



Z-LINK™ Approach to Securing Remote Connectivity

Overview

In order to minimize downtime and expedite repairs, today's hospital environment demands remote connectivity between highly trained service technicians and the imaging equipment located within the hospital. This requirement has driven the need for a comprehensive approach to remote access on critical radiology equipment such as MRI, CT and PET/CT. Deployment of remote diagnostic computer systems like Zetta's own Z-Link™ product generates the need for stringent computer security and performance.

In such an environment, administrators face an ever-growing need to protect critical company and hospital resources from attacks. Controlled access to different resources based on user identity/credentials, user groups, and client devices are some of the top security requirements for these environments.

As a provider of equipment maintenance, Zetta utilizes Z-LINK™ computers with Windows 7, 8 and 10; and under some certain circumstances servers with Windows 2008R or Windows 2012. These computers are placed on the client's network with a static IP address and access to the internet. The Z-LINK™ computer is also connected to the scanner with a secondary IP address on the same subnet as the scanner.



Z-LINK - True Remote Diagnostics

Zetta Medical Technologies, LLC.

1313 Ensell Road · Lake Zurich, IL 60047
Tel: 847-550-9990 Fax: 847-550-9994



Z-LINK™ offers the following 24/7 Access Capabilities:

- Image artifact analysis
- Error logs and data analysis
- Run Scanner Diagnostics
- Remote Fixes
- Access CT tube arc logs
- Add or reconfigure MRI coils
- Helium levels
- Magnet pressure
- Coldhead efficiency
- Chiller temperature
- Shield temperature
- Water flow
- Water temperature
- Room Humidity

Zetta connects to the Z-LINK™ computers remotely via a secure and an encrypted handshake utilizing secure networking protocols. The Z-LINK™ computer on customers site will connect to its assigned equipment via local LAN and may utilize common software applications and protocols such as; Telnet, PUTTY, FTP, TCP/IP and SMTP

Typical Z-LINK™ connection scenario:



Some features of the software are:

Black & Whitelist

Access to Z-LINK™ computers is restricted to whitelisted individuals with specific user ID's and multiple passwords which are assigned and maintained by Zetta.

Creation of a Session and Types of Connections

When establishing a session, the software determines the optimal type of connection. After the handshake through the master servers, in 70% of the cases a direct connection via UDP or TCP

Zetta Medical Technologies, LLC.

1313 Ensell Road · Lake Zurich, IL 60047
Tel: 847-550-9990 Fax: 847-550-9994



is established (even behind standard gateways, NATs and firewalls). The rest of the connections are routed through Zetta's highly redundant router network via UDP, TCP or http-tunneling. You may need to open a minimal number of ports (one port in most cases) in order to work with our software.

Encryption and Authentication

The software works with a complete encryption based on RSA public/private key exchange and AES (256 Bit) session encoding. This technology is used in a comparable form for https/SSL and can be considered completely secure by today's standards. The private key never leaves the client computer, this procedure ensures that the interconnected computers - including the routing servers - cannot decipher the data stream.

Each software client has already implemented the public key of the master cluster and can thus encrypt messages from the masters and check its signature respectively. The PKI (Public Key Infrastructure) effectively prevents "Man-in-the-middle-attacks". Despite the encryption, the password is never sent directly, but only through a challenge-response procedure and is only saved on the local computer.

Brute-Force Protection

Prospective customers who inquire about the security of the software regularly ask about encryption. Understandably, the risk that a third party could gain insight into the connection or that the software access data is being tapped is feared the most. However, in reality, very primitive attacks are the most dangerous ones.

In the context of computer security, a brute force attack is a trial-and-error-method to guess a password, which is protecting a resource. With the growing computing power of standard computers the time needed for guessing long password has been increasingly reduced.

As a defense against brute force attacks, the software exponentially increases the latency between the connection attempts. For 24 attempts it already takes 17 hours. The latency is only reset after successfully entering the correct password.

Zetta Medical Technologies, LLC.

1313 Ensell Road · Lake Zurich, IL 60047
Tel: 847-550-9990 Fax: 847-550-9994



The software not only has a mechanism in place to protect its customers from attacks from one specific computer, but also from multiple computers known as Botnet attacks, trying to access one particular software-ID.

Code Signing

As an additional security feature, all of our software is signed via VeriSign Code Signing. Due to this, the publisher of the software can always be reliably identified. If the software has been changed afterwards, the digital signature becomes automatically invalid.

Challenges

Since the need for security is constantly evolving, we must continue to improve our methods for securing access – one that is cost-effective, easy to manage and secure, while addressing performance and scalability requirements.

Basic security requirements that must remain in place consist of:

- Verification of user credentials and services to define user access.
- Client integrity checks that consists of endpoint security verification and of redirecting users to predefined subnets to download compliant anti-virus software, firewalls, operating system updates, and patches.
- Firewall rules such as granular access control and packet filtering based on protocol, port, and destination.

Client Domain

Hospital IT departments will always remain concerned about all devices placed on their network and will want to apply certain requirements to these computers. Some of these requirements are:

- Windows PCs can be added if these computers are placed on the hospital network domain and managed by the hospital IT department
- A VPN solution must be utilized

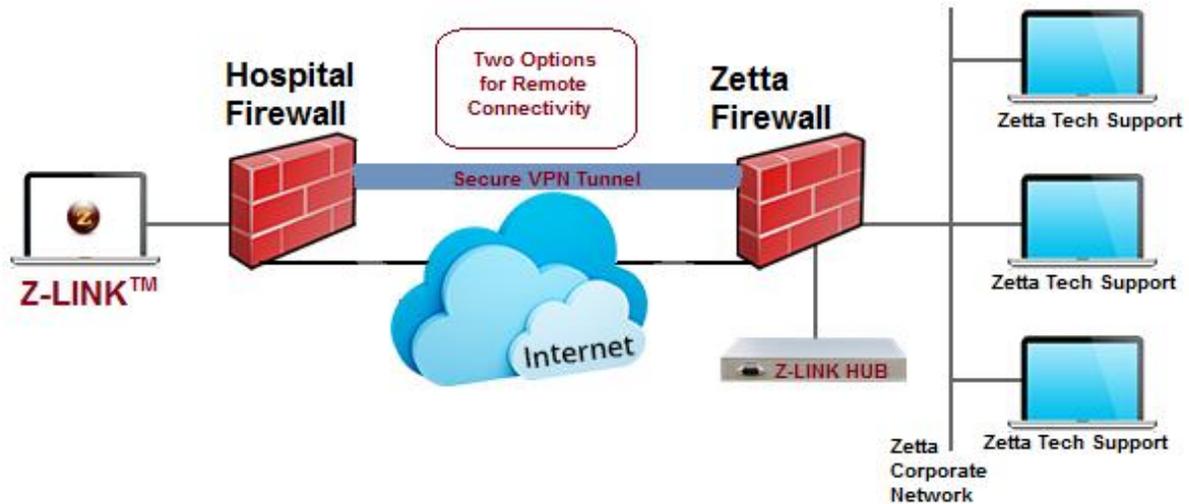
If a client desires either of the two solutions above, Zetta will deliver, grant the EULA and install its Z-LINK™ software on a PC that is managed by the hospital IT department and resides on the

Zetta Medical Technologies, LLC.

1313 Ensell Road · Lake Zurich, IL 60047
Tel: 847-550-9990 Fax: 847-550-9994



hospital domain. Negative impacts on the Z-LINK™ performance, if any, will have to be evaluated based on VPN access provided and restrictions imposed. A full evaluation can be conducted within hours of installation to notify the client of any performance issues.



Conclusion

Z-Link™ security has been tested and approved by many university hospitals in the USA especially by utilizing the VPN driver features while directing the connection via the hospital's dedicated VPN access. Bidirectional traffic can still be end-to-end encrypted using AES (256 bit) session encryption.

Disclaimer:

Verisign and Windows are trademarks of their respective companies