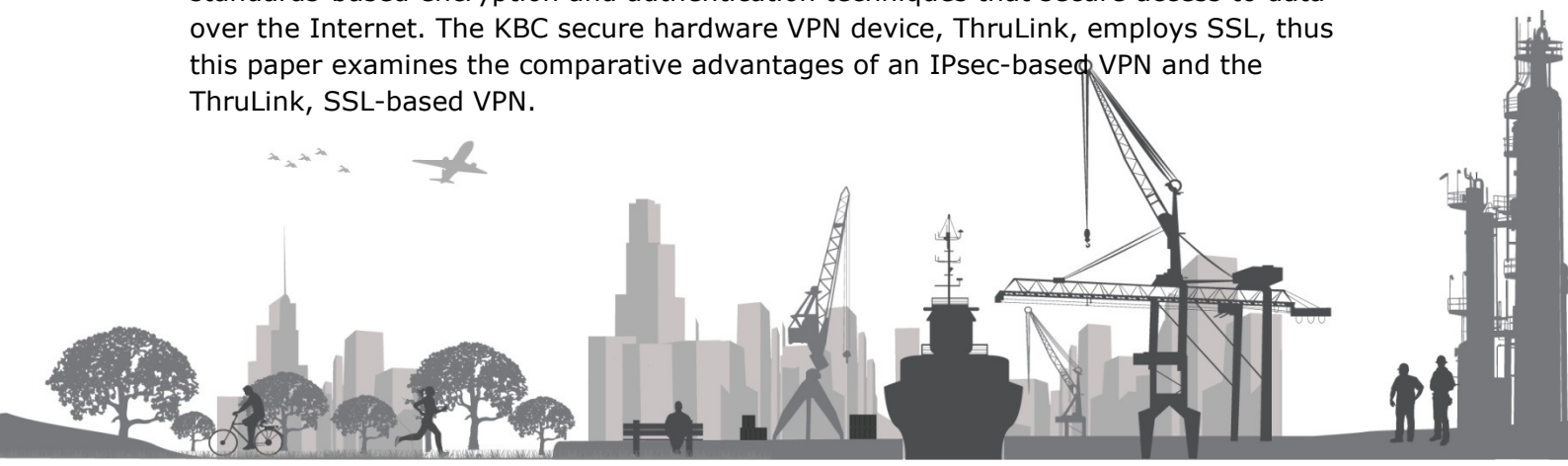
KBC
data delivered

Comparison of IPsec and ThruLink, SSL-based VPNs

ThruLink™

March 2015

Recent years have seen the growth of several types of Virtual Private Network (VPN) service. The common characteristic of these services is to virtualize the service entity using the same physical infrastructure as much as possible. Since ADSL, cable internet and wireless access technologies have become widely available and more cost-effective, IPsec and SSL (Secure Socket Layer) VPN-based technologies have evolved to become the solutions of choice for making use of the public internet. Each technology employs standards-based encryption and authentication techniques that secure access to data over the Internet. The KBC secure hardware VPN device, ThruLink, employs SSL, thus this paper examines the comparative advantages of an IPsec-based VPN and the ThruLink, SSL-based VPN.



1. VPN Access Over a Private or Public Network

1.1. Network Configuration

IPsec was initially developed for site-to-site connectivity (peer-to-peer).
With the growth of remote access requirements, IPsec was extended mostly based on proprietary solutions to support remote access client connections. This involves additional costs since the tunnel security policies have to be administered. ThruLink was developed to be a VPN mesh network (peer-to-peer, multi-to-multi).

1.2. Network Protocols

IPsec is a framework of protocols and arrangements rather than a single protocol. It operates at the lower layers. Similarly a ThruLink VPN is a framework of protocols but operates at the application layer (Level 2 Ethernet device, Level 3 IP device depending whether setup in router or switch mode) which provides full control over a much wider arrangement i.e. not all LAN attached devices need to be part or accessible by the VPN allowing non-IP packets to be transmitted between VPN segments.

1.3. Scalability & Maintenance

IPsec solutions have limitations as the number of VPN connections grow. For large-scale deployments, the administrative and maintenance costs become cumbersome (maintaining end-point-connected devices, security policies, network routes etc.). In a ThruLink, SSL-based VPN maintenance costs are low as the authentication and streaming protocols are self-managed and stateless - nodes can join, disconnect or rejoin on demand without affecting performance or efficiency of the VPN network.

1.4. Mobile Use

IPsec is not well adapted for mobile users, particularly if users move between different locations with varying amount of throughput/bandwidth. ThruLink was designed for mobile use and automatically manages different throughput/bandwidth levels between nodes.

1.5. NAT & Firewall

NAT and firewall traversal often require complex solutions. In some cases it might not be possible at all to establish IPsec connections if the firewall blocks IPsec traffic. The ThruLink SSL solution is immune to NAT and Firewalls, allowing it to work over most existing network topology/architecture, SOCKS5 (secure socket of proxy server) or Proxy server.

1.6. LAN & WAN Operation

IPsec was designed for LAN operation and not to operate within an infrastructure with different IP ranges and subnets. SSL-based systems, on the other hand, operate either within an existing network LAN or as the end point onto the WAN (Physical Ethernet or mobile modem onto public facing internet).

1.7. Throughput

IPsec is widely judged to be faster than SSL since it operates at the lower layers. SSL operates at the application layer thus it has more packet overheads - this impacts the transmission speed. However, even with these overheads, ThruLink still outperforms any WAN capability.

2. Encryption

Both IPsec and ThruLink support strong encryption technologies. The ThruLink, SSL-based solution provides three encryption models and the following comparisons are made:

2.1. Model 1

ThruLink supports AES (128,192,256bit), Camellia (128,192,256bit) cipher keys in CBC mode of operation (Cipher Block Chaining), Blowfish (variable length key length 64 to 448 bits) in OFB mode (Output Feedback – synchronous stream cipher).

Both IPsec and ThruLink implement packet HMAC-SHA1 OR HMAC-MD5 as digest (SHA1 is used if AES, MD5 is used if Blowfish by default). They also both perform Diffie-Hellman key exchange using the public keys of the intended recipients and they both make use of RSA Private and Public keys (1024 – 8192)

2.2. Model 2

Both IPsec and ThruLink are FIPS140-2 compliant (FIPS140-2 specify implementing specific security policies for each portion of the security protocol used.)

ThruLink implements Security Level 4. Security Level 4 provides the highest level of security. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate resetting of all critical security parameters. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defences. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and resetting of all critical security parameters, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module).

Ciphers used are AES (128,192,256), HMAC-SHA1 or HMAC-SHA256. Both SHA1 and SHA256 are suitable as random number generators.

2.3. Model 3

Model 3 is intended for ThruLink HC (High Capacity) devices only, due to the CPU processing requirements to encrypt and decrypt data streams efficiently under large scale deployments. It makes use of ECDSA (Elliptic Curves DSA) certificates, AES (128, 192, 256 bit) or Camellia (128, 192, 256 bit) encryption ciphers, HMAC-SHA256 or HMAC-384 Hashing algorithm.

3. Reliability & Stability

Both IPsec and the ThruLink, SSL- based VPN have been proven to be very reliable technologies. However ThruLink outperforms IPsec when considering stability.

ThruLink supports auto-recovery from a network. IPsec does not support auto-recovery as key and sequence number resync occur on a timed basis rather than through a monitored status change.

ThruLink implements a variable MTU (maximum transmission unit) scheme which manages the maximum packet size between two end points (devices). This maximises protection against packet fragmentation thus reducing packet loss, as fragments of data packets are traditionally dropped by network routers. ThruLink also periodically tests the connection speed.

ThruLink does not rely on a single gateway to remain within the VPN. Hosts are only required to authenticate upon joining the VPN network. Once connected, each device will find the best route to the required end point (node). ThruLink maintains an internal network routing table which is optimised for best performance and minimal node hops. This allows for ThruLink devices to physically be removed or replaced on the VPN network without causing disruption (management of unresponsive nodes) to the existing ThruLink devices on the VPN.

ThruLink is self-managing and will poll other ThruLinks on the VPN network in order to maintain an "active" routing table and notifies others if any device becomes unavailable (i.e. physical network is down) or available again. If a previously connected ThruLink device becomes available, it will resync its encryption keys and sequence number thus performing a full authentication onto the VPN. Erratic network outages don't require an authentication process but instead require resyncing of certificate keys and sequence number.

4. Ease of Use

ThruLink is a low administration/maintenance device designed to work over a broad range of network infrastructures while implementing the strongest possible protection and security within the VPN. It supports administrators by implementing a simple-to-use web GUI (HTTP or HTTPS) for configuration, firmware updates, device and network monitoring interfaces. Configurations can be securely backed up (encrypted using a shared key) and restored. Certificates can manually be implemented or automatically (depending on security policies in place) using the interface.