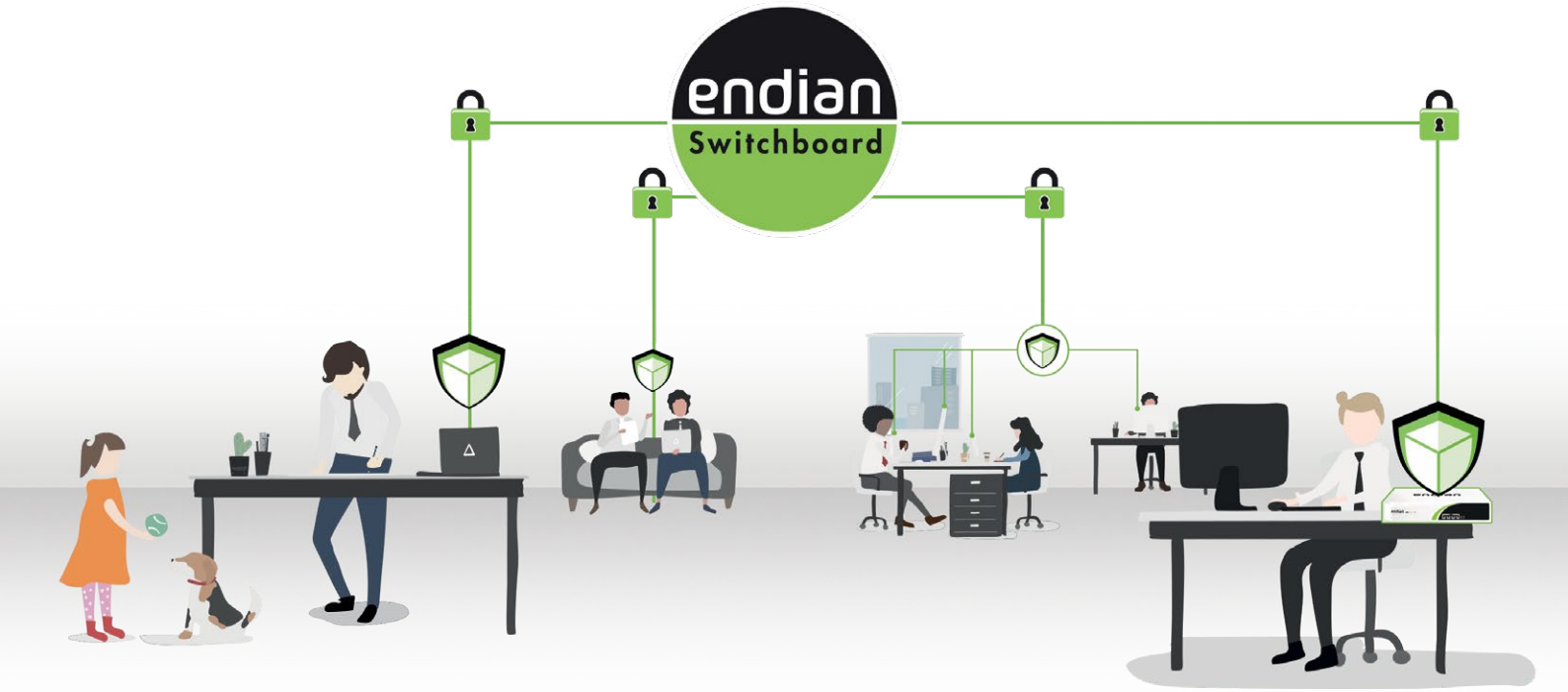
VPN per Smart Working

L'importanza di un collegamento VPN per l'implementazione dello Smart Working.

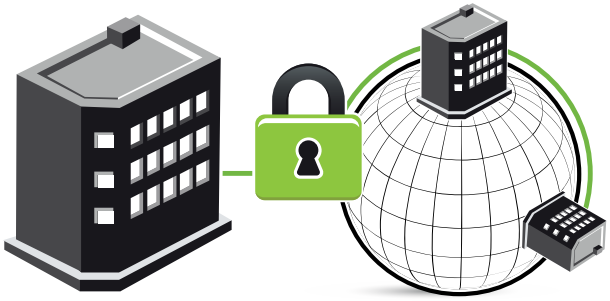


L'emergenza sanitaria del Coronavirus ci ha messo di fronte ad una nuova sfida: attivare lo Smart Working in modo tempestivo sull'intero team Endian. Da una parte per rispettare la normativa vigente sull'isolamento, dall'altra per garantire la continuità dei servizi ai nostri clienti.

Amministrazione, Sales Team, Product&Quality Management e Supporto Tecnico: ogni lavoratore è stato messo in condizioni di svolgere la quasi totalità del proprio lavoro quotidiano da casa. In che modo? Utilizzando un sistema di VPN che permette a ciascuna postazione in smartworking di accedere remotamente e in modo sicuro alle risorse aziendali di propria competenza. Mentre i team tecnici raggiungono i build server, i sistemi di gestione del codice e gli ambienti di test, i programmi gestionali e la documentazione interamente digitalizzata sono disponibili tramite autenticazione a due fattori.

Partendo dalla nostra esperienza di Vendor di una soluzione di Cybersecurity che integra un sistema di VPN per il collegamento sicuro di reti, utenti e dispositivi IoT, desideriamo offrire a Clienti e Partner uno spunto di informazione sulla tecnologia VPN, come funziona e quali sono i vantaggi di avere un servizio di questo tipo attivo.

Che cos'è una VPN



Una Virtual Private Network, o VPN, è un collegamento diretto, sicuro e stabile tra una rete o una workstation locale ed una rete remota. La motivazione principale per l'adozione delle VPN è, quindi, quella di proteggere la privacy dei propri dati da attacchi indesiderati, nonché garantire la sicurezza e la rapidità dell'accesso lecito alle risorse disponibili.

Si tratta in effetti di un tunnel, ovvero di un collegamento cifrato diretto punto a punto (peer-to-peer) tra una risorsa locale, che può essere sia un singolo computer che un'intera rete - ad esempio la rete interna di una sede distaccata - ed una rete remota – tipicamente la sede principale dell'azienda. Questo collegamento permette alla risorsa locale di far parte virtualmente della rete remota, esattamente come se vi si trovasse fisicamente.

Le principali caratteristiche di una VPN:

Crittografia

Il traffico dati che transita nel tunnel della VPN viene automaticamente criptato prima dell'ingresso e decriptato in uscita, aggiungendo un ulteriore livello di protezione alla comunicazione. L'uso di algoritmi di cifratura crittografica concorre quindi a garantire la segretezza delle informazioni circolanti ed è proprio questa caratteristica ad impedire l'intercettazione del traffico da parte di terzi (sniffing).

Autenticazione

L'autenticazione, infine, riveste un ruolo importante per garantire che chi si collega sia effettivamente chi dice di essere. Nella sua forma più semplice, essa prevede semplicemente una password per identificare il tunnel VPN, anche se spesso è previsto l'uso di una combinazione username/password. Tecnologie più avanzate ricadono nella cosiddetta Autenticazione multi-fattore, basate sul possesso, da parte dell'utente, di almeno due tra i seguenti fattori: fattore conoscenza (qualcosa che solo l'utente sa), fattore possesso (qualcosa che solo l'utente ha) e fattore intrinseco o identificativo (qualcuno che solo l'utente è). Abbinare alla combinazione username/password un certificato crittografico digitale è un esempio di autenticazione a due fattori e rappresenta già un buon livello di sicurezza, che può venir incrementato con l'uso di carte magnetiche o metodi biometrici (lettore di impronte digitali o della retina). L'autenticazione permette di ridurre al minimo i rischi collegati allo spoofing. La somma di queste caratteristiche permette di difendere il transito dei dati da tentativi esterni di penetrazione e forzatura.

Le principali e più semplici **modalità di collegamento via VPN** sono due: **host-to-net** (comunemente chiamata roadwarrior) e **net-to-net**.

In modalità roadwarrior una singola workstation si collega ad una rete locale remota ed agisce come se si trovasse fisicamente all'interno di quella rete. Dopo l'autenticazione con il server VPN remoto, infatti, la workstation riceve un indirizzo IP della rete a cui si collega e delle apposite regole di routing per accedervi. Questo è il caso di un tele-lavoratore o di un

collaboratore dell'azienda che si collega alle risorse messe a disposizione da questa senza dover recarvisi di persona

In modalità net-to-net invece, una intera rete locale si collega ad una rete remota. In questo caso solitamente i due punti estremi del tunnel sono i gateway/router delle due reti: in questo modo, il traffico in arrivo ad uno degli estremi può essere correttamente instradato dal punto di accesso della rete, ovvero gateway o router. Questo è il caso, ad esempio, del collegamento di due (o più) filiali di un'azienda che devono poter condividere le stesse risorse in maniera sicura: una Intranet, server di posta etc.

OpenVPN e IPsec, i due protocolli di collegamento VPN più usati

OpenVPN si appoggia alla libreria OpenSSL e ne usa gli algoritmi per crittografare il traffico all'interno del tunnel. IPsec, uno standard IETF, è una famiglia di protocolli di comunicazione, studiata per incrementare la sicurezza di flussi di dati all'interno di una VPN. Trattandosi di un'estensione del protocollo IP, IPsec opera al livello 3 dello standard OSI/ISO e si occupa sia di stabilire ed autenticare il tunnel di comunicazione criptato tra rete locale e rete remota (chiamato Security Association), che dell'integrità, origine e riservatezza dei dati trasmessi. IPsec di fatto è in grado solo di autenticare il tunnel, ma non i singoli utenti che si collegano tramite il tunnel. Per renderlo più sicuro viene spesso impiegato in congiunzione con altri protocolli dedicati all' identificazione ed all'autenticazione degli utenti, quali L2TP e XAuth.

La garanzia offerta dal modello Open Source

La VPN rappresenta indubbiamente la soluzione più efficiente per agevolare il transito protetto dei dati e l'accesso agli stessi da remoto, sia sotto il profilo tecnico che economico. Parlando di Open Source si intende la generazione di codice il cui sorgente è messo a disposizione di chiunque voglia ispezionarlo, rielaborarlo e redistribuirlo. Sono favorite, da parte degli autori, la diffusione, il controllo e l'apporto di modifiche da parte delle community di programmatori indipendenti. I vantaggi presentati dal software libero sono diversi ed interessanti. Principalmente l'interoperabilità e la possibilità di integrazione con altri sistemi, l'indipendenza rispetto alla logica costrittiva del fornitore unico e ultimo – ma primo in ordine di importanza – la garanzia di inaccessibilità da parte del vendor.