WAS IST VPN ?

VPN steht für "**Virtual Private Network**" und beschreibt ursprünglich eine Technik, die es Ihnen erlaubt, von jedem Ort auf der Welt sicher auf Ressourcen in Ihrem privaten Netzwerk zuzugreifen.
VPN verschlüsselt Ihre Internetverbindung beginnend von Ihrer Netzwerkkarte bis hin zu einem VPN-Server. Diese Verschlüsselung findet in Echtzeit statt und verhindert zuverlässig Mitschnitte bzw. das Abhören der übertragenen Informationen. Die Art Ihrer Internetverbindung (Modem, ISDN, GPRS, UMTS, LTE, Kabel, Standleitungen, WLan), die Wahl Ihres Endgerätes oder auch des Standortes, an dem Sie sich befinden, spielt dabei keine Rolle – Ihre Internetverbindung wird durch die Nutzung von VPN vollständig verschlüsselt.

Jetzt websecuritas VPN nutzen ➦ | Serverstandorte

VPN Anwendungen für alle Geräte

websecuritas VPN arbeitet problemlos auf all Ihren Geräten – egal ob Rechner, Laptop, Smartphone, Router oder Tablet. Installieren Sie bequem unsere benutzerfreundliche hidemachine auf dem Gerät Ihrer Wahl. Sie können mit bis zu sieben Geräten zur selben Zeit verbunden sein.

Keine Fachkenntnisse erforderlich

Registrieren, installieren und verbinden. So einfach ist das.

Kompatibilität

Wir haben Apps für Windows, Mac, iOS, Android, Router (eBlocker) und Linux. websecuritas funktioniert mit allen Internetverbindungen – Wi-Fi und Mobilfunknetze eingeschlossen.

Angebotene VPN-Protokolle

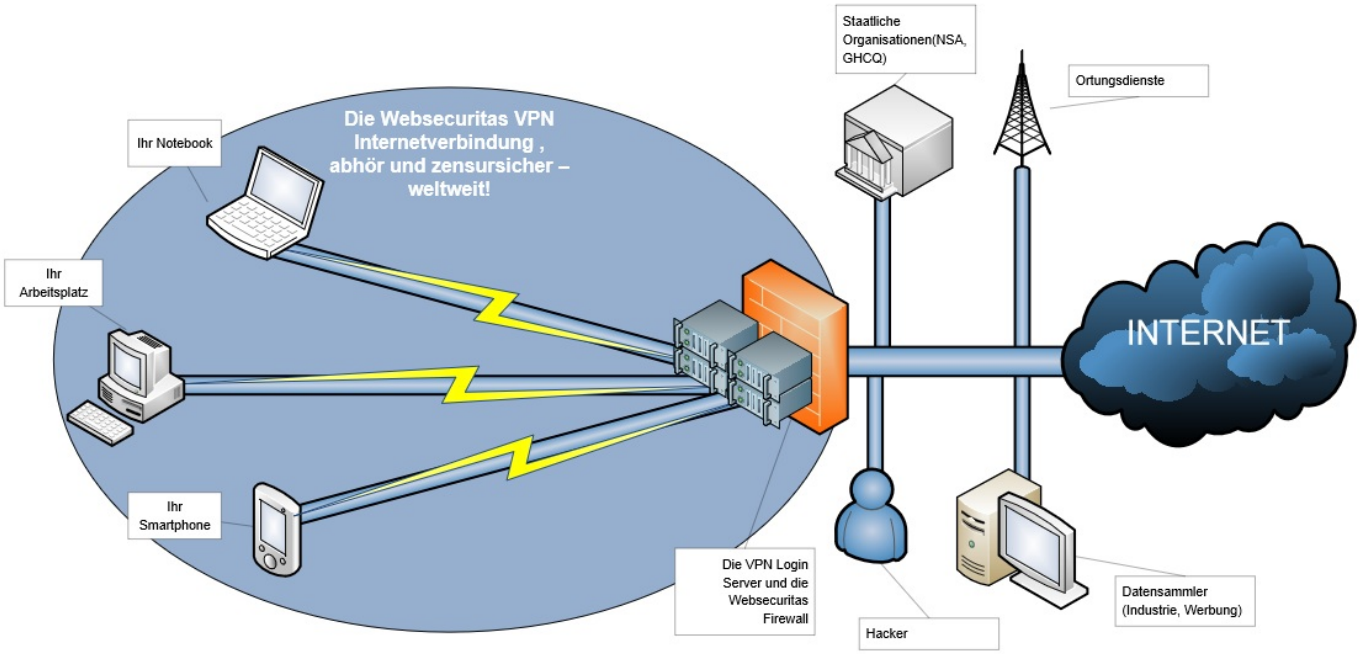
Die websecuritas Hidemachine ist standardgemäß mit OpenVPN UDP konfiguriert. Alternativ bieten wir auch OpenVPN TCP, L2TP/IPsec und wireguard.

Jetzt websecuritas VPN nutzen ➚ | Serverstandorte

WIE FUNKTIONIERT VPN ?

Ein VPN (Virtuelles privates Netzwerk) ist ein in sich abgeschlossenes Teilnetzwerk innerhalb eines größeren IP Netzes in dem die Teilnehmer räumlich (mitunter tausende Kilometer) voneinander getrennt sind. Die Teilnehmer verbinden sich über ein VPN Protokoll zu einem Loginserver (Loginserver stehen weltweit zur Verfügung) und erhalten nach Aufbau des verschlüsselten Tunnels eine eigene , neue (interne) IP. Da nun die gesamte Verbindung zum Internet verschlüsselt ist können Computer außerhalb dieses Netzwerks die Kommunikation nicht mehr mitlesen oder verändern. So ist gewährleistet das der Clientcomputer mit ausgewählten anderen Computern abhörsicher kommunizieren kann. Bewerkstelligt wird dies über eine virtuelle Netzwerkkarte im Computer des Kunden. Diese Netzwerkkarte erscheint im Betriebssystem als normaler Ethernetadapter und wird vom System sowie als auch den Programmen auch so genutzt, einzig der Unterschied das die Daten die über diese Netzwerkkarte transferiert werden automatisch hochgradig verschlüsselt werden. Zusätzlich verhindern Einstellungen des VPN LoginServers das Kunden untereinander sich gegenseitig beeinflussen können, jeder Kunde erhält seinen eigenen Tunnel und seine eigene Verschlüsselung. Sämtliche gesendete oder empfangene Daten werden vom Server dann über eine einzige IP (die IP des jeweiligen VPN LoginServers) ins Internet gesendet – diese Server IP gilt für alle Kunden und sorgt erneut für Anonymität. Ist der Computer nicht mit einer VPN oder mit einem VPN Anbieter der feste Ips verteilt verbunden, ist jeder anhand seiner in diesem Moment weltweit einzigartigen IP identifizierbar.

Durch die Verschlüsslung über die interne, virtuelle VPN Netzwerkkarte ist sichergestellt das die Internetverbindung intransparent für Provider, Datensammler und andere Computer im lokalen Netzwerk sind und dem Internetnutzer nicht zugeordnet werden kann.



Jetzt websecuritas VPN nutzen ➚ Serverstandorte

Surfen mit VPN Verschlüsselung

Eine “normale” Internetverbindung wie zum Beispiel UMTS/ GPRS/ ISDN/ DSL usw. beinhaltet per Standard keine Verschlüsselung: sämtliche Daten, die du generierst (E-Mail,surfen, chatten usw.) werden in kleine Pakete zerteilt und unverschlüsselt durch das TCP/IP-Protokoll zum Empfänger geschickt.
Teilnehmer in lokalen Netzwerken, z.B. öffentlichen Hotspots, können diese Daten schon mit einfachen Mitteln abhören und mitschneiden. Es ist aber auch möglich einfach in der Nähe Ihrer Wohnung zu parken und per Laptop ihr Wlan anzuzapfen.
Nachfolgend ein Beispiel zur Veranschaulichung:
Sie sind zu Hause und surfen über Ihr (nur) WEP-verschlüsseltes WLan. Ihr Nachbar hat parallel „Wireshark“ laufen, ein freies Programm zur Analyse von Netzwerk-Kommunikationsverbindungen, und schneidet alles mit. Da WEP sowie auch WPA schon lange nicht mehr sicher sind, ist es Ihrem Nachbarn ein Leichtes, aus den gewonnenen Daten Ihr WLan-Passwort zu generieren. In einem nächsten Schritt surft er über Ihre Leitung und überwacht in Echtzeit Ihren Laptop und erhält so viele Ihrer privaten Daten – Ihre Bank-/Kontoverbindungen, Ihre E-Mail Zugangsdaten, was Sie wann und wo einkaufen, mit wem Sie chatten und so weiter.
In vielen Ländern wird das Internet durch die jeweilige Regierung zensiert, so dass viele Angebote (z.B. Facebook, YouTube, Wikipedia) nicht zur Verfügung stehen. In diesen Fällen kann das Internet ohne eine VPN-Verbindung nicht vollumfassend genutzt werden, erst das aktivieren der VPN gibt Ihnen wieder Zugriff auf alle Inhalte weltweit.

Gründe für Verschlüsselung

Nicht erst seit den Enthüllungen Edward Snowdens über die weltweite und verdachtsunabhängige Abhörpraxis amerikanischer und englischer Geheimdienste (NSA , GCHQ u.a.) wird die Sicherung der digitalen Kommunikation

zu einem Grundbedürfnis der Gesellschaft. Digitale Kommunikation ist aus der heutigen Zeit nicht mehr wegzudenken und umfasst mittlerweil alle Bereiche des täglichen Lebens. Sensible , private Informationen gehören nicht auf eine Postkarte , vergleichbar zum Brief der die Nachricht schützt, schützt starke Verschlüsselung vor neugierigen Datensammlern überall auf der Welt. Ein weiterer Grund für den flächendeckenden Einsatz von VPNs ist die immer stärker auftretende Zensur – nicht nur in autokratischen Staaten. Gesperrte Webseiten, nicht abrufbare Informationen aus politischen oder religiösen Gründen, auch hier hilft die VPN (Virtuelles Privates Netzwerk) – dadurch das niemand überwachen kann welche Webseiten abgerufen werden, greifen auch keine Sperrungen. Mit ein Grund warum sich Websecuritas.com VPNs in MiddleEast und China so gefragt sind.
Doch auch bei der Wahl der VPN gibt es einige Grundregeln zu beachten – wie zum Beispiel die Wahl des richtigen Anbieters.
VPN Provider gibt es viele , geworben wird mit allem. Günstig, schnell und sicher – einer objektiven Bewertung halten jedoch die wenigsten stand.

Standort des VPN Providers

Wieviel Sinn macht es bei einem Amerikanischen, Englischem oder Osteuropäischen Provider zu buchen? Die Preise mögen sicher verlockend sein, Ihre Daten sind es bei solchen Anbietern aber nicht sicher. Sämtliche in USA ansässige Firmen müssen auf Anfrage der Behörden Kundendaten sowie SSL Schlüssel zu jedem Nutzer aushändigen – auch wenn die Daten in Europa gespeichert sind. Erste Anbieter haben deswegen ihren Service in den USA schon eingestellt. Ein ernst gemeinter Schutz der Kommunikation ist nicht zu gewährleisten. (siehe Lavabit und Cryptoseal) Nirgends ist der Datenschutz stärker im Bewusstsein und im Gesetz verankert als in Deutschland – Anbieter die mit Standort Rumänien werben sind dort nicht wegen Sicherheit und Rechtsstaatlichkeit sondern allein aus steuerlichen Gründen. In Deutschland darf nicht geloggt werden und es gibt keine Vorratsdatenspeicherung, Anfang 2014 wurden vom EuGH in Luxemburg sämtliche Ambitionen voreiliger „Sicherheits“ Politiker als nicht vereinbar mit europäischen Recht klassifiziert und gestoppt.

Protokolle und IPs

Nahezu alle großen Provider werben mit PPTP VPN– einfach und schnell eingerichtet – und genauso schnell entschlüsselt. Dieses Protokoll wird selbst vom Erfinder Microsoft seit Jahren als potentiell gefährlich und unsicher eingestuft. Ein weiterer wunder Punkt sind statische IP’s – Anbieter werben damit Kunden eigene, feste IP’s zur Verfügung zu stellen. Warum? Der Kunde ist dadurch leicht identifizierbar, es ist klar wer welche IP wann , wofür und wie lange genutzt hat. Aus der Sicht der Anonymität macht es mehr Sinn hunderte VPN-Tunnel hinter einer Server IP zu verbergen – die Tunnel schützen die Nutzerverbindungen und die Server IP verschleiert zuverlässig den Traffic eines jeden einzelnen.

Datenschutz

Der Datenschutz ist nach der Rechtsprechung des Bundesverfassungsgerichts ein Grundrecht. Telekommunikationsanbieter in Deutschland sind verpflichtet Kundendaten vor Zugriff Dritter zu schützen und nur auf richterlichen Beschluss (bei schweren Straftaten) hin verpflichtet Daten auszuhändigen. Anders verhält sich das in vielen anderen Staaten, vergleiche hierzu http://de.wikipedia.org/wiki/Datenschutz

---

Logging / Vorratsdatenspeicherung

Wir loggen keine Daten bezüglich dem was gesurft wird. Wir speichern keine Daten was wann wie gemacht wurde. Wir wissen nur wann jemand online war – und das nur um unser Abrechungssystem am laufen zu halten. Websecuritas.com steht für maximalen Datenschutz und Anonymität in einer durch zunehmende Überwachung geprägten Zeit. Wir unterstützen in allen Belangen und sind Mitglied der Electronic Frontier Foundation www.eff.org .

Technische Merkmale

Websecuritas setzt in allen Bereichen auf die beste und sicherste Lösung: Open Source Software. Anders als bei kommerziellen Lösungen können wir den Quellcode selbst auf Hintertüren prüfen und so maximale Sicherheit gewährleisten.

VPN Server
Alle unserer Server laufen unter speziell angepasstem, gehärtetem Linux Betriebssystemen. Wir verfolgen die Philosophie „weniger ist mehr“ , alle Server enthalten nur Software die direkt zur Umsetzung der Aufgabe zwingend notwendig ist. Überflüssige Software bietet unnötige Angriffspunkte. Die Programme werden kontinuierlich weiterentwickelt und von uns sowie der Community auf Schwachstellen geprüft. Alle Server verfügen über IDS (Intrusion Detection Systems), Firewalls und automatische Malwarescanner.

Websecuritas VPN Client
Wir vertrauen keiner Software die nicht von uns auf Herz und Nieren getestet wurde oder die wir selbst entwickelt haben. Unser Client basiert auf Openvpn sowie Java und bietet einige Vorteile gegenüber der sonst auf dem Markt verfügbaren Software.
Der Client ist nur ein VPN Client , du installierst dir keine Malware die mit Werbung und oder schlimmeren nervt. Zweitens ist die Software optimal auf unsere Infrastruktur abgestimmt und basiert auf Java , einer Programmiersprache die weltweit auf vielen hundert Millionen Telefonen (Android), PCs und Notebooks installiert ist.
Ein weiterer Vorteil von Java ist die Kompabilität zu allen Betriebssystemen – somit ist gewährleistet das unser Client auf OSX sowie auf Microsoft und Linux gleich läuft und aussieht.
Die Features im Überblick:

- Autoupdate des Clienten
- Autoupdate aller VPN Server
- Auto Hinzufügen neuer VPN Server
- Autoerkennung von Firewalls , adaptives UDP / TCP
- Link auf GeoIP Database zur IP Überprüfung
- Übersicht über eigene, alte IP sowie verbundenen Server
- Autoerkennung von Man in Middle Attacken , automatischer Neuaufbau des Tunnels

und noch vieles mehr !

VPN einfach erklärt:

Heute noch sicher und entspannt surfen?

➔ jetzt bestellen