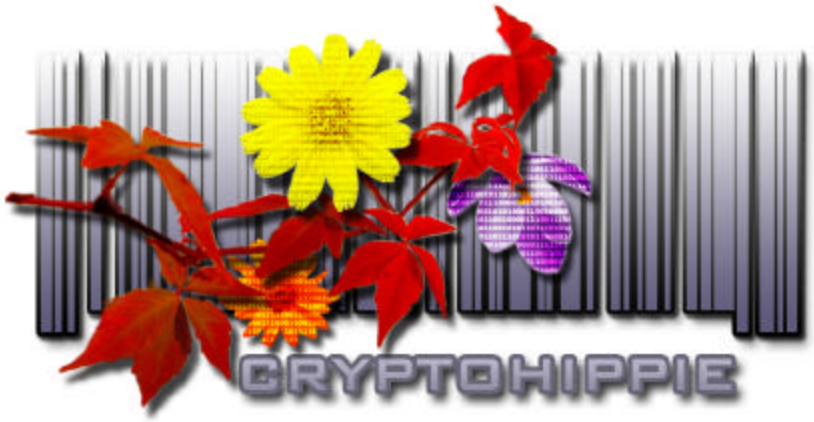

Cryptohippie Technology

Cryptohippie, Inc. develops and operates Internet Security technologies that provide multi-level protection of client information.

Cryptohippie offerings are designed to address threats related to content, context and trust.

> **Content** is the protection that first comes to mind regarding Internet traffic: Keeping transmissions from being intercepted and read by unintended parties.
>
> **Context** is "who talks with whom, and when and where." This information, while not immediately as valuable as content, can be of almost equivalent value in many circumstances. If your competitor knows who you are communicating with, he can develop a very good idea of what your next move will be.
>
> **Trust** involves not only the intent of your security provider, but their ability. There certainly have been anonymization services operated by thieves, but there are more services that simply store their information poorly and expose all their customer records (financials, logs, etc.) to theft and misuse.

Peace of Mind - Second to Nothing

NETWORK STRUCTURE

Cryptohippie's technology suite is designed to protect clients from breaches of both content and context, as will be detailed below. But the corporate and network structures are designed so that clients do not have to depend upon Cryptohippie itself.

In other words, our network is built so that no third party gains any knowledge about the content or context of your communications – not even us. The various parts of our network are insulated from each other and operated by different companies in different jurisdictions. None of the operators can collect the required data to learn about your communication's context and content.

Furthermore, our technology provides jurisdictional routing of communication to make sure that traffic does not enter and leave our closed network through gateways in the same jurisdiction. This way, the effort for an attacker to trace your connection increases substantially.

In addition, our technology allows for the creation of closed groups to communicate with each other in a very secure, globally distributed network, without any interference from, or leakage to, any third parties, including ourselves. We are not aware of any competitor providing this level of communication protection.

CRYPTOROUTERS

Cryptohippie's primary customer product is the CryptoRouter, which can replace or stand alongside other routers, generally in office environments. These routers effectively extend the closed Cryptohippie network into the client's premises, and all computers connected to the router are directly protected.

Several levels of service are available (high bandwidth, high-volume, etc.), but all share essentially the same suite of protection technologies.

KEY TECHNOLOGIES

We support both OpenVPN and IPSec access to our network, operating as follows:

- Connections are relayed through one hop before crypto VPN termination
- Temporary authentication and per-session only authentication
- Party 1 issues Tokens
- Party 2 operates entry nodes
- Party 3 operates termination nodes

- Jurisdictional routing
- Standards-based military cryptography AES256 + RSA2048 + DH2048 + SHA1/SHA256 crypto
- Temporary internal IP space
- Random assignment of outgoing IP, fixed per destination and session
- Mixing of incoming packets at entry node
- Entry node selects termination node
- Exit node does not know internal IP
- Entry node does not know internal IP
- Termination node does not know original IP or new outgoing IP
- Authenticator knows no IPs
- Authenticator does not know login/logout times (only total traffic per session)
- Internal firewall (does not allow traffic back to crypto-router)
- Cryptohippie crypto-routers use firewalling and policy routing to do all-or-nothing protected routing of traffic
- All traffic between the Cryptohippie network and the crypto-router is encrypted
- Full integrity protection of network traffic between routers and nodes (prevents watermark attacks)
- Traffic between entry, termination and exit nodes is encrypted to elevate the difficulty of fingerprinting attacks
- Exit and termination node selection is automated to optimizing crowding
- Padded traffic

For further inquiries, contact info@cryptohippie.com