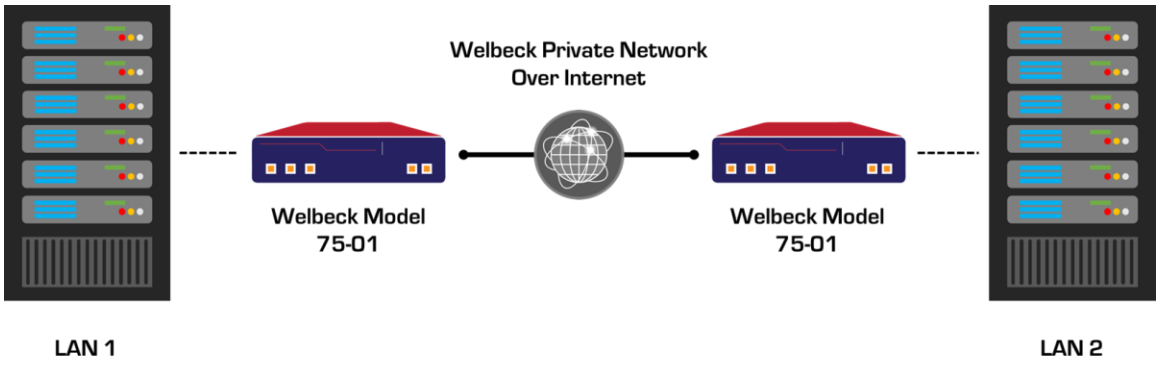
WELBECK/IpTL SECURITY

Welbeck/IpTL provides a suite of 12 security elements plus network monitoring and management tools to ensure the security of the data **and** the network.

Encrypting data is essential, but it is not enough. Effective security solutions must also ensure that users, devices and communications are authorized, and that data is unchanged in transit and verified/authenticated. The Welbeck/IpTL solution suite provides state of the art end-to-end authentication, privacy and security. Welbeck appliances and software provide 12 layers of security as standard, including X.509 Certificates, dynamic key generation, and perfect forward secrecy, as well as strong AES 256 encryption using the TLS v1.2 protocol.

Welbeck:

- **"keeps the good stuff in"** – prevents attacks and hackers that seek to steal private data in transmission (such as "man-in-the-middle" attacks); we ensure that the data enters the tunnel at a trusted endpoint and stays in the tunnel until it reaches its authorized destination;
- **"keeps the bad stuff out"** – prevents malware and other malicious content from entering the data flow; we stop malware from entering the network and corrupting it, or sitting on the network and stealing data through a "back door"; and
- **"keeps the bad guys out"** – prevents unauthorized users or devices from accessing network devices or data; we stop unauthorized devices and un-credentialed users from accessing the network.



12 INTEGRATED SECURITY ELEMENTS

Welbeck appliances include 12 integrated security features as standard out-of-the-box.

Integrated Standard Security Profile	
1	TLSv1.2 Transport (options with L2TPv3 and PPTP Tunneling)
2	AES 256/SHA 1 Confidentiality & Digital Signatures
3	Diffie-Hellman Key Exchange
4	X.509v3 Certificates
5	User-defined TLS HMAC Passphrase
6	Dynamic Keying - no pre-shared keys
7	User-defined auto rekey parameters - Time||Packets||Bytes
8	Perfect Forward Secrecy
9	Wireless MAC Allow/Block list with WPA2/AES256
10	L2/L3/L4 ACL's and integrated stateful firewall
11	Per device username/password
12	Positive device control and revocation even if link is not established

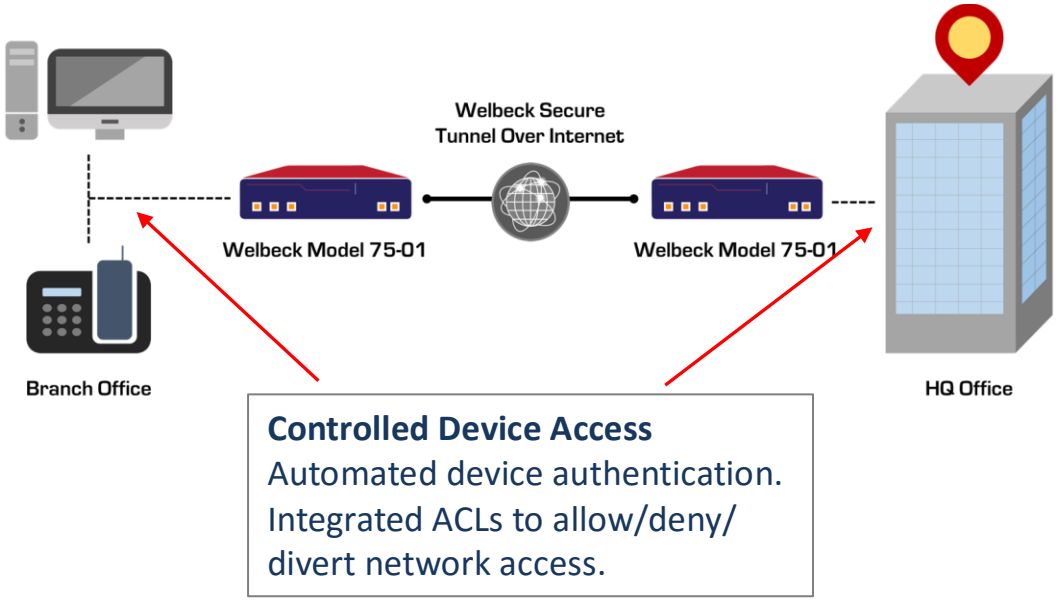
TRUST AND CONTROL™

Welbeck also provides a suite of network monitoring and management tools that provide visibility and full positive control of all endpoints. From the administrative screen, the administrator can see all Welbeck appliances that are connecting to the network, and all network access devices that are connecting though the Welbeck appliance. The administrator controls the Welbeck appliance, including limiting or denying access to the network, and can allow or deny devices seeking to access the network – all from the central administrative screen. All data flows end-to-end between your endpoints and not through a third party server. So unlike a cloud solution, the data is always under the control of your enterprise.

HOW WELBECK DEVICES CONNECT

Our devices securely and transparently connect one or more Ethernet LANs over any IP network. To do this, the devices operate in a client/server mode of operation. The Client endpoint device initiates the communications to the Server endpoint by sending a request to the IP address (or the MAC address and our proprietary technology will resolve the MAC address to the IP address) of the Server. After the sequence, the endpoints negotiate encryption options, and mutually agree on the initial set of keys to use.

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 devices never use any key twice for two way communication, ensuring that each endpoint has a unique sending digital signature, unique receiving digital signature, and unique encryption/decryption keys.



SECURE TUNNEL TRANSMISSIONS END-TO-END

Our security suite of 12 security elements is designed to establish a secure, private tunnel over the internet. After all keys and digital signatures are negotiated, Ethernet packets destined for an opposite endpoint are prepared for forwarding via the Welbeck tunnel. The system adds a 64-bit sequence number to the packet. This packet is then encrypted using the agreed encryption methods (AES 256) and keys. The tunnel provides a wrapper (or envelope) for the encrypted packet and adds additional key information for enhanced 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 its peer (opposite endpoint) but also that the data was not modified in transit. The signed and encrypted packet is then sent down the tunnel to the opposite endpoint for certification, decryption, and forwarding to the local Ethernet LAN.

NETWORK/SERVER PROTECTION

Our solutions protect the network and enterprise servers from unauthorized clients. The Welbeck device provides user-configurable Authentication Passphrase functionality. A secret passphrase – called Tunnel Auth – is used to authorize and authenticate remote endpoints at the very first stage of the connection process. This feature can also be used as a global option within an organization to ensure that only authorized endpoints can connect to the corporate network.

If the passphrase is incorrect, the server will drop the connection without any response to the client and no further communication will take place.

To use this security feature, the server and client endpoints will be configured to have the same Tunnel Auth ID. When a Welbeck client device begins to establish a tunnel it first sends a message to the server. Using the Tunnel Auth passphrase, all communications – including the initial – will be digitally signed (SHA-1 HMAC.) The server will see this signed message and check the digital signature with its own configured passphrase. This will prevent any unauthorized device from connecting to the network.

Tunnel Auth prevents:

- 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)
- Brute-force attacks on a server device (a remote attacker will not even see an active SSL server; all peer-to-peer negotiations will silently fail without revealing the existence of a live server tunnel port).

INDIVIDUAL DEVICE AUTHENTICATION

Following initial handshake authentication, the Welbeck device 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***. This user-configurable feature allows each location to have its own authentication mechanism. It is important to note that the server initiates the authentication; any username/password pairs installed on the client are ignored.

NETWORK SEGMENTATION

Device authentication allows a method of controlling access to the enterprise server from a remote device. It can also be used for network segmentation when there are multiple networks/domains within a corporate environment. For example, the accounting network can limit connections so that only those devices that it administratively controls can access it, and can prevent any access from other departments such as sales.

SECURITY ELEMENTS: TECHNICAL OVERVIEW

TRANSPORT LAYER SECURITY (TLS)

We use Transport Layer Security (TLS) standards as the main framework for security communications within our devices. The TLS protocols provide communication privacy and data integrity as well as negotiating certificates, keys, and which encryption methods to use.

TLS v1.2 provides the main transport medium for all Welbeck devices and provides for privacy and data integrity between endpoints. TLS v1.2 brings privacy and data integrity between two endpoints as well as providing a separate control channel. This control channel negotiates connections for several of the critical security elements including X.509 Certificates, keying and rekeying methods, hash/digital signature methods, and data encryption methods.

Between two endpoints, Ethernet packets from each LAN will use the established TLS encapsulated tunnel to securely move data end-to-end. TLS uses either UDP (default in Welbeck products) or TCP for communications.

X.509 PKI CERTIFICATES

This is the ITU-T standard for public key infrastructure (PKI). It provides the standard methods for certificates and for the handling and use of Public & Private Keys. This element ensures that only paired Welbeck devices can establish communications with each other. The certificates are also used in generating keys for encryption and digital signatures. Using X.509, each Welbeck-enabled endpoint employs both a public key/certificate and a private key. X.509 Certificates are passed between endpoints during the initialization process. The certificate identifies and validates one endpoint to another, and it also includes the public key used in encryption key and signature generation. Using this system ensures that the private and secret password never has to be sent or communicated to any entity.

AES 256 WITH CBC & EXPLICIT IV ENCRYPTION

This security element provides payload data encryption using symmetrical keys at 128 to 256 bit strength. This encrypts data between endpoints using a negotiated key. Cipher-Block-Chaining (CBC) prevents generation of identical encrypted data from payloads which have identical data.

DIFFIE-HELLMAN KEY EXCHANGE

This element provides endpoint negotiated keys. The keys are dynamic and are automatically created during the connection. New keys (re-keying) are generated automatically. The default setting is every five minutes, but users can select shorter or longer time intervals, or chose to have the re-keying occur on the basis of volume of data flow instead of or in addition to time

intervals. The Diffie-Hellman Key Exchange allows two endpoints, without prior configuration, to mutually agree on the keys used for encryption. Welbeck does not use static/pre-shared keys, and therefore we provide for higher system security. This also enables Perfect Forward Secrecy.

SHA-1 HMAC

This element provides for per-packet Digital Signatures with 160 bit one-way hashes. This ensures that each packet received is from the correct endpoint and that the data has not been changed (so it provides for both authenticity and integrity).

EMBEDDED PACKET SEQUENCE NUMBERS

Each packet that is sent between Welbeck-enabled endpoints has an encrypted 64-bit number uniquely identifying the packet. This sequence number as well as the payload data are encrypted. This prevents packet replay attacks and ensures reliable data delivery.

TLS HANDSHAKE PASSPHRASE

This element provides the initial authentication at the server, limiting the starting handshake sequence to only those endpoints with the correct passphrase. It provides a user-configurable passphrase that controls which devices can connect to each other. This is used to prevent connections by an unauthorized third party. The TLS handshake passphrase also prevents Denial-of-Service (DOS) attacks, port-scanning attacks, and Man-in-the-Middle attacks.

PERFECT FORWARD SECRECY

Perfect Forward Secrecy is a unique security property that ensures that even if a session key is discovered for one series of transactions, it does not compromise any prior or future transactions.

PER APPLIANCE NAME/PASSPHRASE

Per-client name/passphrase provides individual endpoint authorization after proper TLS authorization. It is sent encrypted within the Welbeck tunnel. This provides user-configured control over individual endpoints' access after certs, keys, and authorization have been negotiated. It offers administrative control over deployed units within a network and provides additional protection against Man-in-the-Middle attacks.

ACCESS CONTROL LISTS/STATEFUL FIREWALL RULES

Welbeck provides 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 allows the user to accept, drop, and log packets flowing through the device. The system protects as well as monitors 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 configuration by the more advanced system administrator.

An example of host network filtering is configuring 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, computers and other 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 unless initiated by an approved source computer – thus preventing attackers from flooding network connections.

More Information:
Welbeck Secure
7910 Woodmont Ave.
Ste 1250
Bethesda, MD 20814
855-WELBECK (935-2325)
sales@welbecksecure.com

WELBECK
SECURE