How the *Fast*lane™ Series Bridging Gateways Provides Data Security, Integrity, and Assurance

End-to-End Privacy and Security

Using the Internet for site-to-site networking can provide high-quality low-cost connectivity. But using the Internet as a private WAN brings new security requirements and simply encrypting data with a shared secret password is no longer effective. Modern solutions must also ensure communications authorization and that any data is unchanged, and verified/authenticated.

The IpTL Model 70 Series Bridging Gateways not only ensure data security with encryption but also offers data authorization, integrity, and data assurance for all communications. Using TLS/X.509 Certificates, dynamic key generation, and strong encryption, IpTL Model FastLane Series products fully operate within the four cryptographic delivery points of secure communications:

- **Confidentiality** – Assurance that information is accessible only to those authorized to have access.
- **Integrity** – Assurance that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
- **Authentication** – The process of verifying that the source of the data is as known and that the data has not been modified.
- **Non-repudiation** – Assurance that the sender sent and the receiver received the data so neither can deny having processed the information.

How IpTL Devices Provide Overall Data Security

All IpTL Model 70 Series utilize the IpTL BroadLane™ Service Delivery Suite operating firmware. With BroadLane™ all IpTL devices ensure secure communications between end-points and employ multiple tiers of technology coupled with industry best-practices.

SKU: 0100-99-001 REV 6

The IpTL Model 70 Series makes Extensive use of the following Security Technologies:

Supported Security Element	What does the Security Element Do	What is the Benefit of the Security Element
TLSv1.2	The suite of protocols which provide a robust security solution for network communications. This is the same protocol used in HTTPS secure web browsing. (e.g. online banking)	Provides privacy and data integrity between two end-points. Provides a control channel and data channel; negotiates connections for X.509 Certificates, key methods, hash methods; and provides for data encryption methods.
X.509v3 Certificates	ITU-T standard for public key infrastructure (PKI). Provides the standard methods for certificates and for the handling and use of Public & Private Keys.	Ensures that only IpTL devices can establish communications with each other. Also used in generating keys for encryption and digital signatures.
Diffie-Hellman Key Exchange	Provides end-point negotiated keys. Keys are dynamic and are automatically created during the connection. New keys (re-keying) are generated automatically every five minutes.	Allows two end-points, without prior configuration, to mutually agree on keys used for encryption. IpTL does not use static/pre-shared keys allowing for higher system security. Enables Perfect Forward Secrecy.
SHA-2 (SHA384) HMAC	Per packet Digital Signatures with 384 bit one-way hashes. The latest standard to overcome attacks of the older SHA-1 HMAC	Ensures that each packet received is from the correct end-point and that the data was not changed. (e.g authenticity and Integrity)
Handshake Passphrase	Provides initial authentication at the server limiting the starting handshake sequence to only those end-points with the correct passphrase.	User configurable passphrase controls which devices can connect together. Used to prevent connections by an unauthorized third party. Also prevents Denial-of-Service, port-scanning attacks, and Man-in-the-Middle attacks.
Embedded Packet Sequence numbers	Each packet sent has an encrypted 64-bit number uniquely identifying the packet. This sequence number and the payload data are encrypted.	Prevents packet replay attacks and ensures reliable data delivery.

Supported Security Element	What does the Security Element Do	What is the Benefit of the Security Element
AES 256 GCM Encryption	Payload data encryption using symmetrical keys 256 bit strength using the Galois/Counter Mode with a minimum of latency and operation overhead.	Encrypts data between end-points using a negotiated key. This encryption is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. Overcomes CBC limitations improving efficiency and performance.
Per Client Name/Passphrase	Individual end-point authorization after proper SSL/ authorization. Sent encrypted within the tunnel.	Provides user-configured control over individual end-point's access after certs, keys, and authorization have been negotiated. Offers administrative control over deployed units within a network. Provides Man-in-the-Middle attack protection.
Access Control Lists (ACL)	User configurable blocks or permits on traffic. Individual endpoint control of Ethernet or IP packet or Host connectivity.	Used to control which hosts, devices, or applications can access network resources.
Dynamic Tunnel Cloaking	User configurable hash options to eliminate fingerprinting of the TLS tunnel (and it's encrypted contents.)	Used to prevent traffic analysis and identification traffic types.

How the Model 70 Series uses SSL/, X.509 Public Key, and Perfect Forward Secrecy

IpTL BroadLane™ and the Model 70 Series endpoints use the Transport Layer Security (TLS) standards as the main framework for security communications within the Model 70 Series devices. The TLS protocols provide communication privacy and data integrity as well as negotiating certificates, keys, and which encryption methods to use.

SKU: 0100-99-001 REV 6

What about SSL? Isn't TLS just SSL?

Originally created by Netscape for secure web browsing (e.g. HTTPS) SSLv3 is the foundation for v1 as defined in RFC 2246 and updated in RFC5246. The differences between SSL and are generally small mainly offering extensions for adapting to other communications methods as well as enhanced security fixes.
TLS provides the main transport medium and provides for privacy and data integrity between endpoints. The TLS protocol is composed of control channel and a payload channel. The control channel is used to setup and maintain the link and includes the handshake procedures. Ethernet packets from each LAN will then use the established tunnel to securely traverse the Internet. TLS uses either UDP (default in IpTL products) or TCP for communications over the Internet.

SSL is used primarily at the application layer (e.g. Browser, Email, etc) whereas the TLS, as used in the IpTL appliances, encapsulates the lowest level of communications. This allows unique connectivity options and unsurpassed security. To be clear, there is no SSL in IpTL appliances.

X.509v3 Certificates

IpTL makes extensive use of X.509v3 Certificates and public-key cryptography (PKI) techniques which currently offers the highest-level of overall security. Using X.509 each IpTL Model 70 endpoint employs both a public key/certificate and a private key.

X.509 Certificates are passed between endpoints during the initialization process. While the certificate identifies and validates one endpoint to another, it also includes the public key used in encryption key and signature generation.

Using this system ensure that the private and secret password never has to be sent or communicated to any entity.

Perfect Forward Secrecy/Key Exchange

Using the Diffie-Hellman Key Exchange protocol, Perfect Forward Secrecy is achieved. Perfect Forward Secrecy is a unique security property in that ensures that if a session key is discovered for one series of transactions, it does not compromise any future transactions. As the IpTL Model 70 devices do not use pre-shared keys, the endpoints will automatically generate new and unique keys at the start of each session as well as new keys every five (5) minutes.

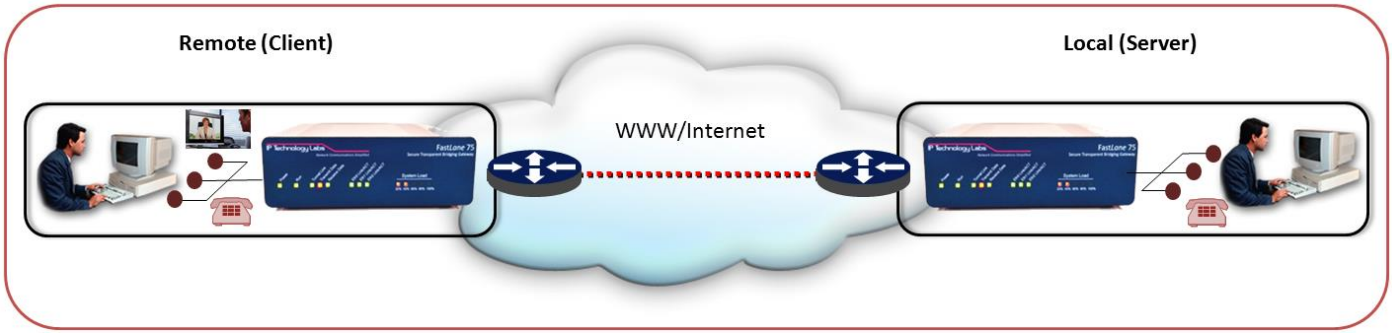
Tunnel Transmissions End-to-End

After all keys and digital signatures are negotiated (four in total) Ethernet packets destined to an opposite endpoint are prepared for forwarding via the tunnel. The system adds a 64-bit sequence number to the packet. Then this packet is encrypted using the agreed encryption methods and keys.

The tunnel provides a wrapper (or envelope) for the encrypted packet and adds additional key information for enhance security. All of this data is then digital signed using the SHA-1 HMAC transform. The digital signature not only assures that it came from our peer (opposite endpoint) but that the data was not modified in transit. Now this signed and encrypted packet is sent to the opposite endpoint for verification, decryption, and forwarding to the local Ethernet LAN.

How IpTL Model 70 Series Devices Connect

Model 70 Series devices seek to securely and transparently connect one or more Ethernet LANs over an IP network. To do this, the Model 70 Series devices operate in a client/server mode of operation. The Client endpoint device initiates the starting communications to the Server endpoint by sending a `<hello>` request to the IP address of the Server. After the `<hello>` sequence, the end-points negotiate encryption options, and mutually agree on the initial set of keys to use.



Typical Connection of Two Model 75's

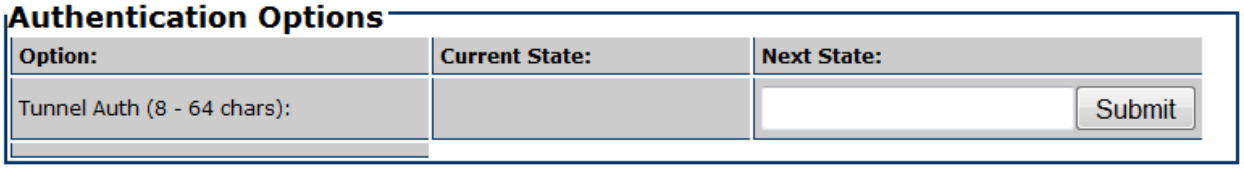
During this handshake each endpoint provides random data to create keys used for the encryption/decryption processes as well as the digital signature (HMAC) keys. The Model 70 Series devices never use any key twice for its two way communication ensuring that each endpoint has a unique sending digital signature, unique receiving digital signature, and unique encryption/decryption keys.

Server Protection from Unauthorized Clients & Initial Security

The Model 70 Series offers user configurable Authentication Passphrase functionality. This secret passphrase – called Tunnel Auth – is a user configured option in each Model 70 Series endpoint. It is used to authorize and authenticate remote endpoints at the very first stage of the connection process.

This feature can be used as global option within an organization to ensure only those authorized endpoints can connect to the corporate network. It will also prevent any other unauthorized IpTL device from connecting to this network unless the Tunnel Auth ID is configured.

To use this facility of security, the server and client endpoints will all be configured to all have the same Tunnel Auth ID. When a Model 70 client device begins to establish a tunnel it first sends a `<hello>` message to the server. Using the Tunnel Auth passphrase, all communications – including the initial `<hello>` will be digitally signed (SHA-1 HMAC.) The server will see this signed `<hello>` message and check the digital signature with its own configured passphrase. If the passphrase is incorrect the server will drop the connection without any response to the client and no further communication with continue.



The following shows the user configuration options within the IPTL software under tunnel options.

Tunnel Auth provides the following security benefits, including preventing the following:

- Denial-of-Service (DoS) attacks
- Port flooding on the server UDP or TCP port (SYN attack)
- Port scanning to determine which server ports are open or in a listening state.
- Buffer overflow attacks.
- Handshake initiations from unauthorized machines (Man-in-the-Middle)

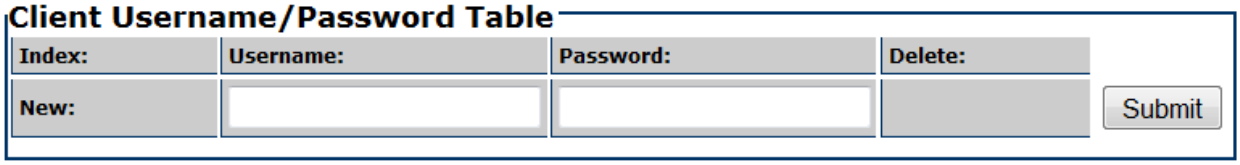
The Model 70 series Tunnel Auth provides a high level of protection against brute-force attacks on a server device. In fact, a remote attacker will not even see an active server at all. All peer-to-peer negotiations silently fail without revealing the existence of a live server tunnel port.

Individual Device Authentication

Following initial handshake authentication options the Model 70 Series can offer an access username/password pair option to authorize remote devices to a server. This option allows the individual authentication of remote devices to the server prior to decrypting and packet forwarding.

It allows a method to control access to the server from a remote device and is used when there are multiple networks/domains within a corporate environment. For example, the accounting network might wish to limit connections to only those devices that it administratively controls and prevent any access from other departments such as sales remote teleworkers.

The following shows the user configuration options within the IPTL software under tunnel options.



This user configurable feature allows each location to have its own authentication mechanism. It is important to note that the server initiates the authentication of this link server, any username/password pairs installed on the client are ignored.

Ethernet Data Packet/Payload Encryption

Data encryption is achieved using one of the built-in encryption algorithms such as AES or Blowfish. Currently, the factory default in the Model 70 Series is the Advanced Encryption Standard AES-256 using a key-length of 256 bits. This algorithm is used to encrypt the data between each Model 70 series endpoints. Because of the unique features of a public key infrastructure, there is no need to provide an agreed upon shared secret and eliminating the security risks when using such a method.

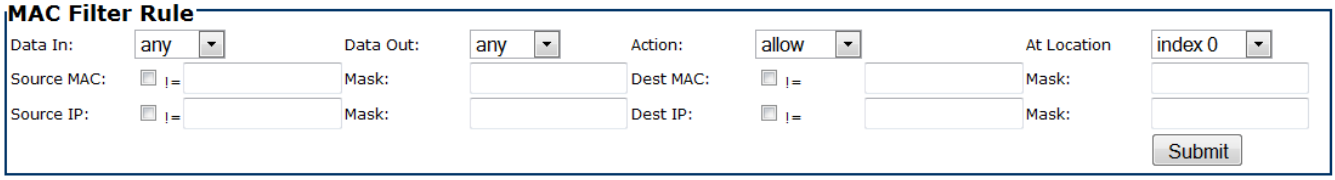
Using the X.509 Certificates and the Diffie-Hellman Key Exchange, the negotiation of a shared secret used in encryption is secure and unavailable to eavesdroppers. Even for the authenticated connection the secret cannot be obtained. This provides further protection for any Man-in-the-Middle attacks. Additionally, this key negotiation is reliable end-to-end as attacker cannot modify any part the negotiations without the communications failing.

Integrated data integrity ensures that the packet that was sent is the one received and not modified in any way during transit. The Model 70 Series uses the SHA-1 HMAC digest on each packet to create a digital summary of the that packet. On the receiving end, the packet is verified prior to being delivered to the LAN network.

Access Control Lists/Firewall Rules for Network Traffic

The Model 70 Series offers a robust traffic filtering suite to manage traffic at the host, network, and application levels. The Access Control filtering rules include a wide range of Layer 2 and Layer 3 filter rules including Ethernet MAC, Ethernet VLAN, and L3 Stateful Packet Inspection. These Access Control Lists (ACLs) can be used to either permit or deny user defined traffic types.

The packet filtering is designed to allow the user to accept, drop, and log packets flowing through the device. The system is designed to protect as well as monitor the packets which are traveling through the device and in/out of the tunnel. The filtering features contain a mix of "single button filtering" functions to allow easy setup of common functions as well as more detailed individual rule sets for the more advanced system administrator.



The following shows the user configuration options within the IPTL software under Filtering options.

An example of host network filtering is configured each endpoint with the Ethernet MAC addresses of computers/hosts which are allowed access to each site. By using the integrated MAC filters, only those computers with the correct hardware MAC address will be able to see the resources of the remote networks. Additionally, all computer devices without the correct MAC address will not be able to traverse out of their own Local Area Network

Unlike IP filters which can be easily changed or spoofed, these MAC address filters can prevent broadcast traffic to flood network connections unless initiated by an approved source computer.

IP Technology Labs
Network Communications Simplified™

3470 Olney-Laytonsville Rd Ste: 313
Olney MD 20832 USA
http://IpTechnologyLabs.com
T: +1 301 570 6611
F: +1 301 570 8049
E: marketing@IpTechnologyLabs.com

IPTL enables access to network resources anywhere, transparently, and with extremely easy-to-use products. Our goal is to transform the way the network is used, regardless of technology, enabling open, reliable, and frustration-free communications.

As the leader for simplified network appliances, IPTL develops and markets network-leading IP/Ethernet solutions for telecommunications and information technology users. Our appliances simplify, lower the cost, and enable the connection of network devices and services over any LAN or WAN infrastructure