WestFax Fax-to-Email Infrastructure

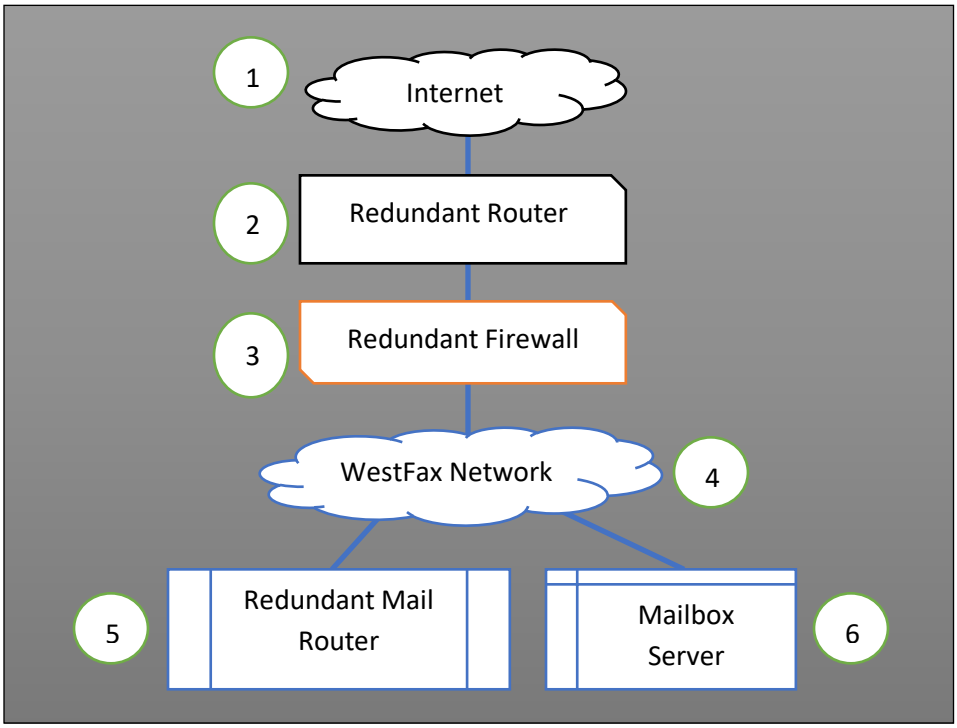
WestFax operates a private cloud infrastructure. We own and operate the hardware in 3 different data centers. While we do have "outside cloud" resources to augment processing, (AWS etc…) customer private data is never stored on these outside systems. In the case of the transport of Fax-to-Email jobs, the "outside cloud" resources are not utilized at all.

While there are several interfaces to the Fax-to-Email capabilities, the one that is most often cited as being a security concern is the SMTP interfaces. While there are legitimate reasons for concern, WestFax has gone to great lengths to address these concerns and to secure the system. WestFax has many customers using this method to transport ePHI and other sensitive information via fax. Additionally, we have assured our customers that we will provide the needed level of protection via signed BAA agreements. Organizations that leverage smtp based Fax to Email and Email to Fax interfaces have also secured their email servers accordingly and have BAA's with their email providers to ensure compliance.

This document describes the mechanisms used by WestFax to assure the privacy of our customers' ePHI data during transport via SMTP.

WestFax Network Description

The following illustration depicts a simplified view the WestFax network. A description of each element and their cooresponding role in the Fax-to-Email process is described below.



Tel: 303-299-9329
Fax: 303-299-9309
info@westfax.com

1. Internet

As one would guess, this represents the WestFax connection to the public internet. While not depicted, WestFax has multiple interfaces to the public internet. Our hosting centers are spread across 3 cities and are interconnected with a persistent site-to-site VPN for cross-site connectivity.

2. Redundant Routers

At the entry point to the network, WestFax maintains redundant routers to guarantee internet connectivity. These routers are the boundary of the network and are the only elements that maintain public IP addresses. All other machines in the network are in a private IP space. Static and dynamic NAT are used to translate between the inside and outside IP address spaces. Basic packet filtering occurs here through the use of access lists (source IP, destination IP, and port filtering). The routers are configured to provide a basic SPI firewall.

3. Redundant Firewalls

The redundant firewalls provide a second and much more sophisticated firewall capability. Protocol level inspection and advanced intrusion detection and prevention capabilities are employed here.

4. WestFax Network

The core of the WestFax network is connected via redundant switches. This network connects all of the WestFax processing servers, web servers, and other needed services. Again, all nodes in this network run in a private IP space.

5. Redundant Mail Router

WestFax maintains redundant mail routers on the inside of the network. Each are configured to receive email form outside, and also to send email. A static NAT configuration is used to map the IP addresses. The mail routers do not sore mail local, but simply forward it to other email servers within the network. For sending email out, these servers are the primary transition mechanism. These mail routers provide a sophisticated scripting mechanism to send, receive, and route email. This mechanism is used to assure that TLS is used in the sending or receiving of email when necessary. The use of this capability to secure customer Email-to-Fax transmission is described later in the SMTP flow portion of this document.

6. Mailbox Server

The mailbox server depicted here is a special purpose machine dedicated to handling inbound email from customers for the Email-to-Fax function. The mail server is not configured to send email, it only receives, and will store the email it receives locally. The mail server supports integration with custom software using a powerful .net interface API. Also present on the network are processing systems that can open and read the content of the mailboxes on this server and take appropriate action (in this case, parse and send a fax based on the email). Following the processing of the email into a fax, the email is removed from the system.

Tel: 303-299-9329
Fax: 303-299-9309
info@westfax.com

SMTP Mail Flow

In many customer solutions, especially solutions that interface with MFP copiers and printer devices, we've found it necessary to support SMTP and a mechanism to send a fax document to our systems. Securing this interaction is of primary concern. To address this and to ensure the appropriate steps are taken to secure the email transmission, WestFax has made two changes to the "normal" treatment of SMTP. These changes are explained below.

1. **Provide an Authenticated Email relay**

   In everyday use, most email will be transmitted at least three (3) times during its journey from sender to receiver. First, the sender will send the email to their own email server. The mail server will store this email, and then send it to the destination server. After it reaches its destination server, the user on the other end will then retrieve the email from their email server. Each of these separate transmissions must use TLS 1.2+ to ensure that the email has been secured during its journey.

   There is just one problem here. The servers and the email client software (outlook or whatever) need to be configured correctly in order to ensure a private transmission. As a sender of an email, there really is no way to guarantee that TLS is used from end to end. Furthermore, the configuration of email server and client software can be tricky. Any error can result in email being transmitted without TLS protection.

   To solve this problem and ensure that all email communication, WestFax provides its customer an Authenticated Email Relay. WestFax will provide customers a username and password on our Email Router systems (described above). These servers receive email directly from the MFP or any other Email transmitting device. This reduces the number of email transmission on the open internet to one.

2. **Guaranteed TLS Transmission**

   WestFax has employed the advanced features of its Email Router to guarantee that the email will be protected by TLS. Because of the sophisticated scripting capabilities on these servers, we are able to guarantee that the transmission will be secured with TLS 1.2. The SMTP connection will be dropped by our receiving mail server if the sender does not properly negotiate when a STARTTLS command is sent in the SMTP session.

   Following the receipt of a secure email from the outside, the mail router then forwards the message to the mailbox server on the private and secure WestFax network.

The combination of these 2 features enables WestFax to guarantee that an email sent using this mechanism will be received securely. For customers that have many MFP devices, we have found that using a unique username and password combination for each (basically customizing the "sender"), allows customers to identify the source of each fax.

Tel: 303-299-9329
Fax: 303-299-9309
info@westfax.com