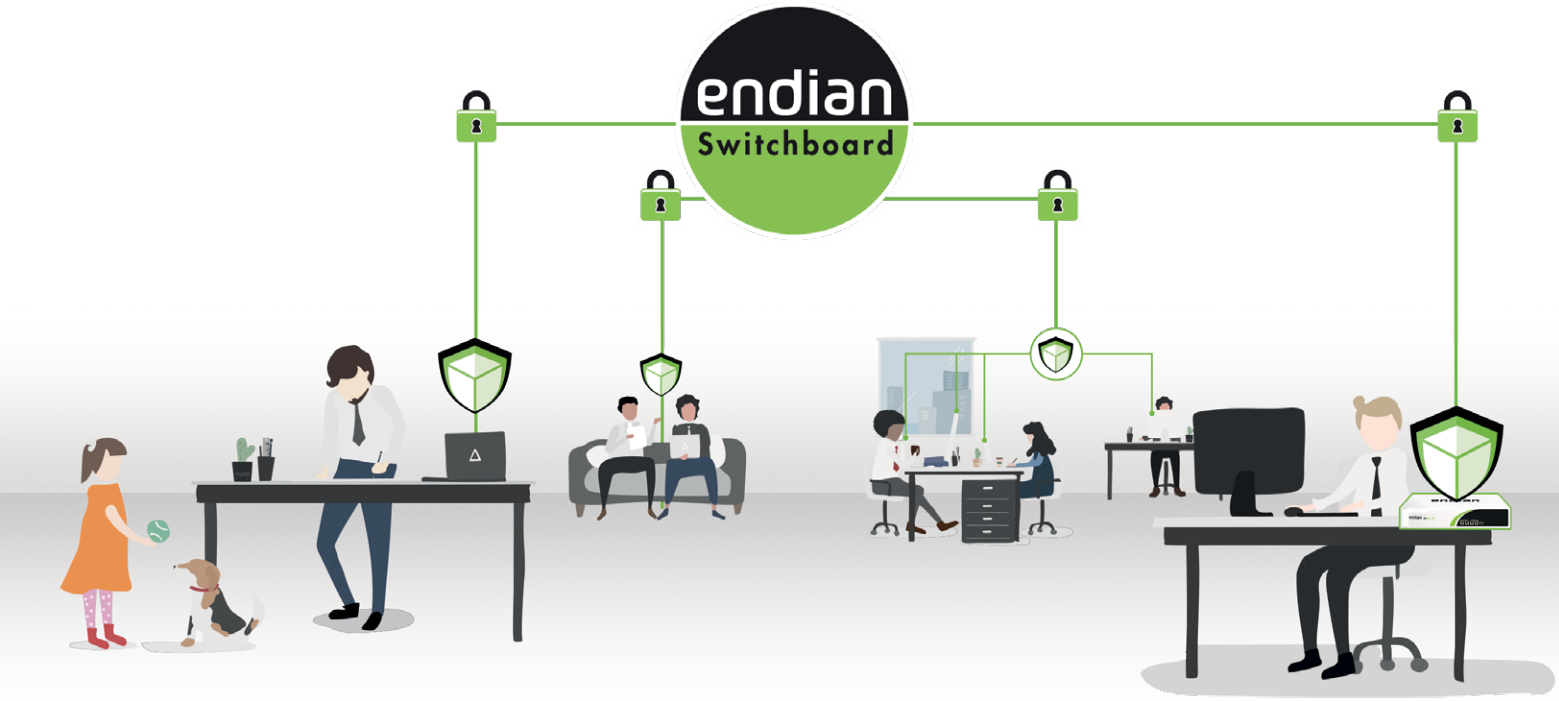
VPN für Smart Working

VPN-Verbindung - Voraussetzung für sicheres und effizientes Smart Working

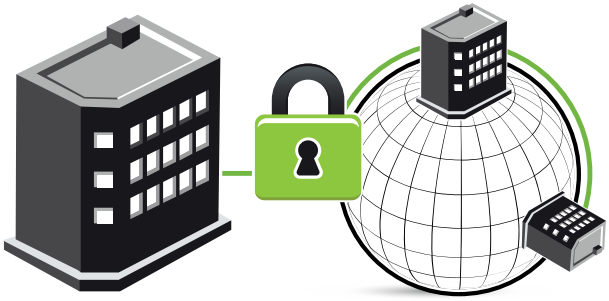


Die Corona-Pandemie hat uns vor eine neue Herausforderung gestellt: Die rechtzeitige Aktivierung von Smart Working im gesamten Endian-Team. Die Verlagerung der gesamten Belegschaft ins Homeoffice war die einzige Möglichkeit, um den sehr strengen Isolationsvorschriften in Italien gerecht zu werden und dabei gleichzeitig den Service für unsere Kunden aufrecht zu erhalten.

Verwaltung, Verkaufsteam, Produkt- und Qualitätsmanagement sowie technischer Support: Jeder Mitarbeiter konnte von einem Tag auf den anderen fast alle seine täglichen Arbeiten von zu Hause aus zu erledigen. Wie war das möglich? Durch die Verwendung eines VPN-Systems, das es jeder Smart-Working-Arbeitsstation erlaubt, aus der Ferne sicher auf die Ressourcen des Unternehmens zuzugreifen. Während technische Teams die Build-Server, Codeverwaltungssysteme und Testumgebungen erreichen, sind Verwaltungsprogramme und vollständig digitalisierte Dokumentation durch Zwei-Faktor-Authentifizierung verfügbar.

Ausgehend von unseren Erfahrungen als Anbieter einer Cybersicherheitslösung, die über ein VPN-System für die sichere Verbindung von Netzwerken, Benutzern und IoT-Geräten verfügt, möchten wir Kunden und Partnern einen Einblick in die VPN-Technologie bieten, wie sie funktioniert und welche Vorteile ein solcher aktiver Dienst bietet.

Was ist ein VPN?



Ein Virtual Private Network (VPN) ist eine direkte, sichere und stabile Verbindung zwischen einem lokalen Netzwerk oder einer Arbeitsstation und einem entfernten Netzwerk. Die Hauptgründe für die Einführung von VPNs sind meistens der Schutz eigener Daten vor unerwünschten Angriffen sowie die Absicherung des Zugriffs die verfügbaren Ressourcen. Es handelt sich dabei um einen Tunnel, d.h. eine auf direkte Punkt-zu-Punkt (Peer-to-Peer)-verschlüsselte Verbindung zwischen einer lokalen Ressource und einem entfernten Netzwerk, meistens dem Hauptsitz des Unternehmens. Bei der lokalen Ressource kann es sich um einen einzelnen Computer oder ein ganzes Netzwerk handeln - beispielsweise das interne Netzwerk einer Zweigstelle. Diese Verbindung ermöglicht es, dass die lokale Ressource praktisch Teil des entfernten Netzwerks ist, so als ob sie sich physisch dort befinden würde.

Hauptmerkmale eines VPNs

Der Datenverkehr, der den VPN-Tunnel durchläuft, wird vor dem Eintritt automatisch verschlüsselt und beim Austritt entschlüsselt, wodurch die Kommunikation zusätzlich geschützt wird. Die Verwendung von kryptographischen Verschlüsselungsalgorithmen trägt daher dazu bei, die Geheimhaltung der zirkulierenden Informationen zu gewährleisten, und genau diese Eigenschaft verhindert das Abfangen des Verkehrs durch Dritte (Sniffing).

Authentifizierung

Schließlich spielt die Authentifizierung eine wichtige Rolle, um sicherzustellen, dass die Nutzer, die sich einloggen, auch wirklich diejenigen sind, für die sie sich ausgeben. In seiner einfachsten Form wird einfach ein Passwort zur Identifizierung des VPN-Tunnels angegeben, obwohl oft eine Benutzername/Passwort-Kombination zum Einsatz kommt. Fortschrittlichere Technologien fallen unter die so genannte Multi-Faktor-Authentifizierung, bei der Benutzer mindestens zwei der folgenden Faktoren aufweisen müssen: Wissensfaktor (etwas, das nur der Benutzer kennt), Besitzfaktor (etwas, das nur der Benutzer hat) und intrinsischer oder identifizierender Faktor (jemand, der nur der Benutzer ist). Die Verknüpfung der Benutzername/Passwort-Kombination mit einem digitalen kryptographischen Zertifikat ist ein Beispiel für die Zwei-Faktor-Authentifizierung und stellt bereits ein gutes Sicherheitsniveau dar, das durch den Einsatz von Magnetkarten oder biometrischen Verfahren (Fingerabdruck- oder Netzhautscanner) erhöht werden kann. Durch die Authentifizierung werden die mit Spoofing verbundenen Risiken minimiert. Die Summe dieser Merkmale erlaubt es, den Datentransit gegen Zugriffs- und Erpressungsversuche zu verteidigen.

Die wichtigsten und einfachsten VPN-Verbindungsmodi sind zwei Szenarien: Entweder Host-zu-Netz, beispielsweise durch einen Außendienstmitarbeiter oder Netz-zu-Netz, etwa durch eine Niederlassung im Ausland.

Im Host-zu-Host Modus verbindet sich eine einzelne Workstation mit einem entfernten lokalen Netzwerk und verhält sich so, als befände sie sich physisch innerhalb dieses Netzwerks. Nach der Authentifizierung mit dem Remote-VPN-Server erhält die Arbeitsstation eine IP-Adresse des Netzwerks, mit dem sie sich verbindet, sowie Routing-Regeln für den Zugriff darauf. Dies ist das klassische Homeoffice-Szenario: Ein Mitarbeiter des Unternehmens verbindet sich mit den vom Unternehmen zur Verfügung gestellten Ressourcen, ohne persönlich in die Firma gehen zu müssen.

Im Netz-zu-Netz-Modus verbindet sich ein gesamtes lokales Netzwerk mit einem Remote-Netzwerk. In diesem Fall sind die beiden Endpunkte des Tunnels in der Regel die Gateways/Router der beiden Netze: Damit kann der Datenverkehr, der an einem Ende ankommt, korrekt vom Netzzugangspunkt, d.h. vom Gateway oder Router, weitergeleitet werden. Dies ist z.B. der Fall bei der Verbindung von zwei oder mehr Niederlassungen eines Unternehmens, die in der Lage sein müssen, die gleichen Ressourcen auf sichere und geschützte Weise gemeinsam zu nutzen: Intranet, Mailserver usw.

OpenVPN und IPsec: Die zwei wichtigsten VPN-Verbindungsprotokolle

OpenVPN basiert auf der OpenSSL-Bibliothek und verwendet deren Algorithmen, um den Verkehr innerhalb des Tunnels zu verschlüsseln. IPsec, ein IETF-Standard, umfasst eine Gruppe von Kommunikationsprotokollen, die die Sicherheit des Datenflusses innerhalb eines VPNs steigern soll. Als Erweiterung des IP-Protokolls arbeitet IPsec auf Ebene 3 des OSI/ ISO-Standards und befasst sich mit dem Aufbau und der Authentifizierung des verschlüsselten Kommunikationstunnels zwischen dem lokalen und dem entfernten Netzwerk (Security Association genannt) sowie mit der Integrität, Herkunft und Vertraulichkeit der übertragenen Daten. IPsec ist tatsächlich nur in der Lage, den Tunnel zu authentifizieren, nicht aber die einzelnen Benutzer, die sich durch den Tunnel verbinden. Um die Sicherheit zu erhöhen, wird es häufig in Verbindung mit anderen Protokollen zur Benutzeridentifizierung und -authentifizierung verwendet, wie beispielsweise L2TP und XAuth.

Die Vorteile von Open Source

VPN ist zweifellos die effizienteste Lösung, um die sichere Datenübertragung und einen sicheren Fernzugriff auf dieselben Ressourcen sowohl technisch als auch wirtschaftlich zu erleichtern. Unter Open Source verstehen wir die Entwicklung von Software, deren Quellcode jedem zur Verfügung gestellt wird, um ihn einzusehen, zu überarbeiten und weiterzuverbreiten. Die Autoren befürworten die Verbreitung, die Kontrolle sowie Modifikationen durch die Community unabhängiger Programmierer. Open Source Software bietet viele interessante Vorteile, wie die Interoperabilität und die Möglichkeit der Integration mit anderen Systemen. Außerdem ist Open Source unabhängig von der Business-Strategie eines einzelnen Anbieters. Und nicht zuletzt kann kein Anbieter die Software für seine eigenen Zwecke und Interessen nutzen.