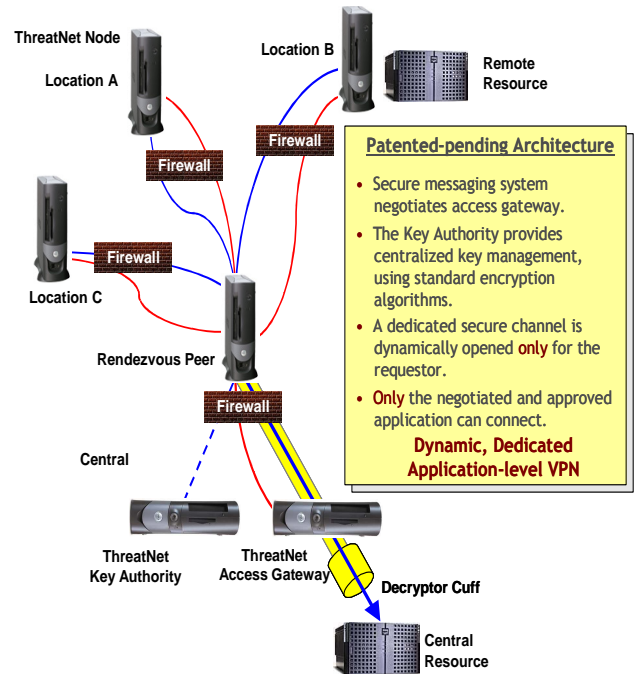


ThreatNet™

Introduction to the ThreatNet's Application-level VPN

ThreatNet is the only fully-encrypted, application-based VPN. Although transmissions are encrypted, users make no trade-offs in network performance. Convenience has finally met security, enabling collaboration, surveillance, crisis management, and information reconnaissance where traditional secure solutions stand in the way of progress. Now, large companies can ensure that telecommuters and remote users will have equally secure connections without the hassle and cost of expensive hardware. ThreatNet also insures security for shared networks. ThreatNet uses layered security, protecting resources behind firewalls and NAT gateways. ThreatNet uses security layers and pinpoint accuracy to keep data safe while still working through firewalls, as if they weren't even there. Small enough to fit on a PDA, the ThreatNet footprint can enable remote security for just about anything with an IP address. Using a unique combination of subscriptions and discrete addressing, ThreatNet can send a message to a single trusted recipient, or a broadcast to an entire organization.



Key Features and Technical Components of ThreatNet

- **Network Security**
 - Ensure the Privacy of each location relative to all others
 - Encrypt all transmissions
 - Minimize threat of spoofing and DoS attacks
 - Introduce no security holes
- **Resource Security**
 - Use strong authentication
 - Facilitate centralized management
 - Allow grant/deny access control on user-application combinations
 - Prevent user-side trojans and viruses from attacking the target resource
- **Usability**
 - Enable target resource access from any Internet connection
 - Security without significant performance degradation
 - Design for use on all platforms, from enterprise servers to cellular phones
- **Easy Integration**
 - Support interfacing from any network-aware language
 - Provide open API's to keep connecting applications well-informed of message-delivery anomalies and success

ThreatNet Uses

- **Mobile professionals:** Traveling workers and telecommuters can be assured that their dial-up and DSL connections are protected. No more private lines or 800-number access are needed. Travelers connecting from hotels and off-site locations avoid the headaches of troubleshooting and configuration changes needed to traverse multiple firewalls.
- **Wireless users:** For users of handheld computing devices, wireless LAN technology or VSATs, the airwaves no longer need to be viewed as an insecure medium for transmitting sensitive company information.
- **Satellite offices:** Employing ThreatGuard's ThreatNet for site-to-site connectivity can result in immediate cost savings from the removal of dedicated circuit equipment and leased lines.
- **Business partners:** Operating on a broad range of platforms in environments out of your control, extranet users can be enabled to securely access specific enterprise resources without configuration hassles or network changes.
- **Internal network/Intranet:** Users will feel at ease knowing their data is protected from prying eyes and network monitoring devices.