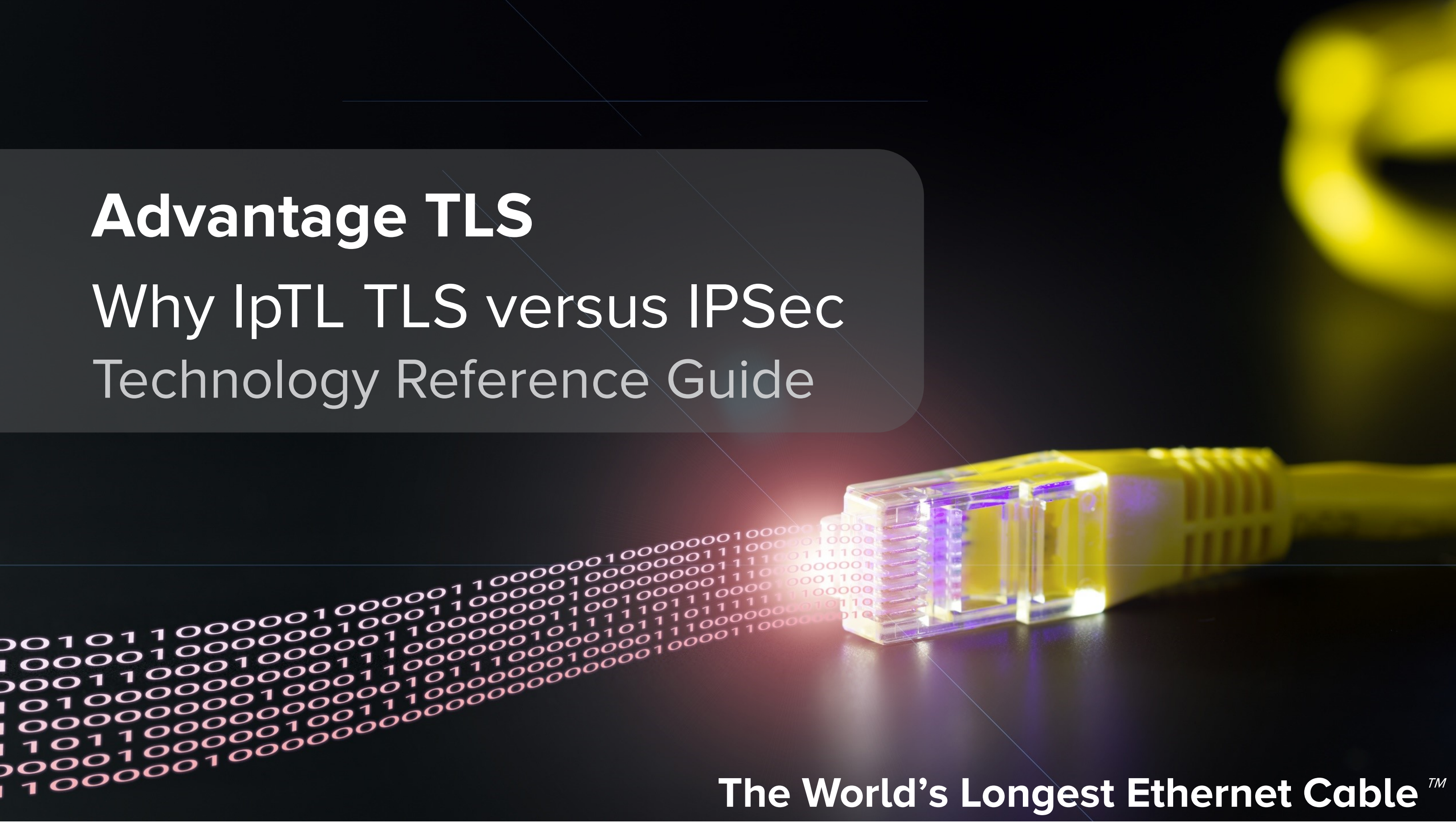
IP Technology Labs

Networking Simplified™

IpTL's Expert Edition



Advantage TLS

Why IpTL TLS versus IPSec

Technology Reference Guide

The World's Longest Ethernet Cable ™

TAKE CONTROL AND GET THE NETWORK YOU WANT WITH THE NETWORK YOU HAVE

Leading the market with TLS based network solutions, only IpTL eliminates the issues with IPSec networking.

Peer reviewed by Moazzam Ali, CCIE R&S 27960

//Connect //Secure //Extend //Access

www.IpTechnologyLabs.com

Networking Simplified™

The World’s Longest Ethernet Cable™

As the World’s Longest Ethernet Cable™ IpTL *Fast*Lane™ appliances easily, securely, and transparently tunnel any Ethernet device or LAN over any IP Network without the blockages or challenges of a traditional VPN.

IpTL’s functionality enables all remote locations and network devices to seamlessly “appear” as if they are on the same Local Area Network. By providing LAN based access, the *Fast*Lane™ solution overcomes wide-area-network integration challenges while enabling the lowest-cost and highest-performance network access services.

Additionally, Ethernet bridging provides seamless network compatibility. IpTL inherently provides support for non-IP or non-standard networking devices, applications, and users over networks which break IPSec and dynamic keyed VPNs. In other words, if it is in an Ethernet frame we can move it end-to-end securely. Details of the IpTL security model can be found in the document Security of the Solution.

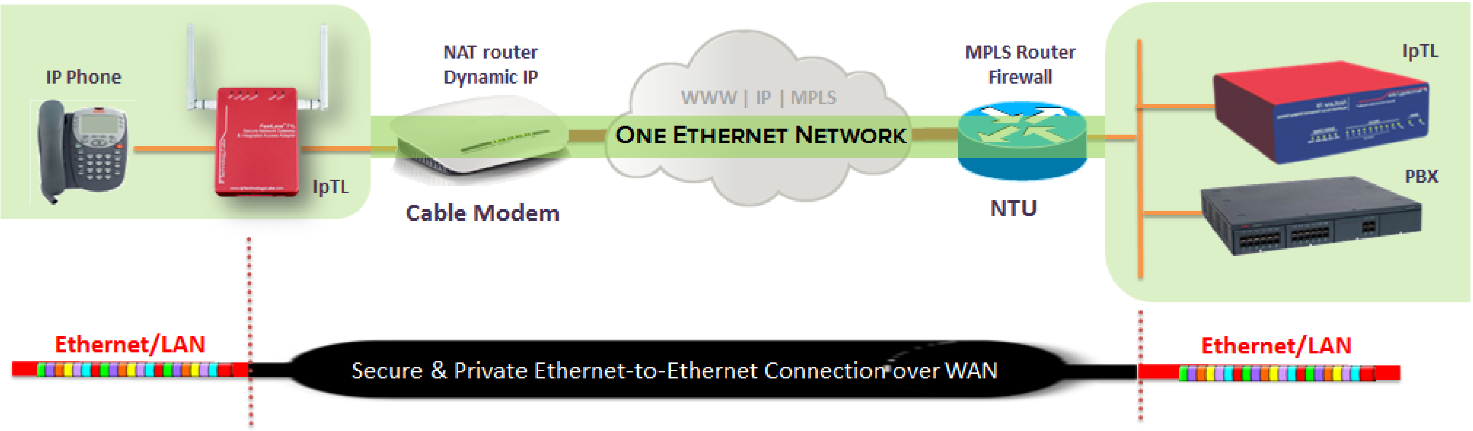
IpTL can be used in the following network environments:

- Dynamic IP network connections—On both ends
- No requirement for Static Public IP service
- Installed on Private IP networks and behind a firewall
- Installed without a port forward on either end

Deployed as a symmetric solution — or an IpTL appliance on each end — offers a security advantage as you can control your network. All data goes between your IpTL appliances and never through a cloud server or service.

Unlike a typical VPN or remote access solution, the IPTL Solution can be deployed supporting emerging and legacy application without difficulties, such as:

- SIP PBXs & VoIP hardphones
- Unified Communications Systems & Video-over-IP
- Network Printers connecting to Cloud applications
- VLAN, VLAN trunking, Multicast, Q-in-Q, MAC-in-MAC
- File Sharing, NAS, & Sharepoint
- Mobile, Workgroup, and VDI Users
- Non IP protocols such as Industrial SCADA such MODBUS
- MPLS/VPLS Leased-Line replacement
- Network redundancy for existing Leased-Lines
- Link bonding and Load Balancing



Here you have a remote site with an IP phone connected over a commodity Internet connection. When the secure tunnel is up, the IP phone is able to register to the IP PBX as if it were on the LAN at the headquarters. If the VoIP system uses VLANs for Voice, Video, Data, the IpTL appliance will extend those same VLAN’s end-to-end.

Networking Simplified™

Security Matters: TLS vs IPSec Encryption

IPSec is a suite of protocols for securing IP packets by encrypting their data payload, verifying their integrity, and discarding replayed packets. To negotiate security services and keys, IPSec relies on a separate protocol called the Internet Key Exchange (IKE). Manual Keys (preshared keys) are used when IKE is not or cannot be configured.

IPSec and IKE excel at securing all IP packets exchanged between peer gateways in a site-to-site VPN. However, IPSec had to be stretched to meet common remote access needs. Extended authentication (XAUTH) was added to relay user logins and passwords. Vendors invented ways to assign private IP addresses to remote hosts. To use these proprietary tweaks, employers had to install vendor-supplied VPN clients.

Almost all firewall appliances employ a NAT as a means for multiple devices to share a single Internet connection. By using extensions to the IPSec protocols, it is possible for IPSec peers to exchange packets even when a NAT device exists between them provided that the NAT traversal extensions are recognized by the NAT device.

When using a Security Protocol to protect IPSec traffic, packets can often grow to be larger than the Maximum Transmission Unit (MTU.) This is due to the growing overhead associated by performing packet encapsulation. Some poorly designed routers may simply refuse to fragment or forward certain traffic and simply drop the traffic altogether. Additionally, there are several blocks to a universal deployment of IPSec. In some instances, key exchange packets can be too large which will also lead to loss. To circumvent these issues, several extensions to the IPSec have been devised but are not universally supported.

IPSec became the de facto standard as it was the only serious option during its time. But now, TLS is providing the promise of security with network simplicity. IpTL, with TLS, uses a single connection for authentication, authorization, and data. With X.509v3 certificates, automatic dynamic keys, and Perfect Forward Secrecy IpTL is has the highest network compatibility with even the most outdated NAT router.

> **“Complexity of IPsec In our opinion, IPsec is too complex to be secure. The Design obviously tries to support many different situations with different options. We feel very strongly that the resulting system is well beyond the level of complexity that can be analyzed or properly implemented with current methodologies. Thus, no IPsec system will achieve the goal of providing a high level of security.”**
>
> **“We therefore repeat: security's worst enemy is complexity. Security systemsshould be cut to the bone and made as simple as possible. There is no substitute for simplicity.”**
>
> **-- “A Cryptographic Evaluation of IPsec” by Niels Ferguson
and Bruce Schneier**

IpTL eliminates these complexities with turn-key and out-of-the-box optimization. Leading the market with TLS based network solutions all of the issues with IPSec are eliminated.

Networking Simplified™

The IpTL TLS Advantage Matrix

Element	TLS	IPSec	Comment
TLSv1.2 security envelope for identity.	✓	✗	IpTL implements TLSv1.2 with x509v3 certificates standard and provides inherent identity and access control within the protocol. IPSec has no built-in identity and relies on other protocols (xauth) and manual configuration to enable connectivity.
Dynamic Keying, Perfect Forward Secrecy, X509v3 Certificate Identity	✓	✗	Only IpTL is highly set out-of-the-box for top-level security and only IpTL maintains this across all models and across all topology deployments without any configuration.
Dynamic Keying standard & Automatic. No Preshared Key!	✓	✗	With IpTL there is preshared key (PSK) to weaken security. Session keys for transmit and receive data and transmit and receive HMACs are automatically calculated. Additionally, new session keys can be configured by the user to automatically update based on time and/or amount of data over the tunnel. The current factory standard for IPTL is re-key every five-minuets. Most IPSec implementations use PRESHARED keys to simplify installation. In fact, once implemented these are not changed frequently, much less several times during a session, and represent a significate security error. Implementing IPSec dynamic keying requires additional configuration and NAT traversal issues.
NAT Support	✓	✗	TLS works great through NAT's and Nested NATs without relying on a router supporting NAT-T. To get IPSec to work requires port forwards or public-facing routers. Dynamic keying (IKE) requires additional support.
Dead Peer Support (disconnected tunnel)	✓	✗	TLS has integrated link-heartbeat to indicated that the you the link is down. The is key as automatic redundancy can't happen the IPSec system thinks the link is still up.

Element	TLS	IPSec	Comment
Use any Port on any Network	✓	✗	TLS isn't an IP protocol and therefore can be used with generic routers & generic networks and implemented without disruption of existing networking services. With IpTL, a single UDP or TCP port can be used for protocol establishment, dynamic keying, & data payload. IPSec calls out specific ports such as Phase 1: UDP/500 and Phase 2: UDP/4500; port 50 for IPSec ESP; on a Cisco ASA you also need to add in a crypto isakmp nat-traversal to try and make the above work assuming it is supported by the modem/
Low tunnel/security overhead	✓	✗	TLS runs about 4%-6% vs IPSec from 12%-15%+. For tunneling need to add GRE and then IPSec.
Unlimited Networks, Hosts, VLANs	✓	✗	Because of our use of TLS, IpTL appliances can move Ethernet based networking topologies such as VLANs and VLAN trunking protocols.
Supports 802.1x and MacSec End-to-End	✓	✗	IpTL can move Ethernet frames natively over the TLS tunnel.
DF fragment support - Auto	✓	✗	IpTL and TLS permits the application to get through end-to-end even if the packet is too large for the net.
TCP MSS for large MTU - Auto	✓	✗	IpTL permits the application to get through end-to-end even if it the application thinks the link MTU is larger than it really is. This is a common IPSec issue where the overheads take up payload dataspace and path discovery doesn't work correctly. This is where you see hangs, instability/drops, and partial data throughput. If any ICMP paths are filtered (e.g. firewall) and/or GRE Tunnel IP MTU is not set for the correct physical interface then blocks/drops will occur.
Seamless NAT/PAT traversal	✓	✗	TLS only requires the most basic NAT service and thus even the most low-end modems/NTU to be seamlessly supported. IPSec requires NAT-T support, and even then, variations of implementations are implemented.

Element	TLS	IPSec	Comment
Agnostic to any device, network protocol, or application	✓	✗	IPSec is only a L3 (IP) protocol. It can only move IP packets. IPTL is transparent end-to-end to the data while able to incorporate all Ethernet devices at the same time. Only IpTL allows broadcast, multicast, and IPv4/IPv6 to co-exist on the same tunnel at the same time. Vendors attempting to replicate transparence with IPSec have to add additional protocols such as GRE and taking more data throughput from the link.
Works with Dynamic IP – on both ends of the link. No public IP or static IP required.	✓	✗	TLS doesn't use or require the IP address as part of the security association. IPSec uses the IP address in order to enable a link. If this IP address changes then the link drops/hangs and is instable until it times out. Only IpTL can support dynamic IP on both ends of the link and does not require a static IP on the headquarters unit. Only IPTL allows you to use any IP network anywhere – including Hotels, Airports, or Home commodity Internet connections.
No change to network or applications for redundancy	✓	✗	IPSec, as a routed IP network, requires topology change and propagation throughout the network applications. Running TLS allows IpTL to use Ethernet as the payload and thus propagations are at the ARP and switch levels. Immediate propagation of network changes.
Touchless Deployment capability	✓	✗	IpTL's patent pending AutoConnect™ technology permits easy point-to-point deployment as well as expansion without punching holes in firewalls. Users value IpTL's ability to NOT require remote customer network modification in order to provide connectivity.
All functions included without recurring subscriptions	✓	✗	Most IPSec implementations require licenses for almost every function or deployment. The licenses also expire, usually on a yearly basis, leading to ongoing costs. With TLS and IpTL there are no recurring fees for using a deployed system.

Networking Simplified™

IP Technology Labs

Network Communications Simplified™

IP Technology Labs, LLC.
3470 Olney-Laytonsville Rd Ste: 313
Olney MD 20832 USA

W: http://IpTechnologyLabs.com
T: +1 301 570 6611
F: +1 301 570 8049
E: marketing@IpTechnologyLabs.com

IPTL is the worldwide provider of network appliances which solve challenges imposed by infrastructure limitations.

Our network-leading IP/Ethernet solutions simplify, lower the cost, and enable the connection of network devices, services, and applications over any LAN or WAN infrastructure.

Our goal is to transform the way the network is used, regardless of technology, enabling open, reliable, and frustration-free communications.