privacy.boutique
— Privacy first! —

https://privacy.boutique
sales@privacy.boutique

CryptoRouter Professional

Vollständig vorkonfigurierter Arbeitsplatzschutz. Sofort sicher und anonym ins Internet – «plug & play».

CryptoRouter Pro bietet Ihnen sichere Kommunikation.
Verschlüsselt, nicht verfolgbar und anonym – für Ihr gesamtes Büro.

CryptoRouter Pro bietet 5 lastverteilte gleichzeitige Verbindungen, jeweils mit mindestens 6 MBit/s Bandbreite. Dies ermöglicht den automatischen Schutz für ein mittelgrosses Büronetzwerk von 20 – 30 Arbeitsplätzen mit jeweils bis zu 3 Geräten.

Für maximalen Komfort und Flexibilität beinhaltet das Produkt die Fernwartung durch die technischen Mitarbeitenden unseres Lieferanten. Die Kontrolle über die Fernwartung haben Sie jederzeit selber in der Hand: Sie geben sie frei und beenden sie auch wieder mit dem mitgelieferten innovativen Hardware-Autorisierungssystem, einem USB-Token. Somit ist der Fernzugriff von Administratoren auf den CryptoRouter Pro nur möglich, wenn Sie als Kunde dies autorisieren, indem Sie den USB-Token am CryptoRouter Pro direkt einstecken.

CryptoRouter Pro automatisiert die Verwaltung von anonVPN-Verbindungen, Authentifizierung / Autorisierung und Lastausgleich sowie das Management lokalter Netzwerke.

Darüber hinaus bietet es die Möglichkeit, die VPN-Verbindung für kundendefinierte Bypass-Routen zu umgehen, um etwa kundenspezifische Verbindungen zuzulassen.

Sie erhalten CryptoRouter Pro als *Komplettlösung* gegen eine jährliche Gebühr. Ein Preis für Hardware inkl. Garantie, Software und Nutzung.

Weiterführende Beratung, Coaching und Spesen werden gesondert verrechnet.

https://privacy.boutique
sales@privacy.boutique

CRpro : Spezifikationen & Information

1 x 1Gbits/s Ethernet (CAT) für die Verbindung zum Internet. Setzt voraus, dass IPv4 und DHCP bei der Erstinstallation verfügbar sind, danach ist auch IPv6 möglich.

2 x 1Gbits/s Ethernet (CAT) für das lokale Netzwerk werden Ports überbrückt (das System kann von zwei Computern genutzt werden, die einen Switch benötigen).
Bedient IPv4 intern, IPv6 optional.

1 GHz 64bit quad core AMD Jaguar CPU

AES-NI Hardwarebeschleunigung.

Core-boot - keine Intel ME oder ähnliche proprietäre Firmware.

2 GB RAM

11 GB SSD

OpenBSD Operating System

OpenBSD pf Firewall

Verwaltet ca. 100 interne Systeme für die lokale Vernetzung.

Durchsatz zu VPN über 5 Verbindungen und eine gute Route: 100 Mbit/s, wenn alle Verbindungen gleichermaßen genutzt werden. 50 Mbit/s typisch.

Die Latenz erhöht die VPN-Volllast: 8 ms.

Bypass-Routen: Latenzsteigerung 2 ms, 600 Mbit/s Durchsatz.

Die integrierte Firewall sorgt für Sicherheit:

Kein Traffic aus dem Internet erreicht ein CRpro-geschütztes System.

Kein Traffic von CRpro-geschützten Systemen kann das Internet erreichen.

Keine offenen Ports auf dem CRpro nach außen oder innen, außer DHCP nach innen.

Kein Datenverkehr aus dem verschlüsselten Anonymisierungsnetzwerk erreicht interne Systeme - es sei denn, er bezieht sich auf eine Verbindung, die von einem internen System initiiert wurde.

IP-Adressen werden rotiert, aber nur, wenn kein aktueller Datenverkehr zu einem Ziel besteht. CRpro merkt sich, welche VPN-Verbindung zuletzt von einem internen System verwendet wurde und verwendet diese Verbindung erneut, so dass Sitzungen nicht unterbrochen werden.

Eigene und hochsichere DNS-Resolver, die periodisch mit diversen Root-DNS Server verschlüsselt abgeglichen werden und die auch als Proxy-Cache fungieren. Damit ist auch der DNS-Traffic komplett anonymisiert und sicher.

Weitere Spezifikationen:
- CryptoRouter Stx (pb._Flyer_CRstx_DE.pdf)
- CryptoRouter Slate (pb_Flyer_CRslate_DE.pdf)
- SoC – Separation of Concerns (pb._Flyer_SoC_DE.pdf)

https://privacy.boutique
sales@privacy.boutique

CRpro : Netzwerkfunktionen und mehr

Professionell gewartet, mit mehr als 10 Jahren aktiver Erfahrung.

Organisatorischer Aufbau und Verfahren für maximale Kundenzufriedenheit.

Multi-juristische und unternehmensüber-greifende Organisation mit klarer Trennung von Zugang und Verantwortlichkeiten.

Selbstverwaltete Zertifizierungsstelle (CA), die für alle Client-Authentifizierungen erzwungen wird.

Statische Schlüssel nur zur Authentifizierung.
Alle Verschlüsselungen erfolgen nur über sog. «ephemeral keys».

Dedizierte, selbstverwaltete DNS-Resolver mit DNSSEC-Validierung.

Gehärtete Betriebssysteme und Konfigurationen:
- OpenBSD
- Hardened Gentoo
- Hardened Arch
- Hardened Buildroot

Aktuelle kryptographische Algorithmen und Schlüssellängen:
RSA4096, AES256-CTR/CBC, SHA256/512, ECDH 384

OpenVPNv2 und IPSEC (IKEv2, tunnel mode)

Out-of-Band-Authentifizierung:
Die Client-Daten sind für die Netzwerk-Router nie verfügbar.

Multi-Hop- und Multi-Jurisdiktionsverbindungen, Knoten, die von verschiedenen Unternehmen in verschiedenen Jurisdiktionen verwaltet werden.

IP-Pool-Randomisierung.

Gemeinsame Nutzung der IP-Adresse zwischen ausgehenden Verbindungen.

Zufällige IP-Adressvergabe für ausgehende Verbindungen.

Keinerlei Aufzeichnungen.

Weitere Spezifikationen: - SoC – Separation of Concerns (pb_Flyer_SoC_DE.pdf)