FRAMA MAILING SYSTEM SPECIFICATION

Network Security Data Sheet - Fs Series & Fx Series

Germany

R01.02

Table of Contents

IMPORTANT INFORMATION

Our machines are approved by the Post of each country where they are sold.
Unlike computers which have quick software updates, the mailing systems lifecycle & working is much more complex (requires new PSD, base software & postal core changes) & approbation period is longer.

This Network security data sheet was created to provide customers, and their IT support, with specific details on the software that runs our Mailing Systems and how it interfaces with their networks

1 FS MAILING SYSTEMS (MS) PORTS USED

Application	Ports Used	Protocol
Funding Server & OLS	443	TCP
Default Proxy Connection	8080	TCP

*NOTE: All local ports are closed until the MS initiates a call

2 PROTOCOL USED

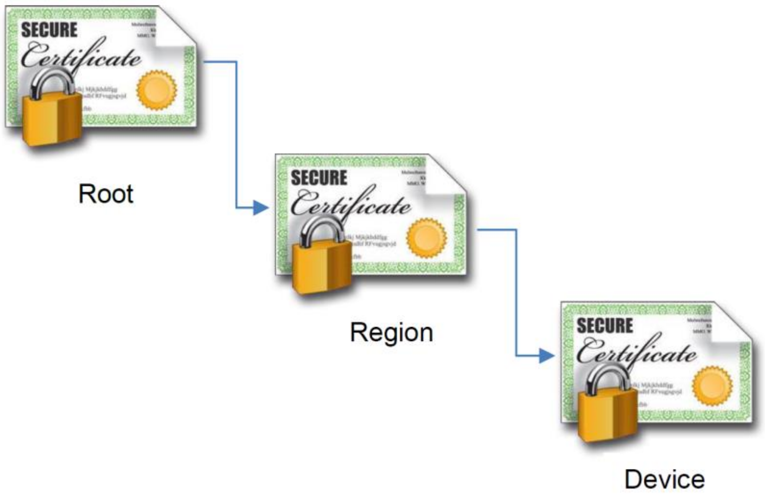
Protocol / Application	Information
Cipher Suite	Fs Series 3.1 and Fx Series 5, 7, 7.5, 9 = SHA-2
SSL	Fs Series 3.1 = TLS 1.2 Fx Series 5, 7, 7.5, 9 = TLS 1.2 Mutual Authentication & X.509 (extensible), self-signed certificates
DHCP	Dynamic and Static configurations on TCP/IP V4.0 (not compatible with V6.0)
DNS	Dynamic and Static configurations (port 53)
Proxy	NTLM V1.0 in transparent proxy mode with basic authentication – does not support NTLM V2.0 or Kerberos
NIC Speeds	Fs Series 3.1 = 10/100Mb/s Fx Series 5, 7, 7.5, 9 = 10/100Mb/s only
MAC OUI	00:1B:00 for Frama Technologies
Host Server SSL	TLS1.0, TLS 1.1 and TLS 1.2. For URL information contact your country distributor

RESTRICTIONS

- Does not contain a browser
- Cannot load 3rd party applications
- Cannot integrate any type of client/server application
- Does not support SNMP, SSH or any other remote management
- Does not support 802.1x
- Does not support RDP or any type of remote login
- Does not support SSL/HTTPS interception, deep inspection (on firewall)
- If URL Filtering is used (on firewall) an exception or bypass rule may be required (on firewall)

3 METER/SERVER COMMUNICATION

Frama maintains its own 3-tier certificate system that enables our meters to connect to our Infrastructure. Since we only communicate with our meters and our meters only communicate with our infrastructure, there is no need for a 3rd party certificate.



The Mailing Systems connect to our Infrastructure using TLS Mutual Authentication. Therefore, our server will not accept any device posing as one of our systems. Further, the mailing systems will not honor any "rogue" servers posing as our infrastructure.

> Note:
>
> Since our server and mailing system do not accept other certificates, SSL inspection cannot be used to monitor encrypted traffic. The mailing systems would see it as a main-in-the-middle attack and disconnect.

3.1 Data exchanged with Postal and Frama Servers (once a month, weekly or daily depending on model and market)

- Statistics for Post
- Ink Level Management
- Backup customer data
- Diagnostic information for Technical
- Support Updates

3.2 Manual Calls from mailing system

Ping Server: is a TCP connect to the Frama server. It is like a Standard call (exchange key with the secure server and then close the connection). When the TCP connect is made, an encrypted tunnel (TLS V1.2) is created to the Frama server.

Test server: same as Ping server with an exchange of data (less than 1Mb), to ensure the quality of the transaction.

Standard call: normal user connection method to our server to download slogan, rate, software update or upload diagnostics, statistics, and ink level information.

System Synchronization: same as Standard call.

3.3 Duration of call

Between 1-10 minutes (depending on customer network)

4 MAILING SYSTEM OS

Model	Windows CE 5.0	Linux
Fs Series 3.1	✓	
Fx Series 5		✓
Fx Series 7, 7.5		✓
Fx Series 9		✓

Both operating systems do not allow any third-party software to be loaded. Any drivers must be signed and incorporated into a software release by Frama R&D. All software updates are in a special format that cannot be read by any other computer or software. New software is only released by Frama through our service organization.

5 ADDITIONAL THINGS THE OS SOFTWARE WILL NOT DO

- Does *not* connect to or embed an email client or server
- Does *not* include or allow a web server or browser
- Does *not* offer access to the BIOS
- Does *not* offer access to a command prompt, root directory or registry
- Will *not* download or propagate a virus or worm
- Is *not* susceptible to a **man-in-the-middle attack** due to TLS protocol

6 MORE INFORMATION

Server communication process:

When the mailing system needs to connect to our servers, it opens a secure communication tunnel, based on TLS V1.2 protocol, over the Internet to the Frama server. The mailing system uses the same port used for HTTPS (Hypertext Transfer Protocol Secured), i.e. **port 443**.

The mailing system doesn’t integrate an email client/server.

Mail spamming is not possible from the mailing system because it doesn't integrate any email client or server.

Remote access from the LAN to the mailing system is not possible.

Internet connections are always initiated by the mailing system and never from the Network toward the mailing system. These are either initiated manually by the user or automatically by the mailing system (normally once a month).

Communication ports are used only during communication with Frama Servers.

The ports used to communicate with our Servers are only open during data transfer. When the communication is finished, the port on the mailing system is closed.

DMZ

The Mailing system can be installed on the DMZ or Guest network. This will prevent the firewall from blocking communications if URL Filtering is used on it.

WiFi

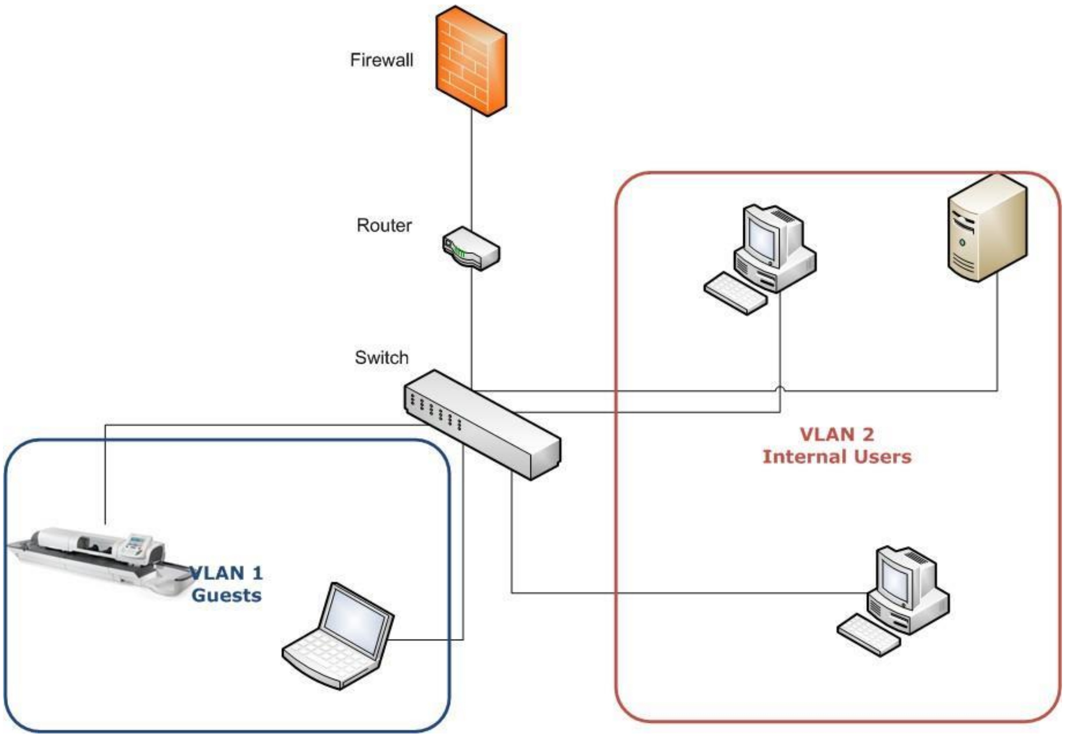
Wireless connection can be established with an external wireless internet adapter, e.g Netgear or Tp-Link.

7 ALTERNATIVE NETWORK CONFIGURATIONS

Some IT managers may not feel comfortable allowing our meters on their network for fear of infiltration by a virus or hacker. Therefore, we offer a solution that can allow our Mailing Systems on the customer network and alleviate some of the concerns that IT may have.

7.1 VLANs

The use of a VLAN is a known way of segmenting a network. Moreover, it is an effective way of securing internal servers and data. By creating a VLAN that only has access to the Internet an IT manager mitigates the risk of successful breach of internal company resources. Many of our customers have setup “Guest” networks that allow our Mailing Systems (MS) to connect to our servers without giving the MS access to internal customer resources. See network diagram below.



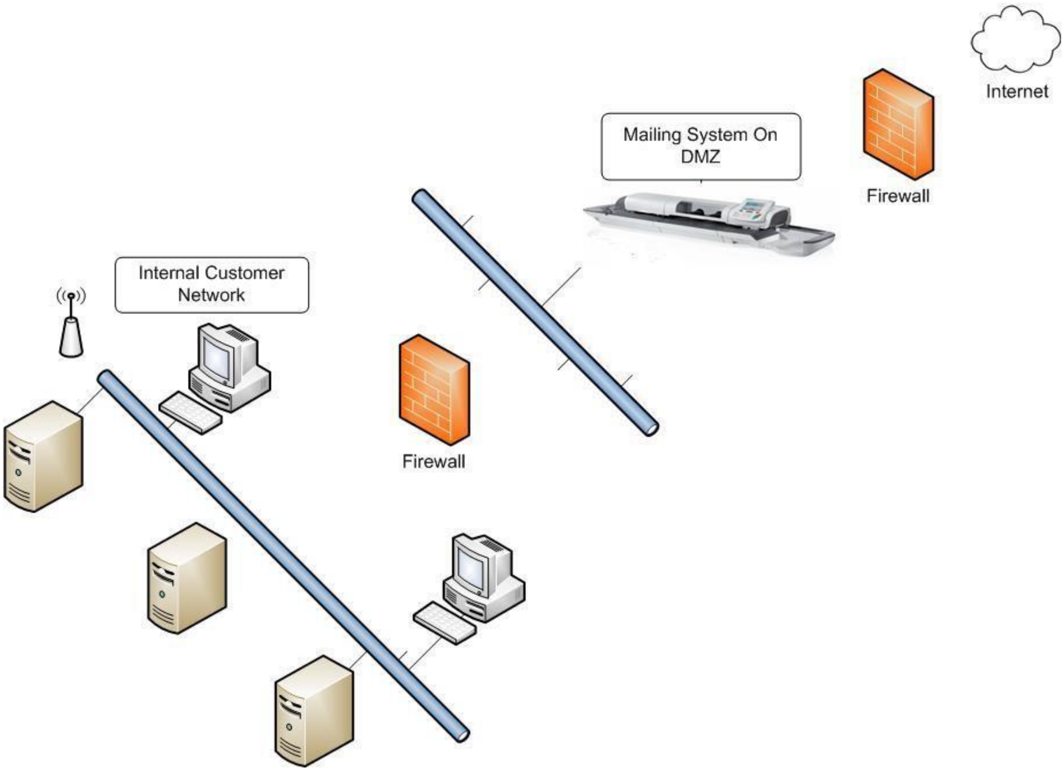
As shown in the diagram above, allocating a network segment for the Mailing System assures that network resources are shielded from possible intrusion by malicious software or users.

7.2 DMZ

This method is very similar to creating a VLAN, however, instead of using switches it is accomplished with routers. A DMZ is a "De-militarized Zone" and is a borrowed term from the military. It designates a danger zone where there is little security. In networking, a DMZ is created to allow a server or system to be seen by the internet with only a firewall to limit access and provide security. Most web servers operate in this fashion.

So, the suggestion is to put our Mailing System on the DMZ and allow it to be seen externally. The machine will not accept requests or load any software so the chances that it will get compromised are slim. In the event that it does get compromised, it has been shielded from the rest of the internal network.

See the following diagram.



Both methods offer similar results and further protection can be achieved by combining them. It is beyond the scope of this article to describe how to setup any of these configurations. Since different networks are configured using different equipment, steps to any of these solutions may vary.

It is up to IT managers to investigate and determine the best configuration for their network.

8 TLS VULNERABILITIES & MITIGATIONS

The below mentioned malware has been checked for its possible impact on our franking systems and/or back-end systems.

None of the listed malware have a deleterious effect or can intrude to any of our franking- or back-end systems software.

Tested malware

- POODLE Attack CVE-2014-3566
- BEAST Attack CVE-2011-3389
- Ripple 20
- DUKH
- Specter meltdown
- Apache LOG4 J