostrarsi pericolosa per il vostro business dato che la sottrazione dei dati di accesso è più semplice di quanto si possa pensare. Il servizio **HyperVPN** è stato recentemente aggiornato alla versione **Plus** che garantisce una maggiore sicurezza e protezione alle reti aziendali e una più ampia possibilità di configurazione.

Allo stato attuale delle cose, con attacchi ransomware e minacce informatiche sempre più insidiose, una **VPN** (Virtual Private Network) dotata di un sistema a doppio fattore di autenticazione è la soluzione essenziale per assicurare l'accesso sicuro alle reti aziendali e ai dati in essa contenuti. Con **HyperVPN Plus** viene creato tunnel virtuale all'interno del quale i dati viaggiano criptati in totale sicurezza. L'uso di protocolli di cifratura robusti rendono impossibile intercettare il traffico che transita sulla VPN, caratteristica di fondamentale importanza anche quando si scambiano informazioni confidenziali.

AUTENTICAZIONE A DUE FATTORI

La prima linea di difesa per tenere fuori dai giochi le intrusioni è l'uso di password sicure che devono necessariamente essere protette da un sistema a doppio fattore di autenticazione (2FA), una tecnologia in grado di proteggere qualsiasi tipologia di password. Purtroppo, nonostante gli indubbi vantaggi sono ancora in molti gli utenti e i responsabili degli uffici IT a considerare scomoda l'autenticazione a due fattori, nonostante sia un piccolo prezzo da pagare per la sicurezza e la protezione dell'infrastruttura e dei suoi dati. Di fatto la **2FA** garantisce un accesso virtualmente inattaccabile dato che si basa su due elementi: qualcosa che conosciamo (login e password) e una cosa che abbiamo (per esempio uno smartphone su cui viene inviato il secondo codice). Grazie agli smartphone è anche possibile introdurre un terzo elemento il “qualcosa che siamo” ovvero l'impronta digitale o il rilevamento biometrico del viso.

ACCESSO SEMPLIFICATO

A rendere più semplice l'accesso a **HyperVPN Plus** ci sono varie soluzioni per ricevere il secondo elemento di autenticazione nel modo per noi più comodo: via SMS tramite una password temporanea (OTP, One Time Password), tramite OTP generato da un'app sullo smartphone o tramite un token hardware. Inoltre, è disponibile l'accesso tramite il riconoscimento del viso o delle impronte digitali. Infine, per chi non vuole (o non può) usare il proprio smartphone per lavoro, **HyperGrid** mette a disposizione l'accesso tramite “chiamata telefonica diretta”. Grazie a questa soluzione l'utente che deve accedere alla rete riceve una chiamata automatizzata in cui viene chiesto di autorizzare il collegamento VPN semplicemente premendo un tasto del telefono. Una soluzione utile anche per risolvere le questioni sindacali sull'uso di dispositivi privati per lavoro. Oltre a soddisfare qualsiasi esigenza per semplificare l'accesso, **HyperVPN Plus** garantisce che tutte le chiamate e gli SMS fanno parte di un servizio flat senza costi aggiuntivi.

OPZIONI DI CONTROLLO PER LA SICUREZZA

Oltre a garantire il trasferimento sicuro dei dati, **HyperVPN Plus** è in grado di verificare il dispositivo da cui si esegue l'accesso. Con il massimo rispetto per la privacy è possibile analizzare se il dispositivo che si collega da remoto sia nelle condizioni ideali per accedere all'infrastruttura. La procedura di sicurezza esegue un rapido check per verificare che il sistema operativo sia aggiornato, che sia presente un antivirus attivo, che il File System del computer sia integro e criptato. Nel caso una (o più) di queste verifiche mettano in evidenza un problema, l'utente dovrà procedere all'aggiornamento prima di poter accedere. Ovviamente l'azienda sarà libera di decidere se mantenere attivi tutti i parametri di controllo o se attivare solo quelli che reputa fondamentali per la propria sicurezza.

GEOLOCALIZZAZIONE SICURA E SOLUZIONI

Profilo di connessione

Per chi desidera attivare funzioni aggiuntive di controllo **HyperVPN Plus** può verificare se il profilo di connessione sia pertinente con le abitudini e gli accessi dell'utente. Per esempio, se la connessione avvenuta poche ore prima da una località in Italia viene eseguita dall'altra parte del mondo, il sistema è in grado di bloccare in modo autonomo l'accesso in attesa di verifiche. Inoltre, è possibile inviare all'utente una notifica con la posizione geografica da cui si sta tentando il collegamento in modo da poter approvare o rifiutare il tentativo di connessione prima che sia elaborata la fase di autenticazione e l'accesso alla rete.

Semplicità di configurazione

Ricordiamo che, nonostante i numerosi parametri implementati, uno dei vantaggi di **HyperVPN Plus** è la semplicità di configurazione che consente ai responsabili dell'ufficio IT dell'azienda (o in mancanza di questi, al team di HyperGrid) di impostare il sistema secondo le reali esigenze dell'azienda. Ovviamente è anche possibile garantire l'accesso dei vari utenti in modo graduale, stabilendo delle precise regole in modo che possano raggiungere solo specifiche aree di competenza dell'infrastruttura aziendale.

Integrazione con soluzioni business

Per quanto riguarda le soluzioni tecniche il servizio **HyperVPN Plus** è integrabile con soluzioni business come per esempio il sistema Active Directory di Windows Server, così come i server RADIUS (Remote Authentication Dial-In User Service) o server LDAP. Ovviamente il team di esperti di **HyperGrid** è sempre disponibile a cercare la migliore soluzione e la configurazione adatta alle esigenze aziendali.

Non solo VPN

Ricordiamo infine che l'autenticazione 2FA è utilizzabile anche per proteggere l'accesso a qualsiasi applicativo del cliente e non solo per gli accessi alla VPN

Per richiedere ulteriori informazioni o un preventivo:

www.hypergrid.it - info@hypergrid.it - Tel. 0382 528875

Garantiamo la sicurezza
del mondo digitale



